Subgroup Lattices of Groups
de Gruyter Expositions in Mathematics 14

Editors

O. H. Kegel, Albert-Ludwigs-Universität, Freiburg
V. P. Maslov, Academy of Sciences, Moscow
W. D. Neumann, The University of Melbourne, Parkville
R. O. Wells, Jr., Rice University, Houston
1 The Analytical and Topological Theory of Semigroups, K. H. Hofmann, J. D. Lawson, J. S. Pym (Eds.)
2 Combinatorial Homotopy and 4-Dimensional Complexes, H. J. Baues
3 The Stefan Problem, A. M. Meirmanov
4 Finite Soluble Groups, K. Doerk, T. O. Hawkes
5 The Riemann Zeta-Function, A. A. Karatsuba, S. M. Voronin
6 Contact Geometry and Linear Differential Equations, V. R. Nazaikinskii, V. E. Shatalov, B. Yu. Sternin
7 Infinite Dimensional Lie Superalgebras, Yu. A. Bahturin, A. A. Mikhalev, V. M. Petrogradsky, M. V. Zaitsev
8 Nilpotent Groups and their Automorphisms, E. I. Khukhro
9 Invariant Distances and Metrics in Complex Analysis, M. Jarnicki, P. Pflug
10 The Link Invariants of the Chern-Simons Field Theory, E. Guadagnini
12 Moduli Spaces of Abelian Surfaces: Compactification, Degenerations, and Theta Functions, K. Hulek, C. Kahn, S. H. Weintraub
13 Elliptic Problems in Domains with Piecewise Smooth Boundaries, S. A. Nazarov, B. A. Plamenevsky
Subgroup Lattices of Groups

by

Roland Schmidt

Walter de Gruyter · Berlin · New York 1994
Author
Roland Schmidt
Mathematisches Seminar
Universität Kiel
Ludewig-Meyn-Straße 4
D-24098 Kiel
Germany

1991 Mathematics Subject Classification: 20—01, 20—02

Keywords: Group, lattice, subgroup lattice, projectivity, duality
To Traute and

Alexander  Katharina  Viktoria  Johannes  Maria
The central theme of this book is the relation between the structure of a group and the structure of its lattice of subgroups. The origin of the subject may be traced back to Dedekind, who studied the lattice of ideals in a ring of algebraic integers; he discovered and used the modular identity, which is also called the Dedekind law, in his calculation of ideals. But the real history of the theory of subgroup lattices began in 1928 with a paper of Ada Rottländer which was motivated by the Galois correspondence between a field extension and its Galois group. Subsequently many group theorists have worked in this field, most notably Baer, Sadovskii, Suzuki, and Zacher. Since the only book on subgroup lattices is still Suzuki's Ergebnisbericht of 1956, there is a clear need for a book on this subject to describe more recent developments.

We denote the subgroup lattice of a group $G$ by $L(G)$. If $G$ and $\overline{G}$ are groups, an isomorphism from $L(G)$ onto $L(\overline{G})$ is called a projectivity from $G$ to $\overline{G}$. Since isomorphic groups have isomorphic subgroup lattices, there is a correspondence between the class of all groups and a certain class of (algebraic) lattices in which a group is sent to its subgroup lattice. This raises the following questions:

(A) Given a class $\mathcal{X}$ of groups, what can we say about the subgroup lattices of groups in $\mathcal{X}$?

(B) Given a class $\mathcal{Y}$ of lattices, what can we say about the class of groups $G$ such that $L(G) \in \mathcal{Y}$?

Since there are nonisomorphic groups having isomorphic subgroup lattices, we may further ask:

(C) If $\mathcal{X}$ is a class of groups, what is the lattice-theoretic closure $\overline{\mathcal{X}}$ of $\mathcal{X}$? Here $\overline{\mathcal{X}}$ is the class of all groups $\overline{G}$ for which there exists $G \in \mathcal{X}$ such that $L(G)$ is isomorphic to $L(\overline{G})$.

(D) Which classes of groups $\mathcal{X}$ satisfy $\overline{\mathcal{X}} = \mathcal{X}$, that is, are invariant under projectivities?

If $\mathcal{X}$ consists of just one group, Problem (D) becomes the following:

(E) Which groups $G$ are determined by their subgroup lattice, that is are isomorphic to every group $\overline{G}$ with $L(\overline{G})$ isomorphic to $L(G)$?

Every isomorphism between two groups induces a projectivity in a natural way; our final question is:

(F) Which groups are not only determined by their subgroup lattice but even have the property that all their projectivities are induced by group isomorphisms?

These are the main problems in the field and they are studied in the first seven chapters of the book. In Chapter 8 we consider dualities between subgroup lattices and in Chapter 9 we briefly handle other lattices associated with a group, namely the lattices of normal subgroups, composition subgroups, centralizers, and cosets.
Although the theory of subgroup lattices is just a small part of group theory, for reasons of space I have been unable to include all the contributions to this theory. I have tried to compensate for omissions by at least including statements and references wherever possible; also many interesting results are cited in the exercises at the end of each section. However, certain parts of the theory have not been covered at all. In writing what is after all a book on group theory I decided to omit those topics which would have led too far away from this subject. Therefore I do not cover embeddings of lattices in subgroup lattices, lattices of subsemigroups, homotopy properties of subgroup lattices, inductive groupoids, or anything about topological groups, although there are also interesting results in these fields. Furthermore I do not study homomorphisms between subgroup lattices. The reason is that when I started to write this book there had been no activity in this area for more than 30 years, so that Suzuki's book remained an adequate reference. This situation changed in 1985 and especially since 1990, but by then there was no room in the book for a chapter on lattice homomorphisms.

Nevertheless I hope that this book will serve as a basic reference in the subject area, as a text for postgraduate studies, and also as a source of research ideas. It is intended for students who have some basic knowledge in group theory and wish to delve a little deeper into one of its many special areas. It is assumed that the reader is familiar with the basic concepts of group theory, but references are given for many well-known group theoretical facts. For this purpose I mainly use the books by Robinson [1982] and Huppert [1967]. I do not assume that the reader is familiar with lattice theory, but the basic facts are developed in §1.1 and at the beginning of some other sections. For a thorough introduction into lattice theory the reader is referred to the books of Birkhoff, Crawley and Dilworth, or Grätzer. Since the book is intended as a textbook for students, I have included a large number of exercises of varying difficulty. While these exercises are not used in the main text they often give alternate proofs or contain supplementary results for which there was no room in the main text.

It is a pleasure to thank the many students and colleagues who have read parts of the manuscript and made helpful suggestions. In particular, I mention O.H. Kegel and G. Zacher who have followed the whole project with much interest. Thanks are also due to Ms. J. Robinson for checking the English text and to Frau G. Christiansen for typing parts of the manuscript. Finally, I thank Dr. M. Karbe and the publisher for their courtesy and cooperation.
## Contents

Preface ................................................................. vii  
Notation .............................................................. xiii  

### Chapter 1  
**Fundamental concepts**  
1.1 Basic concepts of lattice theory ................................................................. 1  
1.2 Distributive lattices and cyclic groups ............................................................. 11  
1.3 Projectivities .............................................................. 16  
1.4 The group of autoproperties ............................................................................. 23  
1.5 Power automorphisms .............................................................. 29  
1.6 Direct products .............................................................. 34  

### Chapter 2  
**Modular lattices and abelian groups** ................................................................. 41  
2.1 Modular lattices .............................................................. 41  
2.2 \(P\)-groups .............................................................. 49  
2.3 Finite \(p\)-groups with modular subgroup lattices ............................................. 54  
2.4 Groups with modular subgroup lattices ............................................................. 69  
2.5 Projectivities of \(M\)-groups ........................................................................... 88  
2.6 Projectivities between abelian groups ............................................................. 101  

### Chapter 3  
**Complements and special elements in the subgroup lattice of a group** ............ 114  
3.1 Groups with complemented subgroup lattices (\(K\)-groups) ............................. 115  
3.2 Special complements ............................................................................... 121  
3.3 Relative complements ............................................................................... 126  
3.4 Neutral elements and related concepts ............................................................ 135  
3.5 Finite groups with a partition ....................................................................... 145  

### Chapter 4  
**Projectivities and arithmetic structure of finite groups** .................................. 157  
4.1 Normal Hall subgroups .............................................................................. 158  
4.2 Singular projectivities .............................................................................. 166  
4.3 \(O_p(G), O^p(G)\), Fitting subgroup and hypercentre ........................................ 178  
4.4 Abelian \(p\)-subgroups and projectivities ........................................................ 185
# Contents

## Chapter 5
**Projectivities and normal structure of finite groups** ........................................... 199

5.1 Modular subgroups of finite groups ................................................................. 200
5.2 Permutable subgroups of finite groups ......................................................... 216
5.3 Lattice-theoretic characterizations of classes of finite groups ....................... 228
5.4 Projective images of normal subgroups of finite groups ................................. 235
5.5 Normal subgroups of $p$-groups with cyclic factor group ............................... 243
5.6 Normalizers, centralizers and conjugacy classes ............................................ 272

## Chapter 6
**Projectivities and normal structure of infinite groups** ........................................ 281

6.1 Subgroups of finite index ................................................................................. 282
6.2 Permodular subgroups .................................................................................... 288
6.3 Permutable subgroups of infinite groups ......................................................... 303
6.4 Lattice-theoretic characterizations of classes of infinite groups ....................... 311
6.5 Projective images of normal subgroups of infinite groups and index preserving projectivities ................................................................. 321
6.6 The structure of $N^G/N_G$ and $\overline{N^G}/\overline{N_G}$ and projective images of soluble groups ................................................................. 330

## Chapter 7
**Classes of groups and their projectivities** ......................................................... 343

7.1 Free groups ....................................................................................................... 345
7.2 Torsion-free nilpotent groups ......................................................................... 360
7.3 Mixed nilpotent groups ................................................................................... 374
7.4 Periodic nilpotent groups ................................................................................ 385
7.5 Soluble groups ................................................................................................ 395
7.6 Direct products of groups ................................................................................ 406
7.7 Groups generated by involutions .................................................................... 421
7.8 Finite simple and lattice-simple groups ........................................................... 439

## Chapter 8
**Dualities of subgroup lattices** .............................................................................. 452

8.1 Abelian groups with duals ............................................................................... 452
8.2 The main theorem ............................................................................................ 458
8.3 Soluble groups with duals ............................................................................... 462
8.4 Finite groups with duals .................................................................................. 468
8.5 Locally finite groups with duals ...................................................................... 476

## Chapter 9
**Further lattices** .................................................................................................. 485

9.1 Lattices of normal subgroups .......................................................................... 486
9.2 Lattices of subnormal subgroups ..................................................................... 498
<table>
<thead>
<tr>
<th>Contents</th>
<th>xi</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3 Centralizer lattices</td>
<td>511</td>
</tr>
<tr>
<td>9.4 Coset lattices</td>
<td>527</td>
</tr>
<tr>
<td>Bibliography</td>
<td>542</td>
</tr>
<tr>
<td>Index of Names</td>
<td>561</td>
</tr>
<tr>
<td>Index of Subjects</td>
<td>564</td>
</tr>
</tbody>
</table>
Notation

Throughout this list, $G$ denotes a group, $X$ a class of groups, $L$ a lattice, $p$ a prime, $\pi$ a set of primes, $n$ a natural number, $x$ and $y$ elements of $G$, $u$ and $v$ elements of $L$, and $\varphi$ a projectivity from $G$ to a group $G$.

$\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$ set of natural numbers, nonnegative integers, integers
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ field of rational numbers, real numbers, complex numbers
$\mathbb{P}$ set of all primes
$GF(p^n)$ field with $p^n$ elements
$U_p$ group of $p$-adic units
$X \subseteq Y, X \subset Y$ $X$ is a subset, a proper subset of the set $Y$
$X \setminus Y$ set of all elements in $X$ which are not contained in $Y$
$|X|$ cardinality of the set $X$
a\mid b, a \notmid b a divides $b$, a does not divide $b$, $(a, b \in \mathbb{Z})$
$(a, b)$ greatest common divisor of $a$ and $b$, $(a, b \in \mathbb{Z})$
p', $\pi'$ $\mathbb{P}\setminus\{p\}, \mathbb{P}\setminus\pi$
$H \cong K$ $H$ is isomorphic with $K$
$X_1 \times \cdots \times X_n, \text{Dr} X_\lambda$ direct product

Lattice theory notation

$\leq, \cap, \cup$ partial order, intersection, union in $L$
$\bigcap S, \bigcup S$ greatest lower bound, least upper bound of the subset $S$
$O, I$ least, greatest element of $L$
$[u/v]$ interval of all $w \in L$ such that $v \leq w \leq u$
$u \text{ mod } L$ $u$ is a modular element of $L$
$C(L)$ set of all cyclic elements of $L$
$M_n$ lattice of length 2 with $n$ atoms

Group theory notation

$x^\gamma$ $y^{-1}xy$
$[x, s]$ $x^{-1}x^s$ where $s$ is an element or an automorphism of $G$
$\langle x \rangle$ cyclic subgroup generated by $x$
o$(x)$ order of $x$
a$(x, y)$ $(y^\sigma)^{-1}(x^\sigma)^{-1}(xy)^\sigma$, amorphy of the map $\sigma$
**Notation**

- $H \leq G, H < G$: $H$ is a subgroup, a proper subgroup of $G$
- $H \trianglelefteq G$: $H$ is a normal subgroup of $G$
- $H \leq G$: $H$ is a subgroup of $G$
- $H \leq G$: $H$ is a normal subgroup of $G$
- $H \leq G$: $H$ is a subnormal subgroup of $G$
- $H \trianglelefteq G$: $H$ is a modular subgroup of $G$
- $H \trianglelefteq G$: $H$ is a permutable subgroup of $G$
- $|G:H|$: index of the subgroup $H$ in $G$
- $\langle X_\lambda \mid \lambda \in \Lambda \rangle$: subgroup generated by subsets $X_\lambda$ of $G$
- $H \cup K, \bigcup_{\lambda \in \Lambda} H_\lambda$: subgroup generated by subgroups $H, K, H_\lambda$ of $G$
- $H^X$: $\langle H^x \mid x \in X \rangle$ for subsets $H$ and $X$ of $G$
- $H^G_H$: normal closure, core of the subgroup $H$ in $G$
- $H^{\phi^{-1}}_z$: $((H^\phi)^z)^{-1}$ for $H \leq G$ and $z \in \bar{G}$
- $H^{\bar{G}, H}$: $((H^\bar{G})^H)^{-1}$, $((H^\bar{G})_H)^{-1}$ for $H \leq G$
- $C_G(H), N_G(H)$: centralizer, normalizer of $H$ in $G$
- $C(G/H)$, $C(G/H/K)$: $\{x \in G \mid [H, x] \leq K\}$
- $\Omega(H)$: orbit of $\alpha \in \Omega$ under the operation of $G$ on the set $\Omega$
- $G_{\alpha}$: stabilizer of the point $\alpha$ under the operation of $G$
- $o(x, H)$: $|\langle x \rangle : \langle x \rangle \cap H|$, order of $x$ modulo the subgroup $H$
- $I(H)$: set of all $x \in G$ such that $o(x, H)$ is infinite or a prime power
- $J(H)$: set of all $x \in G$ such that $o(x, H)$ is a prime power
- $\langle X \mid R \rangle$: group presented by generators $X$ and relations $R$
- $H \triangleright K$: (standard restricted) wreath product of $H$ with $K$
- $C_G(A, B)$: cartesian product of groups $G_A$
- $\text{Aut } G, \text{Inn } G$: automorphism group, inner automorphism group of $G$
- $\text{Pot } G$: group of power automorphisms of $G$
- $\text{End } G$: set of endomorphisms of $G$
- $\text{Hom } (A, B)$: set of homomorphisms from $A$ to $B$
- $P(G)$: group of autopjectivities of $G$
- $\text{PA}(G), \text{PI}(G)$: group of all autopjectivities of $G$ induced by automorphisms, by inner automorphisms
- $G^G$: $\langle x^g \mid x \in G \rangle$
- $\Omega(G), \Omega_n(G)$: $\langle x \in G \mid x^p = 1 \rangle$, $\langle x \in G \mid x^{p^n} = 1 \rangle$ if $G$ is a $p$-group
- $\mathcal{U}_n(G)$: $G^{p^n}$ if $G$ is a $p$-group
- $Z(G)$: centre of $G$
- $N(G)$: norm of $G$
- $[X, S]$: $\langle [x, s] \mid x \in X, s \in S \rangle$ for subsets $X$ of $G$ and $S$ of $G$ or $\text{Aut } G$
- $\text{Com } G$: set of commutators of elements of $G$
- $Z_n(G), K_n(G), G^{(n)}$: terms of the upper central series, the lower central series, the derived series of $G$
- $Z_{\omega}(G)$: hypercentre of $G$
- $F(G)$: Fitting subgroup of $G$
- $\Phi(G)$: Frattini subgroup of $G$
### Notation

- $F_n(G)$, $N_n(G)$: terms of the upper Fitting series, the lower Fitting series of $G$
- $R(G)$: Hirsch-Plotkin radical of $G$
- $S(G)$: locally soluble radical of $G$
- $G^x$: $x$-radical of $G$
- $G_x$: $x$-residual of $G$
- $O_p(G)$, $O_\pi(G)$: maximal normal $p$-subgroup, $\pi$-subgroup of $G$
- $O^{\pi}(G)$, $O^\pi(G)$: minimal normal subgroup of $G$ with factor group a $p$-group, a $\pi$-group
- $G_p$: $p$-component of the nilpotent torsion group $G$
- $T(G)$: torsion subgroup of $G$
- $Syl_p(G)$: set of Sylow $p$-subgroups of $G$
- $\text{Exp } G$: exponent of $G$
- $\pi(G)$: set of all primes dividing the order of an element of $G$
- $c(G)$: nilpotency class of $G$
- $d(G)$: derived length of $G$
- $l_p(G)$: $p$-length of $G$
- $r_o(G)$: torsion-free rank of the abelian group $G$
- $\mathfrak{T}$: class of all locally $\mathfrak{x}$-groups
- $\mathfrak{S}$: classes of abelian, nilpotent, soluble groups
- $P(n, p)$: $P$-groups
- $\text{Sym } X$, $S_n$: symmetric group on the set $X$, on $\{1, \ldots, n\}$
- $\text{Alt } X$, $A_n$: alternating group on the set $X$, on $\{1, \ldots, n\}$
- $C_n$, $C_\infty$: cyclic group of order $n$, of infinite order
- $C_p^\times$: Prüfer group, quasicyclic group
- $D_n$: dihedral group of order $n$
- $Q_{2^n}$: generalized quaternion group of order $2^n$
- $GL(V)$, $GL(n, F)$, $GL(n, q)$: general linear group
- $SL(V)$, $SL(n, F)$, $SL(n, q)$: special linear group
- $PGL(n, q)$, $PSL(n, q)$: projective general linear and projective special linear groups
- $PSp(V)$, $P\Omega(V)$, $PSU(V)$: projective symplectic, orthogonal, unitary groups
- $Sz(q)$: Suzuki groups
- $L(G)$: subgroup lattice of $G$
- $L_n(G)$: set of all subgroups of $G$ generated by $n$ elements
- $\mathfrak{N}(G)$: lattice of normal subgroups of $G$
- $\mathfrak{K}(G)$: lattice of composition subgroups of $G$
- $\mathfrak{C}(G)$: centralizer lattice of $G$
- $\mathfrak{R}(G)$: coset lattice of $G$
- $[X/Y]_N$, $[X/Y]_K$, $[X/Y]_C$: interval in $\mathfrak{N}(G)$, $\mathfrak{K}(G)$, $\mathfrak{C}(G)$
Chapter 1

Fundamental concepts

In this first chapter we briefly introduce the basic concepts of lattice theory and develop the elementary properties of subgroup lattices and projectivities of groups that will be needed later.

In § 1.1, in addition to the purely lattice-theoretic concepts, we define the subgroup lattice \( L(G) \) of a group \( G \), projectivities between groups, and introduce certain sublattices and meet-sublattices of \( L(G) \), namely the lattices of normal subgroups, composition subgroups, centralizers, and cosets of \( G \).

The main result of § 1.2 is Ore's theorem of 1938 which characterizes the groups with distributive subgroup lattices as the locally cyclic groups. It yields the basic fact that every projectivity maps cyclic subgroups to cyclic subgroups. So it seems reasonable to try to construct projectivities between two groups \( G \) and \( \bar{G} \) using maps between the sets of cyclic subgroups or even element maps between \( G \) and \( \bar{G} \). This we study in § 1.3, and then prove Sadovskii's approximation theorems which enable us to extend isomorphisms inducing a given projectivity \( \phi \) on certain sets of subgroups or factor groups of \( G \) to an isomorphism inducing \( \phi \) on the whole group.

In § 1.4 we study the group \( P(G) \) of all autoprojectivities of \( G \) and introduce the subgroups \( PA(G) \) and \( PI(G) \) consisting of all autoprojectivities induced by automorphisms and inner automorphisms, respectively. The kernel of the natural map from \( \text{Aut} G \) to \( PA(G) \) is the group \( \text{Pot} G \) of all power automorphisms of \( G \). In § 1.5 we prove Cooper's theorem that every power automorphism is central and determine the power automorphisms of abelian groups.

Finally, in § 1.6 we investigate direct products of groups and prove Suzuki's theorem that the subgroup lattice of a group \( G \) is a direct product if and only if \( G \) is a direct product of coprime torsion groups. As a nice application we obtain that the number of groups whose subgroup lattice is isomorphic to a given finite lattice \( L \) is finite if and only if \( L \) has no chain as a direct factor.

### 1.1 Basic concepts of lattice theory

A partially ordered set or poset is a set \( P \) together with a binary relation \( \leq \) such that the following conditions are satisfied for all \( x, y, z \in P \):

1. \( x \leq x \).  
   (Reflexivity)

2. If \( x \leq y \) and \( y \leq x \), then \( x = y \).  
   (Antisymmetry)

3. If \( x \leq y \) and \( y \leq z \), then \( x \leq z \).  
   (Transitivity)
An element $x$ of a poset $P$ is said to be a lower bound for the subset $S$ of $P$ if $x \leq s$ for every $s \in S$. The element $x$ is a greatest lower bound of $S$ if $x$ is a lower bound of $S$ and $y \leq x$ for any lower bound $y$ of $S$. By (2), such a greatest lower bound of $S$ is unique if it exists; we denote it by $\inf S$ or $\bigcap S$. Similar definitions and remarks apply to upper bounds and the least upper bound; the latter is denoted by $\sup S$ or $\bigcup S$.

Lattices

A lattice is a partially ordered set in which every pair of elements has a least upper bound and a greatest lower bound. A partially ordered set in which every subset has a least upper bound and a greatest lower bound is called a complete lattice. We can also view lattices as algebras with two binary operations.

1.1.1 Theorem. (a) Let $(L, \leq)$ be a lattice and define the operations $\cap$ and $\cup$ on $L$ (called intersection and union, respectively) by

$$(4) \quad x \cap y = \inf \{x, y\} \quad \text{and} \quad x \cup y = \sup \{x, y\}.$$  

Then the following properties hold for all $x, y, z \in L$:

1. $x \cap y = y \cap x$ and $x \cup y = y \cup x$. \quad \text{(Commutativity)}
2. $(x \cap y) \cap z = x \cap (y \cap z)$ and $(x \cup y) \cup z = x \cup (y \cup z)$. \quad \text{(Associativity)}
3. $x \cap (x \cup y) = x$ and $x \cup (x \cap y) = x$. \quad \text{(Absorption identities)}

Furthermore, we have $x \leq y$ if and only if $x = x \cap y$ (or $y = y \cup x$).

(b) Conversely, let $L$ be a set with two binary operations $\cap$ and $\cup$ satisfying (5)-(7) and define the relation $\leq$ on $L$ by

$$(8) \quad x \leq y \quad \text{if and only if} \quad y = y \cup x.$$  

Then $(L, \leq)$ is a lattice with $x \cap y = \inf \{x, y\}$ and $x \cup y = \sup \{x, y\}$ for all $x, y \in L$.

Proof. (a) Clearly, the operations defined in (4) are commutative. Also it is easy to see that $(x \cap y) \cap z$ and $x \cap (y \cap z)$ both are the greatest lower bound of $\{x, y, z\}$. Hence $(x \cap y) \cap z = x \cap (y \cap z)$ and similarly $(x \cup y) \cup z = x \cup (y \cup z)$. Furthermore $x \leq y$ if and only if $x = \inf \{x, y\} = x \cap y$ (or $y = \sup \{y, x\} = y \cup x$). Since $x \leq x \cup y$ and $x \cap y \leq x$, we therefore have $x \cap (x \cup y) = x$ and $x \cup (x \cap y) = x$.

(b) Let $x, y, z \in L$. We note first that the conditions $x \cap y = x$ and $y \cup x = y$ are equivalent; for, if $x \cap y = x$ holds, then $y \cup x = y \cap (y \cap x) = y$ and conversely $y \cup x = y$ implies $x \cap y = x \cap (y \cap x) = x$. So by (8),

$$(9) \quad x \leq y \quad \text{if and only if} \quad y = y \cup x.$$  

We now show that $(L, \leq)$ is a poset. The absorption identities yield $x \cap x = x \cap (x \cup (x \cap x)) = x$; by (8), $x \leq x$. If $x \leq y$ and $y \leq x$, then $x = x \cap y = y \cap x = y$. If $x \leq y$ and $y \leq z$, then

$$x \cap z = (x \cap y) \cap z = x \cap (y \cap z) = x \cap y = x$$

and hence $x \leq z$. So (1)-(3) hold and $(L, \leq)$ is a poset.
1.1 Basic concepts of lattice theory

Since \((x \cap y) \cap x = x \cap (x \cap y) = (x \cap x) \cap y = x \cap y, x \cap y \leq x\). Similarly \(x \cap y \leq y\). If \(z\) is any lower bound of \(\{x, y\}\), then \(z \cap x = z\) and \(z \cap y = z\). Hence \(z \cap (x \cap y) = (z \cap x) \cap y = z \cap y = z\) and \(z \leq x \cap y\). This shows that \(x \cap y = \inf \{x, y\}\). Replacing \(\cap\) by \(\cup\) and using (9) instead of (8) we get \(x \cup y = \sup \{x, y\}\). In particular, \((L, \leq)\) is a lattice.

Lattices occur in abundance. For any set \(X\), the set of all subsets of \(X\) partially ordered by set inclusion is a complete lattice; the greatest lower bound of any collection of subsets is the set intersection, and the least upper bound is the set union. The subject of this book is the following lattice.

**Subgroup lattice**

If \(G\) is any group, the set \(L(G)\) of all subgroups of \(G\) is partially ordered with respect to set inclusion. Moreover any subset of \(L(G)\) has a greatest lower bound in \(L(G)\), the intersection of all its elements, and a least upper bound in \(L(G)\), the join of all its elements. Thus \(L(G)\) is a complete lattice, the subgroup lattice of \(G\). We denote the operations of this lattice by \(\cap\) and \(\cup\). So we shall write \(X \cap Y\) for the intersection, and \(X \cup Y\) but sometimes also \(\langle X, Y \rangle\) for the join of the subgroups \(X\) and \(Y\) of \(G\). Also, for a set \(\mathcal{S}\) of subgroups of \(G\), \(\bigcup \mathcal{S}\) and \(\langle S | S \in \mathcal{S} \rangle\) both denote the group generated by the subgroups in \(\mathcal{S}\).

**Minimal and maximal elements, chains and antichains**

For elements \(x, y\) of a poset \(P\) we write \(x < y\) if \(x \leq y\) and \(x \neq y\). If \(x < y\) and there is no element \(z \in P\) such that \(x < z < y\), then we say that \(x\) is covered by \(y\) or that \(y\) covers \(x\). Let \(S\) be a subset of \(P\) and \(x \in S\). Then \(x\) is a minimal element of \(S\) if there is no \(s \in S\) with \(s < x\), and \(x\) is a least element of \(S\) if \(x \leq s\) for every \(s \in S\). Certainly the least element of \(S\) is a minimal element of \(S\) and is unique if it exists; on the other hand, it may happen that \(S\) contains many minimal elements but no least element. Similar definitions and remarks apply to maximal elements and the greatest element of \(S\). We write \(O\) and \(I\) for the least and greatest elements of \(P\), respectively (if they exist). An element of \(P\) that covers \(O\) is called an atom, an element that is covered by \(I\) is an antiatom of \(P\). If \(L\) is a complete lattice, then \(\inf L\) is the least and \(\sup L\) the greatest element of \(L\). In the subgroup lattice of the group \(G\) the trivial subgroup \(1\) is the least element, \(G\) is the greatest element, the minimal subgroups are the atoms and the maximal subgroups are the antiatoms of \(L(G)\).

Two elements \(x\) and \(y\) in a poset \(P\) are called comparable if \(x \leq y\) or \(y \leq x\). A subset \(S\) of \(P\) is a chain if any two elements in \(S\) are comparable, \(S\) is an antichain if no two different elements of \(S\) are comparable. The length of a finite chain \(S\) is \(|S| - 1\). The poset \(P\) is said to be of length \(n\), where \(n\) is a natural number, if there is a chain in \(P\) of length \(n\) and all chains in \(P\) are of length at most \(n\). A poset \(P\) is of finite length if it is of length \(n\) for some \(n \in \mathbb{N}\). Similarly \(P\) is said to be of width \(n\) if there is an antichain with \(n\) elements in \(P\) and all antichains in \(P\) have at most \(n\) elements.
A poset $P$ with the property that each of its nonempty subsets contains a maximal element is said to satisfy the maximal condition or the ascending chain condition. The second name comes from the following alternative formulation: $P$ satisfies the maximal condition if and only if it contains no infinite sequence of elements $x_1, x_2, \ldots$ such that $x_1 < x_2 < x_3 < \cdots$. The minimal condition or descending chain condition is defined correspondingly.

Isomorphisms and projectivities

Let $L$ and $\overline{L}$ be lattices. A map $\sigma: L \to \overline{L}$ is called a homomorphism if

$$(10) \quad (x \sqcap y)^\sigma = x^\sigma \sqcap y^\sigma \text{ and } (x \sqcup y)^\sigma = x^\sigma \sqcup y^\sigma$$

for all $x, y \in L$. A homomorphism is an isomorphism if it is bijective, and an isomorphism of a lattice with itself is called an automorphism. We write $L \simeq \overline{L}$ if $L$ and $\overline{L}$ are isomorphic. Finally, we introduce a shorter name for isomorphisms between subgroup lattices. If $G$ and $\overline{G}$ are groups, an isomorphism from $L(G)$ to $L(\overline{G})$ is called a projectivity from $G$ to $\overline{G}$. We also say that $G$ and $\overline{G}$ are lattice-isomorphic if there exists a projectivity from $G$ to $\overline{G}$.

In order to show that a bijective map between two lattices is an isomorphism it suffices to prove that it has one of the two properties in (10) or that it preserves the order relations of the lattices. In addition, every isomorphism preserves union and intersection of arbitrary subsets.

1.1.2 Theorem. Let $\sigma$ be a bijective map of a lattice $L$ to a lattice $\overline{L}$. Then the following properties are equivalent.

(a) For all $x, y \in L$, $x \leq y$ if and only if $x^\sigma \leq y^\sigma$.
(b) $(x \sqcap y)^\sigma = x^\sigma \sqcap y^\sigma$ for all $x, y \in L$.
(c) $(x \sqcup y)^\sigma = x^\sigma \sqcup y^\sigma$ for all $x, y \in L$.

Furthermore, if $\sigma$ satisfies (a) and $S$ is a subset of $L$ such that $\bigcap S$ exists, then also $\bigcap S^\sigma$ exists and $(\bigcap S)^\sigma = \bigcap S^\sigma$; similarly $(\bigcup S)^\sigma = \bigcup S^\sigma$ if $\bigcup S$ exists.

Proof. Let $x, y \in L$. By 1.1.1, $x \leq y$ if and only if $x \cap y = x$ (or $x \cup y = y$). It follows that (b) (and also (c)) implies (a). Conversely, if $\sigma$ satisfies (a) and if $S$ is a subset of $L$ such that $z = \bigcap S$ exists, then $z^\sigma$ is a lower bound of $S^\sigma$ and every lower bound of $S^\sigma$ is of the form $w^\sigma$ where $w$ is a lower bound of $S$. Since $z$ is the greatest lower bound of $S$, $w \leq z$ and hence $w^\sigma \leq z^\sigma$. This shows that $z^\sigma$ is a greatest lower bound of $S^\sigma$ and that $(\bigcap S)^\sigma = \bigcap S^\sigma$. In particular (b) holds. The corresponding result for the least upper bound follows similarly.

An easy, but useful, consequence of this result is that a projectivity of a group is determined by its action on the cyclic subgroups.

1.1.3 Corollary. If $\varphi$ and $\psi$ are projectivities of a group $G$ such that $X^\varphi = X^\psi$ for every cyclic subgroup $X$ of $G$, then $\varphi = \psi$. 
1.1 Basic concepts of lattice theory

Proof. Let \( H \leq G \). Then by 1.1.2, \( H^\circ = \left( \bigcup_{x \in H} \langle x \rangle \right)^\circ = \bigcup_{x \in H} \langle x \rangle^\circ = \bigcup_{x \in H} \langle x \rangle^\circ = H^\circ \).

\[ \square \]

**Hasse diagram**

Every finite poset \( P \), in particular every finite lattice, may be represented by a diagram. Represent each element of \( P \) by a point in the plain in such a way that the point \( p_y \) associated with an element \( y \) lies above the point associated with \( x \) whenever \( x < y \). Then, whenever \( y \) covers \( x \), connect the points \( p_x \) and \( p_y \) by a line segment. We call the resulting figure a *Hasse diagram* of \( P \). It is easy to see that it is possible to construct such a diagram. For the finite poset \( P \) has a maximal element \( z \), \( P \setminus \{z\} \) is a smaller poset, and therefore, by induction, has a diagram; now choose a point \( p_z \) above the points of this diagram and connect it with all the points \( p_x \) associated to elements \( x \) covered by \( z \). Figure 1 shows the Hasse diagrams of all lattices with at most five elements.

![Hasse diagrams of lattices](image)

**Figure 1**

**Sublattices**

A subset of a lattice is called a *sublattice* if it is closed with respect to the operations \( \cap \) and \( \cup \) defined in 1.1.1. It is evident that a sublattice is a lattice relative to the induced operations. Examples of sublattices of a lattice \( L \) are, for \( x, y \in L \), the sets \( S = \{x, y, x \cap y, x \cup y\} \) or, if \( x \leq y \), the intervals

\[ [y/x] = \{z \in L | x \leq z \leq y\}. \]

We mention two sublattices of the subgroup lattice of a group \( G \).

**Lattice of normal subgroups**

\[ \mathfrak{N}(G) = \{N | N \trianglelefteq G\}. \]
Lattice of composition subgroups

We say that the subgroup $H$ of $G$ is subnormal in $G$, and we write $H \leq G$, if there are a nonnegative integer $n$ and a series

$$(11) \quad H = H_n \leq H_{n-1} \leq \cdots \leq H_0 = G$$

of subgroups of $G$. We say that $H$ is a composition subgroup of $G$, if there exists a series (11) for $H$ in which all the factor groups $H_i / H_{i+1}$ are simple; we then call $n$ the type of $H$ and (11) a composition series from $G$ to $H$ of length $n$. Clearly a composition subgroup is always subnormal, but the converse is false.

1.1.4 Lemma. If $H$ is a composition subgroup of type $n$ in $G$, $H < K < G$ and $K \leq G$, then there exist composition series of lengths less than $n$ from $G$ to $K$ and from $K$ to $H$.

**Proof.** Let $K = K_m \leq K_{m-1} \leq \cdots \leq K_0 = G$ and let (11) be a composition series from $G$ to $H$. Then

$$(12) \quad H = K \cap H_n \leq K \cap H_{n-1} \leq \cdots \leq K \cap H_1 \leq K \leq K_{m-1} \leq \cdots \leq K_0 = G$$

is a normal series from $G$ to $H$. By the Schreier refinement theorem, the normal series (11) and (12) have isomorphic refinements. There is no proper refinement of the composition series (11). Hence the isomorphic refinement of (12) is a composition series from $G$ to $H$ of length $n$. Since $H < K < G$, the two parts from $G$ to $K$ and from $K$ to $H$ of this series are composition series of lengths less than $n$. \hfill \Box

1.1.5 Theorem (Wielandt [1939]). Let $G$ be a group. The set $\mathcal{R}(G)$ of all composition subgroups of $G$ is a sublattice of the subgroup lattice $L(G)$.

**Proof.** Let $A, B \in \mathcal{R}(G)$. Then there are composition series

$$A = A_m \leq \cdots \leq A_0 = G \quad \text{and} \quad B = B_n \leq \cdots \leq B_0 = G$$

from $G$ to $A$ and $B$, respectively. We use induction on $\min(m, n)$ to prove that $A \cap B \in \mathcal{R}(G)$, and we may assume that $m \leq n$. If $m = 0$, then $A \cap B = B \in \mathcal{R}(G)$; so let $m \geq 1$. Since

$$A_1 \leq A_1 \cup B = A_1 \cup B_n \leq A_1 \cup B_{n-1} \leq \cdots \leq A_1 \cup B_0 = G$$

and $G/A_1$ is simple, we have either $A_1 \cup B = A_1$ or $A_1 \cup B = G$. In the first case, $A_1 \cap B = B$; in the second, $A_1 \cap B \leq B$ and $B/A_1 \cap B \cong G/A_1$ is simple. In both cases, $A_1 \cap B \in \mathcal{R}(G)$ and 1.1.4 yields that $A_1 \cap B \in \mathcal{R}(A_1)$. By induction $A \cap B = A \cap (A_1 \cap B) \in \mathcal{R}(A_1)$, and so $A \cap B \in \mathcal{R}(G)$ since $G/A_1$ is simple.

We use induction on the ordered pair $(\max(m, n), \min(m, n))$ to prove that $A \cup B \in \mathcal{R}(G)$. Since this is clear if $m = 0$ or $n = 0$, we may assume that $m, n \geq 1$ and that the join of two composition subgroups of types $r$ and $s$ in a group is again a composition subgroup whenever $r \leq s < \max(m, n)$ or $s = \max(m, n)$ and $r < \min(m, n)$. Suppose
that $A$ is not normal in $A \cup B$. Then there exists $b \in B$ such that $A^b \neq A$. Since $A_1 \leq G$, $A^b \leq A_1$ and there are composition series of lengths $m - 1 < \max(m, n)$ from $A_1$ to $A$ and to $A^b$. By induction $A \cup A^b \in \mathcal{R}(A_1)$ and hence $A \cup A^b \leq \leq \leq G$. By 1.1.4 there is a composition series of length less than $m$ from $G$ to $A \cup A^b$. By induction $A \cup B = (A \cup A^b) \cup B \in \mathcal{R}(G)$, as desired. So we may assume that $A \leq A \cup B$ and, similarly, $B \leq A \cup B$. Again by induction $A_{m-1} \cup B \in \mathcal{R}(G)$. If $A_{m-1} \cup B \neq G$, then by 1.1.4 there exist composition series of lengths less than $m$ and $n$ from $A_{m-1} \cup B$ to $A$ and $B$, respectively; by induction $A \cup B \in \mathcal{R}(A_{m-1} \cup B)$ and therefore $A \cup B \in \mathcal{R}(G)$. So we may finally assume that $A_{m-1} \cup B = G$ and, similarly, $A \cup B_{m-1} = G$. Then $A \leq G$ since $A$ is normalized by $A_{m-1}$ and $B$. Similarly $B \leq G$ and so $A \cup B \leq G$. By 1.1.4, $A \cup B \in \mathcal{R}(G)$.

Lemma 1.1.4 shows that in a group $G$ with a composition series (from $G$ to 1) every subnormal subgroup is a composition subgroup. Hence in these groups, in particular in finite groups, subnormal and composition subgroups coincide. Therefore, in this case, $\mathcal{R}(G)$ is also called the lattice of subnormal subgroups of $G$. For subnormal subgroups $A$ and $B$ in an arbitrary group $G$, it is clear that $A \cap B \leq \leq \leq G$, but $A \cup B$ in general is not subnormal in $G$. The reader will find examples and a thorough investigation into the join problem in the book by Lennox and Stonehewer [1987].

**Meet-sublattices**

Let $L$ be a lattice and $M$ a subset of $L$ which is a lattice relative to the induced partial order. Clearly, $M$ need not be a sublattice of $L$; the subgroup lattice of a group $G$ as a subset of the lattice of all subsets of $G$ is an example. If $\cap$ and $\land$ denote the intersection in $L$ and $M$, respectively, then for $x, y \in M$, $x \land y$ is a lower bound of $\{x, y\}$ in $L$ and so $x \land y \leq x \cap y$. We call $M$ a meet-sublattice of $L$ if $x \land y = x \cap y$ for all $x, y \in M$, and $M$ is a complete meet-sublattice of $L$ if $M$ and $L$ are complete lattices and for every subset $S$ of $M$ the greatest lower bounds of $S$ in $M$ and $L$ coincide. Actually, one need not require that $M$ is a lattice here.

**1.1.6 Lemma.** If $M$ is a subset of a complete lattice $L$ such that for every subset $S$ of $M$ the greatest lower bound $\bigcap S$ of $S$ in $L$ is contained in $M$, then $M$ is a complete meet-sublattice of $L$.

**Proof.** For a subset $S$ of $M$ let $S^*$ be the set of upper bounds of $S$ in $M$. By hypothesis, $\inf S^* \in M$. Every $s \in S$ is a lower bound of $S^*$, hence $s \leq \inf S^*$. Thus $\inf S^*$ is an upper bound of $S$ and then, certainly, the least upper bound of $S$ in $M$. Clearly, $\inf S$ is the greatest lower bound of $S$ in $M$. Hence $M$ is a complete lattice and the greatest lower bounds of $S$ in $M$ and $L$ coincide.

If $G$ is a group, $L(G)$ is an example of a complete meet-sublattice of the lattice of all subsets of $G$. We introduce two further lattices of this kind.
Centralizer lattice

Let $\mathcal{C}(G)$ be the set of all centralizers of subgroups of $G$. Since for $H_i \leq G$,

$$
\bigcap_{i \in I} C_G(H_i) = C_G \left( \bigcup_{i \in I} H_i \right) \in \mathcal{C}(G),
$$

$\mathcal{C}(G)$ is a complete meet-sublattice of $L(G)$; in general it is not a sublattice (see Exercise 7). We call $\mathcal{C}(G)$ the centralizer lattice of $G$. The least element of $\mathcal{C}(G)$ is the centre $Z(G)$, the greatest element is $G$.

Coset lattice

Let $\mathcal{R}(G)$ be the set of all right cosets of subgroups of $G$ together with the empty set $\emptyset$. If $\mathcal{S}$ is a nonempty subset of $\mathcal{R}(G)$, then either $\bigcap_{x \in \mathcal{S}} x = \emptyset \in \mathcal{R}(G)$ or there exists an element $x \in \bigcap_{x \in \mathcal{S}} x$. In the latter case, $\mathcal{S} = \{H_i x \mid i \in I\}$ for certain subgroups $H_i$ of $G$, and hence $\bigcap_{x \in \mathcal{S}} x = (\bigcap_{i \in I} H_i) x \in \mathcal{R}(G)$. If $\mathcal{S}$ is the empty subset of $\mathcal{R}(G)$, then $\bigcap_{x \in \mathcal{S}} x = G \in \mathcal{R}(G)$. By 1.1.6, $\mathcal{R}(G)$ is a complete meet-sublattice of the lattice of all subsets of $G$. Since $H x = x (x^{-1} H x)$ for all $H \leq G$ and $x \in G$, every right coset is a left coset, and conversely. So $\mathcal{R}(G)$ is the set of all (right or left) cosets in $G$ and we call $\mathcal{R}(G)$ the coset lattice of $G$. The subgroups of $G$ are precisely the cosets containing the coset $1$. Hence $L(G)$ is the interval $[G/1]$ in $\mathcal{R}(G)$.

Direct products

Let $(L_\lambda)_{\lambda \in \Lambda}$ be a family of lattices. The direct product, $L = \bigoplus_{\lambda \in \Lambda} L_\lambda$, is the lattice whose underlying set is the cartesian product of the sets $L_\lambda$, that is the set of all functions $f$ defined on $\Lambda$ such that $f(\lambda) \in L_\lambda$ for all $\lambda \in \Lambda$, and whose partial order is defined by the rule that $f \leq g$ if and only if $f(\lambda) \leq g(\lambda)$ for all $\lambda \in \Lambda$. Clearly, $f \cap g$ and $f \cup g$ are the functions mapping each $\lambda$ to $f(\lambda) \cap g(\lambda)$ and $f(\lambda) \cup g(\lambda)$, respectively, so that $L$ is a lattice in which intersection and union are performed componentwise. It follows that $L$ satisfies a given lattice identity if and only if each $L_\lambda$ satisfies this identity. If $\Lambda$ is finite, say $\Lambda = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$, we also use the simpler $n$-tupel notation for the elements of $L$. Thus, in this case,

$$
L = L_1 \times \cdots \times L_n = \{(x_1, \ldots, x_n) \mid x_i \in L_i\}
$$

and $(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n)$ if and only if $x_i \leq y_i$ for all $i = 1, \ldots, n$.

We shall need the following simple result which clarifies the structure of a direct product of lattices with greatest and least elements.

1.1.7 Lemma. Let $(L_\lambda)_{\lambda \in \Lambda}$ be a family of lattices, and put $L = \bigoplus_{\lambda \in \Lambda} L_\lambda$. Suppose that $L$ contains a least element $0$ and a greatest element $1$. If $\lambda \in \Lambda$, then $0(\lambda)$ is the least
and \( I(\lambda) \) the greatest element of \( L_\lambda \). Define \( f_\lambda \in L \) by \( f_\lambda(\mu) = 0(\mu) \) for \( \lambda \neq \mu \in \Lambda \) and \( f_\lambda(\lambda) = I(\lambda) \). Then

\[
\begin{align*}
(a) & \quad \bigcup_{v \in \Lambda} f_v = I \quad \text{and} \quad \left( \bigcup_{v \in \Lambda \setminus \{\lambda\}} f_v \right) \cap f_\lambda = 0, \\
(b) & \quad [f_\lambda/0] \simeq L_\lambda, \quad \text{and} \\
(c) & \quad [x \cup y/0] \simeq [x/0] \times [y/0] \quad \text{if} \quad x \in [f_\lambda/0], \ y \in [f_\mu/0] \quad \text{and} \quad \lambda \neq \mu \in \Lambda.
\end{align*}
\]

**Proof.** For \( z \in L_\lambda \), the axiom of choice implies that there is a function \( f \in L \) with \( f(\lambda) = z \). From \( 0 \leq f \leq I \) it follows that \( 0(\lambda) \leq z \leq I(\lambda) \). This shows that \( 0(\lambda) \) is the least and \( I(\lambda) \) the greatest element of \( L_\lambda \). Since union and intersection in \( L \) are performed componentwise, (a) is clear. The map \( \sigma: L_\lambda \to [f_\lambda/0] \) defined by \( z^\sigma(v) = 0(v) \) for \( \lambda \neq v \in \Lambda \) and \( z^\sigma(\lambda) = z \) clearly is an isomorphism; thus (b) holds. Finally, the map

\[
\tau: [x/0] \times [y/0] \to [x \cup y/0]; \quad (u, v) \mapsto w
\]

where \( w(\lambda) = u(\lambda) \), \( w(\mu) = v(\mu) \) and \( w(v) = 0(v) \) for \( v \in \Lambda \) with \( \lambda \neq v \neq \mu \) also is an isomorphism, and this implies (c).

---

### Embedding of lattices in subgroup lattices

We mention without proof three results on subgroup lattices that have little connection with the topics treated in this book. They show how complex subgroup lattices can be.

**1.1.8 Theorem (Whitman [1946]).** Every lattice is isomorphic to a sublattice of the subgroup lattice of some group.

The reader can find a proof of this result in Whitman's paper or in the book by Grätzer [1978]. Whitman first shows that every lattice \( L \) is isomorphic to a sublattice of a partition lattice of some set \( X \); this lattice then is isomorphic to a sublattice of the subgroup lattice of the symmetric group \( \text{Sym} X \) on \( X \) (see Exercise 9). The set \( X \) constructed by Whitman in general is infinite even when \( L \) is finite. However, with a different construction, it is possible to keep the set \( X \) finite in this case.

**1.1.9 Theorem (Pudlák and Tuma [1980]).** Every finite lattice is isomorphic to a sublattice of the subgroup lattice of some finite group.

The situation is more complex if one tries to replace "sublattice" by "interval" in these statements. An element \( c \) in a complete lattice \( L \) is called compact if whenever \( S \subseteq L \) and \( c \leq \bigcup S \) there exists a finite subset \( T \subseteq S \) with \( c \leq \bigcup T \); and a lattice is called algebraic if it is complete and each of its elements is a join of compact...
elements. Now if $H$ is a subgroup of a group $G$ and $g \in G$, then $\langle H, g \rangle$ clearly is a compact element in $[G/H]$. Thus every interval $[G/H]$ is an algebraic lattice, and so the following converse improves Whitman's theorem in this direction as far as possible.

1.1.10 Theorem (Tuma [1989]). Every algebraic lattice is isomorphic to an interval in the subgroup lattice of some group.

The finite analogue, however, is an open problem even for the simplest lattices, for example, for the lattice $M_n$ of length 2 with $n$ atoms. It is easy to construct finite (soluble) groups with such an interval if $n - 1$ is a prime power (see Exercise 11) and the lattices $M_7$ and $M_{11}$ occur in the alternating group $A_{31}$ (see Feit [1983], Pálfy [1988]). However, if $n \geq 13$ and $n - 1$ is not a prime power, it is not known whether $M_n$ is an interval in the subgroup lattice of some finite group.

**Exercises**

1. Let $L$ be a lattice and let $x, y, z \in L$.
   (a) If $y \leq z$, then $x \cap y \leq x \cap z$ and $x \cup y \leq x \cup z$.
   (b) $x \cup (y \cap z) \leq (x \cup y) \cap (x \cup z)$ and $(x \cap y) \cup (x \cap z) \leq x \cap (y \cup z)$.
   (c) If $x \leq z$, then $x \cup (y \cap z) \leq (x \cup y) \cap z$.

2. Which of the Hasse diagrams displayed in Figure 1 represent subgroup lattices?

3. Draw Hasse diagrams for the 15 lattices with 6 elements.

4. Let $G$ be a group and let $A, B \trianglelefteq G$.
   (a) Show that $A \cap B \trianglelefteq G$.
   (b) If $AB = BA$, prove that $A \cup B \trianglelefteq G$.

5. (Curzio [1953]) Show that the abelian group $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = 8$, $o(b) = 2$ and the group $\overline{G} = \langle c, d | c^8 = d^2 = 1, dcd = c^5 \rangle$ have isomorphic coset lattices.

6. If $G = H \times K$, then $\mathfrak{C}(G) \cong \mathfrak{C}(H) \times \mathfrak{C}(K)$.

7. If $G = \langle a, b | a^{15} = b^2 = 1, bab = a^{-1} \rangle$ is the dihedral group of order 30, show that $\mathfrak{C}(G)$ is not a sublattice of $L(G)$.

8. If $G$ and $\overline{G}$ are groups with $\mathfrak{R}(\overline{G}) \cong \mathfrak{R}(G)$, show that $L(\overline{G}) \cong L(G)$ and $|\overline{G}| = |G|$.

9. Let $X$ be a set and let $\Pi(X)$ be the set of all equivalence relations (or partitions) on $X$. For $\rho, \tau \in \Pi(X)$ define $\rho \leq \tau$ if and only if $x \rho y$ implies $x \tau y$ for all $x, y \in X$.
   (a) Show that $\Pi(X)$ is a lattice, the *partition lattice* of $X$.
   (b) Prove that $\Pi(X)$ is isomorphic to a sublattice of $L(\text{Sym } X)$.

10. Show that the compact elements in the subgroup lattice of a group are precisely the finitely generated subgroups.

11. Let $F$ be the field with $p'$ elements, $V$ a vector space of dimension 2 over $F$ and $G$ the group of all permutations $x \to ax + v$ over $V$ where $0 \neq a \in F$ and $v \in V$. If $H = \{x \to ax | 0 \neq a \in F\}$, show that $[G/H] \cong M_{p^r+1}$. 


1.2 Distributive lattices and cyclic groups

In this section we are going to study subgroup lattices of cyclic groups. Since these turn out to be distributive, we shall first determine all groups with distributive subgroup lattices.

**Distributive lattices**

A lattice $L$ is called **distributive** if for all $x, y, z \in L$ the distributive laws hold:

1. $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$,
2. $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$.

**1.2.1 Remark.** Since distributivity is a property defined by identities, sublattices and direct products of distributive lattices are distributive. Furthermore, a lattice $L$ is already distributive if it satisfies one of the two distributive laws. For example, if (1) holds in $L$, then for $x, y, z \in L$ we have

\[
(x \cap y) \cup (x \cap z) = ((x \cap y) \cup x) \cap ((x \cap y) \cup z) = x \cap (z \cup (x \cap y))
\]

\[
= x \cap ((z \cup x) \cap (z \cup y)) = x \cap (y \cup z);
\]

thus (2) holds. The other implication follows similarly.

It is easy to see that every chain is a distributive lattice. We shall also need the following distributive lattices. For $a, b \in \mathbb{N}_0$, the set of nonnegative integers, write $a \leq' b$ if $b$ divides $a$. Clearly, $\leq'$ is a partial order on $\mathbb{N}_0$ for which $\text{sup}\{a, b\}$ is the greatest common divisor and $\text{inf}\{a, b\}$ is the least common multiple of $a$ and $b$. Thus $(\mathbb{N}_0, \leq')$ is a lattice with greatest element 1 and least element 0. We denote this lattice by $T_\infty$ and for $n \in \mathbb{N}$, we write $T_n$ for the interval $[1/n]$ in $T_\infty$. Then $T_n$ is the **lattice of all divisors of $n$**. The reader may check that $T_\infty$ is distributive; this will, however, also follow from 1.2.2 and 1.2.3. As sublattices of $T_\infty$ all the $T_n$ are distributive as well.

![Figure 2: $T_{72}$](image)
Fundamental concepts

Cyclic groups

Let \( n \) be a natural number or the symbol \( \infty \). We write \( n \in \mathbb{N} \cup \{ \infty \} \) to express this and we denote the cyclic group of order \( n \) by \( C_n \). Let \( C_n = \langle g \rangle \). When \( n = \infty \), it is well-known that for every \( r \in \mathbb{N} \) there is a subgroup of index \( r \) in \( \langle g \rangle \), namely \( \langle g^r \rangle \), and every nontrivial subgroup of \( \langle g \rangle \) is of this form. If \( n \) is finite, then for every divisor \( r \) of \( n \) there is exactly one subgroup of index \( r \) in \( \langle g \rangle \), again \( \langle g^r \rangle \). Hence, if we define \( \sigma : T_n \to L(\langle g \rangle) \) by \( r^\sigma = \langle g^r \rangle \) for all \( r \in T_n \), then \( \sigma \) is bijective. Furthermore, for \( r, s \in T_n \), we have \( r \leq s \) if and only if \( s \) divides \( r \), and this holds if and only if \( \langle g^r \rangle \leq \langle g^s \rangle \). By 1.1.2, \( \sigma \) is an isomorphism. Thus we have shown the following.

1.2.2 Lemma. If \( n \in \mathbb{N} \cup \{ \infty \} \), then \( L(C_n) \cong T_n \).

Groups with distributive subgroup lattices

A group \( G \) is called locally cyclic if every finite subset of \( G \) generates a cyclic subgroup. Equivalently we can say that \( \langle a, b \rangle \) is cyclic for every pair \( a, b \) of elements of \( G \). In particular, every locally cyclic group is abelian. The additive group \( \mathbb{Q} \) of rational numbers and the group \( \mathbb{Q}/\mathbb{Z} \) of rational numbers modulo 1 are locally cyclic since finitely many rational numbers have a common denominator \( n \) and therefore are contained in the cyclic group generated by \( \frac{1}{n} \). It is a familiar result that a group is locally cyclic if and only if it is isomorphic to a subgroup of \( \mathbb{Q} \) or of \( \mathbb{Q}/\mathbb{Z} \). We come to our first major result.

1.2.3 Theorem (Ore [1938]). The subgroup lattice of a group \( G \) is distributive if and only if \( G \) is locally cyclic.

Proof. Suppose first that \( L(G) \) is distributive and let \( a, b \in G \). We have to show that \( \langle a, b \rangle \) is cyclic. Since \( \langle a \rangle \cap \langle b \rangle \) is centralized by \( a \) and \( b \), \( \langle a \rangle \cap \langle b \rangle \leq Z(\langle a, b \rangle) \). Also \( \langle ab \rangle \cup \langle a \rangle = \langle a, b \rangle = \langle ab \rangle \cup \langle b \rangle \) and so by (1),

\[
\langle ab \rangle \cup (\langle a \rangle \cap \langle b \rangle) = (\langle ab \rangle \cup \langle a \rangle) \cap (\langle ab \rangle \cup \langle b \rangle) = \langle a, b \rangle.
\]

Thus \( \langle a, b \rangle / \langle a \rangle \cap \langle b \rangle \simeq \langle ab \rangle / (\langle ab \rangle \cap (\langle a \rangle \cap \langle b \rangle)) \) is cyclic and therefore \( \langle a, b \rangle \) is abelian, as a cyclic extension of a central subgroup. By the structure of finitely generated abelian groups (see Robinson [1982], p. 100) there exist \( c, d \in G \) such that \( \langle a, b \rangle = \langle c \rangle \times \langle d \rangle \). By what we have shown, \( \langle c, d \rangle / \langle c \rangle \cap \langle d \rangle \) is cyclic. Since \( \langle c \rangle \cap \langle d \rangle = 1 \), \( \langle a, b \rangle = \langle c, d \rangle \) is cyclic.

Now suppose that \( G \) is locally cyclic and let \( A, B, C \in L(G) \). By 1.2.1, we need only show that the first distributive law holds, or, since \( G \) is abelian, that \( A(B \cap C) = AB \cap AC \). Clearly, \( A(B \cap C) \leq AB \cap AC \). Let \( x \in AB \cap AC \), hence \( x = ab = a'c \) with \( a, a' \in A \), \( b \in B \) and \( c \in C \). Since \( G \) is locally cyclic, there exists \( g \in G \) such that \( \langle a, a', b, c \rangle = \langle g \rangle \). Then \( ab = a'c \) implies that \( \langle g \rangle = (A \cap \langle g \rangle)(B \cap \langle g \rangle) = (A \cap \langle g \rangle)(C \cap \langle g \rangle) \). If one of the three subgroups \( A \cap \langle g \rangle, B \cap \langle g \rangle, C \cap \langle g \rangle \) is trivial, then either \( x = b = c \in B \cap C \) or \( x \in A \). In both cases, \( x \in A(B \cap C) \). So sup-
1.2 Distributive lattices and cyclic groups

pose that all these subgroups are nontrivial and let \( n, r, s \) be the respective indices of \( A \cap \langle g \rangle, B \cap \langle g \rangle, C \cap \langle g \rangle \) in \( \langle g \rangle \). Then \( (n,r) = 1 = (n,s) \), hence \( (n,rs) = 1 \) and therefore

\[
\langle g \rangle = \langle g^n \rangle \langle g^r \rangle = (A \cap \langle g \rangle)(B \cap C \cap \langle g \rangle) \leq A(B \cap C).
\]

Again it follows that \( x \in A(B \cap C) \). Thus \( AB \cap AC \leq A(B \cap C) \), as required.

1.2.4 Corollary. The subgroup lattice of a finite group \( G \) is distributive if and only if \( G \) is cyclic.

Ore's theorem, and perhaps even more its corollary, is one of the most beautiful results on two of the basic problems mentioned in the preface: Which class of groups is the class of all groups with a given lattice property and, conversely, which lattice property characterizes a given class of groups. Here an interesting class of lattices, the finite distributive lattices, belongs to a simple class of groups, the finite cyclic groups. This example is rather atypical. We shall see that nice classes of lattices often lead to fairly complicated classes of groups and, similarly, it is usually very difficult or even impossible to characterize a given interesting class of groups.

**Lattice-theoretic characterizations of cyclic groups**

Using Ore's theorem, however, it is not difficult to characterize the class of cyclic groups.

1.2.5 Theorem. The group \( G \) is cyclic if and only if its subgroup lattice \( L(G) \) is distributive and satisfies the maximal condition.

**Proof.** It is well-known and easy to prove that a group whose subgroup lattice satisfies the maximal condition is finitely generated. Thus if \( L(G) \) is distributive and satisfies the maximal condition, then \( G \) is locally cyclic, by Ore's theorem, and finitely generated; hence \( G \) is cyclic. Conversely, if \( G \) is cyclic, then \( L(G) \) is distributive, by Ore's theorem. Furthermore, if \( 1 < H \leq G \), then \( [G/H] \) is finite. So, clearly, \( L(G) \) satisfies the maximal condition.

1.2.6 Corollary (Baer [1939a]). Let \( G \) be a group. Then \( G \simeq C_\infty \) if and only if \( L(G) \simeq T_\infty \).

**Proof.** If \( G \simeq C_\infty \), then \( L(G) \simeq T_\infty \), by Lemma 1.2.2. Conversely, let \( L(G) \simeq T_\infty \). By 1.2.2, \( L(G) \simeq L(C_\infty) \). By 1.2.5, \( L(G) \) is distributive and satisfies the maximal condition and therefore \( G \) is cyclic. Clearly, \( |G| \) is infinite.

Thus the infinite cyclic group \( C_\infty \) is determined by its subgroup lattice: it is the only group \( G \) such that \( L(G) \simeq L(C_\infty) \). For finite cyclic groups the situation is different since for \( m, m' \in \mathbb{N} \), the lattices \( T_m \) and \( T_{m'} \) may be isomorphic although \( m \neq m' \).
If \( m = p_1^{k_1} \cdots p_r^{k_r} \) is the prime power decomposition of \( m \), then every divisor of \( m \) has the form \( p_1^{k_1} \cdots p_r^{k_r} \) with \( 0 \leq k_i \leq n_i \) for \( i = 1, \ldots, r \). The map \( \sigma \) defined by

\[
(p_1^{k_1} \cdots p_r^{k_r})^\sigma = (p_1^{k_1}, \ldots, p_r^{k_r})
\]

is an isomorphism from \( T_m \) to the direct product of the \( T_{p_i^{n_i}} \), and these \( T_{p_i^{n_i}} \) are chains of lengths \( n_i \). Furthermore, \( T_m \) contains exactly \( r \) antiatoms, namely \( p_1, \ldots, p_r \), and to each \( p_i \) exactly one chain of maximal length through 1 and \( p_i \), namely \( [1/p_i^{n_i}] \) of length \( n_i \). So if \( m' \in \mathbb{N} \) such that \( T_m \cong T_{m'} \) and \( \tau \), say, is an isomorphism from \( T_m \) to \( T_{m'} \), then the \( p_i \) are distinct primes and \( m' = (p_1)^{n_1} \cdots (p_r)^{n_r} \).

1.2.7 Theorem (Baer [1939a]). Let \( n_1, \ldots, n_r \in \mathbb{N} \). The group \( G \) is cyclic of order \( p_1^{n_1} \cdots p_r^{n_r} \) with distinct primes \( p_i \) if and only if \( L(G) \) is a direct product of chains of lengths \( n_1, \ldots, n_r \).

Proof. If \( G \) is cyclic of order \( m = p_1^{n_1} \cdots p_r^{n_r} \), then \( L(G) \cong T_m \) is a direct product of chains of lengths \( n_1, \ldots, n_r \). Conversely, suppose that \( L(G) \) is such a direct product, let \( q_1, \ldots, q_r \) be distinct primes and put \( m' = q_1^{n_1} \cdots q_r^{n_r} \). Then \( L(G) \cong T_{m'} \) is distributive and finite. By 1.2.5, \( G \) is cyclic. Thus \( T_{m'} \cong L(G) \cong T_{|G|} \) and hence \( |G| = p_1^{n_1} \cdots p_r^{n_r} \) with distinct primes \( p_i \).

1.2.8 Corollary. Let \( n_1, \ldots, n_r \in \mathbb{N} \) and let \( p_1, \ldots, p_r \) be distinct primes. If \( G \) is a cyclic group of order \( p_1^{n_1} \cdots p_r^{n_r} \) and \( \bar{G} \) is any group, then \( L(\bar{G}) \cong L(G) \) if and only if \( \bar{G} \) is cyclic of order \( q_1^{n_1} \cdots q_r^{n_r} \) with distinct primes \( q_1, \ldots, q_r \).

Thus the finite cyclic groups are far away from being determined by their subgroup lattices. Indeed, to every finite cyclic group \( C_n \) there exist infinitely many nonisomorphic groups \( C \) with \( L(C) \cong L(C_n) \). However, all these groups are cyclic. And that is the important fact. If \( H \) is a subgroup of a group \( G \), \( L(H) \) is the interval \( [H/1] \) in \( L(G) \). Hence it is possible to decide in the lattice \( L(G) \) whether a given subgroup \( H \) of \( G \) is cyclic or not.

### Lattice-theoretic characterizations and invariance under projectivities

Let us pause for a general remark on the study of classes of groups and their lattices. Ore's theorem, or rather Theorem 1.2.5, is our first example of a lattice-theoretic characterization of a class \( \mathcal{X} \) of groups. By this we mean the specification of a lattice-theoretic property, that is a class \( \mathcal{Y} \) of lattices, such that for every group \( G \),

\[
(3) \quad G \in \mathcal{X} \text{ if and only if } L(G) \in \mathcal{Y}.
\]

We call a class \( \mathcal{X} \) of groups invariant under projectivities if for every projectivity between two groups \( G \) and \( \bar{G} \),

\[
(4) \quad G \in \mathcal{X} \text{ implies } \bar{G} \in \mathcal{X}.
\]
Suppose that a class $\mathcal{X}$ of groups has a lattice-theoretic characterization $\mathcal{Y}$. Then if $G \in \mathcal{X}$ and $\varphi$ is a projectivity from $G$ to $\overline{G}$, $L(\overline{G}) \cong L(G) \in \mathcal{Y}$ and hence $\overline{G} \in \mathcal{X}$, by (3). So we have the following.

1.2.9 Lemma. Let $\mathcal{X}$ be a class of groups. If $\mathcal{X}$ has a lattice-theoretic characterization, then $\mathcal{X}$ is invariant under projectivities.

The converse of this statement is also true. If $\mathcal{X}$ is invariant under projectivities, then the class $\mathcal{Y}$ of all lattices isomorphic to some $L(G)$ with $G \in \mathcal{X}$ satisfies (3). However, we are looking for a lattice-theoretic description of this class $\mathcal{Y}$ as, for example, in Theorem 1.2.5. This result together with 1.2.9 yields the following.

1.2.10 Theorem. Every projectivity maps cyclic groups onto cyclic groups.

If $H$ is a subgroup of $G$ and $\varphi$ is a projectivity from $G$ to $\overline{G}$, then the restriction $\varphi_H$ of $\varphi$ to $[H/1] = L(H)$ clearly is a projectivity from $H$ to $H^\varphi$; we say that $\varphi$ induces the projectivity $\varphi_H$ in $H$. Theorem 1.2.10 shows that if $H$ is cyclic, so is $H^\varphi$ since it is the image of $H$ under the projectivity $\varphi_H$.

Finite and locally finite groups

We conclude this section with a first application of our results on subgroup lattices of cyclic groups. Let $\mathcal{X}$ be a class of groups. We say that $G$ is locally an $\mathcal{X}$-group, if every finitely generated subgroup of $G$ lies in $\mathcal{X}$. We write $L\mathcal{X}$ for the class of all locally $\mathcal{X}$-groups.

1.2.11 Lemma. Let $\mathcal{X}$ be a class of groups. If $\mathcal{X}$ is invariant under projectivities, then so is $L\mathcal{X}$.

Proof. Let $\varphi$ be a projectivity from $G$ to $\overline{G}$ and suppose that $\overline{G} \in L\mathcal{X}$. Let $H = \langle x_1, \ldots, x_n \rangle$ be a finitely generated subgroup of $G$. By 1.2.10 there exist $y_1, \ldots, y_n \in \overline{G}$ such that

$$H^\varphi = \langle x_1 \rangle \cup \cdots \cup \langle x_n \rangle = \langle x_1 \rangle^\varphi \cup \cdots \cup \langle x_n \rangle^\varphi = \langle y_1 \rangle \cup \cdots \cup \langle y_n \rangle.$$ 

Thus $H^\varphi$ is finitely generated and hence $H^\varphi \in \mathcal{X}$, since $\overline{G} \in L\mathcal{X}$. Now $\varphi^{-1}$ induces a projectivity from $H^\varphi$ to $H$, and since $\mathcal{X}$ is invariant under projectivities, $H \in \mathcal{X}$. Thus $G \in L\mathcal{X}$. 

1.2.12 Theorem. A group is finite if and only if its subgroup lattice is finite. Hence every projectivity maps finite groups onto finite groups and locally finite groups onto locally finite groups.

Proof. If $|G|$ is finite, then $G$ has only finitely many subgroups. Conversely, suppose that $L(G)$ is finite. If $C$ is a cyclic subgroup of $G$, then $L(C)$ is an interval in $L(G)$,
hence finite; by 1.2.2, $|C|$ is finite. Since $G$ possesses only finitely many such sub-
groups and every element of $G$ is contained in one of them, $|G|$ is finite. By 1.2.9, the
class of all finite groups is invariant under projectivities. Then 1.2.11 implies that the
class of locally finite groups has the same property.

Exercises

1. Let $p$ be a prime and write $C_{p^\infty}$ for the Prüfer group of type $p^\infty$, that is $C_{p^\infty} = A/\mathbb{Z}$
where $A$ is the additive group of rational numbers whose denominator is a power
of $p$. Show that $L(C_{p^\infty})$ is a chain.

2. If $L(G)$ is a chain, show that $G \cong C_{p^n}$ where $p \in \mathbb{P}$ and $n \in \mathbb{N} \cup \{\infty\}$.

3. (Ore [1938]) The elements $x, y$ of a lattice $L$ are said to be a \textit{\cap-distributive} ("meet-
distributive") pair in $L$ if for all $z \in L$ the distributive law

$$z \cap (x \cup y) = (z \cap x) \cup (z \cap y)$$

holds. Show that the subgroups $A, B$ form a \textit{\cap-distributive} pair in $L(G)$ if and
only if for every $c \in A \cup B$, in neither $A$ nor $B$, there-exist coprime natural num-
bers $m$ and $n$ such that $c^m \in A$ and $c^n \in B$.

4. If $A, B$ is a \textit{\cap-distributive} pair in $L(G)$ with $A \cap B \leq A \cup B$, show that $A$ and $B$
are normal subgroups of $A \cup B$. (Hint: For $a \in A$, $B = (B \cap A) \cup (B \cap B^a) = B^a$
since $A, B$ and $A, B^a$ are \textit{\cap-distributive} pairs.)

5. Use Exercises 3 and 4 to give an alternate proof of Theorem 1.2.3.

6. A \textit{\cap-distributive} pair $x, y$ is said to be trivial if $x \leq y$ or $y \leq x$. Show that $L(G)$
has only trivial \textit{\cap-distributive} pairs if and only if every element of $G$ has prime
power order.

7. (Bruno [1972]) If $A, B$ is a \textit{\cap-distributive} pair in $L(G)$, show that $A, B$ is a
\textit{\cup-distributive} pair in $L(A \cup B)$, that is satisfies

$$C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$$

for all $C \in L(A \cup B)$. Also show that the converse is false.

8. Let $\mathfrak{X}$ be a class of groups and suppose that $\mathfrak{Y}$ is a class of lattices such that (3)
holds. Find a lattice-theoretic characterization of the class $L\mathfrak{X}$ of all locally $\mathfrak{X}$-
groups.

1.3 Projectivities

In this section we shall present some general methods to construct projectivities
between groups and to find isomorphisms that induce a given projectivity.
Construction of projectivities

It is often possible to work with element maps. For such a map \( \sigma : G \to \overline{G} \) and a subset \( X \) of \( G \) we define \( X^\sigma = \{ x^\sigma | x \in X \} \). If \( \sigma \) is bijective and satisfies

\[
(1) \quad X \leq G \text{ if and only if } X^\sigma \leq \overline{G}
\]

for all subsets \( X \) of \( G \), then by 1.1.2, the map

\[
(2) \quad \overline{\sigma}: L(G) \to L(\overline{G}); H \mapsto H^\sigma
\]

is a projectivity from \( G \) to \( \overline{G} \). We call \( \overline{\sigma} \) the projectivity induced by \( \sigma \), and, more generally, we say that a given projectivity \( \varphi \) is induced by an element map \( \sigma \) between the two groups if \( H^\sigma = H^\varphi \) for all \( H \leq G \).

A useful concept in the study of element maps between groups is the amorphy of a map. It measures the deviation from homomorphy. To be precise, if \( \sigma \) is an element map from \( G \) to \( \overline{G} \), then the map

\[
(3) \quad \alpha: G \times G \to G; (x, y) \mapsto (y^\sigma)^{-1}(x^\sigma)^{-1}(xy)^\sigma
\]

is called the amorphy of \( \sigma \). Clearly, \((xy)^\sigma = x^\sigma y^\sigma \alpha(x, y)\) and so \( \sigma \) is a homomorphism if and only if \( \alpha(x, y) = 1 \) for all \( x, y \in G \). Furthermore, we have the associativity identities

\[
(4) \quad \alpha(x, y)^\sigma \alpha(xy, z) = \alpha(y, z)\alpha(x, yz)
\]

for all \( x, y, z \in G \).

For, we can write

\[
((xy)z)^\sigma = (xy)^\sigma z^\sigma \alpha(xy, z) = x^\sigma y^\sigma \alpha(x, y)z^\sigma \alpha(x, y, z)
\]

and

\[
(xyz)^\sigma = x^\sigma (yz)^\sigma \alpha(x, yz) = x^\sigma y^\sigma z^\sigma \alpha(y, z)\alpha(x, yz),
\]

and the associative law in \( G \) implies (4).

If \( \sigma: G \to \overline{G} \) is bijective and induces a projectivity, then \((xy)^\sigma \in \langle x, y \rangle^\sigma = \langle x^\sigma \rangle \cup \langle y^\sigma \rangle = \langle x^\sigma, y^\sigma \rangle \) and hence also \( \alpha(x, y) \in \langle x^\sigma, y^\sigma \rangle \). We show that, conversely, this property and the corresponding one for \( \sigma^{-1} \) suffice to guarantee that \( \sigma \) induces a projectivity. This will be our most useful tool in constructing projectivities.

1.3.1 Theorem. Let \( \sigma \) be a bijective map from \( G \) to \( \overline{G} \) such that

\[
(5) \quad (xy)^\sigma \in \langle x^\sigma, y^\sigma \rangle \text{ for all } x, y \in G, \text{ and}
\]

\[
(6) \quad (uv)^{\sigma^{-1}} \in \langle u^{\sigma^{-1}}, v^{\sigma^{-1}} \rangle \text{ for all } u, v \in \overline{G}.
\]

Then the map \( \overline{\sigma}: L(G) \to L(\overline{G}) \) defined in (2) is a projectivity from \( G \) to \( \overline{G} \).

Proof. Let \( H \leq G \) and let \( x^\sigma, y^\sigma \in H^\sigma \). By (6), \((x^\sigma y^\sigma)^{\sigma^{-1}} \in \langle x, y \rangle \leq H \) and hence \( x^\sigma y^\sigma \in H^\sigma \). If we can show that also \((x^\sigma)^{-1} \in H^\sigma \), then \( H^\sigma \) is a subgroup of \( \overline{G} \). By
symmetry then also $K^{-1} \leq G$ for every $K \leq \overline{G}$. Thus $\sigma$ satisfies (1) and $\overline{\sigma}$ is a projectivity. So it remains to show that $(x^\sigma)^{-1} \in H^\sigma$.

To do this we study an arbitrary pair of elements $a, b \in G$ with $(a^\sigma)^{-1} = b^\sigma = u$, say. By an obvious induction we get from (5),

$$(7) \quad (a^n)^\sigma \in \langle u \rangle \text{ and } (b^n)^\sigma \in \langle u \rangle$$

for all $n \in \mathbb{N}$, and from (6), $(u^n)^{\sigma-1} \in \langle b \rangle$ and $(u^{-n})^{\sigma-1} \in \langle a \rangle$, that is.

$$(8) \quad u^n \in \langle b \rangle^\sigma \text{ and } u^{-n} \in \langle a \rangle^\sigma.$$  

Again by (5), $(ab)^\sigma$ is contained in $\langle a^\sigma, b^\sigma \rangle = \langle u \rangle$ and hence in $\langle b \rangle^\sigma$ or in $\langle a \rangle^\sigma$, by (8). Thus $ab$ lies in $\langle b \rangle$ or in $\langle a \rangle$ and so we get the following.

$$(9) \quad \text{If } a, b \in G \text{ such that } (a^\sigma)^{-1} = b^\sigma, \text{ then } a \in \langle b \rangle \text{ or } b \in \langle a \rangle.$$  

We want to show that $\langle a \rangle = \langle b \rangle$ in (9). For this purpose we suppose that $\langle a \rangle \neq \langle b \rangle$, and, without loss of generality, we may assume that $\langle a \rangle < \langle b \rangle$. Then (7) and (8) show that $\langle u \rangle \subseteq \langle b \rangle^\sigma$ and that $a$, $b$ and $u$ all have infinite order. Write $(b^{-1})^\sigma = v$.

Then (9), applied to $u, v \in \overline{G}$ and $\sigma^{-1}$, yields that $u \in \langle v \rangle$ or $v \in \langle u \rangle$.

Suppose first that $v \in \langle u \rangle$ and let $v = u^r$ with $r \in \mathbb{Z}$. Since $\sigma$ is bijective, $|r| \geq 2$. By (7), $(b^{-n})^\sigma \in \langle u^r \rangle$ for all $n \in \mathbb{N}$ and so $\langle b \rangle^\sigma \subseteq \langle u \rangle$. Thus $\langle b \rangle^\sigma = \langle u \rangle$. Hence for every $i \in \mathbb{N}$ there exist $k, t \in \mathbb{Z}$ such that $u^i = (b^k)^\sigma$ and $(b^{-k})^\sigma = u^t$, and we can choose $i$ so that $|k| \geq 2$ and $|t| \geq 2$. Now (9), applied to $u^r, u^t \in \overline{G}$ and $\sigma^{-1}$, shows that $u^r \in \langle u^r \rangle$ or $u^t \in \langle u^t \rangle$. In both cases, $d = (r, t) \neq 1$ and $(b^{|k|})^\sigma \in \langle u^d \rangle$. Since also $(b^{-|k|})^\sigma \in \langle u^d \rangle \leq \langle u^d \rangle$ for every $n \in \mathbb{N}$, we get by (5)

$$u = b^\sigma = (b^{|k|}b^{-|k|^{-1}})^\sigma \in \langle u^d \rangle,$$

a contradiction. The case that $v \notin \langle u \rangle$ is similar. Here $\langle u \rangle < \langle v \rangle$, let $u = v^s$ where $|s| \geq 2$. Again by (7), $\langle u \rangle \subseteq \langle b \rangle^\sigma \subseteq \langle v \rangle$. Hence for $i \in \mathbb{N}$ there exist $k, t \in \mathbb{Z}$ such that $(b^k)^\sigma = v^i$ and $(b^{-k})^\sigma = v^t$, and we can choose $i$ so that $|k| \geq 2$ and $|t| \geq 2$. Now replace $u$ by $v$ and $r$ by $s$ to get the same contradiction as before.

Thus we have shown that $\langle a \rangle = \langle b \rangle$ in (9) and hence that $(a^\sigma)^{-1} = \langle a \rangle^\sigma$. Returning to the element $x \in H$ we see that $(x^\sigma)^{-1} \in \langle x \rangle^\sigma \subseteq H^\sigma$, as required. \hfill \Box

For $n \in \mathbb{N}$ let $L_n(G)$ be the set of all subgroups of the group $G$ that can be generated by $n$ elements. Since any group is the join of its cyclic subgroups, every projectivity is determined by its action on the set $L_1(G)$. In general the most accessible subgroups of a group are the cyclic ones. Therefore it is important to know under which conditions one can extend a bijection between $L_1(G)$ and $L_1(\overline{G})$ to a projectivity from $G$ to $\overline{G}$.

1.3.2 Theorem. Let $G$ and $\overline{G}$ be groups and suppose that $\tau$ is a bijective map from the set $L_1(G)$ of all cyclic subgroups of $G$ to $L_1(\overline{G})$ such that for all $X, Y, Z \in L_1(G)$,

$$(10) \quad X \leq \langle Y, Z \rangle \text{ if and only if } X^\tau \leq \langle Y^\tau, Z^\tau \rangle.$$

For $H \leq G$ let $H^\sigma$ be the set union of all the $X^\tau$ where $X \in L_1(H)$. Then $\phi$ is a projectivity from $G$ to $\overline{G}$.
1.3 Projectivities

Proof. We first show that $H^\sigma$ is a subgroup of $\bar{G}$. So let $a, b \in H^\sigma$. Then there exist $Y, Z \in L_1(H)$ such that $a \in Y^\tau$ and $b \in Z^\tau$. Since $\tau$ is surjective, there is an $X \in L_1(G)$ such that $X^\tau = \langle ab^{-1} \rangle$. Then $X^\tau \leq \langle a, b \rangle \leq \langle Y^\tau, Z^\tau \rangle$ and by (10), $X \leq \langle Y, Z \rangle \leq H$. Therefore $X \in L_1(H)$ and $ab^{-1} \in X^\tau \subseteq H^\sigma$. Thus $H^\sigma \leq \bar{G}$ and $\phi$ is a map from $L(G)$ to $L(\bar{G})$. Since $\tau^{-1}$ satisfies (10) with $G$ and $\bar{G}$ interchanged, there is a map $\psi : L(\bar{G}) \to L(G)$ defined to $\tau^{-1}$ in the same way as $\varphi$ to $\tau$. For $x \in H \leq G$, $\langle x \rangle^\tau \in L_1(H^\sigma)$ and hence $x \in H^\sigma$; thus $H \leq H^\sigma$. Conversely, the definitions of $\psi$ and $\varphi$ imply that to every $y \in H^\sigma$ there exist $\langle u \rangle \in L_1(H)$ and $Z \in L_1(H)$ such that $y \in \langle u \rangle^{-1}$ and $u \in Z$. Hence $\langle u \rangle \leq Z^\tau$ and therefore $y \in \langle u \rangle^{-1} \leq Z$, by (10). Thus $y \in H$ and so $H^\psi = H$. Similarly, $K^\psi = K$ for all $K \subseteq G$. It follows that $\varphi$ and $\psi$ are bijective maps and they certainly preserve inclusion. By 1.1.2, $\varphi$ is a projectivity.

It does not suffice to assume in Theorem 1.3.2 that $\tau$ is an isomorphism between the partially ordered sets (by inclusion) $L_1(G)$ and $L_1(\bar{G})$. This can be seen by taking any two groups of the same order $p^n$ and exponent $p$, $p$ a prime, that are not lattice isomorphic. One needs the subgroups generated by two elements in (10). But for $n \geq 2$, every isomorphism between $L_n(G)$ and $L_n(\bar{G})$ can be extended to a projectivity. This result, of course, is most interesting for $n = 2$; however, it seems possible that one knows $L_n(G)$ and $L_n(\bar{G})$ for some $n > 2$ without being able to decide which subgroups are cyclic or lie in $L_2(G)$.

1.3.3 Theorem (Poland [1985]). Let $G$ and $\bar{G}$ be groups and let $n \in \mathbb{N}$ with $n \geq 2$. If $\sigma$ is a bijective map from $L_n(G)$ to $L_n(\bar{G})$ such that for all $X, Y \in L_n(G)$,

$$\langle X \rangle \leq Y \text{ if and only if } X^\sigma \leq Y^\sigma,$$

then there exists a unique extension $\varphi$ of $\sigma$ to a projectivity from $G$ to $\bar{G}$.

Proof. We first show that $\sigma$ maps cyclic subgroups of $G$ to cyclic subgroups of $\bar{G}$. So let $H \leq G$ be cyclic. Then $L_n(H^\sigma) \simeq L_n(H) = L(H)$ and therefore $L_n(H^\sigma) \simeq T_m$ where $m = |H| \in \mathbb{N} \cup \{\infty\}$, by 1.2.2. In particular, $L_n(H^\sigma)$ satisfies the maximal condition and hence there exists a maximal cyclic subgroup $\langle x \rangle$ of $H^\sigma$. Suppose that $H^\sigma \neq \langle x \rangle$, take $y \in H^\sigma \setminus \langle x \rangle$ and put $Z = \langle x, y \rangle$. Since $L_n(Z)$ is the interval $[Z/1]$ in $L_n(H^\sigma)$, we have $L_n(Z) \simeq T_r$ for some $r \in \mathbb{N} \cup \{\infty\}$, and if $r = \infty$, then $\langle x \rangle \cap \langle y \rangle \neq 1$. Thus in any case, the interval $[Z/\langle x \rangle \cap \langle y \rangle]$ in $L_n(Z)$ is isomorphic to some $T_s$ where $s \in \mathbb{N}$. Now $y$ operates by conjugation on this interval in which $\langle x \rangle$ is the only complement to $\langle y \rangle$; it follows that $\langle x \rangle^y = \langle x \rangle$. Thus $\langle x \rangle \leq Z$ and $Z/\langle x \rangle$ is cyclic. Therefore, if $K$ is any subgroup of $Z$, $K \cap \langle x \rangle$ is a cyclic normal subgroup of $K$ with cyclic factor group and hence $K \subseteq L_2(Z) \subseteq L_n(Z)$. This shows that $L(Z) = L_n(Z) \simeq T_r$ and by 1.2.5, $Z$ is cyclic, contrary to the maximality of $\langle x \rangle$. We have shown that $H^\sigma$ is cyclic.

Since $\sigma^{-1}$ satisfies the assumptions of the theorem with $G$ and $\bar{G}$ interchanged, $\sigma^{-1}$ maps cyclic subgroups of $\bar{G}$ to cyclic subgroups of $G$. The restriction $\tau$ of $\sigma$ to $L_1(G)$, therefore, is a bijective map from $L_1(G)$ to $L_1(\bar{G})$. For $k \leq n$ and $X_1, \ldots, X_k \in L_1(G)$, by (11) we have $X_1^\sigma = X_1^\tau \leq \langle X_1, \ldots, X_k \rangle^\sigma$ for all $i$ and so $\langle X_1, \ldots, X_k \rangle^\sigma \leq \langle X_1, \ldots, X_k \rangle^\sigma$. The corresponding result for $\sigma^{-1}$ yields the reverse inclusion. Thus

$$\langle X_1, \ldots, X_k \rangle = \langle X_1, \ldots, X_k \rangle^\sigma.$$
Now for $X, Y, Z \in L_1(G)$, (11) and (12) imply that $X \leq \langle Y, Z \rangle$ if and only if $X^* = X^* \leq \langle Y^*, Z^* \rangle$. By 1.3.2 there is a projectivity $\varphi$ from $G$ to $\tilde{G}$ whose restriction to $L_1(G)$ is $\tau$. By (12), $\varphi$ is an extension of $\sigma$ and it is unique since every projectivity is determined by its action on $L_1(G)$.

We shall quite often use 1.3.1 or 1.3.2 to construct projectivities. Theorem 1.3.3, however, is more of theoretical interest. Nevertheless it seems worthwhile to investigate more closely these partially ordered sets $L_n(G)$, in particular, $L_2(G)$.

**Induced projectivities**

An isomorphism $\sigma$ from $G$ to $\tilde{G}$ satisfies (1) and therefore induces a projectivity. It is one of the main problems about subgroup lattices to decide under what conditions a given projectivity $\varphi$ is induced by a group isomorphism $\sigma$. Clearly, it suffices to know that $\varphi$ and $\sigma$ operate in the same way on $L_1(G)$. We shall need the following more general result.

1.3.4 **Lemma.** If $\varphi$ is a projectivity from $G$ to $\tilde{G}$ and $\sigma : G \to \tilde{G}$ is a homomorphism such that $X^\sigma = X^\sigma$ for every cyclic subgroup $X$ of $G$, then $\sigma$ is an isomorphism inducing $\varphi$.

**Proof.** If $X$ is a cyclic subgroup of the kernel of $\sigma$, then $X^\sigma = X^\sigma = 1$ and so $X = 1$. Thus $\sigma$ is injective. Let $H \leq G$. Since $\sigma$ is a homomorphism, $H^\sigma \leq \tilde{G}$. Hence by 1.1.2,

$$H^\sigma = \left( \bigcup_{x \in H} \langle x \rangle \right)^\sigma = \bigcup_{x \in H} \langle x \rangle^\sigma = \bigcup_{x \in H} \langle x \rangle^\sigma = H^\sigma.$$  

In particular, $G^\sigma = \tilde{G}$. Thus $\sigma$ is surjective and induces $\varphi$.

The fact that a projectivity maps cyclic groups onto cyclic groups makes it possible to construct element maps. A general result in this direction is the following.

1.3.5 **Theorem.** A projectivity $\varphi$ from a group $G$ to a group $\tilde{G}$ is induced by a bijective map from $G$ to $\tilde{G}$ if and only if $|\langle g \rangle^\sigma| = |\langle g \rangle|$ for every $g \in G$.

**Proof.** The condition is clearly necessary. Conversely, let $\varphi$ be a projectivity satisfying $|\langle g \rangle^\sigma| = |\langle g \rangle|$ for all $g \in G$. For any cyclic group $C$ let $C^*$ be the set of generators of $C$. If $C \leq G$ is cyclic, then so is $C^\sigma$, by 1.2.10, and since $|C^\sigma| = |C|$, we have $|(C^\sigma)^*| = |C^*|$. Let $\sigma_c$ be a bijection from $C^* \to (C^\sigma)^*$. For $g \in G$ define $g^\sigma = g^{\sigma_c}$ where $C = \langle g \rangle$. Then, clearly, $\sigma$ is injective. If $H \leq G$ and $g \in H$, then $\langle g \rangle^\sigma \leq H^\sigma$ and hence $g^\sigma \in H^\sigma$; conversely, for $y \in H^\sigma$ the preimage $\langle y \rangle^{\sigma^{-1}} = D$ is cyclic and therefore $y = x^\sigma = x^\sigma$ for some $x \in D \leq H$. Thus $H^\sigma = H^\sigma$. This shows that $\sigma$ is bijective and that $\varphi$ is induced by $\sigma$.

The disadvantage of this theorem is that the map $\sigma$ constructed in its proof does not have any nice properties. It is much more interesting to know, for example, that
a given projectivity is induced by an isomorphism. We present two general results due to Sadovskii that reduce this problem to the corresponding problem for finitely generated groups.

**Sadovskii's approximation theorems**

A family $\mathcal{S}$ of subgroups of a group $G$ is called a local system of subgroups of $G$ if

1. For any $X, Y \in \mathcal{S}$ there exists $Z \in \mathcal{S}$ such that $X \cup Y \leq Z$, and
2. every element of $G$ is contained in some $X \in \mathcal{S}$.

**1.3.6 Theorem** (Sadovskii [1941]). Let $\varphi$ be a projectivity from a group $G$ to a group $\bar{G}$ and let $\mathcal{S}$ be a local system of subgroups of $G$. For every $X \in \mathcal{S}$ let $\varphi_X$ be the projectivity induced by $\varphi$ in $X$, and $A_X$ be the set of all isomorphisms from $X$ to $X^\circ$ that induce $\varphi_X$. If $A_X$ is nonempty and finite for all $X \in \mathcal{S}$, then $\varphi$ is induced by an isomorphism from $G$ to $\bar{G}$.

**Proof.** Recall that a directed set is a partially ordered set in which every pair of elements has an upper bound. By (13), $\mathcal{S}$ is a directed set and $(A_X)_{X \in \mathcal{S}}$ is a family of sets indexed by $\mathcal{S}$. For each pair $(X, Y)$ of elements of $\mathcal{S}$ such that $X \leq Y$, we define a mapping $\pi_{XY}: A_Y \to A_X$ in the following way. Take $a \in A_Y$. Then $a$ induces $\varphi_Y$, so the restriction $a|_X$ of $a$ to $X$ induces $\varphi_X$, and $a|_X \in A_X$; now we can define $\pi_{XY}(a) = a|_X$. Clearly, these mappings satisfy the following conditions:

1. For every $X \in \mathcal{S}$, $\pi_{XX}$ is the identity mapping of $A_X$.
2. If $X \leq Y \leq Z$, then $\pi_{XZ} = \pi_{XY} \pi_{YZ}$.

Since every $A_X$ is nonempty and finite, the inverse limit $A = \lim A_X$ of the family $(A_X)_{X \in \mathcal{S}}$ with respect to the mappings $\pi_{XY}$ is not empty (see Bourbaki [1968], Chapter III, § 7.4). An element of $A$ is an element of the cartesian product of the sets $A_X$, hence a function $f$ defined on $\mathcal{S}$ such that $f(X) \in A_X$ for all $X \in \mathcal{S}$, with the property that

$$f(X) = \pi_{XY}(f(Y)) = f(Y)|_X$$

for $X \leq Y$. We take such an $f$ and define a mapping $\rho: G \to \bar{G}$ in the following way. For $g \in G$ there exists $X \in \mathcal{S}$ such that $g \in X$, and we let $g^\rho = g^{f(X)}$. If in addition $g \in Y \in \mathcal{S}$, then there exists $Z \in \mathcal{S}$ such that $X \cup Y \leq Z$, and hence $g^{f(X)} = g^{f(Z)} = g^{f(Y)}$, by (17). Thus $\rho$ is well defined. For $x, y \in G$ there are $X, Y, Z \in \mathcal{S}$ such that $x \in X$, $y \in Y$ and $X \cup Y \leq Z$. Since $\rho|_{Z} = f(Z)$ is an isomorphism inducing the projectivity $\varphi_Z$, $(xy)^\rho = x^\rho y^\rho$ and $\langle x \rangle^\rho = \langle x \rangle^\circ$. By 1.3.4, $\rho$ is an isomorphism inducing $\varphi$.  

If $H = \langle x_1, \ldots, x_n \rangle$ is a finitely generated group and $\psi$ is a projectivity from $H$ to some group $\bar{H}$, then every isomorphism $\alpha: H \to \bar{H}$ that induces $\psi$ has to map $x_i$ to some generator of $\langle x_i \rangle^\psi$, $i = 1, \ldots, n$. Since $\langle x_i \rangle^\psi$ has only a finite number of
generators and since $\alpha$ is determined by the images of the $x_i$, there are only finitely many isomorphisms inducing $\psi$. So we get the following corollary to Theorem 1.3.6 which usually suffices for the applications.

1.3.7 Corollary. Let $\phi$ be a projectivity from $G$ to $\bar{G}$ and let $\mathcal{S}$ be a local system of finitely generated subgroups of $G$. If $\phi$ is induced by an isomorphism on every $X \in \mathcal{S}$, then $\phi$ is induced by an isomorphism on $G$.

We now prove a result dual to Theorem 1.3.6. Clearly, if $\phi$ is a projectivity from $G$ to $\bar{G}$ and $N \leq G$ such that $N^\phi \leq \bar{G}$, then the map

$$\phi^N: L(G/N) \to L(\bar{G}/N^\phi); H/N \mapsto H^\phi/N^\phi$$

is a projectivity from $G/N$ to $\bar{G}/N^\phi$; we call $\phi^N$ the projectivity induced by $\phi$ in $G/N$.

1.3.8 Theorem (Sadovskii [1965a]). Let $\phi$ be a projectivity from a group $G$ to a group $\bar{G}$ and let $\mathcal{S}$ be a family of normal subgroups of $G$ such that

(18) for any $X, Y \in \mathcal{S}$ with $Z \leq X \cap Y$, and

(19) for every $g \in G$ there exists $X \in \mathcal{S}$ such that $<g> \cap X = 1$.

For every $X \in \mathcal{S}$, suppose that $X^\phi \leq \bar{G}$ and let $A_X$ be the set of all isomorphisms from $G/X$ to $\bar{G}/X^\phi$ that induce the projectivity $\phi^X$. If $A_X$ is nonempty and finite for all $X \in \mathcal{S}$, then $\phi$ is induced by an isomorphism from $G$ to $\bar{G}$.

Proof. Let $X, Y \in \mathcal{S}$ and define $X^\ast = \{g \in G | <g> \cap X = 1\}$. Every $\alpha \in A_X$ induces a map $\alpha^\ast$ from $X^\ast$ to $\bar{G}$. For, if $g \in X^\ast$, then $(gX)^\phi \in <g>^\phi X^\phi / X^\phi$, and since $<g>^\phi \cap X^\phi = 1$, there is a unique $g' \in <g>^\phi$ such that $(gX)^\phi = g'X^\phi$. Now we set $g^\ast = g'$ and define $B_X = \{\alpha^\ast | \alpha \in A_X\}$. If $Y \leq X$ and $\beta \in A_Y$, then the isomorphism $\beta: G/Y \to \bar{G}/Y^\phi$ induces in the natural way an isomorphism $\gamma: G/X \to \bar{G}/X^\phi$. Since $\beta$ induces $\phi$ on $G/Y$, it follows that $\gamma$ induces $\phi$ on $G/X$ and hence $\gamma \in A_X$. Now $Y \leq X$ implies $X^\ast \leq Y^\ast$, and for $g \in X^\ast$, $g^\ast = g^\phi$ is an element of $<g>^\phi$ satisfying $(gX)^\phi = g^\phi X^\phi$. Thus $g^\ast = g^\phi$ and hence $\gamma^\ast = \beta^\ast|_{X^\ast}$.

Let us write $X \leq' Y$ if and only if $Y \leq X$. Then $(\mathcal{S}, \leq')$ is a directed set, by (18), and we have just shown that for $X \leq' Y$ there exists a map $\pi_{XY}: B_Y \to B_X$ defined by $\pi_{XY}(\sigma) = \sigma|_{X^\ast}$ for all $\sigma \in B_Y$. Clearly, these maps have the properties (15) and (16) with respect to $\leq'$, and since every $B_X$ is finite and nonempty, the inverse limit $B = \lim B_X$ with respect to the mappings $\pi_{XY}$ is not empty. An element $f \in B$ has the property that $f(X) \in B_X$ and

$$f(X) = \pi_{XY}(f(Y)) = f(Y)|_{X^\ast}$$

if $X \leq' Y$, i.e. $Y \leq X$. We take such an $f$ and define $\rho: G \to \bar{G}$ in the obvious way: if $g \in G$, then by (19) there exists $X \in \mathcal{S}$ such that $g \in X^\ast$, and we define $g^\rho = g^f(X)$. If also $g \in Y^\ast$, then there exists $Z \in \mathcal{S}$ such that $Z \leq X \cap Y$, and hence $g^f(X) = g^f(Z) = g^f(Y)$, by (20). Thus $\rho$ is well defined. Let $x, y \in G$ and consider the amorphity $a(x, y) = (y^\rho)^{-1}(x^\rho)^{-1}(xy)^\rho \in \bar{G}$. Since $\phi$ is a projectivity, there exists $g \in G$ such that $<g>^\phi = <a(x, y)>$, and our assumptions on $\mathcal{S}$ yield the existence of a subgroup
1.4 The group of autoprojectivities

Let $G$ be a group. A projectivity from $G$ to $G$ is called an autoprojectivity of $G$; the group of all autoprojectivities of $G$, that is of all automorphisms of $L(G)$, is denoted by $P(G)$. Clearly, every automorphism of $G$ induces an autoprojectivity, as does every element $g \in G$ via the inner automorphism induced by $g$. We collect these simple facts in the following theorem and introduce important subgroups of $G$, Aut $G$ and $P(G)$.

**Exercises**

1. Let $a: G \to \widetilde{G}$ be a map, $a$ the amorphism of $a$ and write $A = \langle a(x, y) | x, y \in G \rangle$ and $B = \langle g \rangle | g \in G \rangle$. Show that $A \leq B$ and that the map $\sigma^*$ defined by $x^\sigma = xA$ for all $x \in G$ is an epimorphism from $G$ to $B/A$.

2. (Gaschütz and Schmidt [1981]) Let $G$ be a finite group, $a$ a permutation of $G$ and $\sigma$ the amorphism of $\sigma$. Show that the following are equivalent:
   (a) $(Hx)^\sigma = H^\sigma x^\sigma$ and $(xH)^\sigma = x^\sigma H^\sigma$ for all $H \leq G$ and $x \in G$,
   (b) $a(x, y) \in \langle x^\sigma \rangle \cap \langle y^\sigma \rangle$ for all $x, y \in G$. 

3. Let $\sigma$ be a bijective map from $G$ to $\widetilde{G}$ such that
   (a) $(xy)^{-1} \in \langle x^\sigma, y^\sigma \rangle$ for all $x, y \in G$, and
   (b) $(uv^{-1})^\sigma \in \langle u^\sigma, v^\sigma \rangle$ for all $u, v \in \widetilde{G}$.
   Show that the map $\overline{\sigma}: L(G) \to L(\widetilde{G})$ defined in (2) is a projectivity.

4. (a) If $L_2(G)$ is a sublattice of the finite group $G$, show that $L_2(G) = L(G)$.
   (b) Find a group $G$ such that $L_2(G)$ is a meet-sublattice but not a sublattice of $L(G)$.
   (c) Find a group $G$ for which $L_2(G)$ is not a lattice.

5. If $L_2(G)$ is a distributive lattice, show that $G$ is locally cyclic.

6. If $G$ and $\widetilde{G}$ are lattice isomorphic $p$-groups, $p$ a prime, and $\varphi$ is a projectivity from $G$ to $\widetilde{G}$, show that there exists a bijective map $\sigma: G \to \widetilde{G}$ inducing $\varphi$ such that $(x^\sigma)^\varphi = (x^\varphi)^\sigma$ for all $x \in G$. 

1.4 The group of autoprojectivities

Let $G$ be a group. A projectivity from $G$ to $G$ is called an autoprojectivity of $G$; the group of all autoprojectivities of $G$, that is of all automorphisms of $L(G)$, is denoted by $P(G)$. Clearly, every automorphism of $G$ induces an autoprojectivity, as does every element $g \in G$ via the inner automorphism induced by $g$. We collect these simple facts in the following theorem and introduce important subgroups of $G$, Aut $G$ and $P(G)$.
1.4.1 **Theorem.** Let $G$ be a group.

(a) The map $\rho: \text{Aut } G \to P(G)$ defined by $H^\alpha = H^\alpha$ for $H \leq G$, $\alpha \in \text{Aut } G$ is a homomorphism. The kernel of $\rho$ is the group

$$\text{Pot } G = \{\alpha \in \text{Aut } G | H^\alpha = H \text{ for all } H \leq G\}$$

of power automorphisms of $G$, the image of $\rho$ is the group $PA(G)$ of all autoprojectivities of $G$ that are induced by automorphisms. We have $PA(G) \simeq \text{Aut } G/\text{Pot } G$.

(b) The map $\eta: G \to P(G)$ defined by $H^\gamma = g^{-1}Hg$ for $H \leq G$, $g \in G$ is a homomorphism. The kernel of $\eta$ is the group

$$N(G) = \bigcap_{H \leq G} N_G(H),$$

called the norm of $G$, the image of $\eta$ we denote by $PI(G)$. We have $PI(G) \simeq G/N(G)$.

(c) If $\pi: G \to \text{Aut } G$ is the homomorphism mapping $g \in G$ to the inner automorphism induced by $g$, that is $x^g = g^{-1}xg$ for $x \in G$, then $\eta = \pi \rho$ and $N(G)^\pi = G^\pi \cap \text{Pot } G = \text{Inn } G \cap \text{Pot } G$.

**Proof.** Let $\alpha, \beta \in \text{Aut } G$ and $H \leq G$. Then $\alpha^\beta$ is the projectivity induced by $\alpha$ and $H^{\alpha \beta} = H^{\alpha \beta}$. Hence $\rho$ is a homomorphism. For $g \in G$ we have $H^{\alpha \beta} = g^{-1}Hg = H^\gamma$, and therefore $\eta = \pi \rho$ is the product of two homomorphisms. Thus $\eta$ is also a homomorphism. The remaining assertions are trivial or follow from the isomorphism theorem for groups. \(\square\)

If two isomorphisms $\sigma$ and $\tau$ induce the same projectivity between two groups $G$ and $\bar{G}$, then $\sigma \tau^{-1}$ is a power automorphism of $G$, and conversely. Therefore,

1.4.2 **Corollary.** If a projectivity of a group $G$ is induced by an isomorphism, it is induced by exactly $|\text{Pot } G|$ isomorphisms.
There is a large class of groups in which the homomorphisms $\rho$ and $\eta$ described in Theorem 1.4.1 are injective.

1.4.3 Theorem (Baer [1956], Suzuki [1951a]). If $G$ is a group with $Z(G) = 1$, then also $N(G) = 1$ and $\text{Pot} G = 1$, hence $\text{PI}(G) \simeq G$ and $\text{PA}(G) \simeq \text{Aut} G$.

\text{Proof.} This is an immediate consequence of a more general result on power automorphisms of groups, so we shall postpone the proof until 1.5.2 below. But there is a short proof for finite groups which we want to present here. So let $G$ be finite and suppose first that $N(G) \neq 1$. Then there exists a nontrivial Sylow $p$-subgroup $P$ of $N(G)$. Since $N(G)$ normalizes every subgroup, $P \leq N(G)$ and hence $P \leq G$. So if $S \in \text{Syl}_p(G)$, then $P \leq S$ and $P \cap Z(S) \neq 1$; let $1 \neq a \in P \cap Z(S)$. Then $S \leq C_G(a)$ and for primes $q \neq p$, $P$ normalizes every Sylow $q$-subgroup $Q$ of $G$ and hence $QP = Q \times P$. Therefore also $Q \leq C_G(a)$ and $C_G(a) = G$, contrary to $Z(G) = 1$. Thus $N(G) = 1$ and $\text{PI}(G) \simeq G$, by 1.4.1.

The second assertion now follows from the fact that $C_{\text{Aut} G}(\text{Inn} G) = 1$ if $G$ is a group with trivial centre. Indeed, $\text{Pot} G \cap \text{Inn} G = N(G)^* = 1$, by 1.4.1, and since $\text{Net} G$ and $\text{Inn} G$ are normal subgroups of $\text{Aut} G$, they centralize each other. Therefore, if $a \in \text{Pot} G$ and $x, g \in G$,

$$g^{-1} x^g = x^{g^*} = x^{g^*x} = (g^{-1} x g)^* = (g^*)^{-1} x^g g^*$$

and so $g^* g^{-1}$ centralizes $x^g$. Since $x$ was arbitrary, $g^* g^{-1} \in Z(G) = 1$ and hence $g^* = g$. Thus $\text{Pot} G = 1$ and $\text{PA}(G) \simeq \text{Aut} G$.

In the remainder of this section, we shall study $L(G)$ and $P(G)$ for some well-known groups $G$; in particular we want to determine the subgroups $\text{PA}(G)$ and $\text{PI}(G)$ of $P(G)$. Since every automorphism of a cyclic group is a power automorphism, $\text{PA}(C_n) = 1$ for all $n \in \mathbb{N}$ or $\{\infty\}$. The results of Section 1.2 yield the description of $P(C_n)$ given in Exercises 1 and 2. The next example will explain those parts of our terminology and notation that originated in projective geometry.

\textbf{Elementary abelian groups}

Let $p$ be a prime, $n$ a natural number and let $G$ be an elementary abelian group of order $p^n$. Then it is well-known that we can regard $G$ as a vector space of dimension $n$ over $GF(p)$, the field with $p$ elements, and that $L(G)$ is the projective geometry of this vector space. An automorphism of the group $G$ is an invertible linear map of the vector space $G$ onto $G$, and an autoprojectivity of $G$ is simply a projectivity of the projective geometry $L(G)$ onto itself in the sense of projective geometry. It follows that $\text{PA}(G) \simeq PGL(n, p)$. If $n = 2$, then every nontrivial, proper subgroup of $G$ has order $p$ and hence $L(G) \setminus \{G, 1\}$ is an antichain with $p + 1$ elements. Every permutation of these elements yields an autoprojectivity of $G$, and therefore $P(G)$ is isomorphic to the symmetric group $S_{p+1}$ on $p + 1$ letters. If $n \geq 3$, the Fundamental Theorem of Projective Geometry (see, for example, Baer [1952], p. 44) tells us that every
Fundamental concepts

autoprojectivity of $G$ is induced by a semi-linear mapping of the vector space $G$. But since $GF(p)$ has only the trivial automorphism, this mapping is linear, i.e. an automorphism. Thus we have the following result.

1.4.4 Theorem. Let $G$ be an elementary abelian group of order $p^n$, $p$ a prime, $n \in \mathbb{N}$. Then $PA(G) \simeq PGL(n, p)$, and $P(G) = PA(G)$ for $n \geq 3$, but $P(G) \simeq S_{p+1}$ if $n = 2$.

In Section 2.6 we shall show, without using the Fundamental Theorem of Projective Geometry, that for a much larger class of abelian groups all autoprojectivities are induced by automorphisms.

Groups of order $pq$

Let $p$ and $q$ be primes such that $q \mid p - 1$ and let $H$ be a nonabelian group of order $pq$. Then by Sylow’s theorem there are $p$ subgroups of order $q$ and one subgroup of order $p$ in $H$ and so $L(H)$ consists of $H$, 1 and an antichain with $p + 1$ elements. Therefore, again, $P(H) \simeq S_{p+1}$ whereas $PA(H) \simeq \text{Aut } H$ and $PI(H) \simeq H$, by 1.4.3. Thus $PA(H)$ and $PI(H)$ are subgroups of orders $p(p - 1)$ and $pq$, respectively, in $S_{p+1}$.

This shows that in general $PA(G)$ and $PI(G)$ are not distinguished subgroups of $P(G)$; in fact they are not even normal in $P(G)$. However, this is not very surprising if, as is the case here, the subgroup lattice is structurally small, in particular if it does not determine the group. The situation is different in our next example.

The alternating group $A_4$

Let $G$ be the alternating group of degree 4. Then $G$ has 3 subgroups of order 2, generating the Klein 4-group $V$, and 4 maximal subgroups of order 3. It is easy to see that $G$ is determined by its subgroup lattice. Indeed let $\overline{G}$ be a group with isomorphic subgroup lattice; then $\overline{G}$ operates faithfully by conjugation on the set $\Gamma$ of those atoms of this lattice which are also antiatoms. Hence $\overline{G}$ is a subgroup of $S_4$ and it follows that $\overline{G} \simeq G$. Let $\Delta$ be the set of those atoms of $L(G)$ that are not antiatoms, and let $S$, $T$ be the kernels of the actions of $P(G)$ on $\Gamma$, $\Delta$, respectively.

![Figure 4: $L(A_4)$](image-url)
Clearly,

\[ P(G) = S \times T \cong S_3 \times S_4. \]

By 1.4.3, \( PA(G) \cong \text{Aut } G \). An automorphism \( \alpha \) of \( G \) fixing all \( H \in \Gamma \) operates on each of these groups in the same way as on \( G/V \). Hence \( \alpha \) either centralizes or inverts all \( H \in \Gamma \); and since one can easily check that the latter is impossible, \( \alpha = 1 \). Thus \( PA(G) \cap S = 1 \) and \( PA(G) \) is isomorphic to a subgroup of \( T \cong S_4 \). On the other hand, \( S_4 \) operates faithfully by conjugation on its normal subgroup \( A_4 \) and induces an \( S_3 \) on \( V \). It follows that \( PA(G) \cong S_4 \) and \( PA(G)S = P(G) = PA(G)T \). An element of \( S \) normalizing \( PA(G) \) would centralize \( PA(G) \) and therefore also \( PA(G)T = P(G) \); but \( Z(S) = 1 \). Thus \( N_{P(G)}(PA(G)) = PA(G) \) and \( PA(G) \) is one of 6 conjugate subgroups of \( P(G) \).

**Dihedral 2-groups**

The results obtained so far show an obvious general phenomenon. The more structure the subgroup lattice of a group has, the more likely it is that it determines group-theoretic invariants. Compare, for example, the situation for \( A_4 \) and \( S_4 \) (see Exercise 3) or the cases \( n = 2 \) and \( n \geq 3 \) in 1.4.4. The dihedral 2-groups are an exception to this rule.

Let \( n \geq 3 \) and let \( G = D_2^n = \langle x, y | x^{2^n-1} = y^2 = 1, yxy = x^{-1} \rangle \) be the dihedral group of order \( 2^n \). Since \( (x^i y)^2 = x^i x^{-i} = 1 \) for all \( i \in \mathbb{N} \), every element in \( G \setminus \langle x \rangle \) is an involution; in particular, \( \langle x \rangle \) is the only cyclic maximal subgroup of \( G \). It follows that \( \langle x \rangle \) is invariant under \( P(G) \) and that \( P(G) \) operates faithfully on the set \( \Lambda \) of subgroups of order 2 not contained in \( \langle x \rangle \). Every power automorphism has to centralize all these involutions and therefore \( P(G) = 1 \) and \( PA(G) \cong \text{Aut } G \). If \( n = 3 \), it is easily seen that

\[ P(D_8) = PA(D_8) \cong \text{Aut } D_8 \cong D_8. \]
For $n \geq 4$ there are exactly three maximal subgroups in $G$, namely $\langle x \rangle$ and two subgroups, $M_1$ and $M_2$, say, isomorphic to $D_{2n-1}$. Since $M_1 \cap M_2 = \langle x^2 \rangle$, $P(G)$ contains a subgroup isomorphic to $P(M_1) \times P(M_2)$, and because there are even automorphisms of $G$ interchanging $M_1$ and $M_2$, $|P(D_n)| = 2|P(D_{2n-1})|^2$. By an obvious induction we get $|P(D_n)| = 2^{2n-1-1}$ for all $n \geq 4$. Since this is the highest power of 2 dividing $(2^n-1)!$ and $|\Lambda| = 2^{n-1}$, $P(D_n)$ is isomorphic to a Sylow 2-subgroup of the symmetric group $S_{2n-1}$. Every automorphism of $G$ is determined by the images of $y$ and $xy$, and for these there are $2^{n-1}$ and $2^{n-2}$ involutions respectively available. Thus $|\text{Aut } G| = 2^{2n-3}$ so that $P(\text{Aut } D_n)$ is properly contained in $P(D_n)$ for all $n \geq 4$.

**Quaternion groups**

Let $n \geq 3$ and let $G = Q_{2^n} = \langle x, y | x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, y^{-1}xy = x^{-1} \rangle$ be the generalized quaternion group of order $2^n$. Then $Z(G)$ is the only minimal subgroup of $G$ and $G/Z(G) \cong D_{2n-1}$. Thus $P(Q_{2^n}) \cong P(D_{2n-1})$, and since every automorphism of $G/Z(G)$ can be lifted to an automorphism of $G$,

$$P(\text{Aut } G) \cong P(D_{2n-1}) \cong \text{Aut } D_{2n-1}.$$  

![Figure 6: L(Q16)](image)

In particular, $P(Q_8) = P(\text{Aut } Q_8) \cong \text{Sym } P$, $P(Q_{16}) = P(\text{Aut } Q_{16}) \cong D_8$ and $P(\text{Aut } Q_{2^n}) < P(Q_{2^n})$ for $n \geq 5$. For every homomorphism $\sigma: G \to Z(G)$, the map $x: G \to G$ defined by $g^x = gg^\sigma$ for $g \in G$ is a power automorphism of $G$. It follows that $|\text{Pot } G| \geq 4$, and since $G$ is generated by two elements of order 4, $|\text{Pot } G| = 4$.

Finally, we mention that because the quaternion groups are the only noncyclic finite groups with just one minimal subgroup, they are determined by their subgroup lattices. We leave it as an exercise to show that this also holds for the dihedral 2-groups.

**Exercises**

1. Show that $P(C_\infty) \cong \text{Sym } \mathbb{P}$.
2. Let $m \in \mathbb{N}$ and for $i \in \mathbb{N}$ define $n_i$ to be the number of primes $p$ such that $p^i$ is the maximal power of $p$ dividing $m$. Show that $P(C_m) \cong \text{Dr } S_{n_i}$ (where of course, $S_0$ is the trivial group).
3. Draw a Hasse diagram of $L(S_4)$ and show that $P(S_4) = PA(S_4) \cong S_4$.
4. Give details for those parts in the discussion of the dihedral and quaternion groups that have only been sketched in the text.
5. Show that $D_{2^n}$ is determined by its subgroup lattice for $n \geq 2$.
6. Let $p$ be an odd prime and let $G$ be the nonabelian group of order $p^3$ and exponent $p$. Determine $P(G)$, $PA(G)$ and $Pot G$.

1.5 Power automorphisms

In this section we shall prove Cooper's theorem that every power automorphism of a group is central. This will have a number of interesting consequences. First we give an elementary result.

1.5.1 Theorem. Let $G$ be a group. Then $Pot G$ is abelian.

Proof. For $g \in G$ let $F(g) = \{x \in Pot G | gx^a = g\}$. Then $F(g) \trianglelefteq Pot G$ and $Pot G/F(g)$, being isomorphic to a subgroup of $Aut\langle g \rangle$, is abelian. Since $\bigcap_{g \in G} F(g) = 1$, $Pot G$ is abelian.

Commutators

For elements $x, y \in G$ and $\alpha \in Aut G$, $[x, y] = x^{-1}y^{-1}xy = x^{-1}x^\alpha$ is the commutator of $x$ and $y$ and, similarly, $[x, \alpha] = x^{-1}x^\alpha$ is the commutator of $x$ and $\alpha$. Then if $X \subseteq G$ and $S$ is a subset of $G$ or $Aut G$, $[X, S] = \langle [x, s] | x \in X, s \in S \rangle$. Finally, for elements $x \in G$ and $s_1, \ldots, s_n$ of $G$ or $Aut G$ we define inductively

$$[x, s_1, \ldots, s_n] = [[x, s_1, \ldots, s_{n-1}], s_n] \quad \text{for } n \geq 2;$$

for subsets $X$ of $G$ and $S_1, \ldots, S_n$ of $G$ or $Aut G$ we define $[X, S_1, \ldots, S_n]$ similarly. For the convenience of the reader we list the basic properties of commutators which we shall require. So let $x, y \in G$, $s$ and $t$ elements of $G$ or $Aut G$, $X, Y, Z$ subgroups of $G$, $S$ a subset of $G$ or $Aut G$ and let $n \in \mathbb{N}$, $m \in \mathbb{Z}$. Then

1. $[xy, s] = [x, s]^s[y, s]$ and $[x, st] = [x, t][x, s]^t$,
2. $[x^n, s] = [x, s]^n$ if $[x, s]$ and $x$ commute,
3. $[x, s^m] = [x, s]^m$ if $[x, s]^a = [x, s]$,
4. $(xy)^s = x^s y^s [y, x]^s$ if $[x, y]$ commutes with $x$ and $y$,
5. $[x, y]^a = [x^a, y^a]$ for every homomorphism $\sigma$ of $G$,
6. $[X, S]^X = [X, S]$ and $[X, Y] \trianglelefteq X \cup Y$,

The proofs of these results for $s, t \in G$ and $S \subseteq G$ can be found in Robinson [1982], Chapter 5; for $s, t \in \text{Aut } G$ and $S \subseteq \text{Aut } G$, they are similar.

### Cooper's theorem

15.2 Theorem (Cooper [1968]). Let $G$ be a group. Then $[G, \text{Pot } G] \leq Z(G)$.

This result has a number of immediate consequences. First of all, we get the

**Proof of Theorem 1.4.3.** If $G$ is a group with $Z(G) = 1$, then $[G, \text{Pot } G] = 1$ and thus $\text{Pot } G = 1$. Hence also $N(G) = 1$, by 1.4.1, (c). Then 1.4.1, (a) and (b) show that $\text{PA}(G) \simeq \text{Aut } G$ and $\text{PI}(G) \simeq G$. □

Furthermore, we can show that power automorphisms centralize not only $G/Z(G)$ but also the commutator subgroup $G'$ of $G$. In addition they commute with the inner automorphisms. Finally, we get a result of Schenkman's [1960] that the norm of a group $G$ is contained in the second centre $Z_2(G)$.

15.3 Corollary. If $G$ is a group, then

(a) $[G', \text{Pot } G] = 1$,

(b) $[\text{Inn } G, \text{Pot } G] = 1$,

(c) $N(G) \leq Z_2(G)$.

**Proof.** Let $g, x \in G$ and $\alpha \in \text{Pot } G$. By 1.5.2 there exist elements $z, w \in Z(G)$ such that $g^z = gz$ and $x^z = xw$. Hence $[g, x]^z = [g^z, x^z] = [gz, xw] = [g, x]$ and this implies (a). As in 1.4.1 let $\pi$ be the natural homomorphism from $G$ to $\text{Aut } G$. Then

$$x^\alpha = (g^{-1}xg)^\alpha = (g^\alpha)^{-1}x^\alpha g^\alpha = z^{-1}g^{-1}x^\alpha g z = x^{\alpha g},$$

and (b) follows. Finally, if $g \in N(G)$, then $g^x \in \text{Pot } G$ and hence $[x, g] = [x, g^x] \in Z(G)$, by 1.5.2. Thus $g \in Z_2(G)$ and (c) holds. □

**Proof of Theorem 1.5.2.** Let $x, y \in G$ and $\alpha \in \text{Pot } G$. We have to show that $[x, \alpha, y] = 1$. Since $x^\alpha \in \langle x \rangle$, the elements $x^\alpha$ and $[x, \alpha]$ commute with $x$. By (2),

(8) $[x^m, \alpha] = [x, \alpha]^m$ for all $m \in \mathbb{Z}$.

If $H \leq G$, then $H^x = (H^x)^y = (H^x)^\alpha = H^{\alpha}$ and hence $[x, \alpha] = x^{-1}x^\alpha = x^\alpha x^{-1} \in N_G(H)$. Thus

(9) $[x, \alpha] \in N(G)$.

Since $x^\alpha y^\alpha = (xy)^\alpha$ commutes with $xy$, we have $[x, \alpha, y][y^{-1}, \alpha, x^{-1}] = x^{-1}xy^{-1}x^{-1}x^\alpha y^\alpha y^{-1}xy y^{-1}x^{-1} = x^{-1}x^{-1}x^{-1}x^\alpha y^\alpha y^{-1}xy - x^{-1}x^{-1} = 1$. By (9), $[x, \alpha, y] \in \langle y \rangle$ and $[y^{-1}, \alpha, x^{-1}] \in \langle x \rangle$ and hence

(10) $[x, \alpha, y] \in \langle x \rangle \cap \langle y \rangle$. 

1.5 Power automorphisms

In particular, \([x, \alpha, y]\) commutes with \([x, \alpha]\) and \(y\). Therefore the commutator formulas (8), (2) and (3) yield

\[
(11) \quad [x^m, \alpha, y^n] = [[x, \alpha]^m, y^n] = [x, \alpha, y]^mn \text{ for all } m, n \in \mathbb{Z}.
\]

This implies \([y^{-1}, \alpha, x^{-1}] = [y, \alpha, x]\) and so we finally get

\[
(12) \quad [x, \alpha, y][y, \alpha, x] = 1.
\]

Let \(x^r = x^r, y^s = y^s\) and \((y^x)^t = (y^s)^t\) where \(r, s, t \in \mathbb{Z}\). Then \((y^t)^x = (y^s)^t = (y^x)^s = (y^x)^{s^x}\) and hence \(y^s = (y^t)^{s^{x^t}}\) and \(y^r = (y^t)^{r^{x^t}}\). It follows that \(y^{s^2} = (y^s)^{s^2} = ((y^t)^{s^{x^t}})^{s^{x^t}} = ((y^t)^{s^{x^{x^t}}})^{s^{x^{x^t}}} = (y^{s^{x^t}})^{s^{x^{x^t}}} = (y^{s^{x^{x^t}}})^{s^{x^{x^t}}} = y^{s^{x^{x^t}}} \) and this yields \(1 = [x^{r-1}, y^{s^2}] = [[x, \alpha]^{-1}, y^{s^2}]\). Using (11), we get

\[
(13) \quad [x, \alpha, y]^{(r-1)s^2} = 1.
\]

Now suppose that the theorem is false. Then there exist elements \(x, y \in G\) and \(\alpha \in \text{Pot } G\) such that \([x, \alpha, y] \neq 1\). If \(x\) or \(y\) had infinite order, then so would \([x, \alpha, y]\), by (10), and (13) would imply that \(r = 1\). But then \([x, \alpha] = x^{-1} = 1\) and \([x, \alpha, y] = 1\), a contradiction. So \(x\) and \(y\) have finite order and we can choose \(x, y \in G\) with \([x, \alpha, y] \neq 1\) such that \(o(x) + o(y)\) is minimal. By (12), also \([y, \alpha, x] \neq 1\) and so without loss of generality we may assume that \(o([x, \alpha]) \geq o([y, \alpha])\). If \(p\) is a prime divisor of \(o(x)\) or \(o(y)\), then by our choice of \(x\) and \(y\), \([x^p, \alpha, y] = 1\) or \([x, \alpha, y^p] = 1\); in both cases \([x, \alpha, y]^p = 1\), by (11). Hence \(o(x)\) and \(o(y)\) are powers of the same prime \(p\) and

\[
(14) \quad [x, \alpha, y]^p = 1.
\]

Again let \(r, s \in \mathbb{Z}\) such that \(x^r = x^r\) and \(y^s = y^s\). Since \(\alpha\) is an automorphism, \(s \neq 0\) (mod \(p\)). So from (13) we get \([x, \alpha, y]^{r-1} = 1\) and then (12) and (11) yield

\[
1 = [y, \alpha, x]^{r-1} = [y, \alpha, x^{-1}] = [[[y, \alpha], [x, \alpha]]].
\]

Thus \(A = \langle [x, \alpha], [y, \alpha] \rangle\) is an abelian \(p\)-group and \([x, \alpha]\) is an element of maximal order in \(A\). Such an element generates a direct factor (see, for example, the more general Lemma 2.3.11), that is we have \(A = \langle [x, \alpha] \rangle \times B\) where \(B \leq A\). Now \([y, \alpha] \in A\) and so there exist \(b \in B\) and \(n \in \mathbb{Z}\) such that \([y, \alpha] = [x, \alpha]^{-nb}\). Thus

\[
(15) \quad \langle [x, \alpha] \rangle \cap \langle [x, \alpha]^n[y, \alpha] \rangle = 1.
\]

Since \(\langle [x, \alpha, y] \rangle\) is a minimal and \(\langle [x, \alpha] \rangle\) a nontrivial subgroup of the cyclic \(p\)-group \(\langle x \rangle\), we have \([x, \alpha, y] \in \langle [x, \alpha] \rangle\). Hence there exists \(j \in \mathbb{Z}\) such that \([x, \alpha, y] = [x, \alpha]^j\); let \(m = n(1 - j)\). Then by (1),

\[
[x^m, \alpha, y] = [x^{-n/j}x^ny, \alpha] = [x^{-n/j}, \alpha]^xy[x^ny, \alpha]
\]

\[
= ([x, \alpha]^{-n/j})^xy[x^ny, \alpha] \quad \text{(by (8) and (1))}
\]

\[
= [x, \alpha, y]^{-n}[x^ny, \alpha] [x^ny, \alpha, y][y, \alpha] \quad \text{(since \([x, \alpha, y] \in Z(\langle x, y \rangle)\))}
\]

\[
= [x, \alpha]^n[y, \alpha] \quad \text{(by (8) and (11))}.
\]
Now if \([x^m y, x] \neq 1\), then \(\langle [x, x] \rangle\) and \(\langle [x^m y, x] \rangle\) are nontrivial \(p\)-subgroups of \(\langle x \rangle\) and \(\langle x^m y \rangle\), respectively, and they have trivial intersection by (15). Since \(\langle x \rangle\) is a cyclic \(p\)-group and therefore contains only one minimal subgroup, it follows that \(\langle x \rangle \cap \langle x^m y \rangle = 1\). By (10), \([x, x, x^m y] = 1\) in this case; but if \([x^m y, x] = 1\), then clearly \([x^m y, x, x] = 1\) and so \([x, x, x^m y] = 1\), by (12). Hence in any case \([x, x, x^m y] = 1\), and (1) implies that \(1 = [x, x, x^m y] = [x, x, y][x, x, x^m] = [x, x, y]\), a contradiction.

### Power automorphisms of abelian groups

Cooper's theorem does not say anything about abelian groups. However, it is not difficult to determine all power automorphisms of these groups. We call a power automorphism \(\alpha\) of \(G\) universal if there exists an integer \(n\) such that \(x^n = x^m\) for all \(x \in G\). We first remark that every power automorphism of a finitely generated abelian group is universal. More generally we show the following.

**1.5.4 Lemma.** Let \(A\) be a finitely generated abelian group with \(A = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle\). If an automorphism \(\alpha\) of \(A\) fixes \(\langle a_1 \rangle, \ldots, \langle a_r \rangle\) and \(\langle a_1, \ldots, a_r \rangle\), then there exists an integer \(n\) such that \(\alpha^n = \alpha^n\) for all \(a \in A\).

**Proof.** By hypothesis there exist integers \(n, n_i\) such that \(a_i^n = a_i^n\) and

\[
a_i^n \cdots a_r^n = (a_1 \cdots a_r)^n = (a_1 \cdots a_r)^n = a_1^n \cdots a_r^n.
\]

It follows that \(a_i^n = a_i^n\) for \(i = 1, \ldots, r\) and then \(\alpha^n = \alpha^n\) for all \(a \in A\).

An abelian torsion group \(A\) is the direct product of its primary components \(A_p\) and therefore \(\text{Pot} A\) is the cartesian product of the groups \(\text{Pot} A_p\) where \(p\) runs through \(\mathbb{P}\). So let \(A\) be an abelian \(p\)-group and let \(\alpha \in \text{Pot} A\).

Consider first the case \(\text{Exp} A = p^k\), and take an \(x \in A\) with \(o(x) = p^k\). Then \(\alpha\) induces an automorphism in \(\langle x \rangle\) and so there is an integer \(n\) such that \(0 < n < p^k\), \((n, p) = 1\) and \(x^n = x^m\). For every \(a \in A\), \(\alpha\) induces a power automorphism in \(\langle x, a \rangle\) and by 1.5.4 there exists an integer \(m\) such that \(\alpha^m = \alpha^m\) and \(x^n = x^n\). It follows that \(m \equiv n (\text{mod} p^k)\) and \(\alpha^n = \alpha^n\). Hence \(\alpha\) is universal and \(\text{Pot} A \simeq \text{Aut} \langle x \rangle\).

Now suppose that \(\text{Exp} A\) is infinite and consider \(\Omega_k(A) = \{a \in A | a^{p^k} = 1\}\) for \(k \in \mathbb{N}\). Then \(\alpha\) is universal on \(\Omega_k(A)\), so there exist integers \(n_k\) such that \(0 < n_k < p^k\) and \(a^n = a^n\) for all \(a \in \Omega_k(A)\). Since \(\Omega_k(A) \leq \Omega_{k+1}(A)\), we have \(a^{n_k} = a^n = a^{n_{k+1}}\) and therefore \(n_k \equiv n_{k+1} (\text{mod} p^k)\). Hence there exist unique integers \(r_i\) such that \(0 < r_0 < p\), \(0 < r_i < p\) for \(i \in \mathbb{N}\) and \(n_k = \sum_{i=0}^{k-1} r_i p^i\); thus \(\alpha\) determines a \(p\)-adic unit \(r = \sum_{i=0}^{\infty} r_i p^i\). Conversely, such a \(p\)-adic unit yields a power automorphism of \(A\).

**1.5.5 Lemma.** Let \(A\) be an abelian \(p\)-group and let \(r\) be a \(p\)-adic unit, \(r = \sum_{i=0}^{\infty} r_i p^i\), say, where \(r_i \in \mathbb{Z}, 0 < r_0 < p\) and \(0 \leq r_i < p\) for \(i \in \mathbb{N}\). For \(a \in A\) with \(o(a) = p^k (k \in \mathbb{N})\) we
1.5 Power automorphisms

Define \( a^\sigma = a^{n_k} \) where \( n_k = \sum_{i=0}^{k-1} r_i p^i \). Then \( \sigma \) is a power automorphism of \( A \); we shall write \( a^\sigma \) for \( a^\sigma \).

**Proof.** First of all, \( a^\sigma \) is well-defined since the \( r_i \) are uniquely determined by \( r \). Furthermore \( n_j \equiv n_k \pmod{p^j} \) for \( j \leq k \) and therefore \( a^\sigma = a^{n_k} \) for all \( a \in \Omega_k(A) \). Thus \( \sigma \) induces a power automorphism on every \( \Omega_k(A) \). It follows that \( \sigma \) is a power automorphism of \( A \).

Now if \( \exp A \) is infinite, the correspondence between power automorphisms and \( p \)-adic units described above clearly is bijective and multiplicative. Thus we have the following result.

**1.5.6 Theorem** (Robinson [1964]). Let \( A \) be an abelian torsion group and for \( p \in P \) let \( A_p \) be its \( p \)-component.

(a) \( \text{Pot } A \cong \prod_{p \in P} \text{Pot } A_p \).

(b) If \( \exp A_p \) is infinite, then \( \text{Pot } A_p \cong U_p \), the multiplicative group of \( p \)-adic units; in fact, the map sending \( r \in U_p \) to the power automorphism \( \sigma \) defined in 1.5.5 is an isomorphism.

(c) If \( \exp A_p = p^k \) is finite, then every power automorphism of \( A_p \) is universal and \( \text{Pot } A_p \cong \text{Aut } C_{p^k} \), the multiplicative group of units of the ring \( \mathbb{Z}/p^k\mathbb{Z} \) (or of \( p \)-adic units modulo \( p^k \)).

For nonperiodic abelian groups the situation is much simpler.

**1.5.7 Theorem.** If \( A \) is an abelian group with elements of infinite order, then \( |\text{Pot } A| = 2 \) and \( a^\sigma = a^{-1} \) for \( 1 \neq a \in \text{Pot } A \) and all \( a \in A \).

**Proof.** Suppose that \( \alpha \in \text{Pot } A \) and let \( x \in A \) with \( o(x) = \infty \). Since \( \alpha \) induces an automorphism in \( \langle x \rangle \), we have \( x^\alpha = x^n \) where \( n \in \{ +1, -1 \} \). If \( a \in A \), then \( \alpha \) induces a power automorphism in \( \langle x, a \rangle \) which is universal, by 1.5.4. Thus \( a^\alpha = a^n \) for all \( a \in A \). The result follows.

**Power automorphisms of nonabelian groups**

Here we only need the following result; it is an immediate consequence of Cooper's theorem.

**1.5.8 Theorem.** If \( G \) is a nonabelian group generated by elements of infinite order, then \( \text{Pot } G = 1 \).

**Proof.** Suppose that \( 1 \neq \alpha \in \text{Pot } G \). Since \( G \) is generated by elements of infinite order, there exists \( x \in G \) such that \( o(x) = \infty \) and \( x^\alpha \neq x \), and hence \( x^\alpha = x^{-1} \). By 1.5.2, \( x^{-2} = [x, \alpha] \in Z(G) \). Therefore, if \( g \in G \), \( \langle x^2, g \rangle \) is abelian and by 1.5.4, \( \alpha \) induces a
universal power automorphism in this group. Thus \( g^a = g^{-1} \) for all \( g \in G \). But this implies that \( G \) is abelian, a contradiction.

There are also nonabelian groups possessing nontrivial power automorphisms. Universal power automorphisms exist in metacyclic groups (see Exercise 1) and, more generally, in certain groups with modular subgroup lattices (see 2.3.10). Examples of nonuniversal power automorphisms can be found in the quaternion groups and in the groups of Exercise 2.

**Exercises**

1. If \( G = \langle a, b \mid a^p = b^p^{-1} = 1, b^{-1}ab = a^{1+p} \rangle \) where \( p \in \mathbb{P} \), \( p > 2 \) and \( n \geq 2 \), show that \( \alpha : G \to G \) defined by \( x^\alpha = x^{1+p^{n-1}} \) for \( x \in G \) is an automorphism of \( G \).

2. Let \( G \) be a finite \( p \)-group and let \( 1 < K \leq H < G \) such that \( K \leq \langle x \rangle \) for all \( x \in G \setminus H \).
   (a) If \( \sigma : G \to K \) is a homomorphism with \( H \leq \ker \sigma \), show that \( \alpha : G \to G \) defined by \( x^\alpha = xx^\sigma \) for \( x \in G \) is a power automorphism of \( G \).
   (b) If all elements in \( G \setminus H \) have the same order and if \( |G : H| \geq p^2 \), show that there exist power automorphisms of \( G \) that are not universal. (Groups with these properties can be found in Huppert [1967], p. 334.)

3. (Baer [1934]) If \( N(G) \) contains an element of infinite order, show that \( N(G) = Z(G) \).

4. (Cooper [1968]) Let \( G \) be a nonabelian group with elements of infinite order and define \( W(G) = \langle x \in G \mid o(x) = \infty \rangle \). Show that every power automorphism of \( G \) centralizes \( W(G) \) and \( G/W(G) \).

5. (Huppert [1961]) If \( G \) is a nonabelian finite \( p \)-group, show that \( Pot G \) is a \( p \)-group.

**1.6 Direct products**

In this section we shall study the subgroup lattice of a direct product of groups; we also investigate the structure of a group whose subgroup lattice decomposes into a direct product.

**The subgroup lattice of the direct product of two groups**

If \( G = H \times K \), then in general \( L(G) \neq L(H) \times L(K) \); see \( G = C_p \times C_p \) for \( p \in \mathbb{P} \). However, it is possible to construct \( L(G) \) out of \( L(H) \), \( L(K) \) and all isomorphisms between sections of \( H \) and \( K \). This was discovered by Goursat as early as 1890.
1.6 Direct products

1.6.1 Theorem. Let \( H, K \leq G \) and \( G = H \times K \).

(a) For \( U \leq G \) and \( x \in UK \cap H \) define \( x^a = \{y \in K | xy \in U\} \). Then \( \alpha \) is an epimorphism from \( UK \cap H \) onto \( UH \cap K / U \cap K \) with kernel \( U \cap H \).

(b) Conversely, if \( U_1 \leq H, W \leq U_2 \leq K \) and \( \alpha \) is an epimorphism from \( U_1 \) onto \( U_2/W \), then

\[
U = D(U_1, \alpha) = \{xy | x \in U_1, y \in x^a\}
\]

is a subgroup of \( G \) with \( U_1 = UK \cap H, U_2 = UH \cap K, W = U \cap K \) and \( \text{Ker} \alpha = U \cap H \).

(c) For \( U_1, V_1 \leq H \) and epimorphisms \( \alpha, \beta \) as in (b), we have \( D(U_1, \alpha) \leq D(V_1, \beta) \) if and only if \( U_1 \leq V_1 \) and \( x^a \leq x^b \) for all \( x \in U_1 \).

Proof. (a) Let \( U_1 = \{x \in H | xy \in U \text{ for some } y \in K\} \) be the set of \( H \)-components of elements of \( U \). If \( x \in U_1 \) and \( y \in K \) such that \( xy \in U \), then \( x = (xy)y^{-1} \in UK \cap H \); conversely, if \( x \in UK \cap H, x = uk \) with \( u \in U \) and \( k \in K \), say, then \( u = xk^{-1} \) and hence \( x \in U_1 \). Thus \( U_1 = UK \cap H \) and, similarly, \( UH \cap K = U_2 \) is the set of \( K \)-components of elements of \( U \). For \( x \in UK \cap H \), therefore, \( x^a \) is a nonempty subset of \( UH \cap K \). Furthermore, if \( y, z \in x^a \), then \( xy \) and \( xz \) are elements of \( U \) and so \( y^{-1}z = (xy)^{-1}xz \in U \cap K \). Hence \( y \) and \( z \) lie in the same coset of \( U \cap K \), and if \( w \) is another element of this coset \( y(U \cap K) \), then \( w = yu \) with \( u \in U \cap K \) implies \( xw = xyu \in U \), that is \( w \in x^a \). Thus we have shown that \( x^a \in U_2/U \cap K \). For \( x_1, x_2 \in U_1 \) and \( y_1, y_2 \in x^a \) we have \( x_1x_2y_1y_2 = x_1y_1x_2y_2 \in U \) and hence \( y_1y_2 \in (x_1x_2)^a \). Therefore \( y_1y_2 \in (x_1x_2)^a \) and \( \alpha \) is an epimorphism. Finally, \( x \in \text{Ker} \alpha \) if and only if \( x^a = U \cap K \), i.e. \( 1 \in x^a \). It follows that \( \text{Ker} \alpha = U \cap H \).

(b) If \( x_1, x_2 \in U_1 \) and \( y_1, y_2 \in x^a \), then \( y_1y_2^{-1} \in x^a(x_2^a)^{-1} = (x_1x_2^{-1})^a \) and hence \( (x_1y_1)(x_2y_2)^{-1} = x_1x_2^{-1}y_1y_2^{-1} \in U \). Therefore \( U \) is a subgroup of \( G \) and \( U_1 \) is its set of \( H \)-components. Thus \( U_1 = UK \cap H \) and \( \alpha \) is the epimorphism defined in (a) for the subgroup \( U \) of \( G \). The other assertions in (b) now follow from (a).

(c) If \( U = D(U_1, \alpha) \leq D(V_1, \beta) = V \), then \( U_1 = UK \cap H \leq VK \cap H = V_1 \) and \( x^a \leq x^b \) for all \( x \in U_1 \). The converse is obvious.

The isomorphism theorem yields \( U_1/U \cap H \simeq U_2/U \cap K \) in 1.6.1 (b). Therefore we are interested in direct products of isomorphic groups. These are characterized by the existence of diagonals. Here, a subgroup \( D \) of \( G = H \times K \) such that \( DH = G = DK \) and \( D \cap H = 1 = D \cap K \) is called a diagonal in \( G \) (with respect to \( H \) and \( K \)).

1.6.2 Theorem. Let \( H, K \leq G \) and \( G = H \times K \). If \( \delta: H \to K \) is an isomorphism, then

\[
D(\delta) = D(H, \delta) = \{xx^\delta | x \in H\}
\]

is a diagonal in \( G \) (with respect to \( H \) and \( K \)). Conversely, if \( D \) is a diagonal in \( G \) (with respect to \( H \) and \( K \)), then there exists a unique isomorphism \( \delta: H \to K \) such that \( D = D(\delta) \). Thus there is a bijection between diagonals (with respect to \( H \) and \( K \)) and isomorphisms of \( H \) to \( K \), and also, if \( H \cong K \), between diagonals and automorphisms of \( H \).
Proof. If \( \delta : H \to K \) is an isomorphism and \( U = D(H, \delta) \), then it follows from 1.6.1 (b) that \( U \cap H = 1 = U \cap K, H = U_1 \leq UK \) and \( K = U_2 \leq UH. \) Thus \( UK = G = UH \) and \( U \) is a diagonal in \( G. \) Conversely, let \( D \) be a diagonal in \( G \) and consider the epimorphism \( \alpha \) defined for \( D \) in 1.6.1 (a). Then \( \alpha \) maps \( DK \cap H = H \) onto \( DH \cap K/D \cap K = K \) and \( \text{Ker} \alpha = D \cap H = 1. \) Thus \( \alpha \) is an isomorphism from \( H \) to \( K \) and \( D = D(H, \alpha) = D(\alpha). \) Finally, 1.6.1 (c) implies that different isomorphisms \( \delta, \epsilon \) lead to different diagonals \( D(\delta) \) and \( D(\epsilon) \) so that the correspondence \( \delta \to D(\delta) \) is bijective.

1.6.3 Remark. Every subgroup \( U \) of a direct product \( G = H \times K \) is a diagonal in a certain section of \( G. \) More precisely, if \( U = D(U_1, \alpha), U_2 = UH \cap K \) and \( U_0 = (U \cap H) \times (U \cap K), \) then \( U_0 \leq U_1 \times U_2, U_1 U_0 = U_1 \times (U \cap K) \) and \( U_2 U_0 = (U \cap H) \times U_2. \) Thus

\[
U_1 \times U_2/U_0 = U_1 U_0/U_0 \times U_2 U_0/U_0.
\]

Furthermore, \( UU_1 \geq U_2, UU_2 \geq U_1 \) and so \( UU_1 = U_1 \times U_2 = UU_2. \) Now Dedekind's law yields that \( U_1 U_0 \cap U = (U_1 \cap U) U_0 = (U \cap H) U_0 = U_0 \) and, similarly, \( U_2 U_0 \cap U = U_0. \) Hence \( U/U_0 \) is a diagonal in \( U_1 \times U_2/U_0 \) with respect to \( U_1 U_0/U_0 \) and \( U_2 U_0/U_0. \) It is easy to see that the corresponding isomorphism \( \delta: U_1 U_0/U_0 \to U_2 U_0/U_0 \) is the one induced by \( \alpha, \) that is \( (xU_0) = x^2 U_0 \) for \( x \in U_1. \)

Groups with decomposable subgroup lattices

Our description of the subgroup lattice of \( G = H \times K \) shows that \( L(G) \simeq L(H) \times L(K) \) if every epimorphism \( \alpha \) in 1.6.1 (a) is trivial. Clearly, this holds if (and only if) the elements in \( H \) and \( K \) have finite, coprime orders. It is easy to see that this result is also true for more than two factors. Let us say that the groups \( G_{\lambda} (\lambda \in \Lambda) \) are *coprime* if every \( G_\lambda \) is a torsion group and \( (r(x), r(y)) = 1 \) for all \( x \in G_\lambda, y \in G_\mu \) with \( \lambda \neq \mu; \) for finite groups this is equivalent to \( (|G_\lambda|, |G_\mu|) = 1 \) for \( \lambda \neq \mu. \)
1.6 Direct products

1.6.4 Lemma. If \( G = \bigoplus_{\lambda \in \Lambda} G_{\lambda} \) with coprime groups \( G_{\lambda} (\lambda \in \Lambda) \), then \( L(G) \simeq \bigoplus_{\lambda \in \Lambda} L(G_{\lambda}) \); in fact, the map \( \tau: L(G) \to \bigoplus_{\lambda \in \Lambda} L(G_{\lambda}) \) defined by \( H^\lambda(\lambda) = H \cap G_{\lambda} \) for \( \lambda \in \Lambda \) and \( H \leq G \) is an isomorphism.

Proof. Let \( L = \bigoplus_{\lambda \in \Lambda} L(G_{\lambda}) \). Recall that \( L \) is the set of all functions \( f \) defined on \( \Lambda \) such that \( f(\lambda) \in L(G_{\lambda}) \) for all \( \lambda \in \Lambda \); hence \( H^\tau \) is a well-defined element of \( L \). Let \( \rho: L \to L(G) \) be defined by \( f^\rho = \bigoplus_{\lambda \in \Lambda} f(\lambda) \). Then \( f^\rho(\lambda) = \left( \bigoplus_{\mu \in \Lambda} f(\mu) \right) \cap G_{\lambda} = f(\lambda) \) for all \( \lambda \in \Lambda \) and hence \( \rho \tau \) is the identity on \( L \). On the other hand, if \( H \leq G \) and \( x \in H \), then \( x \) is the product of certain \( x_{\lambda} \in G_{\lambda} \) where \( x_{\lambda} y_{\lambda} = y_{\lambda} x_{\lambda} \), \( o(x_{\lambda}) = n \), \( o(y_{\lambda}) = m \) and \( (n,m) = 1 \). There exist integers \( s, t \) such that \( ns + mt = 1 \); thus \( x^m = x_{\lambda}^m y_{\lambda}^m = x_{\lambda}^{1-ns} = x_{\lambda} \). Hence \( x_{\lambda} \in H \) for all \( \lambda \) and \( H = \bigoplus_{\lambda \in \Lambda} (H \cap G_{\lambda}) = H^\rho \). Thus \( \tau \rho \) is the identity on \( L(G) \). It follows that \( \tau \) is bijective and by 1.1.2, \( \tau \) is an isomorphism.

We come now to the main result of this section. We show that any group with decomposable subgroup lattice is a direct product of coprime groups.

1.6.5 Theorem (Suzuki [1951a]). Let \( G \) be a group such that \( L(G) \simeq \bigoplus_{\lambda \in \Lambda} L_{\lambda} \) where \( (L_{\lambda})_{\lambda \in \Lambda} \) is a family of lattices, \( |\Lambda| \geq 2 \) and \( |L_{\lambda}| \geq 2 \) for all \( \lambda \in \Lambda \); write \( L = \bigoplus_{\lambda \in \Lambda} L_{\lambda} \) and suppose that \( \sigma: L(G) \to L \) is an isomorphism. For \( \lambda \in \Lambda \) let \( O_{\lambda} \) be the least and \( I_{\lambda} \) the greatest element of \( L_{\lambda} \), define \( f_{\lambda} \in L \) by \( f_{\lambda}(\mu) = O_{\mu} \) for \( \lambda \neq \mu \in \Lambda \) and \( f_{\lambda}(\lambda) = I_{\lambda} \) and, finally, let \( G_{\lambda} \) be the subgroup of \( G \) with \( \langle g^{\tau} \rangle = f_{\lambda} \). Then \( G = \bigoplus_{\lambda \in \Lambda} G_{\lambda} \), the groups \( G_{\lambda} (\lambda \in \Lambda) \) are coprime and \( L(G_{\lambda}) \simeq L_{\lambda} \) for all \( \lambda \in \Lambda \).

Proof. Clearly, \( G^\sigma \) is the greatest and \( 1^\sigma \) the least element 0 of \( L \), so that by 1.1.7, every \( L_{\lambda} \) has a least and a greatest element and \( L(G_{\lambda}) \simeq [f_{\lambda}/0] \simeq L_{\lambda} \). For \( \lambda \neq \mu \in \Lambda \), \( 1 \neq x \in G_{\lambda} \) and \( 1 \neq y \in G_{\mu} \), furthermore

\[
L(\langle x \rangle \cup \langle y \rangle) \simeq [\langle x \rangle^\sigma \cup \langle y \rangle^\sigma/0] \simeq [\langle x \rangle^\sigma/0] \times [\langle y \rangle^\sigma/0] \simeq L(\langle x \rangle) \times L(\langle y \rangle).
\]

By 1.2.3, \( L(\langle x \rangle) \) and \( L(\langle y \rangle) \) are distributive, as is their direct product. Therefore \( \langle x \rangle \cup \langle y \rangle \) is locally cyclic, and hence cyclic. Since \( x \) and \( y \) generate this cyclic group and \( x \neq 1 \neq y \), \( \langle x \rangle \) and \( \langle y \rangle \) have finite, coprime indices in it, and as \( \langle x \rangle \cap \langle y \rangle = 1 \), \( o(x) \) and \( o(y) \) are finite and coprime. This shows that the groups \( G_{\lambda} (\lambda \in \Lambda) \) are coprime and that they centralize each other. By 1.1.7, \( G = \langle G_{\mu} | \mu \in \Lambda \rangle \) and \( \langle G_{\mu} | \lambda \neq \mu \in \Lambda \rangle \cap G_{\lambda} = 1 \). It follows that \( G_{\lambda} \leq G \) and \( G = \bigoplus_{\lambda \in \Lambda} G_{\lambda} \).

Suzuki's theorem and Lemma 1.6.4 have a number of important consequences. In conjunction with Lemma 1.2.9 they show that the class of nontrivial direct products of coprime groups is invariant under projectivities. Moreover, the direct factors are mapped onto direct factors.
1.6.6 Theorem. Let \( G = \prod_{\lambda \in \Lambda} G_\lambda \) with coprime subgroups \( G_\lambda (\lambda \in \Lambda) \) and let \( \phi \) be a projectivity from \( G \) to a group \( \bar{G} \). Then \( \bar{G} = \prod_{\lambda \in \Lambda} G_\lambda^\phi \) and the subgroups \( G_\lambda^\phi (\lambda \in \Lambda) \) are coprime.

Proof. Let \( \tau : L(G) \to \prod_{\lambda \in \Lambda} L(G_\lambda) \) be the isomorphism defined in 1.6.4. Then \( \sigma = \phi^{-1} \tau \) is an isomorphism from \( L(\bar{G}) \) to \( \prod_{\lambda \in \Lambda} L(G_\lambda) \). In the notation of 1.6.5, \( f_\lambda(\lambda) = G_\lambda = G_\lambda^\phi(\lambda) \) and \( f_\lambda(\mu) = 1 = G_\lambda^\phi(\mu) \) for \( \lambda \neq \mu \in \Lambda \). Hence \( f_\lambda = G_\lambda^\phi \) and so \( (G_\lambda^\phi)^\sigma = f_\lambda \). Now all the assertions follow from 1.6.5.

We mention the following special case of 1.6.6 since we shall often use the result in this form.

1.6.7 Corollary. Let \( H \) and \( K \) be coprime subgroups of a group \( G \) such that \([H, K] = 1\). If \( \phi \) is a projectivity from \( G \) to some group \( \bar{G} \), then \( (HK)^\phi = H^\phi \times K^\phi \) and \( H^\phi, K^\phi \) are coprime.

Proof. Apply 1.6.6 to the projectivity induced by \( \phi \) in \( HK = H \times K \).

Note that neither of the properties \([H, K] = 1\) and \( H, K \) coprime in 1.6.7, is preserved under projectivities. This, for example, is shown by the projectivities between the elementary abelian group of order 9 and the nonabelian group of order 6. As a consequence of 1.6.7 we get a more general result in this direction.

1.6.8 Corollary. Let \( \pi \) be a set of primes and suppose that \( H \) and \( K \) are subgroups of a group \( G \) such that \( H \) is generated by \( \pi \)-elements, \( K \) by \( \pi' \)-elements and \([H, K] = 1\). If \( \phi \) is a projectivity from \( G \) to some group \( \bar{G} \), then \([H^\phi, K^\phi] = 1\).

Proof. For every \( \pi \)-subgroup \( X \) of \( H \) and every \( \pi' \)-subgroup \( Y \) of \( K \), \([X^\phi, Y^\phi] = 1\), by 1.6.7. Since \( H^\phi \) is generated by these \( X^\phi \), it follows that \([H^\phi, Y^\phi] = 1\), and since \( K^\phi \) is generated by these \( Y^\phi \), \([H^\phi, K^\phi] = 1\). We have shown that \( L(G) \) is decomposable if and only if \( G \) is a nontrivial direct product of coprime groups. For finite groups this property is inherited by the Frattini factor group. We remind the reader that the Frattini subgroup \( \Phi(G) \) of an arbitrary group \( G \) is defined to be the intersection of all the maximal subgroups of \( G \), with the stipulation that it shall equal \( G \) if \( G \) should have no maximal subgroups. If \( G \) is finite, then \( \Phi(G) \) is nilpotent and \( \Phi(G)H < G \) for every proper subgroup \( H \) of \( G \).

1.6.9 Theorem. Let \( G \) be a finite group. Then the following properties are equivalent.

(a) \( L(G) \) is directly decomposable.

(b) There exist nontrivial subgroups \( H \) and \( K \) of \( G \) such that \( G = H \times K \) and \((|H|, |K|) = 1\).

(c) \( L(G/\Phi(G)) \) is directly decomposable.
Proof. That (a) implies (b) follows from 1.6.5. If (b) holds, then $G/\Phi(G)$ is the direct product of $H\Phi(G)/\Phi(G)$ and $K\Phi(G)/\Phi(G)$ and these groups are coprime. Since every prime divisor of $|G|$ also divides $|G/\Phi(G)|$ (see Robinson [1982], p. 263), both factors are nontrivial. Now (c) follows from 1.6.4.

Finally, let $L(G/\Phi(G))$ be decomposable, $G/\Phi(G) = H_1/\Phi(G) \times H_2/\Phi(G)$ where $\Phi(G) < H_i$ ($i = 1, 2$) and $|H_1/\Phi(G)|, |H_2/\Phi(G)| = 1$. If $D_i$ is the product of those Sylow $p$-subgroups of $\Phi(G)$ for which $p$ divides $|H_i/\Phi(G)|$, then $D_i \leq G$ ($i = 1, 2$), as characteristic subgroups of $\Phi(G)$. Furthermore, $\Phi(G) = D_1 \times D_2$ since every prime divisor of $|\Phi(G)|$ also divides $|G/\Phi(G)|$. Thus $D_1$ is a normal Hall subgroup of $H_2$. By the Schur-Zassenhaus theorem there exists a complement $G_2$ to $D_1$ in $H_2$ and all these complements are conjugate in $H_2$. Since $D_1$ and $H_2$ are normal subgroups, $G$ operates by conjugation on the set $\Omega$ of these complements and $H_2$ is transitive on $\Omega$. By the Frattini argument, $G = N_G(G_2)H_2$. As $H_2 = G_2D_1$, $G = N_G(G_2)D_1 \leq N_G(G_2)/\Phi(G)$ and hence $G = N_G(G_2)$ since $\Phi(G)$ is the set of nongenerators of $G$. Thus $G_2 \leq G$ with $|G_2| = |H_2/D_1| = |H_2/\Phi(G)|/|D_2|$ and similarly, we get a normal subgroup $G_1$ of $G$ such that $|G_1| = |H_1/\Phi(G)|/|D_1|$. Then $(|G_1|, |G_2|) = 1$, $|G_1||G_2| = |G|$ and so $G = G_1 \times G_2$. Now (a) follows from 1.6.4.

The number of groups with a given subgroup lattice

We finish this chapter with an application of our results on direct products. In 1.2.8 we saw that for every finite cyclic group $G$ there exist infinitely many nonisomorphic groups that are lattice isomorphic to $G$. By 1.6.4 and 1.6.5, this still holds for finite groups $G$ whose subgroup lattice possesses a chain as direct factor; for then $G = C_p \times K$ where $p \in \mathbb{P}$, $n \in \mathbb{N}$, $(p, |K|) = 1$, and every group $G = C_q \times K$ with $q \in \mathbb{P}$ and $(q, |K|) = 1$ is lattice isomorphic to $G$. However, we can show that these are the only finite groups with this property.

1.6.10 Theorem (Suzuki [1951a]). Let $L$ be a finite lattice that has no chain as a direct factor. Then there are only finitely many nonisomorphic groups whose subgroup lattices are isomorphic to $L$. More precisely: If $l$ is the length and $w$ the width of $L$ (see Section 1.1), then $|G| \leq w^{lw}$ for every group $G$ with $L(G) \simeq L$.

Proof. It is clear that the first assertion follows from the second since there are only finitely many groups of order at most $w^{lw}$. To prove the second assertion, we shall show that $p \leq w$ for every prime divisor $p$ of $|G|$. Since a maximal subgroup of a $p$-group has index $p$, the subgroup lattice of a group of order $p^n$ contains a chain of length $n$. Therefore it will follow that $|P| \leq p^l \leq w^l$ for every Sylow $p$-subgroup $P$ of $G$, and since there are at most $w$ primes $p \leq w$, we get $|G| \leq (w^l)^w = w^{lw}$.

So let $p$ be a prime divisor of $|G|$ and let $P$ be a Sylow $p$-subgroup of $G$. If $P$ is not cyclic, then $P$ contains at least $p + 1$ maximal subgroups and these form an antichain in $L(G)$. If $P$ is not normal in $G$, then, by Sylow's theorem, the conjugates of $P$ form an antichain containing at least $p + 1$ elements. In both cases $p < w$. So we may suppose that $P$ is a cyclic normal subgroup of $G$. By the Schur-Zassenhaus theorem, $P$ has a complement $K$ in $G$. If $K$ were normal in $G$, then 1.6.4 would imply
that $L(G) \simeq L(P) \times L(K)$, which is impossible since $L(P)$ is a chain. Thus $K$ is not normal in $G$ and the conjugates of $K$ form an antichain with $p^n$ ($n \in \mathbb{N}$) elements. But then $p \leq w$, as asserted.

Clearly, our bound on $|G|$ is not best possible. It seems worthwhile to look for better bounds and also to ask how many groups $G$ satisfy $L(G) \simeq L$ for a given lattice $L$. Some remarks on the first problem and a characterization of infinite groups with subgroup lattice of finite width can be found in Brandl [1988].

**Exercises**

1. Let $G = H \times K$ and let $U$ be a subgroup of $G$. Show that the following properties are equivalent (the $U_i$ are defined as in 1.6.3).
   (a) $U \trianglelefteq G$.
   (b) $[U_1, H] \leq U \cap H$ and $[U_2, K] \leq U \cap K$.
   (c) $U_0 \trianglelefteq G$ and $U/U_0 \leq Z(G/U_0)$.

2. (Rose [1965]) Let $G = H \times K$, $H \simeq K$ and let $D$ be a diagonal in $G$ with respect to $H$ and $K$. Show that $[G/D]$ is isomorphic to the lattice of normal subgroups of $H$.

3. Show that for $\lambda, \mu \in \Lambda$ with $\lambda \neq \mu$, the groups $G_{\lambda}$ and $G_{\mu}$ defined in 1.6.5 form a $\cap$-distributive pair in $L(G)$ and use Exercises 1.2.3 and 1.2.4 to give an alternate proof of Theorem 1.6.5.

4. Let $G_1$ be a group having only finitely many nonisomorphic projective images—call them $G_1, \ldots, G_r$—and suppose that $\varphi$ is a projectivity from $G = G_1 \times \cdots \times G_r$ to some group $\bar{G}$. If $G_i \not\leq \bar{G}$ for all $i = 1, \ldots, r$, show that $\bar{G} \simeq G$.

5. (Brandl [1988]) Let $p$ be a prime, $n \in \mathbb{N}$. Show that there are only finitely many noncyclic finite $p$-groups whose subgroup lattices have width $n$. 
In this chapter we are going to study subgroup lattices of abelian groups. Since these are modular, we shall more generally investigate groups with modular subgroup lattices, called $M$-groups for short. Unlike the groups with distributive subgroup lattices, these do not form a nice class of groups. However, there are close connections between $M$-groups and abelian groups.

In § 2.1 we give the basic properties of modular lattices and introduce one of the most important concepts of this book, the modular elements of a lattice. These will be used later to study projective images of normal subgroups of groups.

In 1939 Baer determined the projective images of an elementary abelian $p$-group. These were called $P$-groups by Suzuki [1951a], who proved that every projective image of an arbitrary noncyclic finite $p$-group either is a $p$-group or a $P$-group. These results are fundamental for the study of projectivities between finite groups; they are proved in § 2.2.

In 1941 and 1943 Iwasawa investigated the locally finite $M$-groups and those with elements of infinite order; he showed that they are metabelian and determined their exact structure. His results are presented in §§ 2.3 and 2.4, together with the theorem of Schmidt [1986] which characterizes the periodic $M$-groups and thus completes the characterization of groups with modular subgroup lattices.

The main results of § 2.5 are two theorems of Baer [1944] and Sato [1951]. These assert, respectively, that every nonhamiltonian locally finite $p$-group with modular subgroup lattice, and every $M$-group with elements of infinite order admit a projectivity onto a suitable abelian group. In the $p$-group case, there exists a crossed isomorphism which even induces an isomorphism between the coset lattices of the two groups.

In § 2.6 we prove two important theorems of Baer [1939a] on projectivities between abelian groups. He showed that every projectivity between two abelian $p$-groups is induced by an isomorphism if these groups contain with every element of order $p^n$ at least three independent elements of this order. Also, if $G$ is an abelian group with two independent elements of infinite order, then every projectivity of $G$ to an arbitrary group is induced by an isomorphism. Finally, we study projectivities between abelian groups of torsion-free rank 1.

### 2.1 Modular lattices

A lattice $L$ is called modular if for all $x, y, z \in L$ the modular law holds:

1. If $x \leq z$, then $x \cup (y \cap z) = (x \cup y) \cap z$. 

---

Chapter 2

Modular lattices and abelian groups
2.1.1 **Remarks.** Let \( L \) be a lattice and let \( x, y, z \in L \).

(a) If \( x \leq z \), then \( x \leq (x \cup y) \cap z \) and \( y \cap z \leq (x \cup y) \cap z \), so that \( x \cup (y \cap z) \leq (x \cup y) \cap z \) holds in any lattice. Thus only the reverse inclusion is required for the modular law.

(b) Every distributive lattice is modular. For, if \( L \) is distributive and \( x \leq z \), then \( x \cup z = z \) and hence \( x \cup (y \cap z) = (x \cup y) \cap (x \cup z) = (x \cup y) \cap z \).

(c) If \( L \) is modular, then \( x \cup (y \cap (x \cup z)) = (x \cup y) \cap (x \cup z) \) since \( x < x \cup z \). Conversely, if this equation holds in \( L \), then \( x \leq z \) implies \( x \cup z = z \) and hence \( x \cup (y \cap z) = (x \cup y) \cap z \). This shows that modularity can be defined by an identity. Thus sublattices and direct products of modular lattices are modular.

It is easy to see that the only nonmodular lattice with 5 or less elements is the one called \( E_5 \) in Section 1.1. This lattice can be used to characterize modularity.

2.1.2 **Theorem.** The lattice \( L \) is modular if and only if it does not contain a sublattice isomorphic to \( E_5 \).

**Proof.** If \( L \) is modular, then every sublattice of \( L \) is modular and therefore cannot be isomorphic to \( E_5 \). Conversely, we have to show that every nonmodular lattice \( L \) contains a sublattice isomorphic to \( E_5 \). Since \( L \) is not modular, there exist \( x, y, z \in L \) with \( x \leq z \) and \( x \cup (y \cap z) < (x \cup y) \cap z \). Let \( a = y \cap z \), \( b = x \cup (y \cap z) \), \( c = (x \cup y) \cap z \), \( d = y \), \( e = x \cup y \) and \( S = \{a, b, c, d, e\} \). Then, clearly, \( a \leq b < c \leq e \) and \( a \leq d \leq e \). Furthermore

\[
c \cap d = (x \cup y) \cap z \cap y = z \cap y = a
\]

and

\[
b \cup d = x \cup (y \cap z) \cup y = x \cup y = e;
\]

![Figure 8: E₅](image)

it follows that \( b \cap d = a \) and \( c \cup d = e \). Thus \( S \) is a sublattice of \( L \) and as \( b \leq c \) and \( b \cup (d \cap c) = b \neq c = (b \cup d) \cap c \), \( S \) is not modular. Since all the other lattices with at most 5 elements are modular, \( S \cong E_5 \).

We shall also consider the modular law for single elements of a lattice. Thus we come to one of the fundamental concepts of this book.
2.1 Modular lattices

Modular and permutable subgroups

We say that the element \( m \) of the lattice \( L \) is modular in \( L \), and write \( m \mod L \), if

\[(2) \ x \cup (m \cap z) = (x \cup m) \cap z \ \text{for all} \ x, z \in L \ \text{with} \ x \leq z, \ \text{and} \]

\[(3) \ m \cup (y \cap z) = (m \cup y) \cap z \ \text{for all} \ y, z \in L \ \text{with} \ m \leq z; \]

a subgroup \( M \) of a group \( G \) is called modular in \( G \) if \( M \) is modular in \( L(G) \), we write \( M \mod G \) in this case.

Modular elements were introduced by Kurosh in 1940; see also Zassenhaus [1958], p. 74 where they are called "Dedekind elements". Clearly, a lattice \( L \) is modular if and only if every element of \( L \) is modular in \( L \). The following theorem shows why we use just (2) and (3), two of the three possible variants of the modular law, for the definition of a modular element.

2.1.3 Theorem (Ore [1937]). Let \( G \) be a group.

(a) If \( N \leq G \), then \( NH =HN \) for all \( H \leq G \).

(b) If \( M \leq G \) such that \( MH = HM \) for all \( H \leq G \), then \( M \mod G \).

Proof. If \( N \leq G \), then \( Nx = xN \) for all \( x \in G \) and (a) holds. To prove (b), first let \( X \leq Z \leq G \). Then, clearly, \( X \cup (M \cap Z) \leq (X \cup M) \cap Z \). Furthermore, if \( g \in (X \cup M) \cap Z \), then, since \( X \cup M = XM \), there exist \( x \in X \) and \( m \in M \) such that \( g = xm \). Since \( X \leq Z \), we have \( m = x^{-1}g \in Z \) and hence \( g = xm \in X \cup (M \cap Z) \). Thus \( X \cup (M \cap Z) \leq (X \cup M) \cap Z \) and (2) holds. Now let \( Y, Z \leq G \) with \( M \leq Z \). Then \( M \cup (Y \cap Z) \leq (M \cup Y) \cap Z \) and from \( g = my \in (M \cup Y) \cap Z \) and \( m \in M \leq Z \) it follows as above that \( y \in Z \). Therefore \( g \in M \cup (Y \cap Z) \) and (3) holds. Thus \( M \) is modular in \( G \).

Following Stonehewer [1972] we call a subgroup \( M \) of \( G \) permutable in \( G \), and write \( M \per G \), if \( MH = HM \) for all subgroups \( H \) of \( G \). These permutable subgroups had been introduced by Ore [1937] who had called them "quasinormal". Theorem 2.1.3 shows that a normal subgroup is permutable and a permutable subgroup is modular in \( G \). Thus a normal subgroup is modular in \( G \) and the modular laws (2) and (3) are the main properties of a normal subgroup that are visible in the subgroup lattice. We shall use this fact later in our study of images of normal subgroups under projectivities. In this chapter we investigate the connections between commutativity of the group and modularity of its subgroup lattice. Here Theorem 2.1.3 yields the following.

2.1.4 Theorem. The lattice of normal subgroups of an arbitrary group and the subgroup lattice of an abelian group are modular.

Proof. By 2.1.3, every normal subgroup of a group \( G \) is modular in \( L(G) \) and hence also in \( \mathcal{H}(G) \) since this is a sublattice of \( L(G) \). Thus \( \mathcal{H}(G) \) is modular. If \( G \) is abelian, then \( L(G) = \mathcal{H}(G) \).
Properties of modular elements

We give a useful characterization of modular elements in arbitrary lattices, which leads to an important property of elements in modular lattices.

2.1.5 Theorem. The following properties of the element $m$ of a lattice $L$ are equivalent.

(a) $m$ is modular in $L$.

(b) For every $a \in L$, the map $\varphi_{a,m} : [a/a \cap m] \to [a \cup m/m]$; $x \mapsto x \cup m$ is an isomorphism.

(c) For every $a \in L$, the map $\psi_{a,m} : [a \cup m/m] \to [a/a \cap m]$; $z \mapsto z \cap a$ is an isomorphism.

(d) For every $a \in L$, $\varphi_{a,m} \psi_{a,m} = \text{id}_{[a/a \cap m]}$ and $\psi_{a,m} \varphi_{a,m} = \text{id}_{[a \cup m/m]}$.

Proof. (a) $\Rightarrow$ (d). Let $a \in L$. If $x \in [a/a \cap m]$, then by (2),

$$x^{\varphi_{a,m}} \psi_{a,m} = (x \cup m) \cap a = x \cup (m \cap a) = x$$

and if $z \in [a \cup m/m]$, then by (3),

$$z^{\psi_{a,m}} \varphi_{a,m} = (z \cap a) \cup m = (m \cup a) \cap z = z.$$

Thus $\varphi_{a,m} \psi_{a,m} = \text{id}_{[a/a \cap m]}$ and $\psi_{a,m} \varphi_{a,m} = \text{id}_{[a \cup m/m]}$.

(d) $\Rightarrow$ (a). Let $x, z \in L$ such that $x \leq z$. Then $x \cup (m \cap z) \in [z/z \cap m]$ and hence

$$x \cup (m \cap z) = (x \cup (m \cap z))^{\varphi_{x,m}} \psi_{x,m} = ((x \cup (m \cap z)) \cup m) \cap z = (x \cup m) \cap z,$$

that is, (2) holds. If $y, z \in L$ such that $m \leq z$, then $(m \cap y) \cap z \in [y \cap m/m]$ and hence

$$(m \cap y) \cap z = ((m \cap y) \cap z)^{\psi_{y,m}} \varphi_{y,m} = (((m \cap y) \cap z) \cap y) \cup m = (y \cap z) \cup m.$$

Hence (3) also holds and $m$ is modular in $L$.

To prove the equivalence of (b), (c) and (d), let $a \in L$ and write $\varphi_{a,m} = \varphi$ and $\psi_{a,m} = \psi$.

(b) $\Rightarrow$ (d). Let $x \in [a/a \cap m]$. Then $x \leq (x \cup m) \cap a$ and hence $x \cup m \leq ((x \cup m) \cap a) \cup m$. The other inclusion is trivial since $m$ and $(x \cup m) \cap a$ are contained in $x \cup m$. So we get

$$x^\varphi = x \cup m = ((x \cup m) \cap a) \cup m = ((x \cup m) \cap a)^\varphi.$$

Since $\varphi$ is injective, it follows that $x = (x \cup m) \cap a = x^{\varphi \varphi}$. Now let $z \in [a \cup m/m]$. Then $(z \cap a) \cup m \leq z$ and since $\varphi$ is surjective, there exists $b \in [a/a \cap m]$ such that

$$z = b^\varphi = b \cup m.$$

Then $b \leq z \cap a$ and $z = b \cup m \leq (z \cap a) \cup m$. Thus $z = (z \cap a) \cup m = z^{\varphi \varphi}$ and (d) holds.

It is clear that (d) implies both (b) and (c). For, if (d) holds, then $\varphi$ and $\psi$ are bijective and satisfy (c) and (b) of 1.1.2, respectively. So it remains to show that
(c) ⇒ (d). For \( x \in [a/a \cap m] \), again, \( x \leq (x \cup m) \cap a \). Since \( \psi \) is surjective, there exists \( c \in [a \cup m/m] \) such that \( x = c^\psi = c \cap a \). Then \( x \cup m \leq c \) and \( (x \cup m) \cap a \leq c \cap a = x \). Thus \( x = (x \cup m) \cap a = x^\psi \). Now let \( z \in [a \cup m/m] \). Then \( (z \cap a) \cup m \leq z \) and hence \( ((z \cap a) \cup m) \cap a \leq z \cap a \). The other inclusion is trivial and so we get that

\[
z^\psi = z \cap a = ((z \cap a) \cup m) \cap a = ((z \cap a) \cup m)^\psi.
\]

Since \( \psi \) is injective, it follows that \( z = (z \cap a) \cup m = z^\psi \). Thus (d) holds.

Theorem 2.1.5 shows that if \( m \) is a modular element of a lattice \( L \), then

(4) \([a \cup m/m] \simeq [a/a \cap m]\) for every \( a \in L \).

But this condition alone does not imply that \( m \) is modular in \( L \). This is shown by the following example. Take a circle \( K \) in the euclidean plane, choose two points \( I \) and \( 0 \) on \( K \) dividing the circle into two arcs and for \( x, y \in K \), define \( x \leq y \) if and only if \( x \) and \( y \) are on the same arc and \( x \) is nearer to \( 0 \) than \( y \) or \( x = y \). Let \( a, m \in K \); then both \([a \cup m/m]\) and \([a/a \cap m]\) consist of a single element if \( a < m \), and are

![Figure 9](image)

isomorphic to the real unit interval if \( a \leq m \). So \( m \) satisfies (4), but, clearly, \( m \) is not modular in \( K \) if \( 0 \neq m \neq I \). If \( L \) is a finite lattice, it is easy to see that \( m \) is modular in \( L \) if it satisfies (4) (see Exercise 2). However, we shall not need this fact since we shall always use the mappings \( \phi_{a,m} \) and \( \psi_{a,m} \) to prove (4).

We collect the main inheritance properties of modular elements.

2.1.6 Theorem. Let \( L \) be a lattice, \( m, n, a \in L \) and suppose that \( m \) is modular in \( L \).

(a) \( m \cap a \) is modular in \([a/0]\) = \( \{x \in L | x \leq a\} \).

(b) \( m \cup a \) is modular in \([I/a]\) = \( \{y \in L | a \leq y\} \).

(c) If \( m \leq n \) and \( n \) is modular in \([I/m]\), then \( n \) is modular in \( L \).

(d) If \( n \) and \( m \) are modular in \( L \), then so is \( m \cup n \).

(e) If \( \sigma \) is an isomorphism from \( L \) to a lattice \( \bar{L} \), then \( m^\sigma \) is modular in \( \bar{L} \).

Proof. (a) Let \( b \in [a/0] \). If \( x \in [b/b \cap (m \cap a)] = [b/b \cap m] \), then by (2),

\[
x^{\phi_{b,m \cap a}} = x \cup (m \cap a) = (x \cup m) \cap a = x^{\phi_{b,m \cap a}}.
\]
Modular lattices and abelian groups

Hence \( \varphi_{b,m \cap a} \) is the product of \( \varphi_{b,m} \) and the restriction of \( \psi_{a,m} \) to \([b \cup m/m] \). Since these two maps are isomorphisms, \( \varphi_{b,m \cap a} \) is also an isomorphism and by 2.1.5, \( m \cap a \) is modular in \([a/o] \).

(b) Let \( c \in [I/a] \). If \( z \in [c \cup (m \cup a)/m \cup a] = [c \cup m/m \cup a] \), then \( z^{\psi_{c,m\cup a}} = z \cap c = z^{\psi_{c,m}} \). Thus \( \psi_{c,m\cup a} \) is the restriction of \( \psi_{c,m} \) to \([c \cup m/m \cup a] \) and hence an isomorphism. By 2.1.5, \( m \cup a \) is modular in \([I/a] \).

(c) Let \( d \in L \). Then for \( z \in [d \cup n/n] \), we have \( z^{\psi_{d,n}} = z \cap d = z \cap (d \cup m) \cap d = z^{\psi_{d,m,n}\psi_{d,m}} \); note that the right-hand side is well-defined because \( m \leq z \cap (d \cup m) \leq d \cup m \). Since \( \psi_{d,m,n} \) and the restriction of \( \psi_{d,m} \) to \([d \cup m/(d \cup m) \cap n] \) are isomorphisms, \( \psi_{d,n} \) is also an isomorphism. By 2.1.5, \( n \) is modular in \( L \).

(d) By (b), \( m \cup n \) is modular in \([I/n] \) and therefore by (c), \( m \cup n \) is modular in \( L \).

(e) is trivial.

Note that \( m \cap n \) in general is not modular in \( L \) if \( m \) and \( n \) are modular elements in \( L \). This, for example, is shown by the lattice represented by the Hasse diagram of Figure 10. But there are also simple examples in subgroup lattices (see Exercise 3).

Figure 10

It is well-known (see Robinson [1982], p. 66) that the class of groups satisfying the maximal condition (or other chain conditions) is closed with respect to forming extensions. This is a more general property of intervals in lattices.

2.1.7 Lemma. Let \( a, b, m \) be elements of a lattice \( L \) such that \( b \leq m \leq a \) and suppose that \( m \) is modular in \( L \). If \([a/m] \) and \([m/b] \) satisfy the maximal condition, then so does \([a/b] \).

Proof. Let \((c_i)_{i \in N} \) be an ascending chain in \([a/b] \). Then \((c_i \cup m)_{i \in N} \) and \((c_i \cap m)_{i \in N} \) are ascending chains in \([a/m] \) and \([m/b] \), respectively. Since these two intervals satisfy the maximal condition, there exists a natural number \( r \) such that \( c_s \cup m = c_s \cup m \) and \( c_s \cap m = c_s \cap m \) for all \( s \geq r \). Then \( c_r \leq c_s \) and by (2),

\[
c_r = c_r \cup (m \cap c_r) = c_r \cup (m \cap c_s) = (c_r \cup m) \cap c_s = (c_s \cup m) \cap c_s = c_s
\]

for all \( s \geq r \). Thus the chain \((c_i)_{i \in N} \) is also finite.

Semimodular lattices

A lattice \( L \) is called upper semimodular if for all \( x, y \in L \),

\[
(5) \ x \cup y \text{ covers } x \text{ whenever } y \text{ covers } x \cap y;
\]
and $L$ is called lower semimodular if for all $x, y \in L$,

(6) $y$ covers $x \cap y$ whenever $x \cup y$ covers $x$.

By 2.1.5, a modular lattice satisfies (5) and (6) and is therefore upper and lower semimodular. The following theorem shows that for subgroup lattices, property (6) is more important.

2.1.8 Theorem. The lattice of composition subgroups of an arbitrary group and the subgroup lattice of a finite nilpotent group are lower semimodular.

Proof. Let $G$ be a group and let $X, Y$ be composition subgroups of $G$ such that $X \cup Y$ covers $X$ in the lattice $\mathcal{R}(G)$ of composition subgroups of $G$. By 1.1.4, there exists a composition series from $X \cup Y$ to $X$. Clearly, all members of this series belong to $\mathcal{R}(G)$ and since $X \cup Y$ covers $X$ in $\mathcal{R}(G)$, the series must have length 1. So $X \subseteq X \cup Y$ and $X \cup Y/X$ is simple. Hence also $X \cap Y \subseteq Y$ and $Y/X \cap Y$ is simple. Again by 1.1.4, if $H \in \mathcal{R}(G)$ such that $X \cap Y \leq H < Y$, then there exists a composition series from $Y$ to $H$ and it follows that $H = X \cap Y$. So $Y$ covers $X \cap Y$ in $\mathcal{R}(G)$ and $\mathcal{R}(G)$ is lower semimodular. In a finite nilpotent group $G$, every subgroup is subnormal and hence $L(G) = \mathcal{R}(G)$.

The Jordan-Dedekind chain condition

We say that a lattice $L$ satisfies the Jordan-Dedekind chain condition if for every $x, y \in L$ with $x < y$ there exists a finite maximal chain $x = x_0 < \cdots < x_r = y$ from $x$ to $y$ and all maximal chains from $x$ to $y$ have the same length $l(x, y)$.

2.1.9 Theorem. Every upper or lower semimodular lattice $L$ of finite length satisfies the Jordan-Dedekind chain condition.

Proof. We give a proof in the case that $L$ is lower semimodular; the proof for upper semimodular lattices is similar. If $x, y \in L$ with $x < y$, then there exists a finite maximal chain from $x$ to $y$ since $L$ has finite length. We prove by induction on $n$ the following assertion which then, clearly, will imply the Jordan-Dedekind chain condition for $L$.

(*) If $x, y \in L$ with $x < y$ and if there exists a maximal chain from $x$ to $y$ of length $n$, then every maximal chain from $x$ to $y$ has length $n$.

This is clear if $n = 1$, that is if $y$ covers $x$. So assume that (*) is true for $n - 1$, let $x = x_0 < \cdots < x_n = y$ be a maximal chain of length $n$ and suppose that $x = y_0 < \cdots < y_m = y$ is another maximal chain. If $x_{n-1} = y_{m-1}$, then by induction, $n - 1 = m - 1$. So assume that $x_{n-1} \neq y_{m-1}$ and let $z = x_{n-1} \cap y_{m-1}$. Then $y = x_{n-1} \cup y_{m-1}$ and $z$ is covered by $x_{n-1}$ and $y_{m-1}$ since $L$ is lower semimodular. Therefore, if $x = z_0 < \cdots < z_k = z$ is a maximal chain, then $x = z_0 < \cdots < z_k < x_{n-1}$ and $x = x_0 < \cdots < x_{n-1}$ are maximal chains from $x$ to $x_{n-1}$. By the induction assumption, $n - 1 = k + 1$. Thus also $x = z_0 < \cdots < z_k < y_{m-1}$ is a maximal chain of length
Modular lattices and abelian groups

\( n - 1 \) and the induction assumption applied to this chain and to \( x = y_0 < \cdots < y_{m-1} \) yields \( n - 1 = m - 1 \). Thus \( n = m \) and (**) holds.

2.1.10 Theorem. The following properties of a lattice \( L \) of finite length are equivalent.

(a) \( L \) is modular.

(b) \( L \) is upper and lower semimodular.

(c) \( L \) satisfies the Jordan-Dedekind chain condition and \( l(x, x \cup y) = l(x \cap y, y) \) for all \( x, y \in L \).

Proof. That (a) implies (b) is clear. If (b) holds, then \( L \) satisfies the Jordan-Dedekind chain condition as we have just shown. Let \( x = x_0 < \cdots < x_n = x \cup y \) be a maximal chain. Then

\[
\text{(7) } x \cap y = x_0 \cap y \leq \cdots \leq x_n \cap y = y.
\]

For every \( i \in \{0, \ldots, n - 1\} \), since \( x_{i+1} \) covers \( x_i \), either \( x_i \cap y = x_{i+1} \cap y \) or \( x_i \cup (x_{i+1} \cap y) = x_{i+1} \) and then \( x_i \cap y = x_i \cap (x_{i+1} \cap y) \) is covered by \( x_{i+1} \cap y \) since \( L \) is lower semimodular. Therefore (7) yields a maximal chain from \( x \cap y \) to \( y \) of length at most \( n \); that is, we have \( l(x, x \cup y) \geq l(x \cap y, y) \). The other inequality follows similarly from the upper semimodularity of \( L \). Thus (c) holds. Finally, suppose that \( L \) satisfies (c) but is not modular. Then by 2.1.2, there exists a sublattice \( \{a, b, c, d, e\} \) of \( L \) isomorphic to \( E_5 \). If \( a < b < c < e \) and \( a < d < e \), then \( l(a, b) = l(d \cap b, b) = l(d, d \cup b) = l(d, e) \). Similarly, \( l(a, c) = l(d, e) \). Thus \( l(a, b) = l(a, c) \), but this is impossible since \( b < c \). This contradiction shows that (c) implies (a).

Exercises

1. Show that a modular subgroup of a group \( G \) is in general not permutable, and a permutable subgroup is in general not normal in \( G \).

2. (Schenke [1986]) Let \( L \) be a lattice and let \( m \in L \) such that \([a \cup m/m] \cong [a/a \cap m]\) for every \( a \in L \). If \([I/m] \) is finite, show that \( m \) is modular in \( L \).

3. Let \( p \) be an odd prime, \( H = \langle a, b \mid a^{p^2} = b^p = 1, a^b = a^{1+p} \rangle \) the nonabelian group of order \( p^3 \) and exponent \( p^2 \), \( K = \langle c \rangle \) cyclic of order \( p^2 \) and let \( G = H \times K \). Find two modular subgroups of \( G \) whose intersection is not modular in \( G \).

4. Show that a lattice all of whose sublattices are lower semimodular is modular. Deduce that sublattices of lower semimodular lattices are in general not lower semimodular.

5. Let \( L \) be the direct product of lattices \( L_\lambda \). Show that \( L \) is lower semimodular if and only if every \( L_\lambda \) is lower semimodular.

6. Show that for an arbitrary lattice \( L \), no two of the conditions (a)–(c) in Theorem 2.1.10 are equivalent.
7. The element \( m \) of the lattice \( L \) is called \textit{semimodular} in \( L \) if it satisfies (2). Show that
(a) \( m \) is semimodular in \( L \) if and only if \( \varphi_{a,m} \psi_{a,m} = \text{id}_{[a/a \cap m]} \) for all \( a \in L \);
(b) if \( m \) is semimodular in \( L \), then \( \psi_{a,m} \varphi_{m,a} = \text{id}_{[m \cup a/a]} \) for all \( a \in L \);
(c) if \( m \) and \( n \) are semimodular in \( L \), then \( [m \cup n/n] \simeq [n/m \cap n] \);
(d) an antiatom of \( L \) is semimodular in \( L \) if and only if it is modular in \( L \).

8. Let \( L \) be a lattice, \( m, n, a \in L \), and suppose that \( m \) is semimodular in \( L \). Show that
(a) \( m \cap a \) is semimodular in \([a/0]\);
(b) if \( m \) is modular in \( L \), \( m \leq n \) and \( n \) is semimodular in \([I/m]\), then \( n \) is semimodular in \( L \);
(c) if \( m \leq n \) and \( n \) is modular in \([I/m]\), then \( n \) in general is not semimodular in \( L \);
(d) if \([I/m]\) is a chain and \( m \leq n \), then \( n \) is semimodular in \( L \).

2.2 \textbf{P-groups}

By 1.6.6, every projective image of a periodic abelian group \( G \) is the direct product of the images of the primary components of \( G \). However, in general these images are neither abelian nor primary: the nonabelian group of order \( pq \), \( p \) and \( q \) primes with \( q \) dividing \( p - 1 \), and the elementary abelian group of order \( p^2 \) have isomorphic subgroup lattices. This is the first of a series of examples that we shall now investigate more closely.

The classes \( P(n, p) \)

Let \( p \) be a prime and \( n \geq 2 \) be a cardinal number. We say that a group \( G \) belongs to the class \( P(n, p) \) if \( G \) is either elementary abelian of order \( p^n \), or a semidirect product of an elementary abelian normal subgroup \( A \) of order \( p^{n-1} \) by a group of prime order \( q \neq p \) which induces a nontrivial power automorphism on \( A \). Here, if \( n \) is infinite, by an elementary abelian group of order \( p^n \) or \( p^{n-1} \) we shall mean a direct product of \( n \) cyclic groups of order \( p \). We call \( G \) a \textit{P-group} if \( G \in P(n, p) \) for some prime \( p \) and some cardinal number \( n \geq 2 \).

2.2.1 Remarks. Let \( G \) be a nonabelian \( P \)-group, so \( G = A \langle t \rangle \) with an elementary abelian \( p \)-group \( A \) and an element \( t \) of order \( q \) that induces a nontrivial power automorphism on \( A \). By 1.5.6, \( t \) is universal on \( A \), that is, there exists an integer \( r \) such that

\[
(1) \quad t^{-1} at = a^r \quad \text{for all} \quad a \in A.
\]

Since \( t \notin C_G(A) \) and \( t^q = 1 \),

\[
(2) \quad r \not\equiv 1 \pmod{p} \quad \text{and} \quad r^q \equiv 1 \pmod{p}.
\]

Hence \( q \) divides \( p - 1 \). In particular, the classes \( P(n, 2) \) only contain the elementary abelian groups of order \( 2^n \). For \( p > 2 \), however, to every prime divisor \( q \) of \( p - 1 \),
there exists an integer $r$ satisfying (2); then the semidirect product $G = A \langle t \rangle$ of a nontrivial elementary abelian $p$-group $A$ by a cyclic group $\langle t \rangle$ of order $q$ where $t^{-1}a^t = a^r$ for all $a \in A$ is a nonabelian $P$-group. Any two such groups with the same $A$ and $q$ (for different $r$) are isomorphic, as the reader can easily verify. Thus for $p > 2$, the classes $P(n, p)$ contain the elementary abelian group of order $p^n$, and, for every prime divisor $q$ of $p - 1$, exactly one nonabelian $P$-group with elements of order $q$; if $n$ is finite, the order of this group is $p^n - 1$.

We want to show that these $P(n, p)$ are complete classes of lattice-isomorphic groups. For this purpose and for later use, we collect some simple properties of $P$-groups.

2.2.2 Lemma. Let $G$ be a nonabelian $P$-group and suppose that $p$, $q$ and $A$ are as in 2.2.1.

(a) $G' = A = C_G(a)$ for all $1 \neq a \in A$.
(b) $Z(G) = 1$.
(c) The normal subgroups of $G$ are $G$ and the subgroups of $A$.
(d) Every element $x \in G \setminus A$ has order $q$. Hence the subgroups of order $q$ generate $G$.

Proof. (a) Since $G/A$ is cyclic, $G' \leq A$. If $1 \neq a \in A$, in the notation of 2.2.1, then $[a, t] = a^{t^{-1}}$ and $\langle a^{t^{-1}} \rangle = \langle a \rangle$ since $r \neq 1 \pmod{p}$. Hence $\langle a \rangle \leq G'$ and $a \notin Z(G)$. Thus $G' = A$ and $C_G(a) = A$ since $A$ is an abelian maximal subgroup of $G$.
(b) By (a), $Z(G) \leq C_G(A) = A$ and $a \notin Z(G)$ for all $1 \neq a \in A$. Thus $Z(G) = 1$.
(c) Since $A$ is abelian and $t$ induces a power automorphism on $A$, every subgroup of $A$ is normal in $G$. If $N \triangleleft G$ and $N \nsubseteq A$, then $AN = G$ and $G/N \cong A/A \cap N$ is abelian. It follows that $A = G' \leq N$ and hence $N = G$.
(d) If $x \in G \setminus A$, then $G = A \langle x \rangle$ and $x \in C_G(A \cap \langle x \rangle)$. By (a), $A \cap \langle x \rangle = 1$. Hence $\langle x \rangle \cong G/A$ is of order $q$. Since a group cannot be the set-theoretic union of two proper subgroups, $G$ is generated by the elements in $G \setminus A$.

2.2.3 Theorem (Baer [1939a]). For every prime $p$ and every cardinal number $n \geq 2$, all groups in $P(n, p)$ are lattice-isomorphic.

Proof. We show that every nonabelian group $G \in P(n, p)$ is lattice-isomorphic to the elementary abelian group in $P(n, p)$. So let $q$, $r$ and $G = A \langle t \rangle$ be as in 2.2.1. Then $G = A \times \langle t \rangle$, where $o(t) = p$, is the elementary abelian group in $P(n, p)$. We want to construct a bijective map from the set $L_1(G)$ of cyclic subgroups of $G$ to $L_1(G)$ that induces a projectivity from $G$ to $G$. If $x \in G \setminus A$, then by 2.2.2, $\langle x \rangle$ has order $q$ and therefore contains exactly one element out of each coset of $A$, in particular out of $At$. Hence there exists exactly one element $a \in A$ such that $\langle x \rangle = \langle at \rangle$. We define the map $\tau: L_1(G) \to L_1(G)$ by $\langle x \rangle' = \langle x \rangle$ if $x \in A$, and $\langle x \rangle' = \langle a^t \rangle$ if $\langle x \rangle = \langle at \rangle \notin A$. Since every cyclic subgroup of the elementary abelian group $G = A \times \langle t \rangle$ which is not contained in $A$ also contains exactly one element of the form $a^t$ with $a \in A$, we see that $\tau$ is bijective. By 1.3.2, we have to show that for all $X$, $Y$, $Z \in L_1(G)$,

(3) $X \leq \langle Y, Z \rangle$ if and only if $X' \leq \langle Y', Z' \rangle$. 
This is clear if $Y$ and $Z$ are contained in $A$ since $\tau$ is the identity on $L_1(A)$. If $Y \leq A$ and $Z \not\leq A$, that is, $Y = \langle b \rangle$ and $Z = \langle ct \rangle$ with $b, c \in A$, then $\langle Y, Z \rangle \cap A = Y$. Thus, if $X \leq A$, then $X \leq \langle Y, Z \rangle$ if and only if $X \leq Y$, and this is the case if and only if $X^\tau \leq \langle Y, Z \rangle$. For $X \not\leq A$, that is, $X = \langle at \rangle$ with $a \in A$, we have $X \leq \langle Y, Z \rangle$ if and only if $at \leq \langle b, ct \rangle \cap A = \langle \langle b, ct \rangle \cap A \rangle ct = \langle b \rangle ct$, i.e. $a \in \langle b \rangle$; moreover, this is the case if and only if $U^\tau = \langle at \rangle \leq \langle b \rangle \times \langle ct \rangle = \langle Y, Z \rangle$. Finally, if neither $Y = \langle b \rangle$ nor $Z = \langle ct \rangle$ is contained in $A$, then with $W = \langle bc^{-1} \rangle \leq A$ we have $\langle Y, Z \rangle = \langle W, Z \rangle$ and $\langle Y^\tau, Z^\tau \rangle = \langle bc^{-1}, e^\tau \rangle = \langle W^\tau, Z^\tau \rangle$. Thus (3) also holds in this case as we have just shown.

We now want to show that the classes $P(n, p)$ are closed under projectivities. For the case $n = 2$ of this assertion we prove a more general result that will also be used in the next section.

2.2.4 Lemma. Let $G$ be a finite group and suppose that $M$ and $N$ are two different minimal subgroups of $G$ which are modular in $G$. Then $|M \cup N| = pq$ where $p$ and $q$ are primes.

Proof. We may assume that $G = M \cup N$. If $H$ is a maximal subgroup of $G$, then $H$ cannot contain both $M$ and $N$. So if $M \not\leq H$, say, then $H \cap M = 1$, $H \cup M = G$ and, by 2.1.5,

$$[H/1] = [H/H \cap M] \approx [H \cup M/M] = [N \cup M/M] \approx [N/N \cap M] = [N/1].$$

Hence $H$ is a minimal subgroup of $G$. If $H \leq G$, then $|H| = p$ and $|G/H| = q$ are primes and $|G| = pq$. So assume that $H$ is not normal in $G$. Then $H = N_G(H)$ and the conjugates of $H$ in $G$ together contain $|G : H| = |G| - |G : H|$ nontrivial elements, that is, at least $\frac{1}{2}|G|$ but less than $|G| - 1$. Since $H$ is not normal, $G$ is not cyclic and therefore every element of $G$ is contained in a maximal subgroup of $G$. Hence there exists a maximal subgroup $K$ of $G$ that is not conjugate to $H$. But then $K \leq G$ and $|G| = pq$ since otherwise the conjugates of $K$ would contain at least $\frac{1}{2}|G|$ further nontrivial elements of $G$.

2.2.5 Theorem (Baer [1939a]). For every prime $p$ and every cardinal number $n \geq 2$, the class $P(n, p)$ is invariant under projectivities.

Proof. Let $\varphi$ be a projectivity from $G$ to $\bar{G}$ and suppose that $\bar{G} \in P(n, p)$. If $n = 2$, then the nontrivial proper subgroups of $G$ form an antichain with $p + 1$ elements. By 2.2.4, $|G| = qr$ where $q$ and $r$ are primes with $q \geq r$, say. Since the antichain contains more than 2 elements, $G$ is not cyclic and hence elementary abelian of order $q^2$ (if $q = r$) or nonabelian of order $qr$ (if $q \neq r$). In both cases, $G$ has exactly $q + 1$ minimal subgroups. It follows that $q = p$ and $G \in P(2, p)$.

Now let $n \geq 3$. By 2.2.3, we may assume that $G$ is elementary abelian. So if $x$ and $y$ are nontrivial elements of $G$ such that $\langle x \rangle \neq \langle y \rangle$, then $\langle x \rangle^\varphi$ and $\langle y \rangle^\varphi$ are cyclic of
order \( p \), and \( \langle x, y \rangle^p = \langle x \rangle^p \cup \langle y \rangle^p \) is elementary abelian of order \( p^2 \). By the case \( n = 2 \), already settled,

(4) \( \langle x, y \rangle \in P(2, p) \).

In particular, if \( P \) is the set of \( p \)-elements in \( G \), then \( P \neq 1 \) and we show that \( P \) is an elementary abelian normal subgroup of \( G \). For \( 1 \neq x \in P \), \( \langle x \rangle^p \) is cyclic of order \( p \) and hence also \( o(x) = p \). If \( x, y \in P \) with \( o(x) = p = o(y) \) and \( \langle x \rangle \neq \langle y \rangle \), then by (4), \( \langle x, y \rangle \in P(2, p) \). And since a nonabelian group in \( P(2, p) \) has only one subgroup of order \( p \), \( |\langle x, y \rangle| = p^2 \). Thus \( xy^{-1} \in P \) and \( xy = yx \). This also holds if \( \langle x \rangle = \langle y \rangle \) and hence \( P \) is an abelian subgroup of \( G \). Since it is the set of all elements of order \( p \) or \( 1 \) in \( G \), it is clearly normal and elementary abelian.

Now \( P \) and \( P^o \) are lattice-isomorphic elementary abelian \( p \)-groups. If \( P = \bigcup_{\lambda \in \Lambda} P_\lambda \) where \( |P_\lambda| = p \) for all \( \lambda \), then \( P^o = \bigcup_{\lambda \in \Lambda} P_\lambda^o \) and \( P^o = \bigcup_{\mu \not\in \lambda} P_\mu^o = \left( \bigcup_{\mu \not\in \lambda} P_\mu \right)^o \) for all \( \lambda \). Hence \( P^o = \bigcup_{\lambda \in \Lambda} P_\lambda^o \) and \( P^o \simeq P \). Therefore if \( P = G \), we are finished. So assume that \( P \neq G \). Since \( G/P \) does not contain elements of order \( p \), \( |G/P^o| = p \) by the case \( n = 2 \), which is already settled. Thus \( P^o \) and \( P \) are elementary abelian of order \( p^{n-1} \) and \( |G : P| = q \) for some prime \( q \). Let \( t \in G \) with \( o(t) = q \). Then \( G = P \langle t \rangle \). For \( 1 \neq x \in P \), \( \langle x, t \rangle \in P(2, p) \) by (4) and therefore \( \langle x \rangle \leq \langle x, t \rangle \). Thus \( t \) induces a nontrivial power automorphism on \( P \) and \( G \in P(n, p) \).

Projective images of locally finite \( p \)-groups

By 2.2.3 and 2.2.5, the class \( P(n, p) \) is precisely the class of projective images of the elementary abelian group of order \( p^n \). So for \( p > 2 \), this group has projective images that are not even primary groups. We show that the elementary abelian groups are the only finite \( p \)-groups with this property.

2.2.6 Theorem (Suzuki [1951a]). Let \( p \) be a prime, \( n \) a natural number, \( G \) a group of order \( p^n \), and suppose that \( \varphi \) is a projectivity from \( G \) to some group \( \overline{G} \). If \( |\overline{G}| \neq |G| \), then either

(a) \( G \) is cyclic and \( \overline{G} \) is cyclic of order \( q^n \) where \( q \) is a prime different from \( p \), or

(b) \( G \) is elementary abelian, \( n \geq 2 \) and \( \overline{G} \) is a nonabelian \( P \)-group of order \( p^{n-1}q \) where \( q \) is a prime dividing \( p - 1 \).

Proof. We use induction on \( n \). Since \( |\overline{G}| \neq |G| \), \( \overline{G} \) is not a \( p \)-group. If \( G \) is cyclic, then by 1.2.8, (a) holds. In particular our assertion is correct for \( n = 1 \) and we may assume that \( n \geq 2 \) and that \( G \) is not cyclic. Then by the Burnside Basis Theorem, \( G/\Phi(G) \) is elementary abelian of order \( p^m \) where \( m \geq 2 \). Since \( \Phi(G)^o = \Phi(\overline{G}) \), \( \varphi \) induces a projectivity from \( G/\Phi(G) \) to \( \overline{G}/\Phi(\overline{G}) \) and by 2.2.5, \( \overline{G}/\Phi(\overline{G}) \in P(m, p) \). Hence there exists a subgroup \( P \) of \( G \) such that \( \Phi(G) \leq P \) and \( |P^o/\Phi(\overline{G})| = p^{m-1} \). By the induction assumption, \( P^o \) is a \( p \)-group or lies in \( P(k, p) \) for some \( k \); in the latter case by 2.2.2, \( \Phi(\overline{G}) \) is a \( p \)-group as a normal subgroup of \( P^o \). Hence in both cases \( P^o \) is a \( p \)-group. Since \( \overline{G} \) is not a \( p \)-group, \( \overline{G}/\Phi(\overline{G}) \) is nonabelian of order \( p^{m-1}q \) where \( q \) is a prime dividing \( p - 1 \) and \( P^o \) is the Sylow \( p \)-subgroup of \( \overline{G} \).
2.2 P-groups

If \( \Phi(G) = 1 \), then (b) holds and we are finished. So suppose for a contradiction that \( \Phi(G) \neq 1 \). Let \( Q \leq G \) such that \( |Q^p| = q \), take a maximal subgroup \( R \) of \( G \) containing \( Q \) and put \( D = P \cap R \). Since \( P^0Q^p = G \), \( R \neq P \) and so \( G/D \) is elementary abelian of order \( p^2 \). Hence there exists a maximal subgroup \( S \) of \( G \) such that \( D \leq S \) and \( R \neq S \neq P \). Since \( P^0 \) is the only Sylow \( p \)-subgroup of \( G \), \( R^p \) and \( S^p \) are not \( p \)-groups; on the other hand, \( p \) divides the order of \( \Phi(G) \leq R^p \cap S^p \). By induction, \( R \) and \( S \) are elementary abelian. This implies that \( D \leq Z(G) \) and that \( P \) is abelian as a cyclic extension of the central subgroup \( D \). So for \( x, y \in G \), we have \( [y, x] \in G' \leq D \leq Z(G) \) and by (4) of 1.5,

\[
(xy)^p = x^p y^p [y, x]^p = x^p y^p
\]

since \( D \) is elementary abelian and \( p > 2 \). Therefore the set of elements of order dividing \( p \) is a subgroup of \( G \) containing \( R \) and \( S \), hence is \( G \). It follows that \( P \) is elementary abelian. Since \( P^0 \) is a \( p \)-group, it is also elementary abelian, and, by Maschke's Theorem, \( P^0 \) is completely reducible under the action of \( Q^p \). Hence there exists a \( Q^p \)-invariant subgroup \( K^p \) of \( G \) such that \( P^0 = K^p \times \Phi(G) \). Then \( K^pQ^p \) is a proper subgroup of \( G \), but every maximal subgroup of \( G \) containing \( K^pQ^p \) also contains \( K^p \Phi(G)Q^p = P^0Q^p = G \). This contradiction shows that \( \Phi(G) = 1 \) and (b) holds.

The corresponding result for locally finite groups is an easy consequence.

2.2.7 Corollary. Let \( p \) be a prime and let \( G \) be a locally finite \( p \)-group. If there exists a projective image of \( G \) that is not a \( p \)-group, then \( G \) is locally cyclic (that is \( G \simeq C_{p^n} \) for some \( n \in \mathbb{N} \cup \{ \infty \} \)) or elementary abelian.

Proof. Let \( \varphi \) be a projectivity from \( G \) to \( \bar{G} \) where \( \bar{G} \) is not a \( p \)-group and suppose that \( G \) is not elementary abelian. Then there exist elements \( x, y, z \in G \) such that \( \langle x \rangle^p \) is not a \( p \)-group and \( \langle y, z \rangle \) is not elementary abelian. Now if \( g_1, \ldots, g_n \in G \), then \( H = \langle g_1, \ldots, g_n, x, y, z \rangle \) is a finite \( p \)-group, and since \( x, y, z \in H \), we see that \( |H^p| \neq |H| \) and \( H \) is not elementary abelian. By 2.2.6, \( H \) is cyclic and thus \( G \) is locally cyclic.
As another consequence of Suzuki's theorem it is possible to describe the projective closure of the class of finite nilpotent groups, that is, the smallest class of groups which is invariant under projectivities and contains all finite nilpotent groups (see Exercise 7). Nilpotent torsion groups will be handled in Section 7.4.

**Exercises**

1. Show that there is at most one $P$-group of a given finite order (see Remark 2.2.1).

2. Give an alternate proof of Theorem 2.2.3. With the notation used there show the following.
   (a) Every subgroup $H$ of $G$ that is not contained in $A$ has the form $H = A_1 \langle at \rangle$ where $A_1 = H \cap A \leq A$ and $a \in A$.
   (b) For $A_1 \leq A$ and $a_i \in A$, $A_1 \langle a_1t \rangle \leq A_2 \langle a_2t \rangle$ if and only if $A_1 \leq A_2$ and $a_1^{-1}a_2 \in A_2$.
   (c) The map $\varphi: L(G) \to L(\overline{G})$ defined by $H^\varphi = H$ for $H \leq A$ and $(A_1 \langle at \rangle)^\varphi = A_1 \langle at \rangle$ for $A_1 \leq A$ and $a \in A$ is a projectivity from $G$ to $\overline{G}$.

3. Let $p$ be a prime and $2 \leq n \in \mathbb{N}$. If $H$ and $K$ are nonabelian groups in $P(n,p)$ and $P$ is a $p$-group, show that $P \times H$ and $P \times K$ are lattice-isomorphic.

4. Let $G$ be a finite group such that any two different maximal subgroups of $G$ intersect trivially. Show that $G$ is cyclic of prime power order or a semidirect product of an elementary abelian normal subgroup $A$ by a group of prime order operating irreducibly on $A$.

5. Give an alternate proof of Theorem 2.2.6 (avoiding Maschke's Theorem). Show by induction that $|G : \Phi(G)| = p^2$ and $|\Phi(G)| = p$ if $\Phi(G) \neq 1$. Then study the conjugacy classes of subgroups of order $p$ of $P^\varphi$.

6. Illustrate Theorem 2.2.6 by the following examples. That is, without using 2.2.6, show that for primes $p$ and $q$ with $q \mid p - 1$, the groups $G$ and $\overline{G}$ are not lattice-isomorphic if
   (a) $G = C_{p^2} \times C_p$ and $\overline{G}$ is the semidirect product of $C_{p^2}$ by $C_q$ to an automorphism of order $q$ of $C_{p^2}$,
   (b) $G$ is nonabelian of order $p^3$ and exponent $p$, and $\overline{G} = C_p \times H$ where $H$ is nonabelian of order $pq$, and
   (c) $G$ is as in (b), $\overline{G} = \langle a, b, c | a^p = b^p = c^q = 1, ab = ba, c^{-1}ac = a^r, c^{-1}bc = b^{r^2} \rangle$ where $r$ is an integer such that $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$.

7. Show that a finite group is lattice-isomorphic to a nilpotent group if and only if it is a direct product of $p$-groups and $P$-groups with relatively prime orders.

**2.3 Finite $p$-groups with modular subgroup lattices**

In this section and the one following we wish to determine all groups with modular subgroup lattices, called $M$-groups for short. We start with the most difficult part of this program and describe first the finite $p$-groups with this property. So, in this
2.3 Finite $p$-groups with modular subgroup lattices

section, $p$ is a prime and every $p$-group considered is finite. Our aim is to prove the following result.

2.3.1 Theorem (Iwasawa [1941]). A finite $p$-group $G$ has modular subgroup lattice if and only if

(a) $G$ is a direct product of a quaternion group $Q_8$ of order 8 with an elementary abelian 2-group, or

(b) $G$ contains an abelian normal subgroup $A$ with cyclic factor group $G/A$; further there exists an element $b \in G$ with $G = A\langle b \rangle$ and a positive integer $s$ such that $b^{-1}ab = a^{1+ps}$ for all $a \in A$, with $s \geq 2$ in case $p = 2$.

The proof of Iwasawa's theorem will occupy nearly the whole section. In 2.3.3 we shall present a useful criterion for a $p$-group to have modular subgroup lattice. From this it will easily follow that the groups in 2.3.1 are $M$-groups. The converse, however, is much deeper. We first study $p$-groups with modular subgroup lattices in which the quaternion group $Q_8$ is involved, and show in 2.3.8 that they are the groups in (a) of Theorem 2.3.1. Recall that a group is called hamiltonian if it is nonabelian and all of its subgroups are normal. By 2.1.4, these groups have modular subgroup lattices, so the hamiltonian $p$-groups have to show up in Iwasawa's theorem. We shall see in 2.3.12 that they are also exactly the groups in (a) of Theorem 2.3.1. Therefore it remains to consider $p$-groups with modular subgroup lattices in which $Q_8$ is not involved, or which are not hamiltonian. We call these $M^*$-groups and establish a number of important properties that will also be used in later sections, the most noteworthy being 2.3.10, 2.3.11, 2.3.14 and 2.3.16. These properties, of course, can also be proved as soon as one knows that the groups satisfy (b) of Theorem 2.3.1; however, they are not obvious consequences of Iwasawa's theorem and we need them in the proof of it. This proof will finally distinguish the two cases that there exists a cyclic normal subgroup $X$ in the $M^*$-group $G$ such that $|X| = \text{Exp} G$, in which case we get the desired structure for $G$ quite easily (2.3.15), and that there is no such $X$, where the computations become a little more involved (2.3.18). In both cases additional information will be obtained on how to choose the subgroup $A$, the element $b$ and the integer $s$ in Iwasawa's theorem. That these are not uniquely determined by $G$ is shown by the abelian groups, for example. There any integer $s \geq 2$ with $p^s \geq \text{Exp} G$ and every subgroup $A$ and element $b$ with $G = A\langle b \rangle$ will satisfy (b) of 2.3.1.

We start with an elementary remark. If $H$ and $K$ are subgroups of a $p$-group $G$ such that $[K/H/K] \cong [K/H \cap K]$, then $|H \cup K : K| = p^n = |K : H \cap K|$, where $n$ is the length of any of the two isomorphic intervals, and hence $HK = H \cup K = KH$. So 2.1.5 and 2.1.3 yield the following result.

2.3.2 Lemma. A finite $p$-group has modular subgroup lattice if and only if any two of its subgroups permute.

The groups of order $p^3$ are well-known. The dihedral group and the nonabelian group of exponent $p$ for $p > 2$ are generated by two elements of order $p$ and therefore, by 2.2.4, cannot be $M$-groups. In the other groups of order $p^3$ any two elements
of order \( p \) commute and every subgroup of order \( p^2 \) is normal. By 2.3.2, these groups are \( M \)-groups. For an arbitrary \( p \)-group, the sections of order \( p^3 \) decide whether it has modular subgroup lattice or not.

**2.3.3 Lemma.** Let \( G \) be a finite \( p \)-group. Then \( G \) has modular subgroup lattice if and only if each of its sections of order \( p^3 \) does. Therefore if \( G \) is not an \( M \)-group, then there exist subgroups \( H, K \) of \( G \) with \( K \leq H \) such that \( H/K \) is dihedral of order 8 or nonabelian of order \( p^3 \) and exponent \( p \) for \( p > 2 \).

**Proof.** The second assertion follows from the first as our remarks on groups of order \( p^3 \) show. And since sublattices of modular lattices are modular, one part of the first assertion is trivial. So we have to show that \( G \) has modular subgroup lattice if every section of order \( p^3 \) does. We choose a minimal counterexample \( G \) to this statement. Then every proper section of \( G \) is an \( M \)-group. Since \( G \) is not an \( M \)-group, there exist subgroups \( H \) and \( K \) of \( G \) with \( HK \neq KH \); choose \( H \) and \( K \) so that \( |H|\cdot|K| \) is minimal. If \( H_1 \) and \( K_1 \) are maximal subgroups of \( H \) and \( K \), respectively, then \( H_1K_1 = K_1H_1, \) \( H_1K = KH_1 \) and \( HK_1 = K_1H \). For \( X = HK_1 \) and \( Y = H_1K \), it follows that \( HK = HH_1K_1K = KH_1H_1K = XY \) and \( KH = K_1H_1K = YX \). Thus \( X \neq Y \), and furthermore

\[
|X : X \cap Y| = |HK_1 : H_1K_1| = |H : H \cap H_1K_1| \leq |H : H_1| = p.
\]

Similarly \( |Y : Y \cap X| \leq p \) and hence \( X \cap Y \leq X \cap Y \). Since all proper sections of \( G \) are \( M \)-groups, \( X \cap Y = 1 \). In particular, \( |X| = |Y| = p \). If \( N \) is a minimal normal subgroup of \( G \), then, since \( |N| = p \) and \( XY \neq YX \), we see that \( XN/N \) and \( YN/N \) are different subgroups of order \( p \) generating the \( M \)-group \( G/N \). By 2.2.4, \( |G/N| = p^2 \) and hence \( |G| = p^3 \). But then by assumption, \( G \) is an \( M \)-group, a contradiction.

As an easy application of 2.3.3 we get the following criterion.

**2.3.4 Lemma.** Let \( G \) be a finite \( p \)-group and let \( A \) be an abelian subgroup of \( G \) such that every subgroup of \( A \) is normal in \( G \) and \( G/A \) is cyclic. If \( p = 2 \) and \( \text{Exp} \ A \geq 4 \), assume further that there exist subgroups \( A_2 \leq A_1 \) of \( A \) with \( A_1/A_2 \cong C_4 \) and \( [A_1, G] \leq A_2 \). Then \( G \) is an \( M \)-group.

**Proof.** We use induction on \( |G| \). Since \( G/A \) is cyclic, there exists \( b \in G \) with \( G = A \langle b \rangle \). By 1.5.4, \( b \) induces a universal power automorphism on \( A \); that is, there exists an integer \( k \) such that \( b^{-1}ab = a^k \) for all \( a \in A \). If \( p = 2 \) and \( \text{Exp} \ A \geq 4 \), our assumption implies that \( k \equiv 1 \) (mod 4) and so every element of \( A \) with order at most 4 lies in the centre of \( G \). Thus if \( H \) is a proper subgroup of \( G \), every subgroup of \( A \cap H \) is normal in \( H \), and \( H/A \cap H \cong AH/A \) is cyclic; also, if \( p = 2 \) and \( \text{Exp} \ A \cap H \geq 4 \), there exist \( 1 = A_2 < A_1 \leq A \cap H \) such that \( A_1 \cong C_4 \) and \( [A_1, H] \leq [A_1, G] = 1 \). By induction, \( L(H) \) is modular. So if \( G \) were not an \( M \)-group, then by 2.3.3 there would exist a normal subgroup \( N \) of \( G \) with \( G/N \cong D_6 \) or \( G/N \) nonabelian of order \( p^3 \) and exponent \( p \) for \( p > 2 \). Since \( G/AN \) is cyclic, we have \( |G : AN| \leq p \) in both cases. But
every subgroup of $AN/N$ is normal in $G/N$, and this implies that $p = 2$ and $AN/N$ is the cyclic subgroup of order 4 in the dihedral group $G/N$. Hence $A/A \cap N \simeq C_4$ and by assumption, $[A, G] \leq A \cap N$. It follows that $[AN, G] \leq N$, a contradiction. Thus $G$ is an $M$-group.

It will follow immediately from Lemma 2.3.4 that the groups in Theorem 2.3.1 are $M$-groups. We turn to the proof of the more difficult part of this theorem. Recall the definition, for an arbitrary $p$-group $G$ and $i \in \mathbb{N}$, of the characteristic subgroups

$$\Omega_i(G) = \langle x \in G | x^{p^i} = 1 \rangle \quad \text{and} \quad \Omega_i(N) = \langle x^{p^i} | x \in G \rangle;$$

we put $\Omega(G) = \Omega_1(G)$. By 1.2.7, $\Omega_i(G)^p = \Omega_i(\bar{G})$ and $\Omega_i(G)^p = \Omega_i(\bar{G})$ for every projectivity $\phi$ from $G$ to a $p$-group $\bar{G}$.

23.5 Lemma. If $G$ is a finite $p$-group with modular subgroup lattice, then $\Omega(G)$ is elementary abelian and $\Omega_i(G) = \{x \in G | x^{p^i} = 1\}$ for all $i \in \mathbb{N}$.

Proof. Let $P = \{x \in G | x^p = 1\}$. If $x$ and $y$ are nontrivial elements of $P$ with $\langle x \rangle \neq \langle y \rangle$, then by 2.3.2, $\langle x, y \rangle$ is elementary abelian of order $p^2$ and hence $xy^{-1} \in P$ and $xy = yx$. This clearly also holds if $\langle x \rangle = \langle y \rangle$. Thus $P$ is an abelian subgroup of $G$, and therefore $\Omega_i(G) = P$ is elementary abelian. This is the first assertion of the lemma and also the case $i = 1$ of the second. So assume that this second statement is true for $i - 1$. Then for $x, y \in G$ with $x^{p^i} = 1 = y^{p^i}$, we have $x^{p^{i-1}} = y^{p^{i-1}} \in \Omega_i(G)$, and by induction applied to $G/\Omega_i(G)$, we get $(xy)^{p^{i-1}} \in \Omega_i(G)$. It follows that $(xy)^p = 1$ and that $\Omega_i(G)$ only contains elements of order at most $p^i$.

We first determine the 2-groups with modular subgroup lattices in which the quaternion group $Q_8$ is involved. We start with a property of modular 2-groups that will be needed later.

23.6 Lemma. If $G$ is a finite 2-group with modular subgroup lattice, then $\Omega_2(G)$ normalizes every subgroup of $G$, that is $\Omega_2(G) \leq N(G)$, the norm of $G$.

Proof. We use induction on $|G|$. Let $H$ be a nontrivial subgroup of $G$ and let $Z = \langle z \rangle$ be a normal subgroup of order 2 of $H$. By 2.3.2, if $x \in \Omega_2(G)$, then $|\langle x, z \rangle : \langle x \rangle| \leq 2$ and hence $\langle x \rangle^z = \langle x \rangle$. If $z$ did not centralize $x$, then $x^z = x^{-1}$ and $\langle x, z \rangle$ would be a dihedral group of order 8; but this is not an $M$-group. Therefore $\langle x, z \rangle$ is abelian and it follows that $Z \leq H\Omega_2(G)$. The group $H\Omega_2(G)/Z$ has smaller order than $G$, hence by induction, $H/Z$ is normalized by $\Omega_2(H\Omega_2(G)/Z)$ and this group contains $\Omega_2(G)Z/Z$. Thus $\Omega_2(G)$ normalizes $H$.

23.7 Lemma. If $G$ is a finite $M$-group of exponent 4, then $G$ is abelian or $G = Q \times A$ where $Q \simeq Q_8$ and $A$ is elementary abelian.

Proof. Suppose that $G$ is not abelian, let $x, y \in G$ with $xy \neq yx$ and put $Q = \langle x, y \rangle$. By 2.3.6, every subgroup of $G$ is normal in $G$. Hence $1 \neq [x, y] \in \langle x \rangle \cap \langle y \rangle$ and so
Since the dihedral group $D_8$ is not an $M$-group, $Q \cong Q_8$. As a subgroup of $\text{Pot } Q$, $G/C_G(Q)$ is modular of order at most 4. On the other hand, $Q = QC_G(Q)$. For $c \in C_G(Q)$, we have $(xc)^p = x^{-1}c \not= xc$ and since $o(xc) \leq 4$, it follows that $x^{-1}c = (xc)^p = (xc)^{-1} = x^{-1}c^{-1}$. Thus $c^2 = 1$ and $C_G(Q)$ is elementary abelian. Then $G = Q \times A$ where $A$ is a complement to $Z(Q)$ in $C_G(Q)$.

2.3.8 Theorem. Let $G$ be a finite 2-group with modular subgroup lattice. If the quaternion group $Q_8$ is involved in $G$, that is, if there exist $K \leq H \leq G$ with $H/K \cong Q_8$, then $G = Q \times A$ where $Q \cong Q_8$ and $A$ is elementary abelian.

Proof. We use induction on $|G|$ to show that $\text{Exp } G = 4$. Then the theorem will follow from 2.3.7. So suppose that $\text{Exp } G > 4$ and take $u \in G$ with $o(u) = 8$. Assume first that there exists a proper subgroup of $G$ in which $Q_8$ is involved. Then by induction, $Q_8$ is a subgroup of $G$ and hence of $\Omega_2(G)$. By 2.3.7, $\Omega_2(G) = Q \times A$ where $Q \cong Q_8$ and $A$ is elementary abelian. Since $u^2 \in \Omega_2(G)$, there exist $x \in Q$ and $a \in A$ with $o(x) = 4$ and $u^2 = xa$. Let $Q = \langle x, y \rangle$. Then $u^4 = x^2 = y^2$, hence $\langle u^4 \rangle = \langle Q, u \rangle$ and, by 2.3.6 applied to $\langle Q, u \rangle/\langle u^4 \rangle$, it follows that $\langle y \rangle^x = \langle y \rangle$. Since $o(y) = 4$, $y^u = y^a = y^{-1}$, a contradiction.

We are left with the case that $Q_8$ is not involved in any proper subgroup of $G$. Since $Q_8$ is involved in $G$, there exists $N \trianglelefteq G$ with $G/N \cong Q_8$. As $\text{Exp } G > 4$, $N \neq 1$ and we take a minimal normal subgroup $Z$ of $G$ contained in $N$. By induction, $Q_8$ is a subgroup of $G/Z$ and, since it cannot be a proper subgroup, $G/Z \cong Q_8$. Thus $Z = N$ and $|G| = 16$. Since $L(D_8)$ is not modular and $Q_8$ is not a subgroup of $G$, every subgroup of order 8 of $G$ is abelian. Since $G/N \cong Q_8$, we see that $N \leq \langle u \rangle$ and $\langle u^2 \rangle$ is the intersection of abelian maximal subgroups of $G$; thus $\langle u^2 \rangle \leq Z(G)$. On the other hand there exists $v \in G$ with $G/N = \langle uN, vN \rangle$ and $u^v = u^{-1}z$ for some $z \in N$, and it follows that $(u^2)^v = u^{-2}$. This contradiction shows that $\text{Exp } G = 4$. □

M*-groups

We say that a finite $p$-group $G$ is an $M^*$-group if $L(G)$ is modular and the quaternion group $Q_8$ is not involved in $G$. Thus for $p > 2$, every $p$-group with modular subgroup lattice is an $M^*$-group. Furthermore, every subgroup and every factor group of an $M^*$-group is an $M^*$-group. We want to show that every $M^*$-group satisfies (b) of Theorem 2.3.1; in view of 2.3.8 this will finish the proof of that theorem. We start with a useful remark on cyclic permutable subgroups of maximal order in arbitrary $p$-groups.

2.3.9 Lemma. If $X$ is a cyclic permutable subgroup of the $p$-group $G$ such that $|X| = \text{Exp } G$, then $\Omega(X) \leq Z(G)$.

Proof. Let $y \in G$ and $Y = \langle y \rangle$. If $y \in X$, then $y$ clearly centralizes $\Omega(X)$. So assume that $y \notin X$ and let $N$ be a maximal subgroup of $XY$ containing $X$. Then $N \trianglelefteq XY$, and $|N| = |X| = \text{Exp } G$. Then $X \cap N$ is abelian and of maximal order in $N$. But $X \cap N$ is also a cyclic permutable subgroup of $G$; hence $X \cap N \leq \Omega(G) \leq Z(G)$. □
2.3 Finite p-groups with modular subgroup lattices

hence \( X^p \leq N \) and therefore

\[
|X : X \cap X^p| = |XX^p : X^p| < |XY : X^p| = |XY : X| = |Y : X \cap Y|.
\]

Since \( |X| = \text{Exp} G \), we have \( |Y : X \cap Y| \leq |X| \) and it follows that \( X \cap X^p \neq 1 \). But then the minimal subgroup of \( X \cap X^p \) is \( \Omega(X) \) and also \( \Omega(X^p) \), and we get that \( \Omega(X) = \Omega(X^p) = \Omega(X)^p \). Since \( \Omega(X) \) is of order \( p \), it is centralized by \( y \). Thus \( \Omega(X) \leq Z(G) \).

2.3.10 Lemma. Let \( G \) be an \( M^* \)-group of exponent \( p^n \). Then the map \( \sigma \) defined by \( x^\sigma = x^{p^n - 1} \) for \( x \in G \) is a homomorphism from \( G \) to \( \Omega(Z(G)) \).

Proof. That \( x^\sigma \in \Omega(Z(G)) \) for all \( x \in G \) follows from 2.3.9. So we have to show that \( (xy)^{p^n - 1} = x^{p^n - 1} y^{p^n - 1} \) for all \( x, y \in G \), and we do this by induction on \( n \).

The case \( n = 1 \) being trivial, assume first that \( n = 2 \). Then if \( p = 2 \), \( G \) is abelian by 2.3.7. For \( p > 2 \), we let \( H = \langle x, y \rangle \) and show that \( H' \leq \Omega(H) \cap Z(H) \). This is clear if \( |H| \leq p^3 \). And if \( |H| > p^3 \), then \( o(x) = o(y) = p^2 \) and thus \( \Omega(\langle x \rangle) \Omega(\langle y \rangle) \leq Z(H) \) by 2.3.9. Furthermore \( H/\Omega(\langle x \rangle) \Omega(\langle y \rangle) \) is generated by two elements of order \( p \) and hence is abelian. Therefore once again \( H' \leq \Omega(H) \cap Z(H) \) and by (4) of 1.5,

\[
(xy)^p = x^p y^p [y, x]^{(p)} = x^p y^p.
\]

Finally, let \( n \geq 3 \) and assume that the formula is correct for \( n - 1 \). By 2.3.5, \( G/\Omega(G) \) is an \( M^* \)-group of exponent \( p^{n-1} \) and it follows that \( (xy)^{p^{n-2}} = x^{p^{n-2}} y^{p^{n-2}} z \) where \( z \in \Omega(G) \). Since \( x^{p^{n-2}}, y^{p^{n-2}} \) and \( z \) are contained in the \( M^* \)-group \( \Omega_2(G) \) of exponent \( p^2 \), the first part of our proof yields that

\[
(xy)^{p^{n-1}} = (x^{p^{n-2}} y^{p^{n-2}} z)^p = x^{p^{n-1}} y^{p^{n-1}} z^p = x^{p^{n-1}} y^{p^{n-1}}.
\]

The last two results suggest studying elements of maximal order in \( M^* \)-groups. In abelian \( p \)-groups, a fundamental property of such elements is that they generate direct factors. A similar result holds in \( M^* \)-groups.

2.3.11 Lemma. Let \( X \) be a cyclic subgroup of the \( M^* \)-group \( G \) such that \( |X| = \text{Exp} G \). If \( H \leq G \) with \( H \cap X = 1 \), then there exists a complement \( C \) of \( X \) in \( G \) containing \( H \), that is, a subgroup \( C \) of \( G \) such that \( G = XC \), \( X \cap C = 1 \) and \( H \leq C \).

Proof. We use induction on \( |G| \). If \( H \) contains a nontrivial normal subgroup \( N \) of \( G \), then \( XN/N \) is cyclic of maximal order in \( G/N \) and \( XN \cap H = N(X \cap H) = N \). By induction there exists a subgroup \( C \) of \( G \) containing \( N \) and \( H \) such that \( G = XNC \) and \( XN \cap C = N \). Hence \( G = XC \) and \( X \subseteq C \subseteq XN \cap C = XN \cap N = 1 \), that is, \( C \) has the desired properties.

Now let \( H_G = 1 \) and suppose first that there exists a normal subgroup \( Z \) of \( G \) such that \( |Z| = p \) and \( Z \cap X = 1 \); let \( K = HZ \). If \( K \cap X \neq 1 \), then \( \Omega(X) \leq K \) and hence \( \Omega(X)Z \) is an elementary abelian subgroup of \( K \) of order \( p^2 \), which, by 2.3.9, is contained in \( Z(G) \). Since \( |K : H| \leq p \), it would follow that \( 1 \neq H \cap \Omega(X)Z \leq Z(G) \),
contradicting \( H_G = 1 \). Thus \( K \cap X = 1 \), and the first part of our proof shows that there exists a complement to \( X \) in \( G \) containing \( K \) and hence also \( H \).

Finally assume that \( \Omega(Z(G)) \leq X \), let \( p^n = \text{Exp} \, G \) and put \( L = \Omega_{n-1}(G) \). Then \( |\Omega(Z(G))| = p \) and hence \( |G : L| = p \) since \( L \) is the kernel of the homomorphism \( g \mapsto g^{p^n-1} (g \in G) \) defined in 2.3.10. It follows that \( G = XL \). For \( h \in H \), we have \( h^{p^n-1} \in H \cap \Omega(Z(G)) = 1 \) and hence \( H \leq L \). Since \( X \cap L \) is cyclic of maximal order \( p^n-1 \) in \( L \), by induction there exists a subgroup \( C \) of \( L \) such that \( L = (X \cap L)C \), \( X \cap L \cap C = 1 \) and \( H \leq C \). Then \( G = XL = XC \) and \( X \cap C = 1 \), that is, \( C \) has the desired properties.

Hamiltonian \( p \)-groups

2.3.12 Theorem. All the subgroups of a finite \( p \)-group \( G \) are normal if and only if \( G \) is abelian or \( G = Q \times A \) where \( Q \simeq Q_8 \) and \( A \) is an elementary abelian 2-group.

Proof. If \( G \) is such a direct product, then the elements of order 2 in \( G \) are contained in \( Z(G) \) and subgroups of exponent 4 contain \( Z(Q) = G' \). Hence every subgroup of \( G \) is normal. Conversely, suppose that \( G \) is a hamiltonian \( p \)-group. We show by induction that \( G \) has the desired structure. By 2.1.4, \( G \) is an \( M \)-group. If \( G \) were an \( M^* \)-group, then for a cyclic subgroup \( X \) of maximal order in \( G \), by 2.3.11 there would exist a subgroup \( C \) of \( G \) such that \( G = X \times C \). Since \( G \) is not abelian, \( C \) would be hamiltonian and, by induction, \( Q_8 \) would be involved in \( C \), a contradiction. Thus \( G \) is not an \( M^* \)-group and by 2.3.8, \( G \) has the desired structure.

The structure of arbitrary hamiltonian groups is well-known (see Robinson [1982], p. 139), and is described in Exercise 1. Theorems 2.3.8 and 2.3.12 show that a \( p \)-group is an \( M^* \)-group if and only if it is a nonhamiltonian \( M \)-group. So these two notions are the same and we introduce a third, related one.

Iwasawa triples

The triple \((A, b, s)\) is called an Iwasawa triple for the \( p \)-group \( G \) if \( A \) is an abelian normal subgroup of \( G \), \( b \in G \) and \( s \) is a positive integer which is at least 2 in case \( p = 2 \) such that \( G = A\langle b \rangle \) and \( b^{-1}ab = a^{1+p^s} \) for all \( a \in A \). To finish the proof of Iwasawa’s theorem, we have to show that every \( M^* \)-group possesses an Iwasawa triple. We start with a sufficient condition for the existence of such a triple.

2.3.13 Lemma. Let \( A \) be a subgroup of the \( M^* \)-group \( G \) such that every subgroup of \( A \) is normal in \( G \).

(a) Then \( A \) is abelian and \( G/C_G(A) \) is cyclic.

(b) If \( \text{Exp} \, A \neq 4 \) and \( B \) is a cyclic subgroup of \( G \), then there exist a generator \( b \) of \( B \) and an integer \( s \) such that \((A, b, s)\) is an Iwasawa triple for \( AB \).
Proof. By 2.3.12, $A$ is abelian since $Q_8$ is not involved in $G$. Furthermore, the elements of $G$ induce power automorphisms on $A$ which are universal by 1.5.4. So if $x \in A$ with $o(x) = \text{Exp } A = p^n$, then $C_G(A) = C_G(\langle x \rangle)$ and hence $G/C_G(A)$ is isomorphic to a subgroup of $\text{Aut}(\langle x \rangle)$.

If $p > 2$, $\text{Aut}(\langle x \rangle)$ is cyclic of order $p^{n-1}(p - 1)$ and for $s = 1, \ldots, n$, the subgroup of order $p^{s-1}$ of $\text{Aut}(\langle x \rangle)$ is generated by the automorphism $\alpha$ with $x^s = x^{1+p^s}$ (see Huppert [1967], p. 84). In particular, (a) holds in this case. Furthermore, $|B/C_B(\langle x \rangle)| = p^{n-s}$ for some $s \in \{1, \ldots, n\}$, and hence there exists $b \in B$ such that $B = \langle b \rangle$ and $x^b = x^{1+p^s}$. Since $b$ operates as a universal power automorphism on $A$ and $o(x) = \text{Exp } A$, it follows that $a^b = a^{1+p^s}$ for all $a \in A$. Thus $(A, b, s)$ is an Iwasawa triple for $AB$.

Now assume that $p = 2$ and $n \geq 3$. Then $\text{Aut}(\langle x \rangle) = \langle \beta \rangle \times \langle \gamma \rangle$ where $x^\beta = x^{-1}$ and $x^\gamma = x^5$. Suppose that some element $g \in G$ induces an automorphism in $\langle x \rangle$ that does not lie in $\langle \gamma \rangle$. Then every section of order 4 of $\langle x \rangle$ is inverted by $g$. It follows that $|\langle x \rangle \cap \langle g \rangle| \leq 2$ and hence $\langle x \rangle \cap \langle g \rangle \leq \langle x^4 \rangle$. By 2.3.6 applied to $G/\langle x^4 \rangle$, $\langle g, x^4 \rangle$ is normalized by $x$ and there exists $h \in \langle x \rangle \cap \langle x^4 \rangle \langle g \rangle = \langle x^4 \rangle$. Thus $\langle x \rangle/\langle x^4 \rangle$ is centralized by $g$, a contradiction. This shows that $G/C_G(A)$ is isomorphic to a subgroup of $\langle \gamma \rangle$, that is, (a) holds. And since the subgroups of $\langle \gamma \rangle$ are generated by the automorphisms $\delta$ such that $x^\delta = x^{1+p^s}$ for $2 \leq s \leq n$, statement (b) also follows as in the case $p > 2$.

Finally, if $p = 2$ and $n \leq 2$, then $|\text{Aut}(\langle x \rangle)| \leq 2$. In particular, $G/C_G(A)$ is cyclic. If $\text{Exp } A \neq 4$, it follows that $A \leq Z(G)$ and then for every generator $b$ of $B$, $(A, b, 2)$ is an Iwasawa triple for $AB$. 

If $\text{Exp } A = 4$ in 2.3.13, $A$ need not be a member of an Iwasawa triple for $AB$ (see Exercise 4). It is not difficult to determine the structure of $AB$ in this case (see Exercise 5). However, we shall not need this in our proof of Iwasawa's theorem since we can use 2.3.6 if $\text{Exp } A = 4$.

2.3.14 Lemma. Let $G$ be an $M^*$-group, $X$ a cyclic subgroup of $G$ with $|X| = \text{Exp } G$ and suppose that $H \leq G$ such that $H \cap X = 1$.

(a) If $H^X = H$, then every subgroup of $H$ is normal in $G$.

(b) $H/H_G$ is cyclic.

Proof. (a) Let $X = \langle x \rangle$ and $p^n = o(x) = \text{Exp } G$. By 2.3.11 there exists a complement $C$ to $X$ in $G$ with $H \leq C$. Every $g \in G$ therefore has the form $g = x^iy$ where $i \in \mathbb{N}$, $y \in C$, and it follows that $H^x = H^y \leq C$. Thus the normal closure $H^G$ of $H$ is contained in $C$. Therefore, if $K \leq H$ and $g \in G$ with $\langle g \rangle \cap C = 1$, then $K = K(\langle g \rangle \cap H^G) = K\langle g \rangle \cap H^G \leq K\langle g \rangle$.

that is, $g \in N_G(K)$. In particular, $x \in N_G(K)$. And for $y \in C$, by 2.3.10, $(xy)^{p^n-1} = x^{p^n-1+y^{p^n-1}} \notin C$. Thus $\langle xy \rangle \cap C = 1$, hence $xy \in N_G(K)$ and therefore $y \in N_G(K)$. It follows that $N_G(K) \geq XC = G$.

(b) Since our assumptions are inherited by $G/H_G$, we may assume that $H_G = 1$. Then by (a), $C_H(X) = 1$ and hence $N_H(X)$ is cyclic by 2.3.13, (a). On the other hand,
every minimal subgroup $K$ of $H$ normalizes $X$ since $|XK : X| = |K| = p$. Thus $H$ has only one minimal subgroup and therefore is cyclic since $Q_8$ is not involved in $G$.  

2.3.15 Theorem. Let $G$ be an $M^*$-group and suppose that $X$ is a cyclic normal subgroup of $G$ with $|X| = \text{Exp } G$. Then every subgroup of $C_G(X)$ is normal in $G$ and $G/C_G(X)$ is cyclic. If $G = C_G(X)B$ where $B$ is cyclic, then there exists a generator $b$ of $B$ and an integer $s$ such that $(C_G(X), b, s)$ is an Iwasawa triple for $G$.

Proof. By 2.3.13, $G/C_G(X)$ is cyclic. If $C$ is a complement to $X$ in $G$, then $C_G(X) = XC \cap C_G(X) = X \times C_0$ where $C_0 = C \cap C_G(X)$. Let $g \in G$ and $X = \langle x \rangle$. Since $X \triangleleft G$, there exists an integer $r$ such that $x^r = x_0$. For $c \in C_0$ take $y \in X$ with $o(y) = o(c)$. Then $\langle y, c \rangle = \langle y \rangle \times \langle c \rangle$ is abelian and $\langle yc \rangle \cap X = 1 = \langle c \rangle \cap X$. By 2.3.14, $\langle yc \rangle$ and $\langle c \rangle$ are normal subgroups of $G$. Since $y \in X \triangleleft G$, also $\langle y \rangle \triangleleft G$ and by 1.5.4, $g$ induces a universal power automorphism in $\langle y, c \rangle$. Hence $c^g = c'$ and it follows that $a^g = a'$ for all $a \in C_G(X) = X \times C_0$. Thus every subgroup of $C_G(X)$ is normal in $G$. By 2.3.13, $G$ has the desired structure except, possibly, when $\text{Exp } C_G(X) = 4$. But then $\text{Exp } G = o(x) = 4$, $G$ is abelian by 2.3.7 and the assertion holds trivially.  

Of course, $C_G(X)$ is abelian in 2.3.15. In particular, as a useful consequence, we note the following.

2.3.16 Corollary. If $G$ is an $M^*$-group containing an element $z \in Z(G)$ with $o(z) = \text{Exp } G$, then $G$ is abelian.

Theorem 2.3.15 shows how to find an Iwasawa triple in the $M^*$-group $G$ if there exists a cyclic subgroup $X$ of maximal order that is normal in $G$: one can take $C_G(X)$ as the abelian normal subgroup $A$. If there is no such $X$, we cannot describe $A$ so easily. Furthermore, we have to do some unpleasant calculations.

2.3.17 Lemma. Let $L = \langle x, a \rangle$ be an $M^*$-group, $X = \langle x \rangle$, $o(a) < o(x) = \text{Exp } L$ and suppose that $a^s = a'^s x_0$ where $x_0 \in \Omega(X)$ and $s$ is an integer which is at least 2 in case $p = 2$.

(a) If $X$ is not normal in $L$, then $\Omega_{s+1}(X) \subseteq Z(L)$ and there exists $x_1 \in \Omega_{s+1}(X)$ such that $d^s = d'^s$ and $L = \langle x, d \rangle$ where $d = ax_1$.

(b) Suppose that there exists $u \in L$ such that $L = X \langle u \rangle$, $X \cap \langle u \rangle = 1$ and $\langle u \rangle \triangleleft L$. Then $\Omega_{s+1}(X) \subseteq Z(L)$, $u \in \langle a \rangle \Omega_{s+1}(X)$ and $u^s = u'^s$.

Proof. (a) First note that by 2.3.9, $x_0 \in Z(L)$ and therefore $a^x = a^{(1+p^s)x_0^i}$ for all $i \in \mathbb{N}$. Indeed, this is clear by assumption if $i = 1$; and if it is true for some $i \in \mathbb{N}$, then

$$a^{x^{i+1}} = (a^{(1+p^s)x_0^i})^x = (a^x)^{(1+p^s)x_0^i} = a^{(1+p^s)x_0^{i+1}}.$$ 

Let $o(x) = p^n$. Since $X$ is not normal in $L$, $a^p \notin X$ and hence $p^s < o(a) < p^n$, that is, $s < n - 1$. It follows that $(1 + p^s)^{p^{n-s} - 1} \equiv 1$ (mod $p^{n-1}$) and therefore $a^{x^{p^{n-s} - 1}} = a^{(1+p^s)p^{n-s} - 1} x_0^{p^{n-s} - 1} = a$. Thus $\Omega_{s+1}(X) = \langle x^{p^{n-s} - 1} \rangle \subseteq Z(L)$. Finally, $x_0 = x^{p^{n-s} - 1}$ for
some $i \in \mathbb{N}$ and we put $x_1 = x^{ip_{n-1}}$. Then for $d = ax_1$, we clearly have $L = \langle x, a \rangle = \langle x, d \rangle$ and
\[
  d^x = (ax^{ip_{n-1}})^x = a^{1+p^s}x^{ip_{n-1}}x^{ip_{n-1}} = (ax_1)^{1+p^s} = d^{1+p^s}.
\]

(b) By (a), $\Omega_{q+1}(X) \leq Z(L)$ if $X$ is not normal in $L$; and if $X \varsubsetneq L$, then $L = X \times \langle u \rangle$ is even abelian. Since $L/\langle u \rangle \simeq X$ is cyclic, $[a, x] = a^x_0 x_0 \in \langle u \rangle$ and hence $a^{x_0} = (a^x_0 x_0)^P \in \langle a \rangle \cap \langle u \rangle$. Therefore $|\langle a, u \rangle : \langle u \rangle| = |\langle a \rangle : \langle a \rangle \cap \langle u \rangle| \leq p^{s+1}$ and so $\langle a, u \rangle \leq \langle u \rangle \Omega_{s+1}(X)$. Let $u_i \in \langle u \rangle$ and $x_1 \in \Omega_{s+1}(X)$ such that $a = u_i x_1^{-1}$. Then $L = X \langle u \rangle$ and therefore $\langle u \rangle = \langle u_i \rangle \leq \langle a \rangle \Omega_{s+1}(X)$. Finally,
\[
  u_i^x = (ax_1)^x \equiv a^{1+p^s}x_1 \equiv a^{1+p^s}x_1^{1+p^s} = (ax_1)^{1+p^s} = u_i^{1+p^s} \quad (\text{mod } \Omega(X))
\]
and hence $u_i^{1+p^s}(u_i^x)^{-1} \in \Omega(X) \cap \langle u \rangle = 1$. It follows that $u_i^x = u_i^{1+p^s}$ and then also $u^x = u^{1+p^s}$.

2.3.18 Theorem. Let $G$ be an $M^*$-group in which no cyclic subgroup of maximal order is normal. Then there exist a subgroup $A$ of $G$ and an integer $s$ with the property that for every cyclic subgroup $B$ of maximal order in $G$,

(a) there is a generator $b$ of $B$ such that $(A, b, s)$ is an Iwasawa triple for $G$, and

(b) $A$ contains every subgroup $H$ of $G$ that is normalized by $B$ and intersects $B$ trivially.

Proof. We proceed by induction on $|G|$. Let $X$ be a cyclic subgroup of maximal order in $G$ and let $|X| = \text{Exp } G = p^n$. By 2.3.9, $\Omega(X) \leq G$ and hence by induction or 2.3.15 (in the case where there exists a cyclic subgroup of maximal order in $G/\Omega(X)$ that is normal), there exists a subgroup $S/\Omega(X)$ of $G/\Omega(X)$ that is a member of an Iwasawa triple for $G/\Omega(X)$. In particular,

(1) $S/\Omega(X)$ is abelian
and $G/S$ is cyclic; let $t \in G$ with $G = S\langle t \rangle$. If $G \neq SX$, then $SX = S(SX \cap \langle t \rangle) \leq S\langle t^p \rangle$ and hence $at^p$ generates $X$ for some $a \in S$ and $i \in \mathbb{N}$. By 2.3.10, $(at^p)^{p-1} = a^{p-1}t^{ip} = a^{p-1}$ and hence $\Omega(X) \leq \langle a \rangle \leq S$ and $o(a) = p^n$. But then $\langle a \rangle$ would be a cyclic subgroup of maximal order, normal in $G$, a contradiction. Thus

(2) $G = SX$.

Since $X$ is not normal in $G$, 2.3.6 shows that $\text{Exp } (S/\Omega(X)) \neq 4$. By 2.3.13 there exist a generator $x$ of $X$ and an integer $s$ which is at least 2 in case $p = 2$ such that for all $a \in S$,

(3) $a^x = a^{1+p^s}x_a$ where $x_a \in \Omega(X)$.

We want to show next that

(4) $\text{Exp } S < p^n = o(x)$.

In order to obtain a contradiction suppose that there exists an element $a \in S$ with $o(a) = p^n$. Since subgroups $Y$ satisfying $\Omega(X) \leq Y \leq S$ are normal in $G$, we see that
Modular lattices and abelian groups

\( \Omega(X) \not\subseteq \langle a \rangle \) and hence \( X \cap \langle a \rangle = 1 \). Let \( H = \langle X, a \rangle \). Then

\[
(a^p x_a)^y = (a^x)^{p^y} x_a = a^{(1+p^r)p^y} x_a = (a^p x_a)^{1+p^r}
\]

and, as \( a \) centralizes \( a^p x_a \), it follows that \( \langle a^p x_a \rangle \) is abelian and \( H' = \langle a^p x_a \rangle \) is cyclic. It follows that \( H' \cap X = 1 \) or \( H' \cap \langle a \rangle = 1 \). By 2.3.11 there exists a complement \( C \) to \( X \) or \( \langle a \rangle \) in \( H \) containing \( H' \). By 2.3.14, this complement is normal in \( G \) and, by 2.1.5, its subgroup lattice is isomorphic to \( [H/X] \cong L(\langle a \rangle) \) or to \( [H/\langle a \rangle] \cong L(X) \). Hence \( C \) is a cyclic normal subgroup of order \( p^n \) and this contradicts our assumption. Thus (4) holds.

We are now going to construct a subgroup \( A \) of \( G \) that together with the integer \( s \) in (3) satisfies (a) and (b) for \( B = X \); it will then be easy to show that \( A \) and \( s \) also have these properties for arbitrary \( B \). Let \( M \) be a complement to \( X \) in \( G \). If \( g \in G \), then, by (2), there exist \( a \in S \) and \( i \in N \) such that \( g = ax^i \). Then (3) and (4) show that \( L = \langle x, g \rangle = \langle x, a \rangle \) satisfies the assumptions of 2.3.17. Since \( X \) is not normal in \( G \), \( M \) is generated by the elements outside \( NM(X) \). By 2.3.14, \( M/M_0 \) is cyclic and hence there exists an element \( c \in M \setminus NM(X) \) with \( M = M_c \langle c \rangle \). By 2.3.17, \( c \in C_G(\Omega_{s+1}(X)) \) and there exist \( x_1 \in \Omega_{s+1}(X) \) and \( a_1 \in S \) such that for \( d = a_1 x_1, d^x = d^{1+p^r} \) and \( \langle x, c \rangle = \langle x, d \rangle \). Let \(\]

(5) \( A = \langle d, H \mid H \leq G, H \cap X = 1, H^X = H \rangle \).

Then \( AX \geq M_G \langle d \rangle X = M_G \langle c \rangle X = MX \) and hence

(6) \( AX = G \).

We show that any two of the generators of \( A \) given in (5) commute and that they are all mapped by \( x \) to their \((1 + p^r)\)-th power. Then it will be clear that \( A \) is abelian and

(7) \( (A, x, s) \) is an Iwasawa triple for \( G \).

So let \( u \in H \leq G \) where \( H \cap X = 1 \) and \( H^x = H \). By 2.3.14, \( \langle u \rangle \leq G \) and by 2.3.17, \( u \in C_G(\Omega_{s+1}(X)) \), \( u = a_2 x_2 \) for some \( a_2 \in S \) and \( x_2 \in \Omega_{s+1}(X) \) and \( u^x = u^{1+p^r} \). In particular, \( \Omega_{s+1}(X) \) is centralized by \( M_G, c \) and \( X \) and hence lies in the centre of \( G \). Since \( S/\Omega(X) \) is abelian, it follows that

\[
[d, u] = [a_1 x_1, a_2 x_2] = [a_1, a_2] \in \Omega(X) \cap \langle u \rangle = 1.
\]

If \( v \in K \leq G \) where \( K \cap X = 1 \) and \( K^x = K \), then similarly \( v = a_3 x_3 \) with \( a_3 \in S, x_3 \in \Omega_{s+1}(X) \) and \( [u, v] = [a_2, a_3] \in \Omega(X) \cap \langle u \rangle = 1 \). Thus \( A \) is abelian and (7) holds.

Finally, suppose that \( B \) is an arbitrary cyclic subgroup of maximal order in \( G \). By (7), \( B = \langle az \rangle \) where \( a \in A \) and \( z \in X \), and, since there are no cyclic normal subgroups of order \( p^n \) in \( G \), \( o(a) < p^n \). By 2.3.10, \( (az)^{p^{n-1}} = a^{p^{n-1}} z^{p^{n-1}} = z^{p^{n-1}} \) and this implies that \( o(z) = p^n \) and \( \Omega(B) = \Omega(X) \). Thus \( \langle x \rangle = \langle z \rangle \leq AB \) and \( G = AB \). Similarly, if \( \bar{a} \in A \) and \( b \in B \) such that \( x = \bar{a} b \), then \( b \) is a generator of \( B \) and since it induces the same automorphism on \( A \) as \( x \) does, \( (A, b, s) \) is an Iwasawa triple for \( G \). Thus (a) holds. And if \( H \) is a subgroup of \( G \) with \( H \cap B = 1 \) and \( B \leq N_G(H) \), then \( H \leq G \) by 2.3.14 and \( H \cap X = 1 \) since \( \Omega(X) = \Omega(B) \). By (5), \( H \leq A \) and hence (b) too is satisfied.
Iwasawa’s theorem can now be proved; in fact, we only have to quote the results of this section.

**Proof of Theorem 2.3.1.** If $G$ satisfies (a) of 2.3.1, then $G$ is hamiltonian by 2.3.12, and if (b) holds, then 2.3.4 shows that $G$ is an $M$-group. Conversely, let $G$ be a $p$-group with modular subgroup lattice. If the quaternion group $Q_8$ is involved in $G$, then 2.3.8 yields that $G$ satisfies (a) of 2.3.1. And if $G$ is an $M^*$-group, then by 2.3.15 and 2.3.18 there exists an Iwasawa triple for $G$, that is, (b) holds.

A word of warning

There are a number of mistakes in the literature on Iwasawa’s theorem. It starts with Iwasawa [1941], p. 197 where in the proof of his theorem he chooses a certain basis of an abelian group which, in general, does not exist. This gap in the argument is reproduced in Suzuki [1956], p. 16; it was closed in a paper by Napolitani [1967a]. Our method of proof is different. Another mistake that is found, for example, in the papers by Jones [1945], p. 549 and Sato [1951], p. 220 is the claim that an $M^*$-group always has an Iwasawa triple $(A, b, s)$ with $A \cap \langle b \rangle = 1$. However, simple examples show that this is not so.

23.19 Example. Let $p > 2$ and $G = \langle a, x | a^{p^3} = 1, x^{p^3} = a^{p^2}, ax = a^{1+p} \rangle$. Since $a^{p^2}$ is centralized by the automorphism $\sigma$ of $\langle a \rangle$ with $a^\sigma = a^{1+p}$, $G$ is an extension of $\langle a \rangle$ by a cyclic group of order $p^3$. By Iwasawa’s theorem, $G$ is an $M^*$-group of order $p^6$ and has exponent $p^4$ by 2.3.5. Let $\langle x \rangle = X$ and suppose that $Y$ is a cyclic subgroup of order $p^4$ of $G$. Then $|X : X \cap Y| = |XY : Y| \leq p^2$ and hence $X \cap \langle a \rangle = \Omega(X) < X \cap Y$. This implies that $G' = \langle a^p \rangle \not\leq Y$ and since $|G : Y| = p^2$, $Y$ cannot be normal in $G$. Now suppose that $G = AB$ where $B$ is cyclic and every subgroup of $A$ is normal in $G$. Then $\exp A < p^4$ and hence $|B| = p^4$. It follows that $\Omega(X) < B$; but as $G/A$ is cyclic also $\Omega(X) < G' < A$. Thus $A \cap B \neq 1$.

Finally, we mention that in general there are many different Iwasawa triples in a given $M^*$-group. Some examples and results in this direction can be found in Exercises 7–9.

**Characteristic subgroups in $M^*$-groups**

There are a number of interesting results on the existence of certain characteristic subgroups in $M^*$-groups. The following is due to Menegazzo.

23.20 Theorem (Busetto and Menegazzo [1985]). Let $G$ be an $M^*$-group of exponent $p^n$. If $G/\Omega_{n-1}(G)$ is not cyclic, then there exists an abelian characteristic subgroup $A$ of $G$ such that $G/A$ is cyclic and $[G, \text{Aut } G] \leq A$. 


Proof. We choose an Iwasawa triple \((A, b, s)\) for \(G\) such that \(A\) has maximal order. Since \(G/A\) is cyclic and \(G/\Omega_{n-1}(G)\) is not cyclic, \(A < \Omega_{n-1}(G)\) and hence there exists an element \(a \in A\) of order \(p^n\). For every such \(a\), \(\langle a \rangle \leq G\) and \(A \leq C_G(a)\). By 2.3.15, \(C_G(a)\) belongs to an Iwasawa triple for \(G\) and our choice of \(A\) implies that

\((8)\) \(A = C_G(a)\) for all \(a \in A\) with \(o(a) = p^n\).

We want to show that

\((9)\) \(A = \langle X \mid X \leq G, X \text{ cyclic, } |X| = p^n \rangle\).

Since \(A\) is generated by its elements of order \(p^n\), it is certainly contained in the join of all cyclic normal subgroups of order \(p^n\) of \(G\). Conversely, suppose that \(X\) is a cyclic normal subgroup of order \(p^n\) of \(G\). If there exists an element \(a \in A\) of order \(p^n\) with \(\langle a \rangle \cap X = 1\), then \(X \leq C_G(a) = A\) and we are done. So assume that there is no such \(a\). Then \(\Upsilon_{n-1}(A) \leq X\) is cyclic and hence \(\Upsilon_{n-1}(A) = \Omega(X)\). By 2.3.10, \(\Upsilon_{n-1}(G) = \Upsilon_{n-1}(A) \langle b^{p^n-1} \rangle\) is isomorphic to \(G/\Omega_{n-1}(G)\) and therefore is not cyclic. It follows that \(o(b) = p^n\) and \(\langle b \rangle \cap \Upsilon_{n-1}(A) = 1\). Let \(X = \langle x \rangle\) and take \(c \in A\), \(i \in \mathbb{N}\) with \(x = b^i c\). Since

\[1 \neq x^{p^n-1} = b^{i p^n-1} c^{p^n-1} \in \Omega(X) = \Upsilon_{n-1}(A),\]

\(b^{i p^n-1} = 1\) and \(c^{p^n-1} \neq 1\). Thus \(o(c) = p^n\) and \(\Omega(\langle c \rangle) = \Upsilon_{n-1}(A)\). Since \(X \leq G\),

\[[x, b] = [b^i c, b] = [c, b] = c^{p^n} \in X\]

and since \(x\) and \(c\) have the same order, \(\langle c^{p^n} \rangle = \langle x^{p^n} \rangle = \langle b^i c^k \rangle\) for some \(k \in \mathbb{N}\). Hence \(b^i c^k \in \langle b \rangle \cap \langle c \rangle = \langle b \rangle \cap \Upsilon_{n-1}(A) = 1\) and so \(b^i \in \Omega_2(\langle b \rangle)\). Since \(a^b = a^{1+p^n}\) for all \(a \in A\) and \(\text{Exp } A = p^n = o(b)\), it follows that \(\Omega_2(\langle b \rangle) \leq C_G(A) = A\). Thus \(x = b^i c \in A\) and (9) holds.

In particular, \(A\) is a characteristic subgroup of \(G\). Hence for \(x \in \text{Aut } G\) and \(a \in A\) with \(o(a) = p^n\), \(a^x \in A\) and

\[(a^x)^{b^x} = (a^b)^x = (a^{1+p^n})^x = (a^x)^{1+p^n} = (a^x)^b.\]

Thus \(b^{-1} b^x \in C_G(a^x) = A\) by (8). It follows that \(G/A\) is centralized by \(x\) and hence that \([G, \text{Aut } G] \leq A\).

We mention an obvious consequence of Menegazzo's theorem that will be used later.

2.3.21 Corollary. Let \(N\) be an \(M^*\)-group of exponent \(p^n\) such that \(N/\Omega_{n-1}(N)\) is not cyclic. If \(N\) is contained as a normal subgroup with cyclic factor group in a group \(G\), then \(G\) is metabelian.

Proof. By 2.3.20 there exists an abelian characteristic subgroup \(A\) of \(N\) such that \(N/A\) is cyclic and \([N, \text{Aut } N] \leq A\). Then \(A \leq G\) and \(N/A\) is a central subgroup of \(G/A\) with cyclic factor group. It follows that \(G/A\) is abelian. \(\square\)
Another immediate application of Menegazzo’s theorem is an older result of v.d. Waall’s.

2.3.22 Theorem (v.d. Waall [1973]). Every nonabelian $M^*$-group has a characteristic maximal subgroup.

Proof. Let $G$ be a nonabelian $M^*$-group of exponent $p^n$. If $G/O_{n-1}(G)$ is cyclic, then $O_{n-1}(G)$ is a characteristic maximal subgroup of $G$. If $G/O_{n-1}(G)$ is not cyclic, then by 2.3.20 there exists an abelian characteristic subgroup $A$ of $G$ with cyclic factor group. Since $G$ is not abelian, $A \neq G$ and the maximal subgroup of $G$ containing $A$ is characteristic in $G$.

2.3.23 Theorem (Seitz and Wright [1969]). Let $G$ be a nonabelian $M^*$-group. Then there exist (characteristic) subgroups $R$ and $S$ of $G$ such that $\Phi(G) \leq S < R$ and $[R, \text{Aut } G] \leq S$.

Proof. We proceed by induction on $|G|$. Suppose first that there exists a nontrivial characteristic subgroup $K$ of $G$ such that $G' \leq K$. Then $G/K$ is a nonabelian $M^*$-group and by induction there are subgroups $R/K$ and $S/K$ of $G/K$ such that $\Phi(G/K) \leq S/K < R/K$ and $[R/K, \text{Aut}(G/K)] \leq S/K$. Hence $\Phi(G) \leq S < R$ and since every automorphism of $G$ induces an automorphism in $G/K$, it follows that $[R, \text{Aut } G] \leq S$. So we are done in this case and therefore may assume that

(10) $G'$ is the only minimal characteristic subgroup of $G$.

Let $\text{Exp } G = p^n$. If $G/O_{n-1}(G)$ is not cyclic, then by 2.3.20 there exists an abelian characteristic subgroup of $G$ such that $[G, \text{Aut } G] \leq A$. Then $R = G$ and a maximal subgroup $S$ of $G$ containing $A$ have all the desired properties. So let $G/O_{n-1}(G)$ be cyclic, that is, $|G : O_{n-1}(G)| = p$. By 2.3.10, $|O_{n-1}(G)| = p$ and since $G'$ is the only minimal characteristic subgroup of $G$, it follows that

(11) $G' = O_{n-1}(G)$ is of order $p$.

Let $a \in G$ with $o(a) = p^n$. Then $G' = O_{n-1}(G) = \langle a^{p^n-1} \rangle \leq \langle a \rangle$ and hence $\langle a \rangle \leq G$. By 2.3.15 there is an Iwasawa triple $(A, b, s)$ for $G$ in which $A = C_G(a)$. Since $|G'| = p$, $[a, b^p] = [a, b]^p = 1$ and hence $b^p \in C_G(a) = A$. This implies that $|G : A| = p$ and $s = n - 1$. It follows that $O_{n-1}(A) \leq Z(G)$. Since $|A : O_{n-1}(A)| = |O_{n-1}(A)| = p$,

(12) $|G : O_{n-1}(A)| = p^2$ and $O_{n-1}(A) = Z(G)$.

So if we choose $R = O_{n-1}(G)$ and $S = O_{n-1}(A) = Z(G)$, then $R$ and $S$ are characteristic subgroups of $G$ such that $\Phi(G) \leq S < R$. Since $G = AR$, there exist $c \in A$ and $d \in R$ such that $b = cd$. Then $(A, d, s)$ is an Iwasawa triple for $G$. It follows that $d \not\in Z(G) = S$ and hence $R = S \langle d \rangle$. For $g \in G$, there exist $a_1 \in A$, $i \in \mathbb{N}$ such that $g = d^i a_1$ and since $d \in O_{n-1}(G)$,

$[g, d] = [d^i a_1, d] = [a_1, d] = a_1^{p^n-1} = d^i a_1^{p^n-1} = g^{p^n-1}.$

Hence if $x \in \text{Aut } G$, then $[a, d^x] = [a^{x^{-1}}, d]^x = ((a^{x^{-1}})^{p^n-1})^x = a^{x^{-1}}[a, d]$ and therefore $d^x d^{-1} \in C_G(a) = A$. Since $d \in R = R^x$, we have $d^x d^{-1} \in A \cap R = S$, that is, $\text{Aut } G$ centralizes $R/S$. \qed
Power automorphisms of $M^*$-groups

By 1.5.4, every power automorphism of a finite abelian group is universal. On the other hand, the quaternion group of order 8 has nonuniversal power automorphisms of order 2. So it is interesting to note that $M^*$-groups may also possess nonuniversal power automorphisms of order $p$ (see Exercise 11), but only if $p = 2$.

2.3.24 Theorem (Napolitani [1971]). Let $\alpha$ be a power automorphism of order $p$ of the $M^*$-group $G$ and assume that $\alpha$ fixes an element of order 4 in $G$ if $p = 2$ and $\exp G \geq 4$. Then $\alpha$ is universal.

Proof. We use induction on $|G|$. Let $\exp G = p^n$ and put $H = \Omega_{n-1}(G)$. If $p = 2$ and $\exp H \geq 4$, then $H$ contains every element of order 4 of $G$. Thus either $\alpha|_H$ is the identity or it satisfies the assumptions of the theorem. By induction, $\alpha$ is universal on $H$. Let $x \in G$ with $o(x) = p^n$. Then $\alpha$ induces an automorphism of order 1 or $p$ in $\langle x \rangle$ and therefore $x^\alpha = x^{1+r p^n-1}$ where $1 \leq r \leq p$. We have to show that $\alpha$ induces the same power in every cyclic subgroup $Y = \langle y \rangle$ of $G$. If $|Y| < p^n$, then $x^\alpha$ and $y$ are contained in $\Omega_{n-1}(G)$ and, since $\alpha$ is universal on $\Omega_{n-1}(G)$, $y^\alpha = y^{1+r p^n-1} = y$. So let $|Y| = p^n$. If $\langle x \rangle \cap Y \neq 1$, we may choose the generator $y$ of $Y$ such that $y^{p^n-1} = (x^{p^n-1})^{-1}$. By 2.3.10, $(xy)^{p^n-1} = x^{p^n-1} y^{p^n-1} = 1$ and therefore, as we have just shown, $xy = (xy)^\alpha = x^\alpha y^\alpha = x^{1+r p^n-1} y^\alpha$. Thus $y^\alpha = (x^{p^n-1})^{-1} y = y^{1+r p^n-1}$. Finally, if $\langle x \rangle \cap Y = 1$, then $(xy)^{p^n-1} \neq 1$ and therefore $(xy)^{p^n-1} = (xy)^{1+t p^n-1}$ and $y^\alpha = y^{1+s p^n-1}$ where $1 \leq s, t \leq p$. Using 2.3.10 and (1) of 1.5, we get

$$x^{r p^n-1} y^{s p^n-1} = [x, \alpha] [y, \alpha] = [xy, \alpha] = (xy)^{p^n-1} = x^{t p^n-1} y^{t p^n-1}$$

and hence $r = t = s$. Thus $y^\alpha = y^{1+r p^n-1}$. $\Box$

Exercises

1. Show that a group is hamiltonian if and only if it is the direct product of a quaternion group of order 8, an elementary abelian 2-group and an abelian group with all its elements of odd order.

2. If $G$ is an $M^*$-group, show that $U_m(G) = \{ x^{p^m} | x \in G \}$ for every $m \in \mathbb{N}$.

3. Let $G$ be an $M^*$-group with $|G| = p$. Show that there exist elements $a, b \in G$, an integer $m$ and an abelian subgroup $H$ of $G$ such that $G = \langle a, b \rangle \times H$, $o(a) = p^m > \exp H$ and $a^b = a^{1+r p^n-1}$.

4. Let $G = \langle u, v | u^8 = v^2 = 1, u^v = u^5 \rangle$ and $A = \langle u^2 v \rangle$. Show that $A \leq G$, $G/A$ is cyclic, but $A$ is not a member of an Iwasawa triple for $G$.

5. Let $A$ be a subgroup of the $M^*$-group $G$ such that every subgroup of $A$ is normal in $G$ and suppose that $B$ is a cyclic subgroup of $G$. If the assertion of 2.3.13 (b) does not hold in $AB$, show that there exist an element $x$ of order 4, an elementary abelian 2-group $E$, and an integer $t$ such that $A = \langle x \rangle \times E$ and $(EB, x, t)$ is an Iwasawa triple for $AB$. 

68 Modular lattices and abelian groups
6. Let $G = \langle u, v, x | u^{p^m} = v^{p^m} = 1, uv = vu, x^{p^2} = v^{-p}, u^x = u^{1+p^{m-1}}, v^x = v^{1+p^{m-1}} \rangle$ where $m \geq 4$. Determine a complement to $\langle x \rangle$ in $G$.

7. Let $G$ be an $M^*$-group with nilpotency class $c(G) \geq 3$ and suppose that $(A, b, s)$ and $(A_1, b_1, s_1)$ are Iwasawa triples for $G$.
(a) Show that $\text{Exp } A = \text{Exp } A_1$ and hence $s = s_1$.
(b) Show that $|A| = |A_1|$ if $A$ and $A_1$ are maximal among the subgroups that belong to Iwasawa triples for $G$.

8. Let $n \geq 5$ and $G = \langle u, v | u^{p^m} = v^{p^{-1}} = 1, u^v = u^{1+p^2} \rangle$. Show that there are Iwasawa triples $(A, b, s)$ and $(A_1, b_1, s_1)$ for $G$ with $A_1 < A$; note that $c(G) = n - 2 \geq 3$.

9. Let $G = \langle u, v | u^{pq} = v^p = 1, u^v = u^{1+p^2} \rangle$. Show that $(\langle u \rangle, v, 3)$ and $(\langle u^p v \rangle, u^{-1}, 2)$ are Iwasawa triples for $G$. Deduce that in general (a) and (b) of Exercise 7 do not hold if $c(G) = 2$.

10. Construct a nonabelian $M^*$-group $G$ with $[G, \text{Aut } G] = G$. (Hence, in general, one cannot have $R = G$ in Theorem 2.3.23.)

11. Let $n \geq 3$ and $G = \langle a, b | a^{2^n} = b^{2^n} = 1, a^b = a^{1+2^{n-1}} \rangle$. Show that there exists a power automorphism of order 2 of $G$ that is not universal.

### 2.4 Groups with modular subgroup lattices

We continue our study of groups with modular subgroup lattices. We shall describe these groups completely modulo the so-called Tarski groups. First we introduce a class of groups similar to the $P$-groups studied in Section 2.2.

#### $P^*$-groups

We say that $G$ is a $P^*$-group if $G$ is the semidirect product of an elementary abelian normal subgroup $A$ by a cyclic group $\langle t \rangle$ of prime power order such that $t$ induces a power automorphism of prime order on $A$. As for nonabelian $P$-groups, this power automorphism is universal so that there exist primes $p, q$ and integers $m, r$ such that $A$ is a $p$-group, $o(t) = q^m$ and $t^{-1} at = a^q$ for all $a \in A$. Since $t$ induces an automorphism of order $q$ in $A$, $r \equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$ so that $q|p - 1$.

#### 2.4.1 Lemma. Let $G = A \langle t \rangle$ be a $P^*$-group and let $o(t) = q^m$. Then $Z(G) = \langle t^q \rangle = \Phi(G), G/Z(G)$ is a nonabelian $P^*$-group and $L(G)$ is modular.

**Proof.** It is clear that $t^q \in Z(G)$ and $G/\langle t^q \rangle$ is a nonabelian $P$-group. Thus $\Phi(G) \leq \langle t^q \rangle \leq Z(G)$. By 2.2.2, $Z(G)/\langle t^q \rangle = 1$ and hence $\langle t^q \rangle = Z(G)$. Furthermore, for $x \in G/\langle t^q \rangle$, $x \langle t^q \rangle$ is of order $q$ in $G/\langle t^q \rangle$ and hence $\langle x, t^q \rangle \simeq G/A \simeq \langle t \rangle$. It follows that $o(x) = q^m$ and $t^q \in \langle x \rangle$. Therefore, if $H$ is a subgroup of $G$, then either $H \leq A \times \langle t^q \rangle$ or $\langle t^q \rangle \leq H$. In the first case, $H \leq G$. In the second, $H$ is modular in $[G/\langle t^q \rangle]$ since this lattice is isomorphic to the subgroup lattice of an abelian group. It follows from 2.1.6(c) that $H$ is modular in $G$. Thus every subgroup of $G$ is modular.
in $G$, that is $L(G)$ is modular. Finally, if $M$ is a maximal subgroup of $G$, then $\langle t^q \rangle \leq M \cap \langle t \rangle$ by 2.1.5 and so $\langle t^q \rangle = \Phi(G)$.

Conversely, for finite groups, we have the following result.

2.4.2 Lemma. If $G$ is a finite $M$-group such that $G/\Phi(G)$ is a nonabelian $P$-group, then $G$ is a $P^*$-group.

Proof. Suppose that $|G/\Phi(G)| = p^aq$ where $p$ and $q$ are primes with $p > q$, let $A/\Phi(G)$ be the Sylow $p$-subgroup of $G/\Phi(G)$ and $P$ a Sylow $p$-subgroup of $G$. Since $A \leq G$ and $|G:A| = q$, we have $P \leq A$ and hence $A = P\Phi(G)$. By the Frattini argument,

$$G = N_G(P)A = N_G(P)P\Phi(G) = N_G(P)\Phi(G).$$

Since $\Phi(G)$ is the set of nongenerators of $G$, it follows that $G = N_G(P)$, that is, $P \leq G$.

If $Q$ is a Sylow $q$-subgroup of $G$, then $G = AQ = \Phi(G)PQ$ and hence $G = PQ$ as before. Since $G/\Phi(G)$, and therefore also $G$, has only one subgroup of index $q$, $Q$ is cyclic; let $Q = \langle t \rangle$. As $G/\Phi(G)$ is not nilpotent, $t$ operates nontrivially on $P$. But $|G/\Phi(G)| = p^aq$ implies that $Q \cap \Phi(G) = \langle t^q \rangle$ is the Sylow $q$-subgroup of $\Phi(G)$.

Hence $\langle t^q \rangle \leq G$ and $P$ is centralized by $t^q$. Finally, for $H \leq P$,

$$H = H \cup (Q \cap P) = (H \cup Q) \cap P \leq H \cup Q$$

since $P \leq G$. It follows that $t$ induces a power automorphism of order $q$ on $P$.

It remains to be shown that $P$ is elementary abelian. Since $\langle t^q \rangle \leq G$, it follows that $\langle t^q \rangle = Q \cap Q_1$ for every Sylow $q$-subgroup $Q_1 \neq Q$ of $G$. By 2.2.4, $|Q/\langle t^q \rangle \cup Q_1/\langle t^q \rangle| = pq$ and therefore $|Q \cup Q_1| = p|Q|$. This implies that $Q \cup Q_1 \leq \Omega(P)Q$. By 2.2.2, $G$ is generated by its Sylow $q$-subgroups and hence $G = \Omega(P)Q$. It follows that $P = \Omega(P)$ and by 2.3.5, $P$ is elementary abelian.

Finite $M$-groups

2.4.3 Lemma. If $G$ is a finite $M$-group with $\Phi(G) = 1$, then $G$ is a direct product of $P$-groups with relatively prime orders.

Proof. We use induction on $|G|$. If $H \leq G$ and $M$ is a maximal subgroup of $G$, then by 2.1.5, $[H \cup M/M] \simeq [H/H \cap M]$ and hence $H \cap M$ is $H$ or a maximal subgroup of $H$. In both cases, $\Phi(H) \leq M$. It follows that $\Phi(H) \leq \Phi(G) = 1$. In particular,

(1) every Sylow subgroup of $G$ is elementary abelian

and every subgroup of $G$ satisfies the assumptions of the lemma.

Let $R$ and $T$ be subgroups of prime order in $G$. Then by 2.2.4, $|R \cup T|$ is the product of two primes. Therefore if $|R| > |T|$, then $|R \cup T| = |R||T|$ and $R \leq R \cup T$. So we have that

(2) $T \leq N_G(R)$ if $|R| > |T|$ are primes.
Denote by $p$ the maximal prime dividing $|G|$ and let $S$ be a Sylow $p$-subgroup of $G$. By (1) and (2), every subgroup of $S$ is normal in $G$. If $S \leq Z(G)$, then the Schur-Zassenhaus theorem yields that $G = S \times C$ where $C$ is a complement to $S$ in $G$. By induction, $C$ is a direct product of $P$-groups with relatively prime orders; hence $G = S \times C$ also has this structure. So we may assume that $S$ is not central in $G$. Then by (1) there exists a subgroup $Q$ of prime order $q$ in $G$ that does not centralize $S$. Thus

(3) $SQ$ is a nonabelian $P$-group

and we want to show that $Q$ is a Sylow $q$-subgroup of $G$. Suppose that this is not the case and let $T$ be a subgroup of order $q^2$ of $G$ containing $Q$. Let $P \leq S$ with $|P| = p$ and put $H = P \cup T$. By (2), $P \leq H$ and hence $|H| = pq^2$ and $H/P \simeq T$. Since $P$ is not central in $H$, at most one of the $q + 1$ subgroups of order $pq$ containing $P$ may be cyclic. Hence $H$ contains two different nonabelian subgroups $U$ and $V$ of order $pq$. Let $Q_1, Q_2 \leq U$ and $Q_3 \leq V$ be subgroups of order $q$ such that $Q_1 \neq Q_2$. If $|Q_1 \cup Q_3| = pq$, then $U = PQ_1 = Q_1 \cup Q_3 = PQ_3 = V$, a contradiction. By 2.2.4, $|Q_1 \cup Q_3| = q^2$ and similarly $|Q_2 \cup Q_3| = q^2$. It follows that $Q_3$ is centralized by $Q_1 \cup Q_2 \cup Q_3 = U \cup Q_3 = H$; but $V = PQ_3$ is not abelian. This contradiction shows that $Q$ is a Sylow $q$-subgroup of $G$ and that

(4) $SQ$ is a Hall subgroup of $G$.

It remains to be shown that if $r$ is a prime such that $p \neq r \neq q$, then

(5) $SQ$ is centralized by every subgroup $R$ of $G$ with $|R| = r$.

Indeed (1) implies that $SQ \leq G$, and the Schur-Zassenhaus theorem yields the existence of a complement $K$ to $SQ$ in $G$ and again by (5) and (1), $G = SQ \times K$. By induction, $K$ has the desired structure and therefore so does $G$.

If $r < q$ in (5), then by (2), $R$ normalizes every subgroup of $SQ$. Since $Z(SQ) = 1$, Cooper's theorem (or 1.4.3) shows that $R$ centralizes $SQ$. If $p > r > q$ and again $P \leq S$ is of order $p$, then $R$ is normalized by every subgroup of order $q$ of $PQ$. Hence $PQ \leq N_L(R)$ and so $P$ and $R$ are normal subgroups of $L = PQR$. Thus $|L| = pqr$ and $PR = P \times R$. Suppose that $Q$ does not centralize $R$. Then $N_L(Q) = Q$ and $L$ contains $|L : Q| = pr$ Sylow $q$-subgroups. For every Sylow $q$-subgroup $Q_1 \neq Q$ of $L$, by 2.2.4, $Q \cup Q_1$ is a subgroup of order $pq$ or $rq$ of $L$ and hence is $PQ$ or $RQ$. But these two groups contain only $p + r - 1$ Sylow $q$-subgroups. This contradiction shows that $L = PQ \times R$ and that (5) also holds in this case.

2.4.4 Theorem (Iwasawa [1941]). A finite group has modular subgroup lattice if and only if it is a direct product of $P^*$-groups and modular $p$-groups with relatively prime orders.

Proof. Since a direct product of modular lattices is modular, 1.6.4 and 2.4.1 yield that $L(G)$ is modular if $G$ is a direct product of $P^*$-groups and modular $p$-groups with relatively prime orders. Conversely, we show by induction on $|G|$ that every finite $M$-group $G$ is such a direct product. If $L(G)$ is directly decomposable, then by 1.6.5 there exist nontrivial subgroups $H$ and $K$ of $G$ such that $G = H \times K$ and
Modular lattices and abelian groups

([H] | [K]) = 1. By induction, H and K have the desired structure and then so does G. So suppose that L(G) is directly indecomposable. Then by 1.6.9, L(G/Φ(G)) is also directly indecomposable and 1.6.4 and 2.4.3 yield that G/Φ(G) is a P-group. If this P-group is nonabelian, then G is a P*-group by 2.4.2. And if G/Φ(G) is an elementary abelian p-group, then G is a p-group since every prime divisor of |G| also divides |G/Φ(G)|. In any case, G has the desired structure.

Theorems 2.4.4 and 2.3.1 give the precise structure of finite M-groups. As an immediate consequence we note the following.

2.4.5 Theorem. Every finite group with modular subgroup lattice is metabelian.

We shall need some simple properties of elements of prime power order in finite M-groups. They can easily be proved directly but also follow immediately from Iwasawa's theorem.

2.4.6 Lemma. Let G be a finite M-group and x, y ∈ G. If x is a p-element and y a q-element where p and q are primes with p > q, then ⟨x⟩ = ⟨x⟩.

Proof. By 2.4.4, G is a direct product of groups G1, ..., Gn with relatively prime orders such that every Gi is either a P*-group or an M-group of prime power order. If x and y are contained in different components of this decomposition, then xy = yx and hence ⟨x⟩ = ⟨x⟩. So suppose that x, y ∈ Gi for some i. Then Gi is a P*-group and hence ⟨x⟩ ≤ Gi since p is the larger prime dividing |Gi|.

2.4.7 Lemma. Let p be a prime, G a finite M-group and suppose that x, y ∈ G are p-elements.

(a) If o(x) ≠ o(y), then ⟨x, y⟩ is a p-group.
(b) If o(x) ≥ o(y) and o(x) ≥ p², then Ω(⟨x⟩) ≤ ⟨x, y⟩.

Proof. Let G = G1 × · · · × Gn as in the proof of 2.4.6. Since the orders of the Gi are relatively prime, x and y have to lie in the same component Gi.

(a) If Gi is a p-group or a P*-group and p the larger prime dividing |Gi|, then ⟨x, y⟩ is clearly a p-group. So suppose that Gi is a P*-group and p the smaller prime dividing |Gi|. Then by 2.4.1, the maximal subgroups of the Sylow p-subgroups are central in Gi. Since o(x) ≠ o(y), therefore x or y is contained in Z(Gi). It follows that ⟨x, y⟩ is a p-group.

(b) If Gi is a P*-group, then p is the smaller prime dividing |Gi| since o(x) ≥ p². Again ⟨x²⟩ ≤ Z(Gi) and hence Ω(⟨x⟩) ≤ ⟨x, y⟩. And if Gi is a p-group, then 2.3.5 implies that Exp⟨x, y⟩ = o(x) and 2.3.9 yields that Ω(⟨x⟩) ≤ ⟨x, y⟩.

M-groups with elements of infinite order

The structure of M-groups with elements of infinite order is well-known. We first show that the torsion subgroup of such a group and its factor group are abelian.
2.4 Groups with modular subgroup lattices

2.4.8 Lemma. Let $G$ be an $M$-group. Then the set $T(G)$ of all elements of finite order in $G$ is a characteristic subgroup of $G$. If $G$ contains an element of infinite order, then $T(G)$ is abelian and every subgroup of $T(G)$ is normal in $G$.

Proof. For $a, b \in T(G)$, 2.1.5 yields that

\[
\frac{\langle ab \rangle}{\langle ab \rangle \cap \langle a \rangle} = \frac{\langle a, b \rangle}{\langle a \rangle} \simeq \frac{\langle b \rangle}{\langle a \rangle \cap \langle b \rangle}
\]

is a finite lattice. Since also $\langle ab \rangle \cap \langle a \rangle$ is finite, $ab$ has finite order. Thus $T(G)$ is a subgroup and then of course a characteristic subgroup of $G$.

Let $x \in G$ be an element of infinite order. Then $\langle x \rangle \cap T(G) = 1$ and if $H \leq T(G)$, then we see that $H = H \cup (\langle x \rangle \cap T(G)) = (H \cup \langle x \rangle) \cap T(G) \leq H \cup \langle x \rangle$ since $T(G) \leq G$. Thus $x \in N_G(H)$ and since $G$ is generated by the elements outside $T(G)$, it follows that $H \leq G$. In particular, $T(G)$ is abelian or hamiltonian. In the latter case $T(G)$ would contain a finite nonabelian $p$-subgroup since a hamiltonian torsion group is clearly the direct product of its primary components. By 2.3.12, $G$ would contain a subgroup $Q$ isomorphic to the quaternion group $Q_8$ (see also Exercise 2.3.1). Since $Q \leq G$, the element $x \in G$ of infinite order would operate on $Q$ and hence a nontrivial power $y$ of $x$ would centralize $Q$. Then $\langle y \rangle \times Q \cong C_4 \times Q_8$ would be an $M$-group, contradicting 2.3.8. Thus $T(G)$ is abelian. □

2.4.9 Lemma. If $G$ is an $M$-group, then $G/T(G)$ is abelian.

Proof. Since $G/T(G)$ does not contain elements of finite order, we may assume that $T(G) = 1$, that is, $G$ is torsion-free. Let $a, b \in G$. We shall show in several steps that $ab = ba$.

(6) If $b^{-1}a^mb = a^n$ with integers $n$ and $m$, then $n = m$.

Indeed, if $\langle a \rangle \cap \langle b \rangle = \langle a^n \rangle \neq 1$, then the assumption in (6) implies that $a^{km} = b^{-1}a^{km}b = a^{kn}$, therefore $n = m$ since $G$ is torsion-free. In addition, if $\langle a \rangle \cap \langle b \rangle = 1$, the modular law and the assumption in (6) yield that

\[
\langle a^n \rangle = (\langle a^n \rangle \cup \langle b \rangle) \cap \langle a \rangle = (\langle a^m \rangle \cup \langle b \rangle) \cap \langle a \rangle = \langle a^m \rangle,
\]

that is, $n = m$ or $n = -m$. If $n = -m$, then $\langle a^n \rangle$ is inverted by $b$ and hence $\langle a^n, b \rangle/\langle a^{4n}, b^2 \rangle$ is a dihedral group of order 8. But this group is not an $M$-group. Thus $n = m$ and (6) holds.

(7) If $\langle a \rangle \cap \langle b \rangle \neq 1$, then $ab = ba$.

Suppose that this is false. Thus $a \neq a^b$, let $|\langle a \rangle| = n$. Then $a^n = (a^b)^m$ for some integer $m$ and by (6), $n = m$. So if we put $c = a^b$ and $d = a^n$, we have found elements $a \neq c$ and $d \neq 1$ in $G$ satisfying $\langle a \rangle \cap \langle c \rangle = \langle d \rangle$ and $d = a^n = c^n$. Since $\langle a, c \rangle/\langle d \rangle$ is generated by elements of finite order, it is a torsion group by 2.4.8. Hence there exists an integer $r$ such that $(ac^{-1})^r \in \langle d \rangle$ and we can choose $k$ in $\{+1, -1\}$ such that $(ac^{-1})^{kr} = d^s$ where $s \geq 0$. Since $a \neq c$ and $G$ is torsion-free, $s > 0$. Consider the subgroups $U = \langle ad^s \rangle = \langle a^{ns+1} \rangle$, $V = \langle cd^s \rangle = \langle c^{ns+1} \rangle$ and
$W = \langle a \rangle$. Clearly, $U \leq W$ and $U \cup V$ contains $ad'(cd')^{-1} = ac^{-1}$; hence $U \cup V$ also contains $(ac^{-1})^n = d^n$ and so $a$ and $c$. Thus $U \cup V = \langle a, c \rangle \geq W$. Furthermore

$$V \cap W = \langle c^{n+1} \rangle \cap \langle a \rangle = \langle c^{n+1} \rangle \cap \langle c \rangle \cap \langle a \rangle = \langle c^{n+1} \rangle \cap \langle c^n \rangle = \langle c^{n(n+1)} \rangle = \langle a^{n(n+1)} \rangle \leq U.$$  

The modular law yields $\langle a \rangle = W = (U \cup V) \cap W = U \cup (V \cap W) = U = \langle a^{n+1} \rangle$, a contradiction since $n > 0$. Thus (7) holds.

Since $\langle a \rangle \cap \langle b \rangle = (\langle a \rangle \cap \langle b \rangle)^b \leq \langle a \rangle \cap \langle b \rangle$, an immediate consequence of (7) is the following.

(8) If $\langle a \rangle \cap \langle b \rangle \neq 1$, then $ab = ba$.

To deal with the case $\langle a \rangle \cap \langle b \rangle = 1$, we strengthen property (7). Assume that $b^{-1}a^n b^n = a^m$ for integers $n$ and $m$ with $n \neq 0 \neq m$. Then $a^m \in \langle a \rangle \cap \langle ab \rangle$ and by (7), $ab^n = b^n a$. This implies that $b^n \in \langle b \rangle \cap \langle b^n \rangle$ and (7) yields that $ba = ab$. So we have shown:

(9) If $a^n b^n = b^n a$ for integers $n$ and $m$ with $n \neq 0 \neq m$, then $ab = ba$.

The second main step in the proof of the lemma is the following.

(10) If $ab \neq ba$, then $\langle a, b \rangle / \langle a, b \rangle'$ is a nontrivial finite group and $\langle a, b \rangle' = \langle c, d \rangle$ with $cd \neq dc$.

To show this let $H = \langle a, b \rangle$, $K = \langle a, ab \rangle$ and $N = \langle a^2, (a^2)b \rangle$. Since $H = \langle a \rangle \cup \langle b \rangle = \langle a^2 \rangle \cup \langle b \rangle$,

$$K = \langle a \rangle \cup (K \cap \langle b \rangle) = \langle a^2 \rangle \cup (K \cap \langle b \rangle) = K^b$$

and hence $K \leq H$. Similarly, $N \leq \langle a^2, b \rangle$ and $N = \langle a^2, (a^2)b \rangle \leq \langle a^2, a b \rangle$. Thus $N \leq \langle b, ab \rangle = H$. Now $K/N$ is generated by the involutions $aN$ and $abN$. Therefore it is a dihedral group and hence finite since the infinite dihedral group is not an $M$-group. Furthermore, $K \cap \langle b \rangle \neq 1$ since otherwise $a^b \in \langle a \rangle$ and (7) would imply that $ab = ba$. So $K \cap \langle b \rangle = \langle b^r \rangle$ for some positive integer $r$ and $H/K = \langle b \rangle / K \cap \langle b \rangle$ is cyclic of order $r$. It follows that $H/N$ is finite. From (8) we have $\langle b \rangle \cap \langle a \rangle = 1$ and hence $\langle a^2, b \rangle \cap \langle a \rangle = \langle a^2 \rangle$. Thus $N \leq \langle a^2, b \rangle < H$ and so we have shown that $H/N$ is a nontrivial finite $M$-group. By 2.4.5, $H' \neq H$. Since $H/K$ is cyclic, $H' \leq K$; on the other hand, if we put $c = [a, b] = a^{-1}ab$, then $K = \langle a, ab \rangle = \langle a, c \rangle$. It follows that $K = \langle a \rangle \cap H'$ and $H' = \langle c \rangle \cup (\langle a \rangle \cap H') = \langle c, a^m \rangle$ with $\langle a^m \rangle = \langle a \rangle \cap H'$. Suppose that $\langle a \rangle \cap H' = 1$. Then $H' = \langle c \rangle$ is centralized by $a^2$ since $|\mathrm{Aut}(c)| = 2$. Hence $a^2 \in Z(K)$, $a^2 b^r = b^r a^2$ and (9) implies that $ab = ba$, a contradiction. Thus $\langle a \rangle \cap H' \neq 1$. Similarly, $\langle b \rangle \cap H' = \langle b^n \rangle \neq 1$. Then $\langle a^n, b^n \rangle \leq H'$. It follows that $H/H' = \langle ah', bH' \rangle$ is finite and (9) implies that $H'$ is nonabelian. So if we put $d = a^n$, then $H' = \langle c, d \rangle$ and $cd \neq dc$. Thus (10) holds.

To finish the proof of the lemma we suppose that $ab \neq ba$ and put $H = \langle a, b \rangle$. Then $H' = \langle c, d \rangle$ with $cd \neq dc$. Applying (10) two further times we get that $H'' = \langle c, d \rangle = \langle e, f \rangle$ with $ef \neq fe$ and $H''' = \langle e, f \rangle = \langle g, h \rangle$ where $gh \neq hg$. Further-
more all the commutator factor groups $H/H', H''/H''$ and $H''/H''$ are nontrivial finite
groups. But then $H/H''$ is a finite $M$-group that is not metabelian, contradicting
2.4.5. It follows that $ab = ba$. □

We show next that for a nonabelian $M$-group $G$ with elements of infinite order,
the torsion-free abelian group $G/T(G)$ has rank one.

2.4.10 Lemma. Let $G$ be an $M$-group. If $G$ contains two elements $a$ and $b$ of infinite
order such that $\langle a \rangle \cap \langle b \rangle = 1$, then $G$ is abelian.

Proof. Let $S$ be the set of elements of infinite order in $G$. For $u, v \in S$, define $u \sim v$
if and only if $\langle u \rangle \cap \langle v \rangle \neq 1$. If $u \sim v$ and $v \sim w$, then $\langle u \rangle \cap \langle v \rangle = \langle v^{m} \rangle \neq 1$ and
$\langle v \rangle \cap \langle w \rangle = \langle w^{n} \rangle \neq 1$; thus $1 \neq v^{nm} \in \langle u \rangle \cap \langle w \rangle$ and hence $u \sim v$. This shows that
$\sim$ is an equivalence relation on $S$. Let $x, y \in S$. If $x \not\sim y$, that is if $\langle x \rangle \cap \langle y \rangle = 1$,
then every element $g$ of finite order in $\langle x, y \rangle$ satisfies

$$L(\langle g \rangle) \equiv [\langle g \rangle \cup \langle x \rangle/\langle x \rangle] = [\langle y^{n} \rangle \cup \langle x \rangle/\langle x \rangle] \equiv L(\langle y^{n} \rangle)$$

for some integer $n$ and hence $g = 1$. Thus $\langle x, y \rangle$ is torsion-free and by 2.4.9, $xy = yx$.
And if $x \sim y$, that is, if $\langle x \rangle \cap \langle y \rangle \neq 1$, then by assumption there exists an element
$z \in S$ that is not equivalent to $x$ and $y$. Hence, as we have seen, $xz = zx$ and $yz = zy$.
It follows that $\langle y, z \rangle = \langle y \rangle \times \langle z \rangle$ and $\langle yz \rangle \cap \langle y \rangle = 1$. So $yz \in S$ and $yz \not\sim y$,
whence also $yz \not\sim y$. Thus $x(yz) = (yz)x = yxz$ and hence in this case also $xy = yx$.
We have shown that all elements of infinite order in $G$ commute. By 2.4.8, $G$ is
generated by these elements and hence is abelian. □

So far we have obtained a number of restrictions on the structure of a nonabelian
$M$-group with elements of infinite order. We now give the precise structure of these
groups.

2.4.11 Theorem (Iwasawa [1943]). Let $G$ be a nonabelian $M$-group with elements of
infinite order. Then $T(G)$ is abelian and $G/T(G)$ is a torsion-free abelian group of rank
one.

(a) If $G/T(G)$ is cyclic, then $G$ is the semidirect product of $T(G)$ by an infinite cyclic
group $\langle z \rangle$, and for every prime $p$ there exists a $p$-adic unit $r(p)$ with $r(p) \equiv 1 \pmod{p}$
and $r(2) \equiv 1 \pmod{4}$ such that $a^{z} = a^{(p)}$ for all $a \in T(G)$, the $p$-component of $T(G)$.
(See 1.5.5 for the definition of $a^{(p)}$.)

Conversely, for every prime $p$, let $r(p)$ be a $p$-adic unit with $r(p) \equiv 1 \pmod{p}$ and
$r(2) \equiv 1 \pmod{4}$. If $\overline{G}$ is the semidirect product of an abelian torsion group $T$ by an
infinite cyclic group $\langle z \rangle$ to the automorphism given by $a^{z} = a^{(p)}$ for all $a \in T(G)$, then
$HK = KH$ for all $H, K \subseteq \overline{G}$ and $\overline{G}$ is an $M$-group with $\overline{G}/(G)$ infinite cyclic.

(b) Suppose that $G/T(G)$ is not cyclic and let $\exp T(G) = p^{n}$ where $n \in \mathbb{N} \cup \{0, \infty\}$.
Then there exist elements $z_{i} \in G$, $a_{i} \in T(G)$, primes $p_{i}$ and $p$-adic units $r_{i}(p)$ such that
$G = \langle T(G), z_{1}, z_{2}, \ldots \rangle$ and for all primes $p$ and all $i \in \mathbb{N}$,

(11) $r_{i}(p) \equiv 1 \pmod{p}$ and $r_{i}(2) \equiv 1 \pmod{4}$,

(12) $r_{i+1}(p)^{p_{i}} r_{i}(p) \equiv r_{i}(p) \pmod{p^{n}}$ (that is $r_{i+1}(p)^{p_{i}} r_{i}(p)$ if $n = \infty$),
Modular lattices and abelian groups

(13) $o(z_i)$ is infinite,

(14) $a^{r_i} = a^{r(p)}$ for all $a \in T(G)_p$,

(15) $z_i^{r_{i+1}} = z_ia_i$, and

(16) $(z_ia_i)^{r_{i+1}} = z_ia_i$.

Conversely, let $T$ be an abelian torsion group with $\text{Exp} T_p = p^n$, let $a_i \in T$ and $r_i(p)$ be $p$-adic units satisfying (11) and (12) for all primes $p$ and all $i \in \mathbb{N}$. If we extend $T$ successively by cyclic groups $\langle z_i \rangle$ according to the relations (13)–(16), we get an $M$-group $\overline{G} = \langle T, z_1, z_2, \ldots \rangle$ in which any two subgroups permute.

**Proof.** By 2.4.8 and 2.4.9, $T(G)$ and $G/T(G)$ are abelian and $G/T(G)$ is torsion-free. The rank of this group is one since otherwise there would exist two infinite cyclic subgroups with trivial intersection in $G/T(G)$, hence also in $G$; so $G$ would be abelian by 2.4.10.

(a) Suppose that $G/T(G)$ is cyclic and let $z \in G$ with $G/T(G) = \langle zT(G) \rangle$. Then $z$ has infinite order and hence $T(G) \cap \langle z \rangle = 1$. Thus $G$ is the semidirect product of $T(G)$ by $\langle z \rangle$ and 2.4.8 shows that $z$ induces a power automorphism in $T(G)$. So for every prime $p$, by 1.5.6 there exists a $p$-adic unit $r(p)$ such that $a^{r_p} = a^{r(p)}$ for all $a \in T(G)_p$. If $T(G)_p = 1$ or $\text{Exp} T(G)_2 < 2$, we may choose $r(p) = 1$ or $r(2) = 1$, respectively. So suppose that $T(G)_p \neq 1$ and $\text{Exp} T(G)_2 \geq 4$ and take $a \in T(G)$ with $o(a) = p$. If $r(p) \neq 1$ (mod $p$), then a suitable power $b$ of $z$ would induce an automorphism of prime order $q \neq p$ in $\langle a \rangle$; but then $\langle a, b \rangle/\langle b^{p^k} \rangle$ would be a group of order $p^2q$ which, by 2.4.4, would not be an $M$-group. Similarly, if $r(2) \neq 1$ (mod 4), every element $a$ of order 4 in $T(G)$ would be inverted by $z$ and hence $\langle a, z \rangle/\langle z^2 \rangle$ would be a dihedral group of order 8 and not an $M$-group. Thus $r(p) \equiv 1$ (mod $p$) and $r(2) \equiv 1$ (mod 4).

Conversely, suppose that $\overline{G} = T\langle z \rangle$ as described in the theorem, let $H, K \leq \overline{G}$ and take $x \in H$, $y \in K$. If $o(x)$ is finite, then $x \in T$ since $\overline{G}/T$ is infinite cyclic. It follows that $\langle x \rangle \leq \overline{G}$ and $xy = yx \in KH$. So suppose that $o(x)$ is infinite and write $x = az^i$ and $y = bz^j$ with $a, b \in T$ and integers $i, j$. Then $x$ and $y$ are contained in $L = \langle a, b, z \rangle = A \langle z \rangle$ with $A = \langle a, b \rangle \leq T$. Since $A$ is finite, $L/C_{\langle z \rangle}(A)$ too is finite, and therefore $x^k \in C_{\langle z \rangle}(A)$ for some positive integer $k$. Thus if $N = \langle x \rangle \cap C_{\langle z \rangle}(A)$, then $1 
eq N \leq L$ and $L/N$ is finite. For every prime $p$, $r(p) \equiv 1$ (mod $p$) implies that $z$ induces a power automorphism of order some power of $p$ in the Sylow $p$-subgroup of $A$. It follows that $L/N$ is a direct product of finite $p$-groups and since $r(2) \equiv 1$ (mod 4), 2.3.1 shows that these $p$-groups have modular subgroup lattices. By 2.3.2, any two subgroups of these $p$-groups, and hence also of $L/N$, permute. In particular, there exist integers $n, m$ and an element $u \in N \leq \langle x \rangle$ such that $xy = y^n x^m u \in KH$. This shows that $HK = KH$ and by 2.1.3, $\overline{G}$ is an $M$-group.

(b) Now suppose that $G/T(G)$ is not cyclic. As a torsion-free abelian group of rank one, $G/T(G)$ is isomorphic to a subgroup of the rationals (see Robinson [1982], p. 112); hence it is countable and locally cyclic. It follows easily that there exist subgroups $G_i$ of $G$ and primes $p_i$ such that $T(G) < G_1 < G_2 < \cdots < G_i \cup \bigcup_{i \in \mathbb{N}} G_i = G$, $G_i/T(G)$ is infinite cyclic and $|G_{i+1} : G_i| = p_i$ for all $i \in \mathbb{N}$. By (a) there exist $z_1 \in G$ with
2.4 Groups with modular subgroup lattices

$G_1 = T(G) \langle z_1 \rangle$ and $p$-adic units $r_i(p)$ satisfying (11) and (14) for $i = 1$ and all primes $p$. We show that if for some integer $i$, there exist an element $z_i \in G$ with $G_i = T(G) \langle z_i \rangle$ and $p$-adic units $r_i(p)$ satisfying (11) and (14) for $i$, then there are elements $z_{i+1} \in G$, $a_i \in T(G)$ and $p$-adic units $r_{i+1}(p)$ such that $G_{i+1} = T(G) \langle z_{i+1} \rangle$, (11) and (14) hold for $i + 1$, and (12), (15), (16) are satisfied for $i$. This will prove the first assertion of (b). So suppose that $G_i = T(G) \langle z_i \rangle$ as described and let $w \in G_{i+1}$ such that $G_i = T(G) \langle z_i \rangle$. Since $G_i = T(G) (G_i \cap \langle w \rangle)$ has index $p_i$ in $G_{i+1}$, $G_i \cap \langle w \rangle = \langle w^{p_i} \rangle$ and $w^{p_i}$ is congruent to $z_i$ or $z_i^{-1}$ modulo $T(G)$. Let $z_{i+1}$ be the generator of $\langle w \rangle$ satisfying $z_{i+1}^{p_i} = z_i (\mod T(G))$, that is $z_{i+1}^{p_i} = z_ia_i$ for some $a_i \in T(G)$. By (a) there exist $p$-adic units $r_{i+1}(p)$ satisfying (11) and (14) for $i + 1$ and all primes $p$. Since $z_{i+1}^{p_i}$ and $z_i$ induce the same automorphism in $T(G)$, (12) holds; finally (16) follows from $z_ia_i \in \langle z_{i+1} \rangle$.

Conversely, let $\bar{G_1}$ be the semidirect product of $T$ by an infinite cyclic group $\langle z_1 \rangle$ to the automorphism given by $a^{z_1} = a^{r_i(p)}$ for all $a \in T_p$. If $\bar{G_1} = \langle T, z_1, \ldots, z_i \rangle = \langle T, z_i a_i \rangle$ is already constructed, then (14) and (16) define an automorphism of $\bar{G}_i = \langle T, z_i a_i \rangle$ that fixes $z_ia_i$ and whose $p_i$-th power, as (12) shows, is the inner automorphism induced by $z_ia_i$. Thus there exists the extension $\bar{G}_{i+1}$ of $\bar{G_i}$ by a cyclic group $\langle z_{i+1} \rangle$ with respect to this automorphism and the relation $z_{i+1}^{p_i} = z_i a_i$. Hence $\bar{G}$ exists and is the set-theoretic union of the groups $\bar{G}_i$. So if $x, y \in \bar{G}$, there exists an integer $i$ such that $x, y \in \bar{G}_i = T \langle z_i \rangle$. By (a), $\langle x \rangle \langle y \rangle = \langle y \rangle \langle x \rangle$. It follows that any two subgroups of $\bar{G}$ permute and by 2.1.3, $\bar{G}$ is an $M$-group.

It is possible to choose the $p$-adic units $r_i(p)$ in Theorem 2.4.11(b) in such a way that

$$(12') \quad r_{i+1}(p)^{p_i} = r_i(p) \quad \text{for all } i \in \mathbb{N}.$$ 

This has as a consequence the following result.

2.4.12 Theorem (Mainardis [1991]). Every $M$-group with elements of infinite order can be embedded in an $M$-group with divisible (abelian) torsion subgroup.

Proof. First let us prove that we may choose the $r_i(p)$ such that (12') holds. So suppose that $G$ is an $M$-group, $G/T(G)$ is not cyclic and let $z_i$, $p_i$, $r_i(p)$ be as in Theorem 2.4.11(b). If $\Exp T(G)_p = \infty$, then clearly (12') holds. And if $\Exp T(G)_p$ is finite, then also $\Pot T(G)_p$ is finite. Let $\alpha_i$ be the power automorphism induced by $z_i$ in $T(G)_p$; so $t^{\alpha_i} = t^{r_i(p)}$ for all $t \in T(G)_p$. If all the $\alpha_i$ are trivial, we may choose $r_i(p) = 1$ for all $i$ and (12') holds. So suppose that $\alpha_i \neq 1$ for some $j$. Since $r_i(p) \equiv 1 \pmod{p_j}$, $o_\gamma (\alpha_j) = p^u$ for some $u \in \mathbb{N}$. For every $k > j$, $z_j = z_k^d$ where $d = \sum_{i=j}^{k-1} p_i$ and if $v$ of these $p_i$ are equal to $p$, then $o_\gamma (\alpha_k) = p^{u+v}$. Since $\Pot T(G)_p$ is finite, it follows that there exists $k \in \mathbb{N}$ such that $p_k \neq p$ for all $i \geq k$.

For every prime $q \neq p$ and every $p$-adic integer $\gamma \equiv 1 \pmod{p}$, the equation $\beta^q = \gamma$ has a unique solution $\beta \in R_p$ with $\beta \equiv 1 \pmod{p}$. For, let $\gamma = \sum_{i=0}^{\infty} c_i p^i$ where $c_0 = 1$ and $0 \leq c_i < p$ for all $i$ and put $c_m = \sum_{i=0}^{m-1} c_i p^i$. Let $b_0 = 1$ and assume that $b_0, \ldots, b_{m-1}$ are integers such that $0 \leq b_i < p$ for all $i$ and $b_m = \sum_{i=0}^{m-1} b_i p^i$ is the unique integer
Modular lattices and abelian groups

satisfying $1 \leq \beta_m < p^m$, $\beta_m \equiv 1 \pmod{p}$ and $\beta_m^p \equiv \gamma_m \pmod{p^m}$. Since $\gamma \equiv 1 \pmod{p}$, $\gamma_{m+1}$ lies in the Sylow $p$-subgroup of the multiplicative group of integers modulo $p^{m+1}$. In this abelian $p$-group, the map $x \rightarrow x^q$ is an automorphism and hence there exists a unique integer $\beta_{m+1}$ such that $1 \leq \beta_{m+1} < p^{m+1}$, $\beta_{m+1} \equiv 1 \pmod{p}$ and $\beta_{m+1}^p \equiv \gamma_{m+1} \pmod{p^{m+1}}$. If $\beta_{m+1} = \sum_{i=0}^{m-1} d_i p^i$ where $0 \leq d_i < p$, then $\left( \sum_{i=0}^{m-1} d_i p^i \right)^q \equiv \gamma_m \pmod{p^m}$ and the uniqueness of $\beta_m$ implies that $d_i = b_i$ for $i = 0, \ldots, m - 1$. So if we define $b_m = d_m$, then $\beta_{m+1} = \sum_{i=0}^{m} b_i p^i$. Thus, inductively, we obtain that there exists a unique $p$-adic integer $\beta = \sum_{i=0}^{\infty} b_i p^i$ such that $\beta \equiv 1 \pmod{p}$ and $\beta^q \equiv \gamma \pmod{p^m}$ for all $m \in \mathbb{N}$, that is $\beta^q = \gamma$.

Now we define $p$-adic integers $s_i(p)$ satisfying (12') in place of the $r_i(p)$. We put $s_k(p) = r_k(p)$ and, inductively, $s_i(p) = s_{i+1}(p)^{p^i}$ for $i < k$; and if $i \geq k$, then $p_i \neq p$ and we let $s_{i+1}(p)$ be the unique solution of the equation $x^{p^i} = s_i(p)$ in $R_p$ satisfying $s_{i+1}(p) \equiv 1 \pmod{p}$. Then, clearly, (12') holds for the $s_i(p)$ and we have to show that

$$(14') \quad a^{-1} = a^{s_i(p)}$$

then we can replace the $r_i(p)$ by the $s_i(p)$ in Theorem 2.4.11(b). So let $\sigma_i$ be the power automorphism of $T(G)_p$ defined by $a^{\sigma_i} = a^{s_i(p)}$ for $a \in T(G)_p$. Clearly, $\sigma_k = \sigma_k$. If $i < k$ and $u = \prod_{i=1}^{k-1} p_j$, then $\alpha_i = \alpha_i^u = \sigma_k^u = \sigma_i$. If $i \geq k$ and $v = \prod_{j=k}^{k} p_j$, then $\alpha_i^v = \alpha_k = \sigma_k = \sigma_i^v$; since $(v, p) = 1$ and $\alpha_i, \sigma_i$ are $p$-elements of Pot $T(G)_p$, it follows that $\alpha_i = \sigma_i$. Thus (14') holds.

Finally, we prove the assertion of the theorem. Let $G$ be an $M$-group with elements of infinite order. If $G$ is abelian, the theorem is well-known (see Robinson [1982], p. 95). So we may assume that $G$ is nonabelian and therefore has the structure given in 2.4.11. In particular, $T(G)$ is abelian and by the result just cited there exists a divisible abelian torsion group $T$ containing $T(G)$ as a subgroup. If (a) of 2.4.11 holds, the semidirect product of $T$ and $\langle z \rangle$ with respect to the automorphism given by $a^z = a^\sigma(p)$, $a \in T(G)_p$, $p \in \mathbb{P}$, is an $M$-group containing $G = T(G)_p$ as a subgroup. Similarly, if (b) of 2.4.11 holds and the $r_i(p)$ satisfy (12'), then by 2.4.11, the relations (13)-(16) define an $M$-group $T\langle z_1, z_2, ... \rangle$ containing $G$ as a subgroup.

We finally mention that the structure of $G$ in Theorem 2.4.11(b) becomes simpler if $T(G)$ is a $p$-group and also if $T(G)$ is divisible. For, in the first case, we may choose $p_i \neq p$ for all $i \in \mathbb{N}$. And then, in either case, we may take $a_i = 1$ for all $i \in \mathbb{N}$ so that $G$ is the semidirect product of $T(G)$ and $Z$ where $Z = \langle z_1, z_2, ... \rangle$ is a torsion-free, locally cyclic group and the $z_i, r_i(p)$ satisfy (11)-(14) and $z_i^p = z_i$. We leave the proof of the first assertion as an exercise and shall prove the second one in 2.5.13.

Locally finite $M$-groups

An abelian torsion group clearly is locally finite. Hence a projective image of such a group is a locally finite $M$-group. Therefore the structure of these groups is of
particular interest and it will be described in the next two theorems; these may be regarded as extensions of Theorems 2.4.4 and 2.3.1.

2.4.13 Theorem (Iwasawa [1943]). The group $G$ is a locally finite $M$-group if and only if it is a direct product of $P^*$-groups and locally finite $p$-groups with modular subgroup lattices such that elements of different direct factors have relatively prime orders.

Proof. That such a direct product is an $M$-group follows from 1.6.4 and 2.4.1 as in the finite case. Furthermore, it is obvious that every $P^*$-group, and therefore a direct product of such groups, is locally finite. Conversely, suppose that $G$ is a locally finite $M$-group. For every prime $q$, let $G_q$ be the subgroup generated by all the $q$-elements of $G$. Clearly, $G_q$ is a characteristic subgroup of $G$. If any two $q$-elements generate a $q$-group, then $G_q$ is the set of all $q$-elements in $G$ and hence a locally finite $q$-group with modular subgroup lattice. Now suppose that there are $q$-elements $u, v$ such that $\langle u, v \rangle$ is not a $q$-group. Then by 2.4.4, the finite $M$-group $\langle u, v \rangle$ must be a $P^*$-group of order $p^i q^j$ where $p$ is a prime with $p > q$. Since $u \notin Z(\langle u, v \rangle)$, there exists an integer $r$ with $r \neq 1 \mod p$ and $r^* = 1 \mod p$ such that $a^r = a'$ for every $p$-element $a$ of $\langle u, v \rangle$. Let $x, y$ be arbitrary $p$-elements and $z$ an arbitrary $q$-element of $G$. Then $H = \langle u, v, x, y, z \rangle$ is a finite $M$-group and since $\langle u, v \rangle \leq H$, it follows from 2.4.4 that $H$ is a $P^*$-group of order $p^n q^m$ with $n, m \in \mathbb{N}$. The $p$-elements $x$ and $y$ are contained in the Sylow $p$-subgroup of $H$, hence they have order $p$ and commute; furthermore $x^* = x^r$ since $u$ induces a universal power automorphism in this Sylow $p$-subgroup. Since $x$ and $y$ were arbitrary, it follows that $G_p$ is an elementary abelian $p$-group and that $G_p \langle u \rangle$ is a $P^*$-group. By 2.4.1 and 2.2.2, this $P^*$-group is generated by $q$-elements; on the other hand, $z \in H \leq G_p \langle u \rangle$. Since $z$ was an arbitrary $q$-element, $G_q = G_p \langle u \rangle$ is a $P^*$-group. If $g \in G$ with $(o(g), pq) = 1$, then $\langle H, g \rangle$ is a finite $M$-group and by 2.4.4, $g$ centralizes $x$ and $z$. This shows that $G_p$ cannot be contained in a second $P^*$-subgroup $G_s$ of $G$. Clearly $G$ is the product of the $P^*$-groups $G_q$ obtained in this way and the $t$-groups $G_t$ that are not contained in these $P^*$-groups. Since the orders of the elements in different factors of this type are relatively prime, the product is direct.

2.4.14 Theorem (Iwasawa [1943]). Let $p$ be a prime. The group $G$ is a nonabelian locally finite $p$-group with modular subgroup lattice if and only if

(a) $G$ is a direct product of a quaternion group $Q_8$ of order 8 with an elementary abelian 2-group, or

(b) $G$ contains an abelian normal subgroup $A$ of exponent $p^k$ with cyclic factor group $G/A$ of order $p^m$ ($k, m \in \mathbb{N}$) and there exist an element $b \in G$ with $G = A \langle b \rangle$ and an integer $s$ which is at least 2 in case $p = 2$ such that $s < k \leq s + m$ and $b^{-1} ab = a^{1+p^s}$ for all $a \in A$.

Proof. If $G$ satisfies (a), then the elements of order 2 of $G$ are contained in $Z(G)$ and subgroups of exponent 4 contain $G'$. Thus $G$ is hamiltonian and hence $L(G)$ is modular. Clearly, $G$ is locally finite. Now suppose that (b) holds. For $x_1, \ldots, x_n \in G$ there exist $a_i \in A$ and $b_i \in \langle b \rangle$ such that $x_i = a_i b_i$. Then every $x_i$ is contained in
Modular lattices and abelian groups

\langle a_1, \ldots, a_n \rangle \langle b \rangle \) and this group is a finite \( M \)-group by 2.3.1. Thus \( G \) is locally finite and by 2.3.2, \( \langle x_i \rangle \langle x_j \rangle = \langle x_j \rangle \langle x_i \rangle \) for all \( i, j \). It follows that any two subgroups of \( G \) permute. Hence \( L(G) \) is modular and since \( s < k \), \( G \) is not abelian.

Conversely, let \( G \) be a nonabelian locally finite \( p \)-group with modular subgroup lattice. If \( G \) contains a subgroup \( Q \cong Q_8 \), then for \( x \in G \) and \( y \in C_G(Q) \), \( H = \langle Q, x, y \rangle \) is a finite 2-group. By 2.3.8, \( H = QC_G(Q) \) and \( C_H(Q) \) is elementary abelian. It follows that \( x \in QC_G(Q) \) and \( o(y) = 2 \), that is, \( G = QC_G(Q) \) and \( C_G(Q) \) is elementary abelian. Thus \( G = Q \times A \) where \( A \) is a complement to \( Z(Q) \) in \( C_G(Q) \) and (a) holds.

So suppose that \( G \) does not contain a subgroup isomorphic to \( Q_8 \). Again by 2.3.8, every finite subgroup of \( G \) is an \( M^* \)-group. Since \( G \) is not abelian, there exist \( x, y \in G \) with \( xy \neq yx \). Then \( \langle x, y \rangle \) is finite of exponent \( p^n \), say. We claim that

\[ \text{(17)} \quad \text{Exp } G < p^n. \]

For, suppose that there exists an element \( z \in G \) of order \( p^{2n} \). Then \( H = \langle x, y, z \rangle \) is still finite and of exponent \( p^n \) by 2.3.5. For \( w \in H \) with \( o(w) = p^n \) there are \( a \in \Omega_n(H) \geq \langle x, y \rangle \) and \( z_1 \in \langle z \rangle \) such that \( w = az_1 \). It follows that

\[ |\langle w \rangle : \langle z \rangle \cap \langle w \rangle| = |\langle w, z \rangle : \langle z \rangle| = |\langle a, z \rangle : \langle z \rangle| = |\langle a \rangle : \langle a \rangle \cap \langle z \rangle| \leq p^n \]

and hence \( |\langle z \rangle \cap \langle w \rangle| \geq p^n \). Thus \( \Omega_n(\langle z \rangle) \leq \langle w \rangle \). Since \( H \) is generated by its elements of maximal order, \( \Omega_n(\langle z \rangle) \leq Z(H) \). In particular, \( \Omega_n(\langle z \rangle) \leq Z(\Omega_n(H)) \) and by 2.3.16, applied to \( \Omega_n(H) \), this group is abelian. But this is impossible since \( x, y \in \Omega_n(H) \). Thus (17) holds.

Let \( \mathcal{S} \) be the set of all finite subgroups of \( G \) containing \( x \) and \( y \). Any \( H \in \mathcal{S} \) is a nonabelian \( M^* \)-group and hence every Iwasawa triple \((A, b, s)\) for \( H \) satisfies \( p^s < \text{Exp } G \); we denote the maximal integer \( s \) occurring in an Iwasawa triple for \( H \) by \( s(H) \). We choose a subgroup \( M \in \mathcal{S} \) with minimal \( s(M) \) and among these with maximal \( \text{Exp } M' \), that is, satisfying

\[ \text{(18)} \quad s(M) \leq s(H) \text{ for all } H \in \mathcal{S}, \text{ let } s(M) = s, \text{ and} \]

\[ \text{(19)} \quad \text{Exp } M' \geq \text{Exp } H' \text{ for all } H \in \mathcal{S} \text{ with } s(H) = s(M). \]

We shall construct a special Iwasawa triple for \( M \) and from this an Iwasawa triple for \( G \). First we note the following.

\[ \text{(20)} \quad \text{If } M \leq H \in \mathcal{S} \text{ and } (C, d, t) \text{ is an Iwasawa triple for } H \text{ with } t = s(H), \text{ then } t = s \text{ and there is an element } u \in M \text{ such that } (C, u, s) \text{ is an Iwasawa triple for } H. \]

To show this let \( CM = K \) and \( |H : K| = p^j \). Since \( H = C \langle d \rangle \), \( K = C(K \cap \langle d \rangle) = C \langle d^p \rangle \). If \( \text{Exp } C = p^k \), then \( d \) induces an automorphism of order \( p^{k-t} \) in \( C \). Since \( K \) is not abelian, \( d^p \) induces a nontrivial automorphism of order \( p^{k-t-1} \) on \( C \) and there exists a generator \( d_1 \) of \( \langle d^p \rangle \) such that \( (C, d_1, t + j) \) is an Iwasawa triple for \( K \). As \( CM = K \), there exist \( c \in C \) and \( u \in M \) such that \( d_1 = cu \); hence \( (C, u, t + j) \) is an Iwasawa triple for \( K \). Now \( M = (C \cap M) \langle u \rangle \) and so \( (C \cap M, u, t + j) \) is an Iwasawa triple for \( M \). Hence \( t + j \leq s(M) = s \), on the other hand \( s \leq s(H) = t \) by (18). It follows that \( t = s \) and \( j = 0 \). Thus \( (C, u, s) \) is an Iwasawa triple for \( K = H \).
(21) There exists an Iwasawa triple \((A^*, b, s)\) for \(M\) with the property that for every \(M \leq H \in S\) there is an Iwasawa triple \((C, b, s)\) for \(H\) with \(A^* \leq C\).

Suppose that this is false. If \((A_1, b_1, s), \ldots, (A_r, b_r, s)\) are all the Iwasawa triples for \(M\) with third component \(s\), then for every \(i \in \{1, \ldots, r\}\) there exists a subgroup \(H_i\) in \(S\) such that \(M \leq H_i\) and \(H_i\) does not contain an Iwasawa triple of the form \((C_i, b_i, s)\) with \(A_i \leq C_i\). Since \(G\) is locally finite, \(H = H_1 \cdots \cdots \cdots H_r\) is finite; choose an Iwasawa triple \((C, d, t)\) for \(H\) with \(t = s(H)\). By (20), \(t = s\) and there is an element \(u \in M\) such that \((C, u, s)\) is an Iwasawa triple for \(H\). It follows that \((C \cap M, u, s)\) is an Iwasawa triple for \(M\), that is \(C \cap M = A_i\) and \(u = b_i\) for some \(i\). But then \((C \cap H_i, b_i, s)\) is an Iwasawa triple for \(H_i\) with \(A_i \leq C \cap H_i\). This contradiction yields (21).

(22) Let \(H_i \in S\) and suppose that \((A_i, b, s)\) are Iwasawa triples for \(H_i\) such that \(A_i \leq A_i\) for \(i = 1, 2\). Then \(A_1 \cup A_2\) is abelian.

For, the definition of an Iwasawa triple implies that \(U_s(A^*) = M'\) and \(U_s(A_i) = H'_i\). Furthermore by (20), \(s(H_i) = s\) and thus (19) shows that \(\text{Exp } A^* \geq \text{Exp } A_i\) for \(i = 1, 2\). On the other hand, \(A^* \leq A_1 \cap A_2\) and hence \(\text{Exp } A_i = \text{Exp } A^*\) for \(i = 1, 2\). By 2.3.5, \(A_1 \cup A_2\) has the same exponent as \(A^*\) and therefore contains an element \(a \in A^*\) of maximal order in its centre. By 2.3.16, \(A_1 \cup A_2\) is abelian.

Now let \(A\) be the join of all finite abelian subgroups \(C\) of \(G\) such that \(A^* \leq C\) and \(c^b = c^{1+p^s}\) for all \(c \in C\). For any such \(C\), \((C, b, s)\) is an Iwasawa triple for \(H = C \langle b \rangle \geq A^* \langle b \rangle = M\). So (22) shows that any two such \(C\)'s centralize each other, that is, \(A\) is abelian. It follows that \(a^b = a^{1+p^s}\) for all \(a \in A\). If \(g \in G\), then \(H = \langle M, g \rangle \in S\) and by (21), \(g \in C\langle b \rangle \leq A\langle b \rangle\) for some Iwasawa triple \((C, b, s)\) of \(H\) with \(A^* \leq C\). Thus \(G = A\langle b \rangle\) and \(A \leq G\). If \(\text{Exp } A = p^k\) and \(|G : A| = p^m\), then \(s < k\) since \(G\) is not abelian. Furthermore \(b\) induces a power automorphism of order \(p^{k-s}\) in \(A\) and since \(b^{p^m} \in A\) operates trivially on \(A\), \(k - s \leq m\). Finally, \(s \geq 2\) in case \(p = 2\) since \((A^*, b, s)\) was an Iwasawa triple for \(M\). Thus \(G\) satisfies (b).

Clearly, the groups in (a) of Theorem 2.4.14 are the hamiltonian locally finite \(p\)-groups. We shall need an additional property of the other locally finite \(M\)-groups.

**2.4.15 Corollary.** Let \(G\) be a nonabelian locally finite \(p\)-group with modular subgroup lattice. Then \(\text{Exp } G = p^s\) is finite. If \(G\) is not hamiltonian, then there exists a triple \((A, b, s)\) with the properties given in 2.4.14(b) and, in addition, \(o(b) = p^s\) and \(s + m = n\).

**Proof.** That \(G\) has finite exponent follows immediately from 2.4.14. Suppose that \(G\) is not hamiltonian and let \((A, b, s)\) be as in 2.4.14(b). Since \(G/A\) is finite, we may choose \(A\) in such a way that no subgroup of \(G\) containing \(A\) properly occurs in a triple with these properties. Two elements of order at most \(p^{s-1}\) generate a finite subgroup of \(G\) and by 2.3.5, their product has order at most \(p^{s-1}\). Thus \(\Omega_{s-1}(G)\) is the set of elements of order at most \(p^{s-1}\), also in the locally finite \(M\)-group \(G\). Therefore \(G\) is generated by its elements of order \(p^s\) and since \(G/A\) is cyclic, there exists a cyclic subgroup \(C\) of order \(p^s\) such that \(G = AC\). Let \(a_0 \in A\) and \(c \in C\) such that \(b = a_0c\). Then \(G = A\langle c \rangle\) and \(C = \langle c \rangle\); hence \(o(c) = p^s\) and \(a^c = a^{1+p^s}\) for all \(a \in A\). Since \(c^{p^m} \in A\), \(c^{p^m} = (c^{p^m})^c = c^{p^m(1+p^r)}\), that is \(p^{m+s} \equiv 0 \pmod{p^s}\) and hence
$m + s \geq n$. Suppose that $m + s > n$. Then $c^{p^{m-1}} \in C_G(A)$ since the automorphism induced by $c$ in $A$ has order at most $p^{s-1} < p^m$. Thus $A^* = \langle A, c^{p^{m-1}} \rangle$ would be abelian and $(c^{p^{m-1}})^c = c^{p^{m-1}} = (c^{p^{m-1}})^{1+p^r}$, that is, $(A^*, c, s)$ would have all the properties given in 2.4.14(b). This would contradict the choice of $A$. Hence $m + s = n$ and the triple $(A, c, s)$ has the desired properties.

**Torsion groups with modular subgroup lattices**

We say that a group $G$ is a Tarski group if it is infinite but every proper, nontrivial subgroup of $G$ has prime order. For a long time it was not known whether Tarski groups exist until Olshanskii [1979], using an extremely complicated inductive construction, produced the first examples of such groups. Clearly, the set of proper, nontrivial subgroups of a Tarski group $G$ is an infinite antichain and hence $L(G)$ is modular. If one adds a chain to the zero element of this lattice, one clearly also gets a modular lattice. Therefore we call a group $G$ an extended Tarski group if it contains a normal subgroup $N$ such that

1. $G/N$ is a Tarski group,
2. $N$ is cyclic of prime power order $p' \neq 1$, and
3. for every subgroup $H$ of $G$, $H \leq N$ or $N \leq H$.

It follows from (25) that for every minimal subgroup $H/N$ of $G/N$, $L(H)$ is a chain and hence $H$ is cyclic of order $p'^{r+1}$. Thus $N = Z(G)$ and $G$ is a $p$-group with modular subgroup lattice. Groups of this type do also exist (see Olshanskii [1991], p. 344). However, a complete description of all Tarski and extended Tarski groups is not known and seems difficult to establish. So we have to take the following result as our final description of periodic $M$-groups.

**2.4.16 Theorem** (Schmidt [1986]). Let $G$ be a torsion group. Then $G$ has modular subgroup lattice if and only if $G$ is a direct product of Tarski groups, extended Tarski groups and a locally finite $M$-group such that elements of different direct factors have relatively prime orders.
In order to prove this theorem we need four lemmas. The first shows how the Tarski groups get involved.

2.4.17 Lemma. Let \( x \) and \( y \) be elements of prime power order of an \( M \)-group \( G \) and suppose that \( H = \langle x, y \rangle \) is infinite.

(a) (Rudolph [1982]) If \( \langle x \rangle \cap \langle y \rangle = 1 \), then \( H \) is a Tarski group.

(b) If \( \langle x \rangle \cap \langle y \rangle \neq 1 \), then \( H \) is an extended Tarski group.

Proof. (a) Assume that the assertion is wrong and choose a counterexample in which \( o(x) + o(y) \) is minimal. Let \( X = \langle x \rangle \) and \( Y = \langle y \rangle \). Suppose first that \( o(x) \) and \( o(y) \) are primes. A proper, nontrivial subgroup \( K \) of \( H \) cannot contain both \( X \) and \( Y \). And if \( X \not\leq K \), say, then \( X \cap K = 1 \) and by 2.1.5, \([K/1] \simeq [X \cup K/X]\) is an interval in \([H/X] \simeq [Y/1]\), that is, \(|K|\) is a prime. Thus \( H \) is a Tarski group, contradicting the choice of \( G \).

It follows that \( o(x) \), say, is not a prime; let \( A = \Omega(X) \) and \( B = \Omega(Y) \). Again by 2.1.5, \([X \cup B/B]\) is a chain and every minimal subgroup of \( X \cup B \) is contained in the atom \( A \cup B \) of this chain. Thus \( A \cup B = \Omega(X) \cup B \leq X \cup B \). Similarly, \( A \cup B = \Omega(A \cup Y) \leq A \cup Y \) and hence \( A \cup B \leq X \cup Y = H \). Also by 2.1.5, \( X \) is a maximal subgroup of \( X \cup B \) and therefore \( A \leq \Phi(X) \leq X \times X^b \) for every \( b \in B \). It follows that \( A \leq X \cup B \); in particular, \( A \cup B \) is a finite group. Let \( Y_1 = Y \cap N_H(A) \). The modular law yields that \( N_H(A) = (X \cup Y) \cap N_H(A) = X \cup Y_1 \) and \( (A \cup Y_1) \cap X = A \cup (Y_1 \cap X) = A \). Thus \( N_H(A)/A \) is generated by the cyclic subgroups \( X/A \) and \( AY_1/A \) of prime power order intersecting trivially. Since \( N_H(A)/A \) contains the normal subgroup \( A \cup B/A \) of prime order, it is not a Tarski group. The minimality of \( o(x) + o(y) \) implies that \( N_H(A)/A \) is finite. Every conjugate of \( A \) in \( H \) is contained in the finite normal subgroup \( A \cup B \) of \( H \) and hence also the number \( |H : N_H(A)| \) of these conjugates is finite. So, finally, \( H \) is finite, a contradiction. Thus (a) holds.

(b) Let \( N = \langle x \rangle \cap \langle y \rangle \). Then \( N \) is cyclic of prime power order and lies in the centre of \( H \). Therefore \( H/N \) is infinite and hence is a Tarski group by (a). Thus (23) and (24) hold for \( H \). To show (25), suppose that there exists a subgroup \( K \) of \( H \) such that \( K \not\leq N \) and \( N \not\leq K \); let \( X = \langle x \rangle \). Since \( L(X) \) is a chain and \( N \leq X \), it follows that \( K \not\leq X \) and \( D = K \cap X < N \). As \( H/N \) is a Tarski group, \( X \) is a maximal subgroup of \( H \). So \( X \cup K = H \) and \([K/D] \simeq [H/X]\), that is, \( K/D \) is cyclic of prime order. Therefore \( H/D \) is generated by the cyclic subgroups \( X/D \) and \( K/D \) of prime power order intersecting trivially, but is neither finite nor a Tarski group. This contradicts (a). Thus (25) holds and \( H \) is an extended Tarski group.

The following lemma is the main step in the proof of Theorem 2.4.16. It shows in particular that there are no "Tarski groups of higher dimension", that is torsion groups \( G \) with \( L(G) \) modular of length at least 3 in which any two different minimal subgroups generate a Tarski group. For any group \( T \), we denote by \( \pi(T) \) the set of all primes dividing the order of an element of \( T \).

2.4.18 Lemma. Let \( G \) be a torsion group with modular subgroup lattice and suppose that the subgroup \( T \) of \( G \) is a Tarski group.
Modular lattices and abelian groups

(a) If \( x \in G \) of prime power order \( q^n \) (\( q \) a prime, \( n \in \mathbb{N} \)), then \( x \in T \) for \( q \in \pi(T) \) and \( x \in C_G(T) \) in case \( q \notin \pi(T) \).

(b) \( T \) is the set of all \( \pi(T) \)-elements in \( G \) and \( G = T \times C_G(T) \).

Proof. (b) is an immediate consequence of (a). For, every \( g \in G \) is the product of its primary components. Therefore by (a), every \( \pi(T) \)-element of \( G \) lies in \( T \) and every element of \( G \) is contained in \( \langle T, C_G(T) \rangle \). Since \( T \cap C_G(T) = Z(T) = 1 \), it follows that \( G = T \times C_G(T) \).

To prove (a) we use induction on \( n \) and first consider the case \( n = 1 \). So let \( x \in G \) with \( o(x) = q \) and suppose that \( x \notin T \); we have to show that \( x \in C_G(T) \) and \( q \notin \pi(T) \).

To do this let \( X = \langle x \rangle \), \( H = T \cup X \) and \( 1 \neq a \in T \). Take \( b \in T \) with \( T = \langle a, b \rangle \) and put \( S = \langle b, x \rangle \). Since \( \langle b \rangle \) and \( \langle x \rangle \) are different minimal subgroups of \( H \) and \( L(H) \) is modular of length 3, \( S \) is a maximal subgroup of \( H \). If \( S = S^a \), then \( S \cap T = \langle b \rangle \) would be invariant under \( a \) which is clearly not the case. Thus \( S \neq S^a \) and \( S \cap S^a \) is a minimal subgroup of \( H \) different from \( \langle a \rangle \). So, finally, \( K = \langle a \rangle \cup (S \cap S^a) \) is a maximal subgroup of \( H \). Since \( a \notin S \) and \( a \notin S^a \), \( K \cap S = S \cap S^a = K \cap S^a \) and hence

\[
(S \cap S^a)^a = (K \cap S)^a = K \cap S^a = S \cap S^a,
\]

that is, \( S \cap S^a \) is normalized by \( a \). Thus \( S \cap S^a \leq K \) and \( K \) is finite. As \( x \in S \), \( X \cap K = X \cap S \cap K = X \cap (S \cap S^a) \). So if \( X \neq S \cap S^a \), then \( X \cap K = 1 \) and hence \( X \cup K = H \). By 2.1.5, \( L(K) \cong [H/X] \cong L(T) \), a contradiction, since \( K \) is a finite and \( T \) an infinite group. Therefore \( X = S \cap S^a \). So \( X \) is normalized by \( a \) and as \( a \) was an arbitrary nontrivial element of \( T \), it follows that \( x \in C_G(T) \). Finally, if \( q \in \pi(T) \), then there would exist an \( a \in T \) with \( o(a) = q \). Then \( \langle a, x \rangle \) would be elementary abelian of order \( q^2 \) and \( ax \) would be an element of order \( q \) in \( G \) not contained in \( T \). But then \( ax \in C_G(T) \), as we have just shown, and hence also \( a \in C_G(T) \), a contradiction. Consequently, \( q \notin \pi(T) \) and this finishes the case \( n = 1 \).

Now let \( n \geq 2 \) and suppose that the assertion of the lemma is correct for \( n - 1 \); again let \( X = \langle x \rangle \) and \( H = T \cup X \), and put \( Z = \Omega(X) \). If \( T \cap X \neq 1 \), then \( T \cap X = Z \) and \( H = T \cup X = Y \cup X \) for some cyclic subgroup \( Y \) of \( T \) with \( T = Y \cup Z \). As \( H \) is neither finite nor a Tarski group, this would contradict 2.4.17. Hence \( T \cap X = 1 \) and the case \( n = 1 \) already settled shows that \( Z \leq C_G(T) \) and \( q \notin \pi(T) \). Thus \( Z \leq Z(H) \) and, by induction, \( TZ/Z \) is centralized by \( X/Z \). In particular, \( X \leq H \) and, as before, it follows that \( x \in C_G(T) \) since \( T \) cannot operate on \( X \).

We prove the corresponding result for the extended Tarski groups.

2.4.19 Lemma. Let \( G \) be a torsion group with modular subgroup lattice and suppose that the subgroup \( T \) of \( G \) is an extended Tarski group; let \( \pi(T) = \{ p \} \).

(a) If \( x \in G \) of prime power order \( q^n \) (\( q \) a prime, \( n \in \mathbb{N} \)), then \( x \in T \) for \( q = p \) and \( x \in C_G(T) \) in case \( q \neq p \).

(b) \( T \) is the set of all \( p \)-elements in \( G \).

Proof. Since \( T \) is a \( p \)-group, (b) clearly follows from (a). To prove (a), we first show that \( Z(T) \trianglelefteq G \). So suppose that \( Z(T) \) is not normal in \( G \). Then there exists \( g \in G \)
such that \( Z(T)^p \neq Z(T) \). Take \( c \in Z(T)^p \) with \( \langle c^p \rangle = Z(T) \cap Z(T)^p \), let \( H = T \cup \langle c \rangle \) and consider a maximal subgroup \( \langle a \rangle \) of \( T \). Since \( a \) and \( c \) are \( p \)-elements of different orders, \( \langle a, c \rangle \) is neither a Tarski nor an extended Tarski group. By 2.4.17, \( \langle a, c \rangle \) is a finite subgroup of \( G \) and then a \( p \)-group as 2.4.7(a) shows. Since \( c^p \in \langle a \rangle \), \( \langle a \rangle \) is a maximal subgroup of \( \langle a, c \rangle \) and hence normal in this finite \( p \)-group. It follows that \( Z(T) \leq H \). But then \( cZ(T) \) is an element of order \( p \) in \( H/T \) that does not lie in the Tarski \( p \)-subgroup \( T/Z(T) \); this contradicts 2.4.18.

Thus \( Z(T) \leq G \). By 2.4.18, \( xZ(T) \in T/Z(T) \) for \( q = p \), that is, \( x \in T \) in this case. So let \( q \neq p \). Then \( T/Z(T) \) is centralized by \( xZ(T) \). Therefore if \( \langle a \rangle \) is a maximal subgroup of \( T \), it follows that \( [x, a] \in Z(T) = \langle a^p \rangle \). So \( x \) induces an automorphism in \( \langle a \rangle \) centralizing \( \langle a \rangle/\Phi(\langle a \rangle) \) and as \( o(x) \) is prime to \( p \), \( x \) centralizes \( \langle a \rangle \). Since \( \langle a \rangle \) was an arbitrary maximal subgroup of \( T \), we conclude that \( x \in C_G(T) \).

The last of our four lemmas will be used to show that the product of all Tarski and extended Tarski groups in \( G \) has a locally finite complement.

2.4.20 Lemma. Let \( G \) be an \( M \)-group and let \( x_1, \ldots, x_r \in G \). If \( \langle x_i, x_j \rangle \) is finite for all \( i \) and \( j \), then also \( \langle x_1, \ldots, x_r \rangle \) is finite.

Proof. We may assume that the \( x_i \) are elements of prime power order; for, the primary components of the \( x_i \) satisfy the same assumptions as the \( x_i \) and also generate \( \langle x_1, \ldots, x_r \rangle \). So we prove the lemma under this additional assumption and use induction on \( o(x_1) + \cdots + o(x_r) \). Let \( H = \langle x_1, \ldots, x_r \rangle \) and let \( p \) be the largest prime dividing the order of one of the \( x_i \).

Suppose first that there exists another prime dividing one of these orders. Without loss of generality, let \( x_1, \ldots, x_s \) be the \( p \)-elements among the \( x_i \). Then for \( i \leq s \) and \( j > s \), the subgroup \( \langle x_i, x_j \rangle \) is a finite \( M \)-group and by 2.4.6, \( \langle x_i \rangle,x_j = \langle x_i \rangle \). Thus \( \langle x_1, \ldots, x_r \rangle \leq H \) and \( H = \langle x_1, \ldots, x_s \rangle \langle x_{s+1}, \ldots, x_r \rangle \) is finite since, by induction, \( \langle x_1, \ldots, x_s \rangle \) and \( \langle x_{s+1}, \ldots, x_r \rangle \) are finite.

Now suppose that all the \( x_i \) are \( p \)-elements and let \( x_1 \) be an element of maximal order among the \( x_i \). If \( o(x_1) \geq p^2 \), then 2.4.7(b) shows that \( \Omega(\langle x_1 \rangle) \) is normalized by every \( x_i \) and hence is normal in \( H \). By induction \( H/\Omega(\langle x_1 \rangle) \), and hence \( H \), is finite.

We are left with the case that \( o(x_i) = p \) for all \( i \). If all the \( \langle x_i, x_j \rangle \) are \( p \)-groups, any two of the \( x_i \) commute; it follows that \( H \) is abelian and hence finite. Finally, suppose that \( \langle x_1, x_2 \rangle \), say, is not a \( p \)-group. Then by 2.2.4, \( |\langle x_1, x_2 \rangle| = pq \) where \( q \) is a prime with \( q > p \). Let \( Q \) be the subgroup of order \( q \) in \( \langle x_1, x_2 \rangle \). We claim that \( \langle Q, x_1 \rangle \) is finite for all \( i \geq 3 \). For otherwise \( \langle Q, x_i \rangle \) would be a Tarski subgroup of the torsion group \( \langle x_1, x_2, x_i \rangle \), by 2.4.17. By 2.4.18, \( \langle Q, x_1 \rangle \) would have to contain the \( p \)-elements \( x_1 \) and \( x_2 \); but a Tarski group cannot have a subgroup \( \langle x_1, x_2 \rangle \) of order \( pq \). So \( \langle Q, x_1 \rangle \) is finite and by 2.4.6, \( Q \leq \langle Q, x_1 \rangle \). Thus \( Q \leq H \) and by induction, \( H/Q = \langle x_2, Q, \ldots, x_r, Q \rangle \) is finite. Therefore \( H \) too is finite.

Proof of Theorem 2.4.16. If \( G \) has the structure given in this theorem, then by 1.6.4, \( L(G) \) is isomorphic to a direct product of modular lattices and hence is modular. Conversely, suppose that \( G \) is a torsion group with modular subgroup lattice, let \( \mathcal{F} \) be the set of all Tarski subgroups and extended Tarski subgroups of \( G \) and let \( \pi \) be
the union of all the $\pi(T)$ with $T \in \mathcal{T}$. By 2.4.18 and 2.4.19, every $T \in \mathcal{T}$ is the set of all $\pi(T)$-elements of $G$ and hence is a normal subgroup of $G$. Since the Tarski groups are simple and every extended Tarski group has only one minimal subgroup, any two such groups intersect trivially and the $\pi(T)$ with $T \in \mathcal{T}$ form a partition of $\pi$.

Let $K$ be the set of all $\pi'$-elements in $G$. We shall show that $K$ is a locally finite subgroup of $G$. Then, clearly, $K$ is a normal subgroup of $G$ and since $K$ and the $T \in \mathcal{T}$ are coprime subgroups, $G$ is the direct product of $K$ and all the $T \in \mathcal{T}$. This will prove the theorem. First we show that

\[ \langle x, y \rangle \] is finite for all $x, y \in K$.

For, if $x = x_1 \ldots x_n$ and $y = y_1 \ldots y_s$ are written as products of their primary components, then all the $x_i, y_k$ are $\pi'$-elements and, clearly, $\langle x_i, x_j \rangle \leq \langle x \rangle$ and $\langle y_i, y_j \rangle \leq \langle y \rangle$ are finite for all $i$ and $j$. If $\langle x_i, y_j \rangle$ were infinite, then $\langle x_i, y_j \rangle$ by 2.4.17 and then $x_i$ would be a $\pi$-element, a contradiction. Thus all the $\langle x_i, y_j \rangle$ are finite. By 2.4.20, $\langle x_1, x_2, \ldots, x_n, y_1, \ldots, y_s \rangle = \langle x, y \rangle$ is finite and (26) holds.

We show now that $K$ is a subgroup of $G$. For this let $x, y \in K$ and suppose that $xy^{-1} \notin K$. Then there exists a prime $p \in \pi$ dividing $o(xy^{-1})$; let $T \in \mathcal{T}$ with $p \in \pi(T)$.

By (26), $\langle x, y \rangle$ is finite and by 2.4.18 or 2.4.19, $T \cap \langle x, y \rangle$ is the set of $\pi(T)$-elements in $\langle x, y \rangle$. Hence $T \cap \langle x, y \rangle$ is a normal Hall subgroup of $\langle x, y \rangle$ and the Schur-Zassenhaus theorem yields that there exists a complement $S$ to $T \cap \langle x, y \rangle$ in $\langle x, y \rangle$. This centralizes $T \cap \langle x, y \rangle$, again by 2.4.18 or 2.4.19. Thus $S$ is a normal subgroup of $\langle x, y \rangle$ and therefore contains the $\pi(T)'$-elements $x$ and $y$. Hence also $xy^{-1} \in S$, but $p$ divides $o(xy^{-1})$. This contradiction shows that $xy^{-1} \in K$ and that $K$ is a subgroup of $G$. By (26) and 2.4.20, $K$ is locally finite.

**Further topics**

Theorems 2.4.11, 2.4.13 and 2.4.14 (or 2.4.4 and 2.3.1 in the finite case), and finally 2.4.16 give the structure of nonabelian $M$-groups. These results are basic and will often be used. In the remainder of this section we point out some immediate consequences and report on related results.

In 2.4.5 we noted that every finite $M$-group is metabelian. The results mentioned above show that this is also true for locally finite $M$-groups and $M$-groups with elements of infinite order. Considering 2.4.16, we get the following result.

**2.4.21 Theorem.** Let $G$ be an $M$-group. If $G$ contains elements of infinite order or if no Tarski group is involved in $G$, then $G$ is metabelian. In particular, every projective image of an abelian group is metabelian.

If any two subgroups of the group $G$ permute, then $G$ is an $M$-group by 2.1.3. And, clearly, $G$ is locally finite if it is a torsion group. So 2.4.11 and the results on locally finite $M$-groups give the structure of these groups (see Exercise 3). In particular, we note the following.

**2.4.22 Theorem** (Iwasawa [1943]). If any two subgroups of the group $G$ permute, then $G$ is metabelian.
In the theory of finite groups, for inductive proofs, it is often useful to know for a certain class $\mathcal{X}$ of groups the class of all groups in which every proper subgroup (or proper factor group) is an $\mathcal{X}$-group. For the class $\mathcal{X}$ of $M$-groups, these classes have been studied extensively. First Napolitani [1971] determined the finite groups all of whose proper subgroups are $M$-groups. Since every finite $M$-group is supersoluble, these groups are soluble and Napolitani gave a complete list of them. Then Fort [1975] investigated finite groups $G$ in which

\[(27) \ [G/H] \text{ is modular}\]

for every nontrivial subgroup $H$ of $G$, that is, with weakly modular subgroup lattices. Also these groups are soluble, since the minimal simple groups do not have this property and Fort was able to determine them completely. Finally, Longobardi [1982] studied finite groups $G$ satisfying (27) for every nontrivial normal subgroup $H$ of $G$, that is, in which all proper factor groups are $M$-groups. Since every finite simple group has this property, Longobardi restricted herself to supersoluble groups of this type and produced a complete list of them. Slightly smaller than the class studied by Longobardi is the class of all finite groups in which (27) holds for every nontrivial modular subgroup $H$ of $G$. This class is interesting since it is clearly invariant under projectivities. Longobardi and Maj [1985] showed that the nonnilpotent groups in both classes coincide and, using Longobardi's list, determined the nilpotent groups in the smaller class. All these results are much too technical to be presented here.

Finally we mention a theorem of a quite different character. Fort [1983] proved that a finite group $G$ has modular subgroup lattice if and only if every maximal subgroup of $G$ is dually modular in $L(G)$; here an element $d$ of a lattice $L$ is called dually modular in $L$ if it satisfies

\[(28) \ x \cap (d \cup z) = (x \cap d) \cup z \text{ for all } x, z \in L \text{ with } x \geq z, \text{ and}\]

\[(29) \ d \cap (y \cup z) = (d \cap y) \cup z \text{ for all } y, z \in L \text{ with } d \geq z.\]

Note that these conditions are dual to (2) and (3) of 2.1 in the definition of modular elements of a lattice.

**Exercises**

1. (Jones [1945]) Let $G$ be a $P^*$-group of order $p^n q^m$ with $n, m \in \mathbb{N}$ and primes $p > q$ and suppose that $m \geq 2$ (that is, $G$ is not a $P$-group). Show that the group $\overline{G}$ is lattice-isomorphic to $G$ if and only if $\overline{G}$ is a $P^*$-group of order $p^n r^m$ where $r$ is a prime dividing $p - 1$.

2. Let $G$ be a nonabelian finite $P$-group. Determine $\text{Aut } G$ and eliminate Cooper's theorem (or 1.4.3) from the proof of Lemma 2.4.3.

3. Show that the following properties of a torsion group $G$ are equivalent.
   (a) Any two subgroups of $G$ permute.
   (b) $G$ is the direct product of its $p$-components and these are locally finite $p$-groups with modular subgroup lattices.
   (c) $G$ is a locally nilpotent $M$-group.
4. Let $G$ be an $M$-group with elements of infinite order. Show that $G$ is locally nilpotent but in general not nilpotent.

5. Let $G$ be a nonabelian $M$-group such that $T(G)$ is a $p$-group and $G/T(G)$ is not cyclic.
   (a) Show that in Theorem 2.4.11(b) we may choose $p_i \neq p$ for all $i \in \mathbb{N}$. (Hint: If $a \in T(G)$ and $k \in \mathbb{N}$ such that $a^{p^k} \neq a$, show that there are only finitely many $j > k$ with $p_j = p$.)
   (b) If $p_i \neq p$ for all $i$, show that there exist $b_i \in T(G)$ such that the elements $x_i = z_i b_i$ satisfy $x_i^{p^j} = x_i$ for all $i \in \mathbb{N}$. Conclude that $G$ is the semidirect product of $T(G)$ and the torsion-free, locally cyclic group $Z = \langle x_1, x_2, \ldots \rangle$.

6. (Napolitani [1971]) Let $G$ be a finite group in which every proper subgroup is an $M$-group.
   (a) Show that $G$ is soluble.
   (b) If $|G|$ is divisible by 3 different primes, show that $G$ is supersoluble.
   (c) If $|G|$ is divisible by 4 different primes, show that $G$ is an $M$-group.

7. Let $G = H \times K$ be an $M$-group. Show that $G$ is abelian if to every $x \in H$ there exists $y \in K$ and to every $y \in K$ there exists $x \in H$ such that $o(x) = o(y)$. (In particular, $G$ is abelian if $H \cong K$; for a short direct proof of this result see Lukács and Pálfy [1986].)

2.5 Projectivities of $M$-groups

It is a remarkable fact that large classes of nonabelian $M$-groups admit projectivities onto abelian groups. In particular, all $M$-groups with elements of infinite order and all nonhamiltonian locally finite $p$-groups with modular subgroup lattices have this property. We shall construct these projectivities using special element maps, so-called crossed isomorphisms, in the locally finite case. More generally, we want to determine all projectivities of an arbitrary $M$-group. We start with the torsion groups and, in the light of 1.6.6, we may restrict our attention to the direct factors that appear in Theorems 2.4.16 and 2.4.13.

Tarski groups and extended Tarski groups

Clearly, every projective image of a Tarski group or an extended Tarski group is a Tarski group or extended Tarski group, respectively. Since a Tarski group is generated by two elements, it is countable. Therefore any two Tarski groups have the same number of minimal subgroups and are lattice-isomorphic. And two extended Tarski groups are lattice-isomorphic if and only if their subgroup lattices have the same lengths. Finally, the group of autoprojectivities of a Tarski or extended Tarski group is isomorphic to $\text{Sym } \mathbb{N}$, the symmetric group on a countable set.
We saw in Section 2.2 that every P-group is lattice-isomorphic to an elementary abelian group. It is not difficult to describe the projectivities of those \( P^* \)-groups that are not P-groups (see Exercise 2.4.1). Even without such a description, the results of 2.2 show that a \( P^* \)-group is lattice-isomorphic to an abelian group if and only if it is a P-group. For, if \( G \) is a \( P^* \)-group with nonnormal Sylow subgroup of order \( q^m \) and \( \phi \) is a projectivity from \( G \) to an abelian group \( \bar{G} \), then a subgroup \( H \) of order \( pq^m \) of \( G \) has indecomposable subgroup lattice. Its abelian projective image \( H^\alpha \) therefore must be a primary group and by 2.2.6, \( H^\alpha \) is elementary abelian. Thus \( m = 1 \) and \( G \) is a P-group.

Autoprojectivities of elementary abelian groups, and hence also P-groups, were described in 1.4.4; see also 2.6.7. If \( G \) is a \( P^* \)-group and not a P-group, every autoprojectivity of \( G \) fixes \( \Phi(G) \) and the p-component \( A \) of \( G \) where \( p \) is the larger prime involved in \( G \). It follows that \( P(G) \) is isomorphic to the subgroup of elements of \( P(G/\Phi(G)) \) fixing \( A\Phi(G) \), that is, to the group of autoprocessivities of an elementary abelian group fixing a maximal subgroup.

Hamiltonian 2-groups

These groups clearly cannot be lattice-isomorphic to an abelian group since the quaternion group \( Q_8 \) is determined by its subgroup lattice. In fact, this holds for an arbitrary hamiltonian 2-group and we prove an even stronger result.

2.5.1 Theorem (Baer [1939a]). Every projectivity of a hamiltonian 2-group is induced by exactly four isomorphisms.

Proof. Let \( G \) be a hamiltonian 2-group, that is, \( G = Q \times A \) where \( Q \cong Q_8 \) and \( A \) is elementary abelian, and let \( \phi \) be a projectivity from \( G \) to some group \( \bar{G} \). Since \( Q^\alpha \) contains only one minimal subgroup, \( Q^\alpha \cong Q_8 \cong Q \). If \( x \in Q \) has order 4 and \( 1 \neq a \in A \), then \( \langle x^2, a \rangle^\phi \) is a four-group. Hence \( |\langle a \rangle^\phi| = 2 \) and \( A^\phi \) is an elementary abelian 2-group (see also 2.2.5). Furthermore, \( \langle x, a \rangle^\phi \) is a group of order 8 with 3 minimal subgroups and therefore is abelian since \( Q_8 \) has 1 and \( D_8 \) has 5 minimal subgroups. It follows that \( Q^\phi \leq C_G(A^\phi) \) and hence \( \bar{G} = Q^\phi \times A^\phi \).

Let \( H = Z(Q) \times A \) and define \( \tau: H \to H^\phi \) by \( \langle a^\tau \rangle = \langle a \rangle^\phi \) for \( a \in A \). Then, clearly, \( \tau \) is the only element map inducing \( \phi \) on \( H \). If \( a, b \in H \), and \( \langle a, b \rangle \) is a four-group, then \( \langle ab \rangle^\phi = \langle a^\tau b^\tau \rangle \) is the minimal subgroup different from \( \langle a \rangle^\phi \) and \( \langle b \rangle^\phi \) in \( \langle a, b \rangle^\phi \). Thus \( \langle ab \rangle^\phi = \langle a^\tau b^\tau \rangle \) and this, of course, also holds if \( |\langle a, b \rangle| \leq 2 \). Now let \( Q = \langle x, y \rangle \), \( \langle x \rangle^\phi = \langle u \rangle \), \( \langle y \rangle^\phi = \langle v \rangle \) and let \( \sigma: G \to \bar{G} \) be the isomorphism satisfying \( x^\sigma = u \), \( y^\sigma = v \) and \( a^\sigma = a^\tau \) for all \( a \in A \). This isomorphism clearly induces \( \phi \) on \( Q \) and on \( H \). And if \( g \in G \) with \( g \notin Q \) and \( g \notin H \), then there exist \( z \in Q \) and \( a \in A \) with \( o(z) = 4 \) and \( g = za \). As \( \langle z \rangle^\phi = \langle z^\phi \rangle \) and \( \langle a \rangle^\phi = \langle a^\phi \rangle \), also \( \langle z, a \rangle^\phi = \langle z, a \rangle^\phi \) and since \( \langle g \rangle \) is the only cyclic maximal subgroup different from \( \langle z \rangle \) in \( \langle z, a \rangle \), it follows that \( \langle g \rangle^\phi = \langle g^\phi \rangle \). Thus \( \sigma \) induces \( \phi \). We had a choice of two elements each for \( u \) and \( v \). So we have shown that there are 4 different isomorphisms inducing \( \phi \). On the
other hand, every isomorphism inducing $\varphi$ has to map $x$ and $y$ onto a generator of $\langle x \rangle^\sigma$ and $\langle y \rangle^\sigma$, respectively. Hence there are exactly 4 such isomorphisms. □

Crossed isomorphisms

Let $G$ be a group and let $f$ be a map from $G$ into the set $\text{End} G$ of all endomorphisms of $G$. A bijective map from $G$ to a group $\bar{G}$ is called an $f$-isomorphism if it satisfies

1. $x^\sigma y^\sigma = (x^{f(y)} y)^\sigma$ for all $x, y \in G$.

A crossed isomorphism is an $f$-isomorphism for some map $f : G \to \text{End} G$. Examples of crossed isomorphisms are isomorphisms—here $f(x)$ is the identity for all $x \in G$—and antiisomorphisms. For, if $f(x)$ is the inner automorphism induced by $x^{-1}$, that is, $g f(x)(g^{-1}) = x g x^{-1}$ for all $g, x \in G$, then a bijective map $\sigma : G \to \bar{G}$ is an $f$-isomorphism if and only if $x^\sigma y^\sigma = (y x y^{-1} x)^\sigma = (y x)^\sigma$ for all $x, y \in G$.

We want to use crossed isomorphisms to construct projectivities between locally finite, nonhamiltonian $p$-groups and abelian groups. So we have to find out for which maps $f$ there exist $f$-isomorphisms and when they induce projectivities. The first question is easy to answer.

2.5.2 Theorem. Let $G$ be a group and $f : G \to \text{End} G$. If there exists an $f$-isomorphism from $G$ to some group $\bar{G}$, then

1. $f(1)$ is the identity,
2. $f(x) \in \text{Aut} G$ for all $x \in G$, and
3. $f(x)f(y) = f(x f(y) y)$ for all $x, y \in G$.

Conversely, suppose that (2)–(4) hold and define a new operation $\circ$ on $G$ by

$x \circ y = x^{f(y)} y$

for $x, y \in G$. Then $G^* = (G, \circ)$ is a group and the identity on $G$ is an $f$-isomorphism from $G$ to $G^*$.

Proof. Let $x, y, z \in G$. If $\sigma$ is an $f$-isomorphism from $G$ to $\bar{G}$, then $1^\sigma y^\sigma = (1^{f(y)} y)^\sigma = y^\sigma$ and hence

$1^\sigma = 1$.

Therefore $x^\sigma = x^\sigma 1^\sigma = (x^{f(1)})^\sigma$ and since $\sigma$ is injective, $x = x^{f(1)}$. Thus (2) holds. To prove (3), suppose that $x^{f(y)} = z^{f(y)}$. Then $x^\sigma y^\sigma = (x^{f(y)} y)^\sigma = (z^{f(y)} y)^\sigma = z^\sigma y^\sigma$. As $\sigma$ is injective, $x = z$ and hence $f(y)$ is injective. Since $\sigma$ is surjective, there exists $g \in G$ with $g^\sigma = (x y)^\sigma (y^\sigma)^{-1}$ and hence $(x y)^\sigma = g^\sigma y^\sigma = (g^{f(y)} y)^\sigma$. Again the injectivity of $\sigma$ implies that $x = g^{f(y)}$. Thus $f(y)$ is also surjective. It follows that $f(y) \in \text{Aut} G$ and (3) holds. Finally,

$(z^{f(x f(y) y)} x^{f(y) y})^\sigma = z^\sigma (x^{f(y)} y)^\sigma = z^\sigma x^\sigma y^\sigma = (z^{f(x)} x)^\sigma y^\sigma = (z^{f(x)} f(y) x^{f(y) y})^\sigma$

and since $\sigma$ is injective, it follows that $z^{f(x)f(y)} = z^{f(x f(y) y)}$. Thus also (4) holds.
Conversely, suppose that (2)–(4) are satisfied. Then

\[(x \circ y) \circ z = (x^{f(y)} y)^{f(z)} z = x^{f(y) f(z)} y^{f(z)} z = x^{f(y) f(z)} (y^{f(z)} z) = x \circ (y \circ z),\]

that is, the operation \(\circ\) is associative. Furthermore, \(1 \circ y = 1^{f(y)} y = y\). Since \(f(y)\) is surjective, there exists \(g \in G\) such that \(g^{f(y)} = y^{-1}\) and hence \(g \circ y = g^{f(y)} y = 1\). Thus \(G^* = (G, \circ)\) is a group and (5) implies that the identity is an \(f\)-isomorphism from \(G\) to \(G^*\).

2.5.3 Corollary. If \(\sigma: G \to G\) is an \(f\)-isomorphism, then the map \(v: G \to \text{Aut} G\) given by \(u^v := f(u^{\sigma^{-1}})\) for \(u \in G\) is a homomorphism.

**Proof.** Let \(u, v \in G\) and take \(x, y \in G\) with \(x^\sigma = u, y^\sigma = v\). By (3), \(u^v \in \text{Aut} G\) and (1) and (4) imply that

\[(uv)^v = (x^\sigma y^\sigma)^v = ((x^{f(y)} y)^\sigma)^v = f(x^{f(y)} y) = f(x) f(y) = u^v v^v.

Thus \(v\) is a homomorphism from \(G\) to \(\text{Aut} G\).

2.5.4 Lemma. Let \(G\) be a group, \(f: G \to \text{End} G\) and suppose that \(\sigma: G \to G\) is an \(f\)-isomorphism. For \(H \leq G\) and \(x \in G\),

1. \((Hx)^\sigma = H^\sigma x^\sigma\) if and only if \(H f(x) = H\), and
2. \(H^\sigma\) is a subgroup of \(G\) if and only if \(H^f(x) = H\) for all \(z \in H\).

**Proof.** By (3), \(f(x)^{-1}\) exists and (1) implies that for all \(z \in H\), \(z^\sigma x^\sigma = (z^{f(x)} x)^\sigma\) and \((zx)^\sigma = (z^{f(x)} z)^\sigma x^\sigma\). Since \(\sigma\) is injective, it follows that \((Hx)^\sigma = H^\sigma x^\sigma\) if and only if for all \(z \in H\), \(z^{f(x)} z\) is contained in \(H\), that is, \(H^{f(x)} = H\). Thus (7) holds. To prove (8), suppose first that \(H^\sigma \leq G\). Then for all \(z \in H\), \((Hz)^\sigma = H^\sigma = H^\sigma z^\sigma\) and hence \(H^{f(z)} = H\) by (7). Conversely, let \(H^{f(z)} = H\) for all \(z \in H\). If \(y, z \in H\), then (7) shows that \(y^\sigma z^\sigma \in (H^\sigma z)^\sigma = H^\sigma z^\sigma\). Furthermore there exists \(w \in H\) such that \(w^{f(z)} = z^{-1}\). By (6) and (1), \(1 = 1^\sigma = (w^{f(z)} z)^\sigma = w^\sigma z^\sigma\) so that \((z^\sigma)^{-1} = w^\sigma \in H^\sigma\). Thus \(H^\sigma\) is a subgroup of \(G\).

The lemma shows that if an \(f\)-isomorphism \(\sigma\) is to induce a projectivity, every endomorphism \(f(x)\) has to fix all subgroups containing \(x\). However, this condition is not sufficient. Even if all the \(f(x)\) are power automorphisms, \(\sigma\) need not induce a projectivity.

2.5.5 Example. Let \(G\) be an abelian group and suppose that \(N\) is a nontrivial subgroup of index 2 in \(G\). For \(a \in N\), let \(f(a) = id\), the identity map on \(G\); if \(x \in G\setminus N\), let \(f(x) = -id\), that is, \(g^{f(x)} = g^{-1}\) for \(g \in G\). Then (2) and (3) are satisfied and since \(|G : N| = 2\), it is easy to see that also (4) holds. So if we define the operation \(\circ\) on \(G\) by (5), then \(H = (G, \circ)\) is a group and \(\sigma = id\) is an \(f\)-isomorphism from \(G\) to \(H\). If \(x \in H \setminus N\) and \(a \in N\), then \(x \circ x = x^{f(a)} x = x^{-1} x = 1\) and \(x \circ a \circ x = (xa) \circ x = a^{-1} x^{-1} x = a^{-1}\). Since the multiplication in \(N\) has not changed, \(a^{-1}\) is also the inverse
to \(a\) in \(H\) and it follows that \(H\) is a generalized dihedral group. In particular, if \(G\) is cyclic, then \(H\) is a dihedral group and clearly not lattice-isomorphic to \(G\). Note that by (8), every subgroup of \(G\) is also a subgroup of \(H\), but \(H\) may contain additional subgroups.

In our computations with crossed isomorphisms we shall need some simple number-theoretic facts.

2.5.6 Lemma. Let \(p\) be a prime and suppose that \(i, k, n\) are natural numbers such that \(2 \leq k \leq n\). If \(p^i\) divides \(n\), then \(p^{i+1}\) divides \(m = \binom{n}{k} p^{k-1}\), except in the case \(p = 2, k = 2\) in which \(m\) is divisible just by \(p^i\).

**Proof.** The assertion certainly is correct if \(k \geq i + 2\); assume therefore that \(k < i + 1\). Now \(n = p'a\) where \(a \in \mathbb{N}\) and \(m = \frac{p^i a}{k^{k-1}} \prod_{j=1}^{k-1} \frac{p^j a - j}{j}\). Since \(j \leq i\), the powers of \(p\) in the factor \(j\) of the denominator cancel with those in \(p^i a - j\). Therefore, if \(k = p's\) with \((s, p) = 1\) and \(r \geq 0\), then \(m\) is divisible by \(p^r\) where \(t = p's - 1 + i - r\). Clearly \(t \geq i + 1\), except in the case \(r = s = 1, p = 2\) in which \(t = i\).

2.5.7 The Functions \(\mu_r\). For every integer \(r\), define \(\mu_r: \mathbb{N} \to \mathbb{Z}\) by

\[
\mu_r(n) = \sum_{j=0}^{n-1} r^j.
\]

Then for all \(n, m \in \mathbb{N}\),

\[
\mu_r(n)r^m + \mu_r(m) = \sum_{i=0}^{n-1} r^{i+m} + \sum_{j=0}^{m-1} r^j = \mu_r(n + m).
\]

We shall use the functions \(\mu_r\) to compute powers of elements. In fact, if \(\sigma\) is an \(f\)-isomorphism from \(G\) to \(\bar{G}\) and \(x^{f(x)} = x^r\) where \(r \in \mathbb{Z}\), then

\[
(x^\sigma)^n = (x^{\mu_r(n)})^\sigma.
\]

For, if \(n = 1\), then \(\mu_r(n) = 1\). And if (11) holds for \(n - 1\), then (1) and (10) imply that

\[
(x^\sigma)^n = (x^{\mu_r(n-1)})^\sigma x^\sigma = (x^{\mu_r(n-1)r + 1})^\sigma = (x^{\mu_r(n)})^\sigma.
\]

Let \(r = 1 + p^s a\) where \(p\) is a prime and \(a, s \in \mathbb{N}\) with \((p, a) = 1\) and \(s \geq 2\) in case \(p = 2\). Then \(x^r = \sum_{k=0}^{n} \binom{n}{k} p^{ks} a^k\) and hence

\[
\mu_r(n) = \frac{r^n - 1}{r - 1} = n + \sum_{k=2}^{n} \binom{n}{k} p^{(k-1)s} a^{k-1}.
\]

Let \(i \in \mathbb{N}\). If \(p^i | n\), then by 2.5.6, every summand on the right hand side of (12) is divisible by \(p^i\) and hence \(p^i | \mu_r(n)\). Conversely, suppose that \(p^i | \mu_r(n)\) and let \(n = p^jb\)
2.5 Projectivities of $M$-groups

with $(p, b) = 1$. By (12), $\mu_r(n) \equiv n \pmod{p}$ and hence $j \geq 1$. Since $s \geq 2$ in case $p = 2$, 2.5.6 shows that every summand $\binom{n}{k} n^{(k-1)s} a^{k-1}$ in (12) is divisible by $p^{i+1}$. Then (12) yields that $i < j + 1$. Thus $p^i | n$. We have shown that for all $i, n \in \mathbb{N}$,

$\hspace{1cm} (13) \ p^i | n \text{ if and only if } p^i | \mu_r(n).$

It follows that for all $x, y, m \in \mathbb{N}$,

$\hspace{1cm} (14) \ x \equiv y \pmod{p^m}$ if and only if $\mu_r(x) \equiv \mu_r(y) \pmod{p^m}.$

This is clear if $x = y$. If, say, $x = n + y$ with $n \in \mathbb{N}$, then $\mu_r(x) = \mu_r(n)r^y + \mu_r(y)$ by (10). Since $r \equiv 1 \pmod{p}$, therefore $\mu_r(x) \equiv \mu_r(y) \pmod{p^m}$ if and only if $\mu_r(n) \equiv 0 \pmod{p^m}$ and by (13), this is the case if and only if $n \equiv 0 \pmod{p^m}$. This proves (14). Now (14) shows that the map $\mu_{r,m}: \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ given by $\mu_{r,m}(x + p^m\mathbb{Z}) = \mu_r(x) + p^m\mathbb{Z}$ is well-defined and injective. Since $\mathbb{Z}/p^m\mathbb{Z}$ is finite, this map is also surjective and it follows that

$\hspace{1cm} (15) \text{ to every } i \in \mathbb{N} \text{ there exists } j \in \mathbb{N} \text{ such that } \mu_r(j) \equiv i \pmod{p^m}. \hfill \square$

We leave open the question exactly when a crossed isomorphism induces a projectivity, and content ourselves with the following result. Note that property (d) of the theorem only contains conditions on $f$ that are easy to control in $G$.

2.5.8 Theorem (Baer [1944]). Let $G$ be a group, $f: G \to \text{End } G$ and suppose that $\sigma: G \to \overline{G}$ is an $f$-isomorphism. Then the following properties (a)–(d) are equivalent.

(a) $\sigma$ induces a projectivity from $G$ to $\overline{G}$ and satisfies $(Hx)^\sigma = H^x x^\sigma$ for all $H \leq G$ and $x \in G$.

(b) For every $x \in G$, $f(x)$ is a power automorphism and $\langle x \rangle^\sigma = \langle x^\sigma \rangle$.

(c) For every $x \in G$, $f(x)$ is a power automorphism and $o(x^\sigma) = o(x)$.

(d) For all $x, y \in G$, the following conditions are satisfied.

(i) $f(x)$ is a power automorphism.

(ii) If $o(x)$ is infinite, then $x f(x) = x$.

(iii) If $o(x) = 2^m$ with $m > 1$, then $x f(x) = x^{1+4^i}$ with $i \in \mathbb{N}$.

(iv) If $xy = yx$ and $o(x)$ and $o(y)$ are finite and relatively prime, then $x f(y) = y f(x)$.

Proof. (a) $\Rightarrow$ (b). By (7), every $f(x)$ is a power automorphism. Since $\sigma$ induces a projectivity, $\langle x \rangle^\sigma = \langle x^\sigma \rangle$.

(b) $\Rightarrow$ (c). Since $\sigma$ is bijective, $o(x^\sigma) = |\langle x^\sigma \rangle| = |\langle x \rangle^\sigma| = o(x)$.

(c) $\Rightarrow$ (d). Clearly (i) holds. If $o(x)$ is infinite and $x f(x) \neq x$, then $x f(x) = x^{-1}$ and $x^\sigma x^\sigma = (x f(x))^{\sigma} = 1^{\sigma} = 1$ by (6). This would contradict the assumption $o(x^\sigma) = o(x)$. Hence (ii) holds and (iii) follows similarly. For, if $o(x) = 2^m$ with $m > 1$ and $x f(x) = x^{-1+4^i}$ with $j \in \mathbb{N}$, then $(x^\sigma)^2 = (x f(x))^{\sigma}$ by assumption would have order $2^{m-1}$, on the other hand its order would divide $2^{m-2}$. Finally, if $x, y \in G$ with $xy = yx$ and $(o(x), o(y)) = 1$, then $\langle xy \rangle = \langle x \rangle \times \langle y \rangle$. By (8), $\langle xy \rangle^\sigma$ is a subgroup of order $|\langle xy \rangle|$ containing the element $(xy)^\sigma$ of this order. Thus $\langle xy \rangle^\sigma$ is cyclic and since $x^\sigma, y^\sigma \in \langle xy \rangle^\sigma = \langle xy \rangle^{\sigma}$, we have $(x f(y))^\sigma = x^\sigma y^\sigma = y^\sigma x^\sigma = (y f(x))^\sigma$. Hence $x f(y) = y f(x)$ and since $x f(y) \in \langle x \rangle$ and $y f(x) \in \langle y \rangle$, it follows that $x f(y) = x$.  


(d) ⇒ (b). By (8), \( \langle x \rangle^a \) is a subgroup of \( \widetilde{G} \); we have to show that it is generated by \( x^a \). First let \( o(x) \) be infinite and write \( H = \langle x \rangle \). For \( 1 \neq y \in H \), \( x^{f(y)} = x \) or \( x^{f(y)} = x^{-1} \). In the latter case, it would follow that \( y^{f(y)} = y^{-1} \), contradicting (ii). Thus \( f(y) \) is the identity on \( H \). By (2), this also holds for \( y = 1 \) and therefore \( y^a z^a = (y^{f(z)} z^a) = (yz)^a \) for all \( y, z \in H \). Thus \( \sigma \) induces an isomorphism on \( H \) and it follows that \( \langle x \rangle^a = \langle x^a \rangle \). Now let \( o(x) \) be finite and suppose first that \( o(x) = p^m \) for some prime \( p \) and \( m \in \mathbb{N} \). If \( m = 1 \), then by (6), \( x^a \) is a nontrivial element in the group \( \langle x \rangle^a \) of order \( p \) and hence \( \langle x \rangle^a = \langle x^a \rangle \). So suppose that \( m \geq 2 \). Then \( |\langle x \rangle^a| = p^m \) and by 2.5.3, \( f(x) \) is the image of the \( p \)-element \( x^a \) under a homomorphism. Thus \( f(x) \) is a \( p \)-element in \( \text{Pot } G \) and therefore \( x^{f(x)} = x^r \) with \( r \equiv 1 \pmod{p} \); let \( r = 1 + p^s a \) where \( (p, a) = 1 \) and \( s \geq 1 \). The assumption (iii) implies that \( s \geq 2 \) in case \( p = 2 \). By (13), \( p^m \) does not divide \( \mu(p^{m-1}) \) and then (11) and (6) yield that \( (x^a)^{p^{m-1}} = (x^{\mu(p^{m-1})})^a \neq 1 \). It follows that \( x^a \) generates \( \langle x \rangle^a \). Finally suppose that \( x \) is of composite order, that is, \( x = yz \) with \( y \neq 1 \neq z, yz = zy \) and \( (o(y), o(z)) = 1 \), and assume that the assertion is true for elements of smaller order. Then \( o(y^a) = o(y) \), \( o(z^a) = o(z) \) and by (iv),
\[
y^a z^a = (y^{f(z)} z^a) = (yz)^a = (z^a)^a = (z^{f(y)})^a = z^a y^a.
\]
It follows that \( o(x^a) = o(y^a) o(z^a) = o(x) \) and this implies that \( \langle x \rangle^a = \langle x^a \rangle \).

(b) ⇒ (a). By 2.5.4, \( H^a \leq \widetilde{G} \) and \( (Hx)^a = H^a x^a \) for all \( H \leq G \) and \( x \in G \). We have to show that preimages of subgroups of \( \widetilde{G} \) are subgroups in \( G \). Let \( S \leq G \) satisfy \( S^a \leq \widetilde{G} \) and take \( x, y \in S \). Then \( x^a(y^a)^{-1} \in S^a \). Hence there exists \( z \in S \) such that \( x^a(y^a)^{-1} = z^a \), that is, \( x^a = z^a y^a = (z^{f(y)})^a \). It follows that \( x = z^{f(y)} y \) and hence \( xy^{-1} = z^{f(y)} \in \langle z \rangle \) since \( f(y) \) is a power automorphism. Thus \( (xy^{-1})^a \in \langle z \rangle^a = \langle z^a \rangle \leq S^a \), that is, \( xy^{-1} \in S \). Therefore \( S \) is a subgroup of \( G \) and \( \sigma \) induces a projectivity.

We remark that element maps satisfying condition (a) of Theorem 2.5.8 can be regarded as special types of isomorphism between the coset lattices of \( G \) and \( \widetilde{G} \), the so-called right affinities.

**Nonhamiltonian locally finite \( M \)-groups**

We use Theorem 2.5.8 to construct projectivities between abelian and nonabelian \( p \)-groups.

**2.5.9 Theorem** (Baer [1944]). Let \( \widetilde{G} \) be a locally finite \( p \)-group with modular subgroup lattice. If \( \widetilde{G} \) is not hamiltonian, then there exist an abelian \( p \)-group \( G \) and a crossed isomorphism \( \sigma: G \to \widetilde{G} \) that induces a projectivity between \( G \) and \( \widetilde{G} \) and satisfies \( (Hx)^a = H^a x^a \) for all \( H \leq G \) and \( x \in G \).

**Proof.** If \( \widetilde{G} \) is abelian, then \( G = \widetilde{G} \) and the identity \( \sigma \) on \( G \) has the desired properties. So suppose that \( \widetilde{G} \) is not abelian and take an Iwasawa triple \((A, b, s)\) for \( \widetilde{G} \) as described in 2.4.15. Then \( A \) is an abelian normal subgroup of \( \widetilde{G} \) with \( |\widetilde{G}: A| = p^m \), \( b \) is
an element of $\overline{G}$ with $o(b) = p^n = \text{Exp } \overline{G}$ and $s$ is an integer with $s \geq 2$ in case $p = 2$ such that $\overline{G} = A \langle b \rangle$, $b^{-1}ab = a^{1 + p^s}$ for all $a \in A$ and

(16) $m + s = n$. 

Let $r = 1 + p^s$ and $\mu = \mu_r$ the function defined in 2.5.7. By (13), $p^{-m}\mu(p^m)$ is an integer prime to $p$; let $t \in \mathbb{N}$ such that $0 < t < p^n$ and

(17) $t \equiv p^{-m}\mu(p^m) \pmod{p^n}$. 

Then $t \not\equiv 0 \pmod{p}$ and therefore the map $a \to a^t$ is an automorphism of $A$. Now $b^{p^n} \in A$ since $|\overline{G} : A| = p^n$, and hence there exists a unique element $a_0 \in A$ such that

(18) $b^{p^n} = a_0^t$. 

Let $G$ be the abelian group obtained by adjoining to $A$ an element $c$, subject to the relation

(19) $c^{p^n} = a_0$. 

Then $o(c) = o(b) = p^n = \text{Exp } G$. We want to construct a map $f : G \to \text{End } G$ satisfying (2)–(4) and property (d) of Theorem 2.5.8.

For this let $\alpha$ be the power automorphism of $G$ defined by $g^\alpha = g'^p = g^{1 + p^s}$ for all $g \in G$. By (16), $o(\alpha) = p^s$. Since $|G : A| = p^n$, every element $x \in G$ can be written uniquely in the form $x = ac^{i(x)}$ with $a \in A$ and $1 \leq i(x) \leq p^n$. By (15) there exist integers $j$ such that $\mu(j) \equiv i(x) \pmod{p^n}$ and (14) shows that any two such integers are congruent modulo $p^s$. Therefore, since $o(\alpha) = p^n$,

(20) $f(x) = \alpha^j$

is independent from the choice of the integer $j$ satisfying $\mu(j) \equiv i(x) \pmod{p^n}$ and hence is a well-defined power automorphism of $G$. Now $f(x)$ is the identity if and only if $p^n | j$ and by (13), this holds if and only if $p^n \equiv \mu(j) \equiv i(x) \pmod{p^n}$, that is, if and only if $x \in A$. Thus

(21) $A = \{x \in G | f(x) = id\}$. 

In particular, (2) holds and (3) is trivial. To prove (4), consider elements $x = a_1c^{i(x)}$ and $y = a_2c^{i(y)}$ of $G$, and let $j, k \in \mathbb{N}$ satisfy $\mu(j) \equiv i(x) \pmod{p^n}$ and $\mu(k) \equiv i(y) \pmod{p^n}$. Then $c^{p^n} \in A$, and the definition of $f(y)$ and (10) yield that modulo $A$,

$$x^{f(y)}y \equiv (c^{i(x)})^{f(y)}c^{i(y)} \equiv c^{\mu(j)p^k + \mu(k)} \equiv c^{\mu(j+k)}.$$ 

Thus $i(x^{f(y)}y) \equiv \mu(j + k) \pmod{p^n}$ and hence $f(x^{f(y)}y) = \alpha^{j+k} = \alpha^j\alpha^k = f(x)f(y)$.

So if we write $x \circ y = x^{f(y)}y$ for $x, y \in G$, then by 2.5.2, $G^* = (G, \circ)$ is a group and the identity $\sigma$ is a $f$-isomorphism from $G$ to $G^*$. Since $s \geq 2$ in case $p = 2$, $f$ has all the properties in (d) of 2.5.8 and therefore $\sigma$ induces a projectivity from $G$ to $G^*$ and satisfies $(Hx)^\sigma = H^\sigma x^\sigma$ for all $H \leq G$ and $x \in G$. If we can show that $G^*$ and $\overline{G}$ are isomorphic, then the theorem will be proved.

By (21), $f(x)$ is the identity for all $x \in A$ and hence elements of $A$ have the same product in $G$ and $G^*$. Furthermore $i(c) = 1$ and $\mu(1) = 1$ so that

(22) $f(c) = \alpha$. 

Since \( f(x \circ y) = f(x^{f(y)}) = f(x)f(y) \) for \( x, y \in G^* \), the map \( f \) can be regarded as an epimorphism from \( G^* \) to \( \langle x \rangle \leq \text{Aut} G \) with kernel \( A \). It follows from (22) that \( G^* \) is generated by \( A \) and \( c \). If \( d \) is the inverse to \( c \) in \( G^* \), then \( d^{f(c)}c = d \circ c = 1 \). So (21) and (22) imply that for \( a \in A \),

\[
d \circ a \circ c = (d^{f(a)}a) \circ c = (da)^{f(c)}c = d^{f(c)}ca^{f(c)} = a'.
\]

And if \( e \) is the \( p^m \)-th power of \( c \) in \( G^* \), then (11), (17), (19) and (18) yield that

\[
e = c^{\mu(p^m)} = c^{b^{p^m}} = a_0^t = b^{p^m}.
\]

Thus \( G \) and \( G^* \) are extensions of \( A \) by elements \( b \) and \( c \), respectively, inducing the same automorphism on \( A \) and subject to the same relation \( z^{p^m} = a_0^t \). Hence these groups are isomorphic and the proof of the theorem is complete.

By 1.6.4 and 1.6.5, the results of Section 2.2 and Theorem 2.5.9 give the structure of projective images of abelian torsion groups.

2.5.10 Theorem. The group \( G \) is lattice-isomorphic to an abelian torsion group if and only if \( G \) is a direct product of coprime \( P \)-groups and nonhamiltonian locally finite \( p \)-groups with modular subgroup lattices.

\( M \)-groups with elements of infinite order

Every nonabelian \( M \)-group with elements of infinite order admits a projectivity onto an abelian group. We shall prove this beautiful theorem of Sato [1951] in the remainder of this section. Our proof follows Mainardis [1991], [1992]; its main idea is to embed the given \( M \)-group into an \( M \)-group with divisible torsion subgroup. For such a group \( G \), the infinite cyclic subgroups can be described quite easily and Sato's construction of the projectivity between \( G \) and an abelian group becomes much simpler. To describe these cyclic subgroups, we have to compute powers of elements in \( G \) and for this we need the following functions.

2.5.11 The Functions \( \mu_r \) and \( \nu_r \). Let \( p \) be a prime and let \( U_p \) be the set of \((p \text{-adic})\) units in the ring \( R_p \) of \( p \)-adic integers. For \( r \in U_p \), the formula

\[
(9) \quad \mu_r(n) = \sum_{j=0}^{n-1} r^j
\]

again defines a function \( \mu_r \); this time, \( \mu_r \colon \mathbb{N} \rightarrow R_p \).

Let \( s \in \mathbb{N} \) with \( s \geq 2 \) in case \( p = 2 \) and assume that \( r = 1 + p^s a \) where \( 0 \neq a \in R_p \). Write \( n = p^t b \) where \( t \geq 0 \) and \( (b, p) = 1 \); then \( b \in U_p \) and hence there exists \( d \in U_p \) such that \( bd = 1 \). As in (12),

\[
\mu_r(n) = \frac{r^n - 1}{r - 1} = n + \sum_{k=2}^{n} \binom{n}{k} p^{(k-1)s} a^{k-1}.
\]
Again by 2.5.6, \( p^{t+1} \) divides \( \binom{n}{k} p^{(k-1)s} \) for \( 2 \leq k \leq n \) and hence there exists \( f \in R_p \) such that

\[
\mu_r(n) = n + p^{t+1}f = n + bdp^{t+1}f = n(1 + pdf).
\]

Thus there exists one and, since \( R_p \) is an integral domain, only one element \( g \in R_p \) such that \( \mu_r(n) = ng \). That is, we have a second function \( \nu_r : \mathbb{N} \to R_p \) given by

\[
(23) \quad \mu_r(n) = n\nu_r(n)
\]

and satisfying

\[
(24) \quad \nu_r(n) \equiv 1 \pmod{p} \text{ for all } n \in \mathbb{N}.
\]

As mentioned above, we can use the functions \( \mu_r \) and \( \nu_r \) to compute powers of elements.

2.5.12 Remark. Let \( G \) be a nonabelian \( M \)-group and let \( z \in G \) be an element of infinite order. Then by 2.4.11 there exist \( p \)-adic units \( r(p) \) with \( r(p) \equiv 1 \pmod{p} \) and \( r(2) \equiv 1 \pmod{4} \) such that \( c^z = c^{r(p)} \) for all \( c \in T(G)_p \), the \( p \)-component of \( T(G) \). And an obvious induction then shows that for every finite subset \( \pi \) of \( \mathbb{P} \), for all \( n \in \mathbb{N} \) and \( a_p \in T(G)_p \),

\[
(25) \quad \left( z \prod_{p \in \pi} a_p \right)^n = z^n \prod_{p \in \pi} a_p^{\mu(p)} = z^n \prod_{p \in \pi} a_p^{\nu(p)}.
\]

For, since \( \mu_{r(p)}(1) = 1 \), the first equation is clear if \( n = 1 \). And if it holds for \( n \), then

\[
\left( z \prod_{p \in \pi} a_p \right)^{n+1} = \left( z \prod_{p \in \pi} a_p \right) \left( z^n \prod_{p \in \pi} a_p^{\mu(p)} \right) = z^{n+1} \prod_{p \in \pi} a_p^{r(p) + \nu(p)} = z^{n+1} \prod_{p \in \pi} a_p^{\mu(p) + \nu(p)}.
\]

The second equation now follows from (23).

To simplify the notation, we define maps \( v(z, n) : T(G) \to T(G) \) by

\[
(26) \quad \left( \prod_{p \in \pi} a_p \right)^{v(z, n)} = \prod_{p \in \pi} a_p^{\nu(p)} \text{ for } a_p \in T(G)_p, \pi \subset \mathbb{P}, \pi \text{ finite.}
\]

By (24) and 1.5.5, the map \( c \to c^{\nu(p)} \) is a power automorphism of \( T(G)_p \) and hence

\[
(27) \quad v(z, n) \in \text{Pot } T(G) \text{ for all } z \in G \setminus T(G), n \in \mathbb{N}.
\]

And if we use these maps, we can rewrite (25) in the form

\[
(28) \quad (za)^n = z^n a^{v(z, n)} \text{ for all } z \in G \setminus T(G), a \in T(G), n \in \mathbb{N}.
\]

We need a result on the structure of \( M \)-groups with divisible torsion subgroup, due to Mainardis [1991], which is of independent interest.
2.5.13 Lemma. Let \( G \) be a nonabelian \( M \)-group with divisible torsion subgroup \( T(G) = T \).

(a) For every \( z \in G \setminus T, a \in T \) and \( n \in \mathbb{N} \), there exists \( b \in T \) such that \( z^n a = (zb)^n \).

(b) There exists a torsion-free, locally cyclic subgroup \( Z \) of \( G \) such that \( G = T Z \).

Proof. (a) Since \( T \) is divisible and \( v(z, n) \in \text{Pot } T \), there exists \( b \in T \) such that \( b_{\text{v}(z, n)} = a \). By (28), \((zb)^n = z^n b_{\text{v}(z, n)} = z^n a \).

(b) The assertion is clear if \( G/T \) is cyclic. So suppose that \( G/T \) is not cyclic. Then \( G \) has the structure given in 2.4.11(b). In particular, \( G = T \langle z_1, z_2, \ldots \rangle \) and \( z_{i+1}^p = z_i a_i \) with \( a_i \in T, p_i \in \mathbb{P} \). We show that there exist \( b_i \in T \) such that the elements \( x_i = z_i b_i \) satisfy \( x_i^{p_i} = x_i \) for all \( i \in \mathbb{N} \). For this we may take \( b_1 = 1 \). And if \( b_i \) exists, then \( a_i^{-1} b_i \in T \) and hence by (a) there exists \( b_{i+1} \in T \) such that

\[
x_{i+1}^p = (z_{i+1} b_{i+1})^{p_i} = z_i a_i^{-1} b_i = z_i b_i = x_i.
\]

Thus the \( x_i \) exist and \( \langle x_1, \ldots, x_i \rangle = \langle x_i \rangle \) is infinite cyclic for all \( i \). So \( Z = \langle x_1, x_2, \ldots \rangle \) is a torsion-free, locally cyclic subgroup of \( G \) satisfying \( T Z \geq T \langle z_1, z_2, \ldots \rangle = G \).

The main step in the proof of Sato's theorem is the following lemma.

2.5.14 Lemma (Mainardis [1992]). Let \( \bar{G} = T \langle z \rangle \) be a nonabelian \( M \)-group with divisible torsion subgroup \( T(\bar{G}) = T \) and \( o(z) \) infinite; let \( G = T \times \langle w \rangle \) where \( o(w) \) is infinite. For every \( \beta \in \text{Pot } T \), we define a map \( \tau : L_1(G) \rightarrow L_1(\bar{G}) \) in the following way. If \( X \in L_1(T) \), let \( X^\tau = X \); and if \( X \in L_1(G) \) such that \( X_T \), that is, \( X = \langle (wa)^n \rangle \) where \( n \in \mathbb{N} \) and \( a \in T \), define \( X^\tau = \langle (za^\beta)^n \rangle \). Then \( \tau = \tau(w, z; \beta) \) is a bijective map from \( L_1(G) \) onto \( L_1(\bar{G}) \) satisfying for all \( X, Y, Z \in L_1(G) \),

\[
(29) \ X \leq \langle Y, Z \rangle \text{ if and only if } X^\tau \leq \langle Y^\tau, Z^\tau \rangle.
\]

Thus, by 1.3.2, \( \tau \) induces a projectivity from \( G \) onto \( \bar{G} \).

Proof. First of all, note that \( \tau \) is well-defined. For, if \( X \) is an infinite cyclic subgroup of \( G \), then just one of its two generators is of the form \( w^n b \) with \( n > 0 \) and \( b \in T \). Since \( T \) is divisible, there exists \( a \in T \) such that \( b = a^n \); thus \( X = \langle (wa)^n \rangle \). And if \( X = \langle (wa)^n \rangle = \langle (wc)^m \rangle \) where \( n, m \in \mathbb{N} \) and \( a, c \in T \), then \( n = m \) and \( a^n = c^m \). So if \( v(n) = v(z, n) \) is as in 2.5.12, then by (28),

\[
(za^\beta)^n = z^n a^{\text{v}(z, n)} = z^n a^{n \beta v(n)} = z^n c^{n \beta v(n)} = (zc^\beta)^n.
\]

This shows that \( \tau \) is a well-defined map from \( L_1(G) \) to \( L_1(\bar{G}) \). If \( \bar{X} \) is a cyclic subgroup of infinite order in \( \bar{G} \), again one of the two generators of \( \bar{X} \) has the form \( z^n b \) where \( n \in \mathbb{N} \) and \( b \in T \). By (a) of 2.5.13 and since \( \beta \in \text{Pot } T \), there exists \( a \in T \) such that \( z^n b = (za^\beta)^n \) and hence \( \bar{X} = \langle (wa)^n \rangle^\tau \). Thus \( \tau \) is surjective. And if \( \langle (wa)^n \rangle^\tau = \langle (wc)^m \rangle^\tau \), then \( z^n a^{\beta v(n)} = z^m c^{\beta v(m)} \) and since \( n, m \in \mathbb{N} \), this implies that \( n = m \) and \( (a^n)^{\beta v(n)} = (c^m)^{\beta v(m)} \). Since the map \( t \rightarrow t^{\beta v(n)} \) is an automorphism of \( T \), it follows that \( a^n = c^m \). Thus \( \tau \) is bijective.
It remains to be shown that $\tau$ satisfies (29). So let $X, Y, Z \in L_1(G)$. Note that by 2.4.11, any two subgroups of $G$ permute so that $\langle Y', Z' \rangle = Y'Z'$ and also, of course, $\langle Y, Z \rangle = YZ$. If $Y$ and $Z$ are finite, then $Y, Z \leq T$ and since $\tau$ is the identity on $L_1(T)$, (29) clearly holds for $X, Y, Z$. Suppose next that $Y$ is infinite and $Z$ is finite. Then $Y = \langle (wa)^n \rangle$ and $Z = \langle b \rangle$ where $n \in \mathbb{N}$ and $a, b \in T$. Let $X \leq YZ$. If $X$ is finite, $X < T$ and since $\tau$ is the identity on $L_1(T)$, (29) clearly holds for $X, Y, Z$. Suppose next that $Y$ is infinite and $Z$ is finite. Then $Y = \langle (wa)^n \rangle$ and $Z = \langle b \rangle$ where $n \in \mathbb{N}$ and $a, b \in T$. Let $X < YZ$. If $X$ is finite, $X < T$ and (29) holds. So let $X$ be infinite, that is $X = \langle (wa)^n b^j \rangle$ where $i, j \in \mathbb{N}$. Since $T$ is divisible, there exists $c \in T$ such that $c^n = b^j$. Thus $Y' = \langle (za^\beta)^n \rangle$ and $Z' = \langle b \rangle \geq \langle c^n \rangle$; since $\beta$ and $v(za^\beta, ni)$ are power automorphisms of $T$, using (28), we obtain

$$X' = \langle (wac)^n \rangle' = \langle (z(ac)^\beta)^n \rangle = \langle (za^\beta)^n c^n (za^\beta, ni) \rangle \leq Y'Z'. $$

Conversely, assume that $X' \leq Y'Z'$ and $X' \not\leq Z'$. Then $X' = \langle (za^\beta)^{nk} b^m \rangle$ where $k, m \in \mathbb{N}$. Since $T$ is divisible and $\beta$ and $v(nk)$ are power automorphisms of $T$, there exists $d \in T$ such that $b^m = d^{\beta nk(v(nk))}$. By (28),

$$X' = \langle (za^\beta)^{nk} b^m \rangle = \langle z^{nk} d^{\beta nk(v(nk))} d^{\beta nk(v(nk))} \rangle = \langle (z(ad)^\beta)^{nk} \rangle $$

and since $d^{nk} = b^{mv(nk) - 1} b^{-1} \in Z$, it follows that $X = \langle (wad)^{nk} \rangle = \langle (wa)^{nk} d^{nk} \rangle \leq YZ$. Thus (29) holds for $X, Y, Z$.

Finally suppose that $Y$ and $Z$ are infinite. We shall reduce this case to the one just dealt with. Now $YZ$, being a subgroup of $G = T \times \langle w \rangle$, has the form $H \times U$ where $H = YZ \cap T$ is the torsion subgroup of $YZ$ and $U$ is infinite cyclic. Clearly, $H \simeq HY/Y$ is cyclic. By the case already settled, $Y' \leq H'U'$ and $Z' \leq H'U'$, so that $Y'Z' = K'V'$ where $K' \leq H'$ and $V' \leq H'U'$ is infinite cyclic. Applying this case once again, we get that $Y \leq KV$ and $Z \leq KV$. Thus $HU = YZ \leq KV$ and therefore again $H' \leq K'V'$ and $U' \leq K'V'$. So we finally get that $Y'Z' = K'V' = H'U'$. Since (29) holds in this case, $X \leq YZ = HU$ if and only if $X' \leq H'U' = Y'Z'$. This finishes the proof of (29) and of the lemma.

2.5.15 Theorem (Sato [1951]). Let $\tilde{G}$ be an M-group with elements of infinite order. Then there exists an abelian group $G$ lattice-isomorphic to $\tilde{G}$.

Proof. The assertion is clear if $\tilde{G}$ is abelian; so let $\tilde{G}$ be nonabelian. By 2.4.12, we may assume that $T(\tilde{G}) = T$ is divisible. By 2.5.13, $\tilde{G} = TZ$ where $Z$ is a torsion-free, locally cyclic subgroup of $G$. Finally, by 2.5.14, we may assume that $Z$ is not cyclic. Thus there exist $z_i \in Z$ and primes $p_i$ such that $Z = \langle z_1, z_2, \ldots \rangle$ and $z_i^{p_i} = z_i$ for all $i \in \mathbb{N}$. Take a group $W = \langle w_1, w_2, \ldots \rangle$ isomorphic to $Z$ via the natural isomorphism mapping $z_i$ to $w_i$, let $G = T \times W$, $\tilde{G}_i = T \langle z_i \rangle \leq \tilde{G}$ and $G_i = T \times \langle w_i \rangle$ for all $i \in \mathbb{N}$. Then the $(G_i)_{i \in \mathbb{N}}$ form an ascending chain of subgroups of $G$ whose set-theoretic union is $\tilde{G}$; similarly for $\tilde{G}$. Inductively we define power automorphisms $\beta_1 = 1$ and $\beta_{i+1} = \beta_i v(z_{i+1}, p_i)^{-1}$ of $T$ where $v$ is as in (27). Then by 2.5.14, for every $i \in \mathbb{N}$, the map $\tau_i = \tau(w_i, z_i; \beta_i): L_1(G_i) \to L_1(\tilde{G}_i)$ is bijective and induces a projectivity from $G_i$ onto $\tilde{G}_i$. All the $\tau_i$ clearly coincide on $L_1(T)$. If $X$ is an infinite cyclic subgroup of $G_i$, then $X = \langle (w_i a)^n \rangle$ for some $n \in \mathbb{N}$, $a \in T$ and since $T$ is divisible, there exists $b \in T$
such that \( b^{p_i} = a \); using (28), we obtain that

\[
X^{\tau_{i+1}} = \langle (w_i a)^{p_i} \rangle^{\tau_{i+1}} = \langle (w_{i+1} b)^{p_i} \rangle^{p_i} = \langle (z_{i+1} b^{p_i}) \rangle^{p_i} = \langle (z_i b^\beta) \rangle = X^\tau.
\]

Thus \( \tau_i \) is the restriction of \( \tau_{i+1} \) to \( L_1(G_i) \). If \( X \) is a cyclic subgroup of \( G \), there exists \( i \in \mathbb{N} \) such that \( X \leq G_i \) and we define \( X^{\tau} = X^\tau \). Then \( \tau \) is a well-defined bijective map from \( L_1(G) \) onto \( L_1(G) \). And if \( X, Y, Z \in L_1(G) \), there exists \( G_k \) such that \( X, Y, Z \leq G_k \) and it follows that (29) holds for \( X, Y, Z \) and \( \tau \). By 1.3.2, \( \tau \) induces a projectivity from \( G \) onto \( \overline{G} \).

Finally we mention that Sato's theorem also implies that every locally finite nonhamiltonian \( p \)-group with modular subgroup lattice is lattice-isomorphic to an abelian group (see Exercise 7). However, we chose to present Baer's proof since it is independent of Iwasawa's theorem on \( M \)-groups with elements of infinite order; what is more, it even yields an isomorphism between the coset lattices of the two groups. Unfortunately, as Exercise 6 shows, Baer's method cannot be used to prove Sato's theorem.

**Exercises**

1. Let \( G \) be a group, \( f: G \to \text{End} \ G, \sigma \) an \( f \)-isomorphism from \( G \) to a group \( \overline{G} \) and \( E = \{ x \in G | f(x) = \text{id} \} \). Show that for all \( x, y \in G \) and \( a \in E \),
   (a) \( E \) and \( E^\sigma \) are subgroups of \( G \) and \( G^\sigma \), respectively,
   (b) \( f(x) = f(y) \) if and only if \( x^{-1} y \in E \),
   (c) \( (x^\sigma)^{-1} a^\sigma x^\sigma = (x^{-1} a^{f(x)})^{x^\sigma} \).

2. Let \( A \) be an abelian group, \( f: A \to \text{Pot} \ A, \sigma \) an \( f \)-isomorphism from \( A \) to a group \( B \) and \( E = \{ a \in A | f(a) = \text{id} \} \). Show that every subgroup of \( E^\sigma \) is normal in \( B \) and that \( E^\sigma \) and \( B/E^\sigma \) are abelian.

3. Prove Theorem 2.5.10.

4. Show that an abelian \( p \)-group possesses a projectivity onto a nonabelian group if and only if it is not cyclic and has finite exponent which is at least 8 in case \( p = 2 \).

5. Let \( G = T \times Z \) where \( T \) is an abelian torsion group and \( Z \) is infinite cyclic. Show that \( G \) is lattice-isomorphic to a nonabelian group if and only if \( T \) contains an element of order 8 or there is a prime \( p > 2 \) such that \( T \) contains an element of order \( p^2 \).

6. Let \( G = T \times \langle w \rangle \) where \( T = \langle a \rangle \times \langle b \rangle \) with \( o(a) = o(b) = p^n \) for some prime \( p \), \( n \in \mathbb{N} \) and \( o(w) \) is infinite. Show that if \( \sigma \) is a crossed isomorphism from \( G \) to some group \( \overline{G} \) inducing a projectivity from \( G \) to \( \overline{G} \), then \( \overline{G} \) is abelian.

7. (Mainardis [1992]) Let \( G \) be a locally finite nonhamiltonian \( p \)-group with modular subgroup lattice. Show that there exists an \( M \)-group \( G^* \) with elements of infinite order such that \( G \) is isomorphic to a factor group of \( G^* \). (Hint: Show that, for arbitrary groups, if \( G = TZ, T \leq G \) and \( \mu: X \to Z \) is an epimorphism, then \( G \) is isomorphic to a factor group of a semidirect product of \( T \) by \( X \).)
2.6 Projectivities between abelian groups

We have seen that many abelian groups admit projectivities onto nonabelian groups (Exercises 2.5.4 and 2.5.5). In this section we shall show that, on the other hand, lattice-isomorphic abelian groups are nearly always isomorphic, and that frequently every projectivity between them is induced by a group-isomorphism. Exceptions to these classical results of Baer [1939a] are the groups of torsion-free rank 1. Their projectivities will be studied at the end of this section.

Element maps derived from projectivities

We want to construct group-isomorphisms from projectivities between abelian groups. In the definition of the element maps, we do not require the image group to be abelian. In general it will be an $M$-group and we shall use the following.

2.6.1 Lemma. Let $H$ be an $M$-group, $H = X \cup Y$ with $X$, $Y$ cyclic and $X \cap Y = 1$ and suppose that $Z$ is a cyclic subgroup of $H$ such that $X \cup Z = H = Y \cup Z$.

(a) If $Z = \langle xy \rangle$ where $x \in X$ and $y \in Y$, then $\langle x \rangle = X$ and $\langle y \rangle = Y$.

(b) If either $X$ is infinite or $H$ is a finite $p$-group and $|X| \geq |Y|$, then to every generator $\bar{x}$ of $X$ there exists exactly one generator $\bar{y}$ of $Y$ such that $Z = \langle \bar{x}\bar{y} \rangle$.

Proof. (a) Since $\langle x \rangle \cup Y \supseteq Z \cup Y = H$ and $H$ is an $M$-group, $X = (\langle x \rangle \cup Y) \cap X = \langle x \rangle \cup (Y \cap X) = \langle x \rangle$. Similarly, $Y = \langle y \rangle$.

(b) Suppose first that $X$ is infinite. If $Y$ is finite, then $Y \subseteq H$ and $Z$ is infinite by 2.4.8. If $Y$ is infinite, then $H$ is abelian by 2.4.10 and $Z$ clearly is infinite. In both cases, $H = XY$ and hence $Z = \langle xy \rangle$ where $x \in X$, $y \in Y$. Since $Z$ is infinite, $xy$ and $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^k$, for some integer $k$, are the generators of $Z$. By (a), $\bar{x} = x$ or $\bar{x} = x^{-1}$ and the assertion is clear.

Now suppose that $H$ is a finite $p$-group and $|X| \geq |Y|$. By 2.3.2, $H = XY$; let $Z = \langle xy \rangle$ where $x \in X$, $y \in Y$. By 2.3.5, $\text{Exp} H = |X| = p^n$, say, and 2.3.8 shows that $Q_8$ is not involved in $H$, that is, $H$ is an $M^*$-group. Since $x$ and $y$ are generators of $X$ and $Y$, respectively, $o(y) \leq o(x) = p^n$. By 2.3.10, $(xy)^{p^{n-1}} = x^{p^{n-1}}y^{p^{n-1}} \notin Y$ and, similarly, $(yx)^{p^{n-1}} \notin Y$. It follows that $|Z| = p^n = |X|$ and $\langle xy \rangle \cap Y = 1$. Suppose that there is another element $y_0 \in Y$ such that $\langle xy_0 \rangle = Z = \langle xy \rangle$. Then there exists $k \in \mathbb{N}$ such that $xy_0 = (xy)^k = x(yx)^{k-1}y$ and hence $y_0y^{-1} = (yx)^{k-1} \in \langle xy \rangle \cap Y = 1$, that is, $y_0 = y$. This shows that to every $x \in X$ there is at most one element $y \in Y$ with $Z = \langle xy \rangle$. Since $Z$ and $X$ have the same number of generators, it follows from (a) that to every generator $\bar{x}$ of $X$ there is exactly one $\bar{y} \in Y$ such that $Z = \langle \bar{x}\bar{y} \rangle$.

2.6.2 Lemma. Let $\varphi$ be a projectivity from the group $G$ to the group $\bar{G}$ and let $a, b \in G$ such that $\langle a, b \rangle = \langle a \rangle \times \langle b \rangle$. Assume that either $o(a)$ is infinite or $G$ and $\bar{G}$ are finite $p$-groups and $o(a) \geq o(b)$. Then if $\langle a \rangle^\varphi = \langle \bar{a} \rangle$, there exists a unique element $\bar{b} \in \bar{G}$ such that

(1) $\langle b \rangle^\varphi = \langle \bar{b} \rangle$ and $\langle ab \rangle^\varphi = \langle \bar{ab} \rangle$. 
We write \( \bar{b} = f(b; a, \bar{a}, \varphi) \) or, briefly, \( \bar{b} = f(b; a, \bar{a}) \) since we are never going to change the projectivity.

**Proof.** Since \( \langle a, b \rangle \) is abelian, \( H = \langle a, b \rangle^\circ \) is an \( M \)-group and \( X = \langle a \rangle^\circ, \ Y = \langle b \rangle^\circ, \) and \( Z = \langle ab \rangle^\circ \) satisfy the assumptions of 2.6.1(b). It follows that to the given generator \( \bar{a} \) of \( X \) there corresponds exactly one generator \( \bar{b} \) of \( Y = \langle b \rangle^\circ \) such that \( \langle \bar{a} \bar{b} \rangle = Z = \langle ab \rangle^\circ. \)

2.6.3 **Lemma.** Let \( G = \langle a \rangle \times B \) and let \( \varphi \) be a projectivity from \( G \) to some group \( \bar{G} \). Assume that either \( o(a) \) is infinite or \( G \) and \( \bar{G} \) are finite \( p \)-groups and \( o(a) \geq \text{Exp} \ B \). Let \( \langle a \rangle^\circ = \langle \bar{a} \rangle \) and define \( \sigma : B \to B^\circ \) by \( b^\circ = f(b; a, \bar{a}) \) for \( b \in B \). Then \( \sigma \) is bijective and induces \( \varphi \) on \( B \).

**Proof.** For every \( b \in B \), \( \langle a, b \rangle \) satisfies the assumptions of 2.6.2. Hence \( f(b; a, \bar{a}) \) is a uniquely determined element of \( \langle b \rangle^\circ \leq B^\circ \) and thus \( \sigma \) is a well-defined map from \( B \) to \( B^\circ \). If \( b_1, b_2 \in B \) such that \( b_1^\circ = b_2^\circ \), then \( \langle ab_1 \rangle^\circ = \langle \bar{a} \bar{b}_1 \rangle^\circ = \langle \bar{a} \bar{b}_2 \rangle^\circ = \langle ab_2 \rangle^\circ \). Since \( \sigma \) is bijective, \( \langle ab_1 \rangle = \langle ab_2 \rangle \) and there exists an integer \( k \) such that \( ab_1 = (ab_2)^k = a^k b_2^k \). It follows that \( a = a^k \) and hence \( k = 1 \) if \( o(a) \) is infinite and \( k = 1 \) (mod \( o(a) \)) if \( o(a) \) is finite. In both cases, \( b_1 = b_2^k = b_2 \). Thus \( \sigma \) is injective. To show that \( \sigma \) is also surjective take \( c \in B^\circ \) and let \( Y, Z < G \) such that \( Y^\circ = \langle c \rangle \) and \( Z^\circ = \langle ac \rangle \). If \( X = \langle a \rangle \), then \( X^\circ \cup Y^\circ = \langle \bar{a}, c \rangle = X^\circ \cup Z^\circ = Y^\circ \cup Z^\circ \) and hence \( H = X \cup Y = X \times Y \) satisfies the assumptions of 2.6.1(b). It follows that to the generator \( a \) of \( X \) there is a generator \( b \) of \( Y \) such that \( \langle ab \rangle = Z \). So \( \langle b \rangle^\circ = Y^\circ = \langle c \rangle \) and \( \langle ab \rangle^\circ = Z^\circ = \langle ac \rangle \), that is, \( c = f(b; a, \bar{a}) = b^\circ \). Thus \( \sigma \) is surjective. Finally, (1) shows that \( \langle b^\circ \rangle = \langle f(b; a, \bar{a}) \rangle = \langle b \rangle^\circ \) for all \( b \in B \) and it follows that \( H^\circ = H^\circ \) for all \( H \leq B \). Thus \( \sigma \) induces \( \varphi \) on \( B \).

2.6.4 **Lemma.** Under the hypotheses of 2.6.3, assume moreover that \( G \) and \( \bar{G} \) are abelian and let \( b, c \in B \).

(a) If \( \langle b \rangle \cap \langle c \rangle = 1 \), then \( (bc)^n = b^n c^n \).

(b) If \( \langle b \rangle \cap \langle c \rangle = \langle b \rangle \cap \langle c \rangle = 1 \), then \( (c^n)^n = (c^n)^n \) for all \( n \in \mathbb{Z} \).

**Proof.** (a) Since \( G \) and \( \bar{G} \) are abelian, \( \langle a, b, c \rangle = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \) and \( \langle a, b, c \rangle^\circ = \langle a \rangle^\circ \times \langle b \rangle^\circ \times \langle c \rangle^\circ \). Furthermore \( b^\circ = f(b; a, \bar{a}), \ c^\circ = f(c; a, \bar{a}) \) and \( (bc)^\circ = f(bc; a, \bar{a}) \) are by definition generators of \( \langle b \rangle^\circ, \langle c \rangle^\circ \) and \( \langle bc \rangle^\circ \), respectively, such that \( \langle ab \rangle^\circ = \langle \bar{a} b^\circ \rangle, \ \langle ac \rangle^\circ = \langle \bar{a} c^\circ \rangle \) and \( \langle abc \rangle^\circ = \langle \bar{a} (bc)^\circ \rangle \). If \( o(a) \) is infinite, then also \( o(ac) \) is infinite and if \( o(a) \) is finite, then \( o(ac) = o(a) \geq o(b) \). In both cases, \( \langle ac, b \rangle = \langle ac \rangle \times \langle b \rangle \) so that by 2.6.2 there exists \( \bar{b} = f(b; ac, \bar{a} c^\circ) \in \langle b \rangle^\circ \) with \( \langle acb \rangle^\circ = \langle \bar{a} c^\circ \bar{b} \rangle \). Similarly, we have \( \bar{c} = f(c; ab, \bar{a} b^\circ) \in \langle c \rangle^\circ \) with \( \langle abc \rangle^\circ = \langle \bar{a} b^\circ \bar{c} \rangle \).

Hence

\[
\langle abc \rangle^\circ = \langle \bar{a} (bc)^\circ \rangle = \langle \bar{a} b^\circ c^\circ \rangle = \langle \bar{a} \bar{b} \bar{c}^\circ \rangle
\]

and there exist integers \( r, s \) such that \( \bar{a} (bc)^\circ = (\bar{a} b^\circ c^\circ)^r = (\bar{a} \bar{b} \bar{c}^\circ)^r \). Since \( \bar{a} \in \langle a \rangle^\circ, \ b, b^\circ \in \langle b \rangle^\circ, \ c, c^\circ \in \langle c \rangle^\circ \) and the product of these three groups is direct, it follows that \( \bar{a} = \bar{a}^r = \bar{a}^r, \ b^r = (b^\circ)^r \) and \( (bc)^g = (bc)^g \). If \( o(a) \) is finite, this implies that \( r = s = 1 \) (mod \( o(\bar{a}) \)) and, since \( o(\bar{a}) = \text{Exp} \ G \), that \( x^r = x = x^s \) for all \( x \in \bar{G} \). If \( o(a) \) is infinite, \( r = s = 1 \). In both cases, it follows that \( \bar{b} = b^\circ \) and \( (bc)^g = \bar{b} c^\circ = b^\circ c^\circ \).
(b) Clearly, \((c^n)^\sigma = (c^\sigma)^n\) holds for \(n = 0\) and \(n = 1\). Suppose it is true for \(n - 1 \in \mathbb{N}\). Then by (a),

\[
b^\sigma(c^n)^\sigma = (b c^n)^\sigma = (b c c^{n-1})^\sigma = (b c)^\sigma(c^{n-1})^\sigma = b^\sigma c^\sigma(c^{n-1})^\sigma = b^\sigma(c^\sigma)^n
\]

and hence \((c^n)^\sigma = (c^\sigma)^n\). This proves the assertion for \(n > 0\). Again by (a), \(b^\sigma = (b c)^\sigma(c^{-1})^\sigma = b^\sigma c^\sigma(c^{-1})^\sigma\) and hence \((c^{-1})^\sigma = (c^\sigma)^{-1}\). Since \(b^{-1}\) and \(c^{-1}\) satisfy the same assumptions as \(b\) and \(c\), it follows that for \(n > 0\), \((c^{-n})^\sigma = ((c^{-1})^n)^\sigma = ((c^{-1})^\sigma)^n = (c^\sigma)^{-n}\).

2.6.5 Lemma. Let \(B\) and \(\bar{B}\) be abelian groups and suppose that \(\sigma : B \to \bar{B}\) is a bijective map satisfying \((c^n)^\sigma = (c^\sigma)^n\) for all \(c \in B\), \(n \in \mathbb{Z}\) and \((bc)^\sigma = b^\sigma c^\sigma\) for all \(b, c \in B\) with \(\langle b \rangle \cap \langle c \rangle = 1\). Then \(\sigma\) is an isomorphism.

Proof. If \(x, y \in B\), then by the structure of finitely generated abelian groups there are \(b, c \in B\) such that \(\langle x, y \rangle = \langle b \rangle \times \langle c \rangle\). Hence \(x = b^i c^j\), \(y = b^r c^s\) where \(i, j, r, s\) are integers and our assumptions yield that \((xy)^\sigma = (b^{i+r} c^{j+s})^\sigma = (b^\sigma)^{i+r} (c^\sigma)^{j+s} = x^\sigma y^\sigma\).

We summarize the results obtained so far.

2.6.6 Lemma. Let the hypotheses of 2.6.3 hold. Assume in addition that \(G\) and \(\bar{G}\) are abelian and that to every \(c \in B\) there exists \(b \in B\) such that \(\langle b \rangle \cap \langle c \rangle \neq \langle bc \rangle \cap \langle c \rangle = 1\). Then \(\sigma\) is an isomorphism inducing \(\varphi\) on \(B\).

Proof. By 2.6.3, \(\sigma\) is bijective and induces \(\varphi\) on \(B\). Then 2.6.4 yields that \(\sigma\) satisfies the assumptions of 2.6.5 and therefore is an isomorphism.

Torsion groups

We can now prove our first main result on projectivities between abelian groups.

2.6.7 Theorem (Baer [1939a]). Let \(G\) be an abelian \(p\)-group with the following property:

(3) If \(G\) contains an element of order \(p^n\), then \(G\) contains at least three independent elements of this order.

Then any projectivity \(\varphi\) of \(G\) onto an abelian group \(\bar{G}\) is induced by an isomorphism.

Proof. Let \(\mathcal{S}\) be the family of all finitely generated subgroups of \(G\) that satisfy (3). Clearly, \(\mathcal{S}\) is a local system of subgroups of \(G\) and by 1.3.7, it suffices to prove that \(\varphi\) is induced by an isomorphism on every \(X \in \mathcal{S}\). Thus we may assume that \(G\) itself is finitely generated and hence a finite group.

Our assumptions then imply that \(G = \langle a \rangle \times B\) where \(o(a) = p^n = \text{Exp } G\) and \(B\) contains two independent elements of order \(p^n\). Hence if \(c \in B\), there exists \(b \in B\) such
that $o(b) = p^n$ and $\langle b \rangle \cap \langle c \rangle = 1$, and therefore also $\langle bc \rangle \cap \langle c \rangle = 1$. Since $\bar{G}$ is abelian, $\bar{G} = \langle a \rangle \times B^e$ and by 2.2.6, $\bar{G}$ is a p-group. So all the assumptions of 2.6.6 are satisfied and if we choose $\bar{a} \in \bar{G}$ with $\langle \bar{a} \rangle = \langle a \rangle^p$, then $\sigma: B \to B^e$ given by $b^e = f(b; a, \bar{a})$ for $b \in B$ is an isomorphism inducing $\varphi$ on $B$. We define $\tau: G \to \bar{G}$ by $(a^i b)^i = a^i b^e$ for $b \in B$ and $i \in \mathbb{N}$. Then $\tau$ is clearly an isomorphism as well and we want to show that it induces $\varphi$. Since every group is the join of its cyclic subgroups, it suffices to prove that

$$(4) \langle a^i b \rangle^e = \langle (a^i b)^i \rangle \quad \text{for all } b \in B, i \in \mathbb{N}.$$ 

So let $b \in B$ and take $c \in B$ with $o(c) = p^n$ and $\langle c \rangle \cap \langle b \rangle = 1$. By 2.3.11 there exists a complement $D$ of $\langle c \rangle$ in $G$ containing $\langle a, b \rangle$. Hence $G = \langle c \rangle \times D$ and by 2.6.6, the map $v: D \to D^e$ defined by $d^e = f(d; c, c^e)$ is an isomorphism inducing $\varphi$ on $D$. Since $\sigma$ induces $\varphi$ on $B$, $\langle cb \rangle^e = \langle (cb)^e \rangle = \langle c^e b^e \rangle$ and the definition of $f$ in 2.6.2 shows that $b^e = f(b; c, c^e) = b^e$. Similarly,

$$\langle ca \rangle^e = \langle ac \rangle^e = \langle a f(c; a, a) \rangle = \langle a c^e \rangle = \langle c a \rangle$$

implies that $\bar{a} = f(a; c, c^e) = a^e$. Since $v$ induces $\varphi$ on $D$, we finally get that

$$\langle a^i b \rangle^e = \langle (a^i b)^e \rangle = \langle (a^e)^i b^e \rangle = \langle a^i b^e \rangle = \langle (a^i b)^e \rangle.$$ 

Thus (4) holds and $\tau$ induces $\varphi$.

2.6.8 Theorem (Baer [1939a]). Let $G$ and $\bar{G}$ be abelian p-groups for some prime $p$ and suppose that $\varphi$ is a projectivity from $G$ to $\bar{G}$. Then there exists an isomorphism $\sigma: G \to \bar{G}$ inducing $\varphi$ on $H = \langle \Omega_m(G) | \Omega_m(G)/\Omega_{m-1}(G) \rangle \geq p^3$.

Proof. If $x \in H$ is of order $p^n$, then $\Omega_n(H) = \Omega_n(G)$ is a direct product of cyclic groups (see Robinson [1982], p. 105) and since $|\Omega_n(G)/\Omega_{n-1}(G)| \geq p^3$, at least three of the direct factors are of order $p^n$. By 2.6.7 there exists an isomorphism $\tau: H \to H^e$ inducing $\varphi$ on $H$. If $H = G$, we are done. So suppose that $H < G$ and take a basic
2.6 Projectivities between abelian groups

Subgroup $B$ of $G$. Then $B$ is a direct product of cyclic groups and $G/B$ is a direct product of quasicyclic groups. Since $H < G$, $B$ has finite exponent and therefore is a direct factor of $G$ (see Robinson [1982], p. 106). Thus $G$ is a direct product of cyclic and quasicyclic groups and it follows that $G = X_1 \times X_2 \times Y$ where the $X_i$ are cyclic (possibly trivial) or quasicyclic and $Y \leq H$. Then $\overline{G} = X_1^* \times X_2^* \times Y^*$ and clearly there are isomorphisms $\sigma_i : X_i \rightarrow X_i^*$ extending the restrictions of $\tau$ to $X_i \cap H$. Thus there is an isomorphism $\sigma : G \rightarrow \overline{G}$ extending $\tau$.

Using 1.6.6, it is not difficult to extend our results from $p$-groups to arbitrary torsion groups (see Exercise 1).

**Groups with elements of infinite order**

We want to show that if $G$ is an abelian group of torsion-free rank $r_0(G) \geq 2$, then every projectivity of $G$ is induced by an isomorphism. To prove this we must first handle the following special case.

2.6.9 Lemma. If $G = \langle a \rangle \times \langle b \rangle$ where $o(a)$ and $o(b)$ are infinite, then every projectivity $\varphi$ from $G$ to some group $\overline{G}$ is induced by an isomorphism.

Proof. By 2.4.10, $\overline{G}$ is abelian and hence $\overline{G} = \langle a \rangle^* \times \langle b \rangle^* \cong G$. Let $\langle a \rangle^* = \langle \overline{a} \rangle$ and put $\overline{b} = f(b; a, \overline{a})$ where $f$ is the function defined in 2.6.2. Then $\langle b \rangle^* = \langle \overline{b} \rangle$, $\overline{G} = \langle \overline{a} \rangle \times \langle \overline{b} \rangle$ and we want to show that the isomorphism $\tau : G \rightarrow \overline{G}$ mapping $a$ to $\overline{a}$ and $b$ to $\overline{b}$ induces $\varphi$.

For $k \in \mathbb{N}$, $\varphi$ induces a projectivity from $G/\langle b^k \rangle = \langle a, b^k \rangle/\langle b \rangle \times \langle b \rangle/\langle b^k \rangle$ to $\overline{G}/\langle b^k \rangle^*$ and since $\langle a, b^k \rangle/\langle b^k \rangle$ is infinite cyclic, $|\langle b \rangle/\langle b^k \rangle| = |\langle b \rangle^*/\langle b^k \rangle^*|$ by 2.6.3. It follows that $\langle b^k \rangle^* = \langle \overline{b}^k \rangle$ and, similarly, $\langle a^k \rangle^* = \langle \overline{a}^k \rangle$.

Let $n, m \in \mathbb{Z}\setminus\{0\}$. Then by (1), $x = f(b^n; a^n, \overline{a}^n)$ is a generator of $\langle b^m \rangle^*$ satisfying $\langle a^n b^m \rangle^* = \langle \overline{a}^n x \rangle$. Since $\overline{b}^m$ and $\overline{b}^{-m}$ are the only generators of $\langle b^m \rangle^*$, it follows that there exists a sign $\varepsilon(n, m) \in \{+1, -1\}$ such that

$$\langle a^n b^m \rangle^* = \langle \overline{a}^n \overline{b}^{\varepsilon(n, m)m} \rangle.$$

We have to show that $\varepsilon(n, m) = 1$ for all $n, m$ since this will imply that $X^\varphi = X^\tau$ for all cyclic subgroups $X$ of $G$ and hence that $\varphi$ is induced by $\tau$. First of all,

$$\varepsilon(n, m) = \varepsilon(-n, -m).$$

For, $\langle a^{-n} b^{-m} \rangle^* = \langle a^n b^m \rangle^* = \langle \overline{a}^{-n} \overline{b}^{\varepsilon(n, m)m} \rangle = \langle \overline{a}^{-n} \overline{b}^{\varepsilon(n, m)(-m)} \rangle$ yields $\varepsilon(n, m) = \varepsilon(-n, -m)$, and $\varepsilon(n, m) = -\varepsilon(-n, -m)$ would imply that $\langle a^{-n} b^{-m} \rangle^* = \langle \overline{a}^{-n} \overline{b}^{\varepsilon(n, m)m} \rangle = \langle a^n b^m \rangle^*$, a contradiction. We show next that

$$\varepsilon(n, m) = \varepsilon(n - 1, m)$$

for $n \geq 2$.

For, since $\langle a \rangle \cap \langle a^{-1} b^{-1} \rangle = 1$, there exists $y = f(a^{-1} b^{-1}; a, \overline{a})$ satisfying $\langle y \rangle = \langle a^{-1} b^{-1} \rangle^* = \langle \overline{a}^{-1} \overline{b}^{\varepsilon(n-1, m)m} \rangle$ and $\langle \overline{y} \rangle = \langle a(a^{-1} b^{-1}) \rangle^* = \langle \overline{a} \overline{b}^{\varepsilon(n-1, m)m} \rangle$. Hence there exist $\mu, \nu \in \{+1, -1\}$ such that $\overline{a}^{1 + \mu(n-1)} \overline{b}^{\nu(n-1, m)m} = \overline{a}^{\nu} \overline{b}^{\nu e(n, m)m}$. It follows that $1 - \mu = (\nu - \mu)n$ and $\mu e(n-1, m) = \nu e(n, m)$. Since $n \geq 2$, the first equation
implies that \( v = \mu \) and the second then yields (7). Finally we claim that

\[
(8) \quad \varepsilon(n, m) = \varepsilon(n, m - 1) \text{ for } m \geq 2.
\]

Indeed \( z = f(a^n b^{m-1}; b, \bar{b}) \) satisfies \( \langle z \rangle = \langle a^n b^{m-1} \rangle^\varphi = \langle \bar{a}^n \bar{b}^{\varepsilon(n, m - 1)(m-1)} \rangle \) and \( \langle \bar{b}z \rangle = \langle ba^n b^{m-1} \rangle^\varphi = \langle \bar{a}^n \bar{b}^{\varepsilon(n, m)m} \rangle \), so that there exist \( \mu, \nu \in \{+1, -1\} \) such that \( \bar{a}^\mu b^{\mu(n, m-1)(m-1)+1} = \bar{a}^\nu b^{\nu(n, m)m} \). This implies that \( \mu = \nu \) and \( \mu \varepsilon(n, m - 1) - 1 = \mu m(\varepsilon(n, m - 1) - \varepsilon(n, m)); \) since \( m \geq 2 \) it follows that \( \varepsilon(n, m - 1) = \varepsilon(n, m) \).

By induction, (7) and (8) yield that \( \varepsilon(n, m) = \varepsilon(1, 1) \) for all \( n, m \in \mathbb{N} \). Since \( \bar{b} = f(b; a, \bar{a}), \langle ab \rangle^\varphi = \langle \bar{a} \bar{b} \rangle \) and hence \( \varepsilon(1, 1) = 1 \). By (6), \( \varepsilon(n, m) = 1 \) for all \( n, m \in \mathbb{Z} \setminus \{0\} \).

2.6.10 Theorem (Baer [1939a]). Let \( G \) be an abelian group which contains two elements \( a \) and \( b \) of infinite order such that \( \langle a \rangle \cap \langle b \rangle = 1 \). Then any projectivity of \( G \) is induced by exactly two isomorphisms.

Proof. Let \( \varphi \) be a projectivity from \( G \) to some group \( \overline{G} \). We have to show that \( \varphi \) is induced by an isomorphism; by 1.5.7, \( |\text{Pot } G| = 2 \), so that \( \varphi \) will then be induced by exactly two isomorphisms. By 2.4.10, \( \overline{G} \) is abelian.

We note first that 2.6.9 has a number of immediate consequences for the functions \( f(\ ; a, \bar{a}) \) defined in 2.6.2. Let \( a, b \in G \) be elements of infinite order such that \( \langle a \rangle \cap \langle b \rangle = 1 \); let \( \langle a \rangle^\varphi = \langle \bar{a} \rangle \) and put \( \bar{b} = f(b; a, \bar{a}) \). If \( \tau \) is an isomorphism from \( \langle a, b \rangle \) to \( \langle a, b \rangle^\varphi \) inducing \( \varphi \) there and if \( x, y \in \langle a, b \rangle \) such that \( \langle x \rangle \cap \langle y \rangle = 1 \), then \( \langle y \rangle^\varphi = \langle y^\tau \rangle \) and \( \langle xy \rangle^\varphi = \langle (xy)^\tau \rangle = \langle x^\tau y^\tau \rangle \) so that

\[
(9) \quad f(y; x^\tau) = y^\tau.
\]

Exactly one of the two isomorphisms inducing \( \varphi \) on \( \langle a, b \rangle \) satisfies \( a^\tau = \bar{a} \). It follows from (9) that for this \( \tau, b^\tau = f(b; a, \bar{a}) = \bar{b} \) and hence that

\[
(10) \quad \bar{a} = f(a; b, \bar{b}) \quad \text{and} \quad a \bar{b} = f(ab; a, \bar{a}).
\]

Again by (9), since \( (x^n)^\tau = (x^\tau)^n \) for every integer \( n \),

\[
(11) \quad f(x^n; a, \bar{a}) = f(x; a, \bar{a})^n \quad \text{for all } x \in \langle a, b \rangle \text{ with } \langle x \rangle \cap \langle a \rangle = 1.
\]

Finally we claim that

\[
(12) \quad f(x; a, \bar{a}) = f(x; b, \bar{b}) \quad \text{for all } x \in G \text{ with } \langle x \rangle \cap \langle a \rangle = 1 = \langle x \rangle \cap \langle b \rangle.
\]

For, if \( 1 \neq x^n \in \langle a, b \rangle \) for some \( n \in \mathbb{N} \), it follows from (9) that \( f(x^n; a, \bar{a}) = (x^n)^\tau = f(x^n; b, \bar{b}) \) and then (11) applied to \( \langle a, x \rangle \) and \( \langle b, x \rangle \) yields that

\[
f(x; a, \bar{a})^n = f(x^n; a, \bar{a}) = f(x^n; b, \bar{b}) = f(x; b, \bar{b})^n.
\]

This implies \( f(x; a, \bar{a}) = f(x; b, \bar{b}) \) since both elements generate the same infinite cyclic group \( \langle x \rangle^\varphi \). And if \( \langle x \rangle \cap \langle a, b \rangle = 1 \), then 2.6.4(a) and (10) yield that

\[
f(xab; a, \bar{a}) = f(x; a, \bar{a})f(ab; a, \bar{a}) = f(x; a, \bar{a})\bar{a}b.
\]

By (1), this implies that \( \langle abx \rangle^\varphi = \langle \bar{a} \bar{b} f(x; a, \bar{a}) \rangle \) and hence \( f(x; a, \bar{a}) = f(x; ab, \bar{a}b) \). Similarly, \( f(x; b, \bar{b}) = f(x; ab, \bar{a}b) \) and this yields (f2).
Now we define a map \( \sigma : G \rightarrow \bar{G} \) that will turn out to be an isomorphism inducing \( \varphi \). We choose a fixed pair \( u, v \) of elements of infinite order in \( G \) such that \( \langle u \rangle \cap \langle v \rangle = 1 \), put \( \bar{u} = f(v; u, \bar{u}) \). Let \( x \in G \). If \( \langle x \rangle \cap \langle u \rangle = 1 \), define \( x^\sigma = f(x; u, \bar{u}) \); and if \( \langle x \rangle \cap \langle u \rangle \neq 1 \), then \( \langle x \rangle \cap \langle v \rangle = 1 \) and we define \( x^\sigma = f(x; v, \bar{v}) \). By 2.6.3, \( \sigma|_x \) is a bijective map from \( X \) to \( X^\sigma \) for every cyclic subgroup \( X \) of \( G \) and since \( \varphi \) is a projectivity, this implies that \( \sigma \) is bijective and induces \( \varphi \). We claim that for every \( w \in G \) of infinite order with \( \langle u \rangle \cap \langle w \rangle = 1 \),

\[
(13) \quad x^\sigma = f(x; w, w^\sigma) \quad \text{for all} \ x \in G \text{ with } \langle x \rangle \cap \langle w \rangle = 1.
\]

For, \( w^\sigma = f(w; u, \bar{u}) \). So if \( \langle x \rangle \cap \langle u \rangle = 1 \), then \( x^\sigma = f(x; u, \bar{u}) = f(x; w, w^\sigma) \) by (12). And if \( \langle x \rangle \cap \langle u \rangle \neq 1 \), there exist \( n, m \in \mathbb{Z} \) such that \( x^n = u^m \) and (11) and (10) yield that

\[
f(x; w, w^\sigma)^n = f(x^n; w, w^\sigma) = f(u^m; w, w^\sigma) = f(u; w, w^\sigma)^m = \bar{u}^m.
\]

Thus \( f(x; w, w^\sigma) \) is the unique generator of \( \langle x \rangle^\sigma \) whose \( n \)-th power is \( u^m \), and since this description is also true of \( f(x; v, v^\sigma) = x^\sigma \), we obtain \( x^\sigma = f(x; w, w^\sigma) \).

Now we are able to prove that \( \sigma \) is an isomorphism. Let \( x, y \in G \) and suppose first that \( \langle x, y \rangle \cong C_\infty \times C_\infty \). Since in such a group there exist infinitely many infinite cyclic groups, every pair intersecting trivially, there is \( 1 \neq w \in \langle x, y \rangle \) such that \( \langle w \rangle \cap \langle x \rangle = \langle w \rangle \cap \langle y \rangle = \langle w \rangle \cap \langle xy \rangle = \langle w \rangle \cap \langle u \rangle = 1 \). If \( \tau : \langle x, y \rangle \rightarrow \langle x, y \rangle^\sigma \) is the isomorphism inducing \( \varphi \) on \( \langle x, y \rangle \) and satisfying \( w^\tau = w^\sigma \), then by (13) and (9), \( z^\sigma = f(z; w, w^\sigma) = f(z; w, w^\tau) = z^\tau \) for every \( z \in \{x, y, xy\} \). Thus \( (xy)^\sigma = (xy)^\tau = x^\tau y^\tau = x^\sigma y^\sigma \). Now suppose that \( \langle x, y \rangle \not\cong C_\infty \times C_\infty \). Then by the structure of finitely generated abelian groups, there exists a subgroup \( B \) of \( G \) of torsion-free rank 1 such that \( \langle x, y \rangle \subseteq B \). If \( \langle u \rangle \cap B = 1 \), take \( w = u \); if \( \langle u \rangle \cap B \neq 1 \), take any \( w \in G \) of infinite order satisfying \( \langle w \rangle \cap B = 1 \). In both cases, \( x^\sigma = f(c; w, w^\sigma) \) for all \( c \in B \). It follows from 2.6.4 that \( (bc)^\sigma = b^\sigma c^\sigma \) for all \( b, c \in B \) with \( \langle b \rangle \cap \langle c \rangle = 1 \) and that \( (c^\sigma)^\sigma = (c^\sigma)^\tau \) for all \( c \in B \) of finite order; if \( o(c) \) is infinite, then \( (c^\sigma)^\sigma = f(c^n; w, w^\sigma) = f(c; w, w^\sigma)^n = (c^\sigma)^n \) by (11). Thus 2.6.5 shows that \( \sigma|_B \) is an isomorphism and hence that \((xy)^\sigma = x^\sigma y^\sigma\). \( \square \)

In view of Baer's theorem it remains to study projectivities between abelian groups of torsion-free rank 1; we start with the torsion-free groups of this type.

**Torsion-free groups of rank one**

The structure of these groups is well-known (see Robinson [1982], p. 112); we review the basic facts. In general, if \( G \) is an abelian group, written additively, an element \( g \in G \) is said to be divisible in \( G \) by a positive integer \( m \) if \( g = mg \), for some \( g_1 \in G \). If \( p^k \) is the largest power of the prime \( p \) dividing \( g \), then \( h \) is called the \( p \)-height of \( g \) in \( G \); should \( g \) be divisible by every power of \( p \), we say that \( g \) has infinite \( p \)-height in \( G \). Let \( p_1, p_2, \ldots \) be the sequence of primes written in their natural order. Then the height of \( g \) in \( G \) is the vector \( h(g) = (h_1, h_2, \ldots) \) where \( h_i \) is the \( p_i \)-height of \( g \) in \( G \). Two such vectors \( h \) and \( t \) are called equivalent if \( h_i = k_i \) for almost all \( i \) and \( h_i = k_i \).
whenever \( h_i \) or \( k_i \) is infinite. This is an equivalence relation on the set \( \mathcal{H} \) of all such vectors, and the equivalence classes are termed types. The type of a group element \( g \) is defined to be the type of its height vector. If \( G \) is a torsion-free abelian group of rank 1, then all nonzero elements of \( G \) have the same type, which is referred to as the type of \( G \), in symbols \( t(G) \). The structure theorem now states that two torsion-free abelian groups of rank 1 are isomorphic if and only if they have the same type. Furthermore, every such group is isomorphic to a subgroup of the additive group \( \mathbb{Q} \) of rationals containing the integers. So we only have to study projectivities of these subgroups of \( \mathbb{Q} \) and the basic tool here is the following.

2.6.11 Lemma. Let \( \mathbb{Z} \leq G \leq \mathbb{Q} \) and suppose that \( \varphi \) is a projectivity from \( G \) to some subgroup \( \overline{G} \) of \( \mathbb{Q} \). If \( \langle p \rangle^\varphi = \langle p \rangle \) for all \( p \in \mathbb{P} \), then \( \overline{G} = G \) and \( \varphi \) is the trivial autoprojectivity of \( G \).

Proof. We want to show that \( \varphi \) fixes every cyclic subgroup of \( G \). First of all, \( \mathbb{Z}^\varphi = \mathbb{Z} \) since \( \mathbb{Z} = \langle 2 \rangle \cup \langle 3 \rangle \); in particular, \( Z \leq \overline{G} \). If \( p \) is a prime, \( r \in \mathbb{N} \) and \( s \) a nonnegative integer such that \( p^{-s} \in G \), then \( \langle p^r \rangle \leq \mathbb{Z} \leq \langle p^{-s} \rangle \leq G \) and \( \langle p^{-s} \rangle / \langle p^r \rangle \) is cyclic of order \( p^{r+s} \). By 1.2.8, \( \langle p^{-s} \rangle / \langle p^r \rangle \) is cyclic of order \( q^{r+s} \) for some prime \( q \) and as \( |\mathbb{Z}^\varphi / \langle p \rangle^\varphi| = |\mathbb{Z} / \langle p \rangle| = p \) divides the order of this group, \( q = p \). Since \( \mathbb{Z}^\varphi = \mathbb{Z} \), it follows that \( \langle p^r \rangle^\varphi = \langle p^r \rangle \) and \( \langle p^{-s} \rangle^\varphi = \langle p^{-s} \rangle \). Next, suppose that \( m = p_1^{r_1} \cdots p_k^{r_k} \) is the primary decomposition of the positive integer \( m \). Then \( \langle m \rangle = \langle p_1^{-r_1} \rangle \cap \cdots \cap \langle p_k^{-r_k} \rangle \) and hence \( \langle m \rangle^\varphi = \langle m \rangle \). If \( m^{-1} \in G \), then also \( p_i^{-r_i} \in G \) for all \( i \), and \( \langle m^{-1} \rangle = \langle p_1^{-r_1} \rangle \cup \cdots \cup \langle p_k^{-r_k} \rangle \) implies that \( \langle m^{-1} \rangle^\varphi = \langle m^{-1} \rangle \). Finally, if \( m, n \in \mathbb{Z} \) are coprime and \( \frac{m}{n} \in G \), then \( \langle m \rangle \) and \( \langle \frac{1}{n} \rangle \) are subgroups of \( G \) and the group \( \langle \frac{m}{n} \rangle \) is the unique subgroup \( H \) of \( \langle \frac{1}{n} \rangle \) satisfying \( \langle \frac{1}{n} \rangle = H \cup \mathbb{Z} \) and \( H \cap \mathbb{Z} = \langle m \rangle \). Since \( \langle \frac{1}{n} \rangle \), \( \mathbb{Z} \) and \( \langle m \rangle \) are invariant under \( \varphi \), it follows that \( \langle \frac{m}{n} \rangle^\varphi = \langle \frac{m}{n} \rangle \). Thus every cyclic subgroup of \( G \) is fixed by \( \varphi \) and hence \( G \leq \overline{G} \). If we apply this result to \( \varphi^{-1} \), we get that \( \overline{G} = G \) and then \( \varphi \) clearly is the trivial autoprojectivity of \( G \).

2.6.12 Corollary. If \( \mathbb{Z} \leq G \leq \mathbb{Q} \) and \( \varphi \) and \( \psi \) are projectivities from \( G \) to some group \( \overline{G} \) such that \( \langle p \rangle^\varphi = \langle p \rangle^\psi \) for all \( p \in \mathbb{P} \), then \( \varphi = \psi \).

Proof. Apply 2.6.11 to the autoprojectivity \( \varphi \psi^{-1} \) of \( G \).
Proof. It is well-known and easy to prove that Aut \( \mathbb{Q} \) is isomorphic to the multiplicative group of rational numbers: for \( q \in \mathbb{Q} \setminus \{0\} \), the multiplication \( \bar{q} : x \mapsto qx \) is an automorphism of \( \mathbb{Q} \) and every automorphism is of this form. If we write \( \rho_q \) for the autoprojectivity induced by \( \bar{q} \), then

\[
(14) \quad \langle x \rangle^{\rho_q} = \langle qx \rangle \quad \text{for all } x \in \mathbb{Q}
\]

and by 1.4.1, the map \( \rho : \bar{q} \to \rho_q \) is an epimorphism from Aut \( \mathbb{Q} \) to \( PA(\mathbb{Q}) \). Since \( \ker \rho = \{1, -1\} \), it follows that \( PA(\mathbb{Q}) \) is isomorphic to the multiplicative group of positive rational numbers.

Let \( \varphi \in P(\mathbb{Q}) \). Since \( \mathbb{Z} \) is cyclic, \( \mathbb{Z}^\varphi = \langle q \rangle = \mathbb{Z}^{\rho_q} \) for some \( q \in \mathbb{Q} \). Hence \( \rho_q^{-1} \varphi \in S \) and \( \varphi \in PA(\mathbb{Q})S \). If \( \varphi \in PA(\mathbb{Q}) \cap S \), then \( \varphi = \rho_r \) for some \( r \in \mathbb{Q} \) and \( Z = \mathbb{Z}^{\rho_r} = \langle r \rangle \). It follows that \( r \in \{1, -1\} \) and \( \varphi \) is the trivial autoprojectivity. Thus \( P(\mathbb{Q}) = PA(\mathbb{Q})S \) and \( PA(\mathbb{Q}) \cap S = 1 \).

We show next that \( S \cong Sym \mathbb{N} \). For this recall that \( p_1, p_2, \ldots \) is the sequence of primes written in their natural order. If \( \sigma \in Sym \mathbb{N} \), we define a map \( \bar{\sigma} : \mathbb{Q} \to \mathbb{Q} \) by

\[
(15) \quad 0^{\bar{\sigma}} = 0, \quad \left( \prod_{i=1}^{n} p_{i}^{k_{i}} \right)^{\bar{\sigma}} = \prod_{i=1}^{n} p_{\sigma(i)}^{k_{i}} \quad \text{for } k_{i} \in \mathbb{Z}, n \in \mathbb{N} \text{ and } (-x)^{\bar{\sigma}} = -x^{\bar{\sigma}} \text{ for } x > 0.
\]

Clearly, \( \bar{\sigma} \) is bijective and satisfies \( (xy)^{\bar{\sigma}} = x^{\bar{\sigma}}y^{\bar{\sigma}} \) for all \( x, y \in \mathbb{Q} \). Furthermore \( \mathbb{Z}^{\bar{\sigma}} = \mathbb{Z} \) and therefore \( \langle x \rangle^{\bar{\sigma}} = \langle xZ \rangle^{\bar{\sigma}} = x^{\bar{\sigma}}Z = \langle x^{\bar{\sigma}} \rangle \) for all \( x \in \mathbb{Q} \). Since every finitely generated subgroup of \( \mathbb{Q} \) is cyclic, Theorem 1.3.3 shows that \( \bar{\sigma} \) induces an autoprojectivity \( \psi_{\sigma} \) of \( \mathbb{Q} \) and as \( \mathbb{Z}^{\bar{\sigma}} = \mathbb{Z}, \psi_{\sigma} \in S \). We claim that the map \( \psi : Sym \mathbb{N} \to S; \sigma \mapsto \psi_{\sigma} \) is an isomorphism. Clearly,

\[
(16) \quad \langle x \rangle^{\psi_{\sigma}} = \langle x^{\bar{\sigma}} \rangle \quad \text{for all } x \in \mathbb{Q};
\]

in particular, \( \langle p_i \rangle^{\psi_{\sigma}} = \langle p_{\sigma(i)} \rangle = \langle p_{\sigma(i)} \rangle \) for all \( i \) and this shows that \( \psi \) is injective. Every \( \varphi \in S \) permutes the maximal subgroups of \( \mathbb{Z} \). So if we define \( \tau \in Sym \mathbb{N} \) by \( \langle p_i \rangle^\varphi = \langle p_{\tau(i)} \rangle \), then \( \langle p_i \rangle^\varphi = \langle p_i \rangle^{\psi_{\sigma}} \) for all \( i \) and by 2.6.12, \( \varphi = \psi_{\sigma} \). Thus \( \psi \) is surjective. And if \( \sigma, \tau \in Sym \mathbb{N} \), then

\[
\langle p_i \rangle^{\psi_{\sigma}\psi_{\tau}} = \langle p_{\sigma(i)} \rangle^{\psi_{\tau}} = \langle p_{\tau(i)} \rangle^{\psi_{\sigma}} = \langle p_i \rangle^{\psi_{\sigma\tau}}
\]

for all \( i \) and again by 2.6.12, \( \psi_{\sigma}\psi_{\tau} = \psi_{\sigma\tau} \). Thus \( \psi \) is an isomorphism. Finally, for \( q \in \mathbb{Q}, \sigma \in Sym \mathbb{N} \) and \( p \in \mathbb{P} \),

\[
\langle p \rangle^{\rho_q\psi_{\sigma}} = \langle qp \rangle^{\psi_{\sigma}} = \langle (qp)^{\bar{\sigma}} \rangle = \langle q^{\bar{\sigma}}p^{\bar{\sigma}} \rangle = \langle p^{\bar{\sigma}} \rangle^{\rho_{q_{\sigma}}} = \langle p \rangle^{\psi_{\sigma}}
\]

and hence, again by 2.6.12, \( \rho_q^{-1} \rho_q \psi_{\sigma} = \rho_{q_{\sigma}} \in PA(\mathbb{Q}) \). Since \( P(\mathbb{Q}) = PA(\mathbb{Q})S \), it follows that \( PA(\mathbb{Q}) \trianglelefteq P(\mathbb{Q}) \) and \( P(\mathbb{Q}) \) is the semidirect product of \( PA(\mathbb{Q}) \) by \( S \).

We finish our study of torsion-free abelian groups of rank 1 by showing that two such groups are lattice-isomorphic if and only if their types can be obtained from each other by a suitable permutation of the primes. Note that \( Sym \mathbb{N} \) operates on the set \( \mathcal{S} \) of height vectors by \( h^{\sigma} = (h_{\sigma^{-1}(1)}, h_{\sigma^{-1}(2)}, \ldots) \) for \( h = (h_1, h_2, \ldots) \in \mathcal{S} \) and \( \sigma \in Sym \mathbb{N} \). If \( h \) and \( f \) are equivalent, then so are \( h^{\sigma} \) and \( f^{\sigma} \) and it follows that for any type \( t, t^{\sigma} = \{h^{\sigma} | h \in t \} \) is again a type. Thus \( Sym \mathbb{N} \) also operates on the set of types.
For example, if $Z \leq G \leq Q$ and $t$ is an integer, then $p_i^t \in G$ if and only if $p_i^t = (p_i)^t \in G^\varphi$. This shows that $h_i = k_{-i(t)}$ if $b = (h_1, h_2, \ldots)$ and $t = (k_1, k_2, \ldots)$ are the height vectors of $1$ in $G$ and $G^\varphi$, respectively. Hence $k_i = h_{-i(t)}$ for all $i$, that is $t = h^x$ and it follows that

\begin{equation}
(17) \quad t(G^\varphi) = t(G)^x \text{ for all } Z \leq G \leq Q \text{ and } x \in \text{Sym } \mathbb{N}.
\end{equation}

2.6.14 Theorem (Fuchs [1960]). Two torsion-free abelian groups $G$ and $\bar{G}$ of rank 1 are lattice-isomorphic if and only if there exists a permutation $\sigma \in \text{Sym } \mathbb{N}$ such that $t(G)^x = t(\bar{G})^x$.

Proof. Let $G$ and $\bar{G}$ be torsion-free abelian groups of rank 1; we may assume that $G$ and $\bar{G}$ are subgroups of $Q$ containing $Z$. First suppose that $G$ and $\bar{G}$ are lattice-isomorphic and consider a projectivity $\varphi$ from $G$ to $\bar{G}$. Then $Z^\varphi$ is a cyclic subgroup of $\bar{G}$ and hence $Z^\varphi = \langle q \rangle$ for some $q \in Q$. Since $\varphi$ maps every maximal subgroup of $Z$ to a maximal subgroup of $\langle q \rangle$, there exists a permutation $\sigma \in \text{Sym } \mathbb{N}$ such that $\langle p_i \rangle^\varphi = \langle p_{\sigma(i)} q \rangle$ for all $i \in \mathbb{N}$. Let $\zeta$ be the projectivity induced by $(\psi_\sigma q)^{-1}$ in $\bar{G}$. Then $\varphi \zeta$ is a projectivity from $G$ to some subgroup $G^\varphi$ of $Q$ satisfying

\begin{equation}
(18) \quad \langle p_i \rangle^\varphi \zeta = \langle p_{\sigma(i)} q \rangle^\psi_\sigma \psi_1 = \langle p_{\sigma(i)} \rangle^\psi_1 = \langle p_i \rangle
\end{equation}

for all $i$. By 2.6.11, $G^\varphi \zeta = G$ and hence $\bar{G} = G^\varphi = G^\psi q$. Since $\rho_q$ is induced by an isomorphism, $G \simeq G^\varphi$ and therefore by (17), $t(\bar{G}) = t(G^\varphi) = t(G)^x$. For later use, we record what has been proved so far:

Theorem 2.6.14 shows that $Q$ is determined by its subgroup lattice, whereas, for example, all the groups $\mathbb{Q}_p$ of rational numbers with denominator a power of the prime $p$ are lattice-isomorphic but pairwise nonisomorphic.

Mixed groups of torsion-free rank one

It is an open problem to determine the projective closure of an arbitrary abelian group $G$ of torsion-free rank 1. Using the methods developed in this section, we give some necessary conditions for an abelian group to be lattice-isomorphic to $G$. We resume the multiplicative notation and write $G_p$ for the $p$-component of the torsion subgroup $T(G)$ of $G$. Define

\begin{equation}
M_p(G) = \langle \Omega_i(G_p) | \Omega_i(G_p) / \Omega_{i-1}(G_p) \rangle \text{ is not cyclic}\langle \rangle
\end{equation}

and put $M(G) = \langle M_p(G) | p \in \mathbb{P} \rangle$. 

2.6 Projectivities between abelian groups

2.6.15 Theorem. Let G be an abelian group of torsion-free rank 1 and let \( \varphi \) be a projectivity from G to an abelian group \( \overline{G} \). Then

(a) \( T(G) \cong T(\overline{G}) \),

(b) \( \varphi \) is induced by an isomorphism on \( M(G) \),

(c) \( \overline{G}/T(\overline{G}) \) is of rank 1 and there exists \( \sigma \in \text{Sym } \mathbb{N} \) fixing every \( i \in \mathbb{N} \) for which \( G_{p_i} \neq 1 \) such that \( t(G/T(G))^{p_i} = t(\overline{G}/T(\overline{G}))^{p_i} \).

Proof. Since cyclic groups are preserved under projectivities, \( T(G)^p = T(\overline{G}) \) and \( r_0(\overline{G}) = r_0(G) = 1 \). Let \( a \in G \) be of infinite order, take \( \bar{a} \in \overline{G} \) such that \( \langle a \rangle^p = \langle \bar{a} \rangle \) and consider the map \( v: T(G) \to T(\overline{G}) \) given by \( b^v = f(b; a, \bar{a}) \) where \( f \) is the function defined in 2.6.2. By 2.6.3, \( v \) is bijective and induces \( \varphi \) on \( T(G) \). In particular, \( |\langle b \rangle| = |\langle \bar{b} \rangle^p| \) for all \( b \in T(G) \) and hence \( G_p^p \) is the \( p \)-component of \( T(\overline{G}) \). By 2.6.8, \( G_p^p \cong G_p \) and therefore \( T(G) = Dr G_p^p \cong T(\overline{G}) \).

If \( c \in M_p(G) \) and \( o(c) = p^a \), say, then \( \Omega_n(G_p) \subseteq M_p(G) \) and \( \Omega_n(G_p)/\Omega_{n-1}(G_p) \) is not cyclic. Now \( \Omega_n(G_p) \) is a direct product of cyclic groups and it follows that there are at least two direct factors of order \( p^a \). Hence there exists \( b \in \Omega_n(G_p) \) such that \( \langle b \rangle \cap \langle c \rangle = 1 = \langle bc \rangle \cap \langle c \rangle \). By 2.6.6, the restriction of \( v \) to \( M_p(G) \) is an isomorphism inducing \( \varphi \) on \( M_p(G) \). It follows that \( v|_{M(G)} \) is an isomorphism inducing \( \varphi \) on \( M(G) = Dr M_p(G) \).

Finally, \( \varphi \) induces a projectivity \( \overline{\varphi} \) over the torsion-free groups \( G/T(G) \) and \( \overline{G}/T(\overline{G}) \) of rank 1. By (18), \( (T(G/T(G)))^p = (T(G/T(\overline{G})))^p \) where \( \sigma \in \text{Sym } \mathbb{N} \) satisfies \( \langle x \rangle^{\overline{\varphi}} = \langle y \rangle \) and \( \langle x^p \rangle^{\overline{\varphi}} = \langle y^{p^2} \rangle \) for a suitable nontrivial element \( x \in G/T(G) \). Take \( u \in G \) with \( \langle x \rangle = \langle uT(G) \rangle \). Then \( o(u) \) is infinite and \( \langle y \rangle = \langle \bar{u}T(\overline{G}) \rangle \) where \( \langle \bar{u} \rangle = \langle u \rangle^p \). If \( G \) contains an element \( b \) of order \( p \), then \( \langle u, b \rangle/\langle u^p \rangle \) is elementary abelian of order \( p^2 \) and by 2.2.5, \( |\langle u, b \rangle/\langle u^p \rangle| = p^2 \) as well. Hence \( \langle x^p \rangle^p = \langle \bar{u}^p \rangle \) and it follows that \( \langle x^p \rangle^{\overline{\varphi}} = \langle y^p \rangle \). This shows that \( p_{\sigma(i)} = p_i \) for those \( i \) for which \( G_{p_i} \neq 1 \).

If \( G \) does not split over \( T(G) \), then \( G \) and \( \overline{G} = T(G) \times (G/T(G)) \) satisfy (a) and (c) of Theorem 2.6.15; but clearly these are not lattice-isomorphic. For groups that split over their torsion subgroups, however, our conditions are necessary and sufficient.

2.6.16 Theorem (Ostendorf [1991]). Let \( G \) be an abelian group of torsion-free rank 1 that splits over its torsion subgroup. Then the abelian group \( \overline{G} \) is lattice-isomorphic to \( G \) if and only if \( \overline{G} \) splits over its torsion subgroup and satisfies

(a) \( T(\overline{G}) \cong T(G) \),

(b) \( \overline{G}/T(\overline{G}) \) is of rank 1 and there exists \( \sigma \in \text{Sym } \mathbb{N} \) fixing every \( i \in \mathbb{N} \) for which \( G_{p_i} \neq 1 \) such that \( t(G/T(G))^{p_i} = t(\overline{G}/T(\overline{G}))^{p_i} \).

Proof. If \( \varphi \) is a projectivity from \( G \) to \( \overline{G} \) and \( G = T(G) \times H \), then \( \overline{G} = T(G)^p \times H^p = T(\overline{G}) \times H^p \) since \( \overline{G} \) is abelian. Thus \( \overline{G} \) splits over \( T(\overline{G}) \) and the other assertions follow from 2.6.15. Conversely, suppose that \( G \) and \( \overline{G} \) satisfy the conditions of the theorem. Then \( G = T \times R \) and \( \overline{G} = \overline{T} \times \overline{R} \) where \( T, \overline{T} \) are isomorphic torsion groups, \( R, \overline{R} \) are torsion-free of rank 1 and there exists \( \sigma \in \text{Sym } \mathbb{N} \) fixing every \( i \in \mathbb{N} \) for which \( T_{p_i} \neq 1 \) such that \( t(R)^p = t(\overline{R}) \). Then \( R \) is isomorphic to a subgroup \( H \) of \( \mathbb{Q} \) containing \( \mathbb{Z} \) and by (17), \( t(H^{\psi_\sigma}) = t(H)^p = t(R)^p = t(\overline{R}) \) where \( \psi_\sigma \) is the auto-
projectivity of \( Q \) defined in (15) and (16). Hence \( H^\psi \simeq \bar{R} \) and, since we only want to show that \( G \) and \( \bar{G} \) are lattice-isomorphic, we may assume, using additive notation again, that \( G = T \oplus H \) and \( \bar{G} = T \oplus K \) where \( T \) is a torsion group, \( Z \leq H \leq Q \) and \( K = H^\psi = H^\bar{\psi} \). We want to construct a bijective map \( \tau \) from the set \( L_1(G) \) of cyclic subgroups of \( G \) to \( L_1(\bar{G}) \) such that for all \( X, Y, Z \in L_1(G) \),

\[
(19) \quad X \leq Y + Z \text{ if and only if } X' \leq Y' + Z'.
\]

Then by Theorem 1.3.2, \( \tau \) will induce a projectivity from \( G \) to \( \bar{G} \). For this let \( X \) be a cyclic subgroup of \( G \). If \( X \leq T \), we define \( X' = X \), that is, \( \tau \) is the identity on \( L_1(T) \). Let \( X \not\leq T \). Then \( X \) can be written uniquely in the form \( X = \langle a + h \rangle \) where \( a \in T \) and \( 0 < h \in H \). Since \( \sigma \) fixes the primes involved in \( T \), the definition of \( \sigma \) in (15) shows that

\[
\frac{h\sigma}{h} = q_1^{n_1} \cdots q_r^{n_r}
\]

where \( n_i \in Z \) and the \( q_i \) are primes not dividing \( o(a) \). It follows that

\[
\frac{h\sigma}{h} a = q_1^{n_1} \cdots q_r^{n_r} a
\]

is a well-defined element of \( \langle a \rangle \); here \( q^n a \), for \( n < 0 \), is the unique element \( b \in \langle a \rangle \) satisfying \( q^a b = a \). We put \( X' = \left( \frac{h\sigma}{h} a + h\bar{\sigma} \right) \). This defines a map from \( L_1(G) \) to \( L_1(\bar{G}) \) which is bijective since there is an obvious inverse map defined in the same way to \( \sigma^{-1} = \bar{\sigma}^{-1} \), that is, sending \( \langle a + k \rangle \) to \( \left( \frac{k\sigma^{-1}}{k} a + k\bar{\sigma}^{-1} \right) \) for \( a \in T \) and \( 0 < k \in K \). We want to show that \( \tau \) satisfies (19). So let \( X, Y, Z \in L_1(G) \). If \( Y \) and \( Z \) are finite, then \( Y, Z \leq T \) and since \( \tau \) is the identity on \( L_1(T) \), (19) clearly holds for \( X, Y, Z \). Suppose next that \( Y = \langle b \rangle \) is finite and \( Z = \langle a + h \rangle \) is infinite. Then \( X = \langle i b + j(a + h) \rangle \) where \( i, j \in Z \). If \( j = 0 \), then \( X' = X \leq Y = Y' \); and if \( j \neq 0 \), since \( \sigma \) is multiplicative,

\[
X' = \left( \frac{(jh)\bar{\sigma}}{jh} (ib + ja) + (jh)\bar{\sigma} \right) = \left( \frac{i(jh)\bar{\sigma}}{jh} b + j\bar{\sigma} \left( \frac{h\bar{\sigma}}{h} a + h\bar{\sigma} \right) \right) \leq Y' + Z'.
\]

Similarly, \( X' \leq Y' + Z' \) implies that \( X \leq Y + Z \) and hence (19) holds. Finally suppose that \( Y \) and \( Z \) are infinite. Since \( r_0(G) = 1 \), \( Y + Z = U \oplus R \) where \( U \) and \( R \) are cyclic and \( U \) is finite. As in the proof of Lemma 2.5.12, the result just proved shows that \( Y' + Z' \leq U' + R' \). Hence \( Y' + Z' = V' \oplus S' \) where \( V' \leq U' \) and \( S' \leq U' + R' \) is infinite cyclic. It follows that \( U + R = Y + Z \leq V + S \) and hence \( U' + R' \leq V' + S' \). Thus \( Y' + Z' \leq U' + R' \) so that this case is reduced to the one just settled. This finishes the proof of (19) and of the theorem.

The above theorem has been proved independently and generalized to larger classes of mixed abelian groups of torsion-free rank 1 by Mahdavi and Poland [1992], [1993].

**Exercises**

1. Let \( G \) be an abelian torsion group with the property that if \( G \) contains an element of order \( n \), then \( G \) contains at least three independent elements of this order.
2.6 Projectivities between abelian groups

Show that every projectivity from $G$ to an abelian group $\hat{G}$ is induced by an isomorphism.

2. Let $p > 2$, $n \geq 2$ and let $G$ be the abelian group of type $(p^n, p)$. Determine $P(G)$ and $PA(G)$.

3. Let $G$ be an abelian group of type $(2^*, 2, \ldots, 2)$. Show that every projectivity from $G$ to an abelian group $\hat{G}$ is induced by an isomorphism.

4. Suppose that $G = \langle a \rangle \times B$ is an abelian group, $o(a) = p^n > p^m = \text{Exp} B$ and that $m \geq 2$ if $p = 2$. Let $N = \langle a^{p^m} \rangle$ and let $\sigma$ be the automorphism of $G/N$ satisfying $(bN)^\sigma = bN$ for all $b \in B$ and $(aN)^\sigma = (aN)^{1 + p^m - 1}$ if $m \geq 2$ and $(aN)^\sigma = a^2N$ if $m = 1$.
   (a) Show that there is a unique autoprojectivity $\varphi$ of $G$ that fixes every subgroup of $\Omega_{n-1}(G)$ and is induced by $\sigma$ on $G/N$.
   (b) This projectivity is not induced by an automorphism of $G$.

5. Let $p > 2$ and $G = A \times B$ be an abelian group with $A$ of type $(p^n, p^n)$ and $\text{Exp} B = p^m < p^n$. For every subgroup $N$ of order $p$ of $A$ let $\sigma_N$ be an automorphism of $G/N$ fixing every subgroup $U/N$ of $G/N$ for which $\Omega(A) \leq U$ or $U \leq \Omega_{n-1}(G)$.
   (a) Show that there is a unique autoprojectivity $\varphi$ of $G$ that fixes every subgroup of $\Omega_{n-1}(G)$ and is induced by $\sigma_N$ on $G/N$ for every $N$.
   (b) Find automorphisms $\sigma_N$ such that $\varphi$ is not induced by an automorphism of $G$.

6. Let $Z \leq G \leq \mathbb{Q}$. Show that every projectivity $\varphi$ from $G$ to some subgroup of $\mathbb{Q}$ is induced by a unique autoprojectivity of $\mathbb{Q}$.

7. (Gasparini and Metelli [1984]) Let $Z \leq G \leq \mathbb{Q}$. Show that $P(G)$ is the semi-direct product of $PA(G)$ and a group isomorphic to the subgroup $\{ \sigma \in \text{Sym } \mathbb{N} | t(G)^\sigma = t(G) \}$ of $\text{Sym } \mathbb{N}$. 

Chapter 3

Complements and special elements
in the subgroup lattice of a group

The main subject of this chapter is groups with complemented subgroup lattices. Since not much is known about these groups in general, various stronger complementary conditions and related lattice-properties are also considered. All these are far less important than distributivity or modularity since there are no natural classes of groups connected with them.

The group $G$ is called a $K$-group if its subgroup lattice is complemented, that is, if to every $H \leq G$ there exists $K \leq G$ such that $G = \langle H, K \rangle$ and $H \cap K = 1$. We show in § 3.1 that $G$ is a $K$-group if and only if its Fitting subgroup $F(G)$ is a direct product of abelian minimal normal subgroups of $G$ and has a complement that is a $K$-group; from this we derive a characterization of soluble $K$-groups. In particular, we get that a finite soluble group $G$ is a $K$-group if and only if $\Phi(G/F_i(G)) = 1$ for all $i \geq 0$; this was proved by Zacher in 1953. However, the structure of finite $K$-groups in general is not known. Therefore, in § 3.2, we study groups $G$ in which every subgroup $H$ has a complement $K$ satisfying $G = HK$; groups with this stronger property are called $C$-groups. As early as 1937 P. Hall proved that the finite $C$-groups are precisely the finite supersoluble $K$-groups and determined the structure of these groups. We generalize his result to infinite groups and also consider groups with the weaker property that every subgroup $H$ has a sectional complement, that is a subgroup $K$ such that $X \cap K$ is a complement to $H$ in $X$ for every subgroup $X$ of $G$ containing $H$.

In § 3.3 we mainly investigate groups with relatively complemented subgroup lattices and $IM$-groups. A group $G$ is called an $RK$-group (or $RC$-group) if for all $L, H, M \leq G$ such that $L \leq H \leq M$ there exists $K \leq G$ such that $H \cap K = L$ and $\langle H, K \rangle = M$ (or $HK = M$, respectively). In 1952 Zacher proved that a finite group is an $RK$-group if and only if it has elementary abelian Sylow subgroups and normality is a transitive relation in every subgroup; in particular, such a group is supersoluble. We further show that the $RC$-groups are precisely the soluble (or locally finite) $RK$-groups and have a similar structure to finite $RK$-groups. An $IM$-group is a group in which every proper subgroup is the intersection of maximal subgroups. Clearly, every $RK$-group is an $IM$-group. The classification of finite simple groups yields that every finite $IM$-group is soluble. The structure of arbitrary soluble $IM$-groups was determined by Menegazzo in 1970. It follows from his result that a finite group is a (soluble) $IM$-group if and only if it is an $RK$-group.

The last two sections of this chapter are concerned with some isolated topics. An element $a$ of a lattice $L$ is called neutral if every triple $a, x, y$ of elements in $L$ generates a distributive sublattice; equivalently $a$ is join-distributive (that is, satisfies
a ∪ (x ∩ y) = (a ∪ x) ∩ (a ∪ y) for all x, y ∈ L), meet-distributive (defined dually) and uniquely complemented (that is, a ∪ x = a ∪ y and a ∩ x = a ∩ y implies x = y for all x, y ∈ L). We investigate these and similar properties in subgroup lattices of groups and, as our final result in § 3.4, present the characterization of neutral elements in the subgroup lattice of a finite group that was given by Suzuki and Zappa, independently, in 1951.

A partition of a group G is a set Σ of nontrivial subgroups of G such that every nonidentity element of G is contained in a unique subgroup X ∈ Σ; it is called nontrivial if X ≠ G for all X ∈ Σ. Possession of a nontrivial partition is a lattice-property of a group. In 1961 Baer and Suzuki determined all finite groups having a nontrivial partition; their results are presented in § 3.5. It is shown, among other things, that the projective special linear groups PSL(2, p^n) and the Suzuki groups Sz(2^n) are the only finite simple groups with this property.

3.1 Groups with complemented subgroup lattices (K-groups)

Let L be a lattice with least element 0 and greatest element I. For a ∈ L, an element c ∈ L is called a complement to a in L if a ∩ c = 0 and a ⋃ c = I; for a group G, we say that K is a complement to H in G if it is a complement to H in L(G). The lattice L is said to be complemented if every element of L has a complement in L. In this section we want to study groups with complemented subgroup lattices, K-groups for short. First of all we note an obvious necessary condition for a group to have this property.

3.1.1 Lemma. The Frattini subgroup of a K-group is trivial.

Proof. Let 1 ≠ x ∈ G and take a complement K to ⟨x⟩ in G. Consider the set S of all subgroups of G containing K but not x. Then S is not empty since K is a member. Clearly S is partially ordered by inclusion; moreover the union of any chain in S is likewise in S. By Zorn's Lemma S has a maximal element M. If M < H ≤ G, then K ≤ H and as H ∈ S, x ∈ H; it follows that H ≥ ⟨x⟩ ∪ K = G. Hence M is a maximal subgroup of G and therefore contains the Frattini subgroup Φ(G). Since M ∈ S, x ∉ M and so, finally, x ∉ Φ(G). Thus Φ(G) = 1.

It follows from 3.1.1, for example, that a finite p-group has complemented subgroup lattice if and only if it is elementary abelian. There are also large classes of nonsoluble K-groups.

3.1.2 Theorem. If G is a primitive permutation group and the stabilizer of a point is a K-group, then G is a K-group. In particular, every finite symmetric or alternating group has complemented subgroup lattice.

Proof. Let G be primitive on the set Ω and suppose that 1 ≠ H ≤ G. Since G is faithful on Ω, there exists an x ∈ Ω such that H ⊈ G.x. The stabilizer of a point in a
primitive permutation group is a maximal subgroup and therefore $H \cup G_\alpha = G$. Since $G_\alpha$ is a $K$-group, there exists a complement $K$ to $H \cap G_\alpha$ in $G_\alpha$. It follows that $H \cap K = H \cap G_\alpha \cap K = 1$ and $H \cup K = H \cup (H \cap G_\alpha) \cup K = H \cup G_\alpha = G$. Thus $K$ is a complement to $H$ in $G$ and $G$ is a $K$-group. For $n \geq 3$, the symmetric group $S_n$ and the alternating group $A_n$ are primitive permutation groups and the stabilizer of a point is $S_{n-1}$ and $A_{n-1}$, respectively. Since $S_3$ and $A_3$ are $K$-groups, it follows by induction that all finite symmetric and alternating groups are $K$-groups.

In general the structure of finite $K$-groups is not known. In particular, it is unknown whether every finite simple group is a $K$-group. Previato [1982] proved this conjecture for the alternating groups, the projective special linear groups $PSL(n, p^k)$ and the Suzuki groups $Sz(q)$.

Theorem 3.1.2 shows that subgroups of $K$-groups need not be $K$-groups. For factor groups and direct products of $K$-groups, the situation is different.

3.1.3 Lemma. If $N \trianglelefteq G$, $N \trianglelefteq H \trianglelefteq G$ and $K$ is a complement to $H$ in $G$, then $NK/N$ is a complement to $H/N$ in $G/N$. In particular, every epimorphic image of a $K$-group is a $K$-group.

Proof. Clearly, $H \cup NK \geq H \cup K = G$ and by Dedekind's law, $H \cap NK = N(H \cap K) = N$. Thus $NK/N$ is a complement to $H/N$ in $G/N$. □

3.1.4 Lemma. Let $H \subseteq G = AB$ and assume that $C$ and $D$ are complements to $H \cap A$ in $A$ and $(H \cup A) \cap B$ in $B$, respectively. If $CD = DC$, then $CD$ is a complement to $H$ in $G$.

Proof. Suppose that $x = cd \in H$ where $c \in C$ and $d \in D$. Then
\[
d = c^{-1}x \in (H \cup C) \cap D \leq (H \cup A) \cap B \cap D = 1
\]
and hence $x = c \in H \cap C = H \cap A \cap C = 1$. Thus $H \cap CD = 1$. Now $H \cup CD \geq (H \cap A) \cup C = A$ and therefore $H \cup CD \geq H \cup A \cup D \geq B$. Hence $G = AB \leq H \cup CD$ and $CD$ is a complement to $H$ in $G$.

3.1.5 Corollary. The direct product of two $K$-groups is a $K$-group.

Proof. If $H \leq G = A \times B$ with $K$-groups $A$ and $B$, then the complements $C$ and $D$ in 3.1.4 exist and they certainly satisfy $CD = DC$. Thus $H$ has a complement in $G$. □

The Fitting subgroup of a $K$-group

The Fitting subgroup $F(G)$ of a group $G$ is the subgroup generated by all the normal nilpotent subgroups of $G$. Since the product of two normal nilpotent subgroups is nilpotent, $F(G)$ is the unique largest normal nilpotent subgroup of $G$ if $G$ is finite. In general, $F(G)$ need not be nilpotent.
3.1.6 Lemma. The Fitting subgroup of a $K$-group is abelian.

Proof. Let $G$ be a $K$-group. We first show by induction on the nilpotency class $c(N)$ that every normal nilpotent subgroup $N$ of $G$ is abelian. This is clear if $c(N) = 1$. Thus we can suppose that $c(N) \geq 2$ and consider a complement $K$ to $Z(N)$ in $G$. As a characteristic subgroup of $N$, $Z(N)$ is normal in $G$. Hence $G = Z(N)K$ and $N = Z(N)(N \cap K) = Z(N) \times (N \cap K)$. Furthermore $N \cap K$ is normal in $K$ and centralized by $Z(N)$. Thus $N \cap K$ is a normal subgroup of $Z(N)K = G$ and its nilpotency class is $c(N) - 1$ since $N \cap K \cong N/Z(N)$. By induction, $N \cap K$ is abelian and then $N = Z(N) \times (N \cap K)$ is abelian as well. Now $F(G)$ is generated by abelian normal subgroups of $G$; thus they centralize each other. It follows that $F(G)$ is abelian.

We want to show next that the Fitting subgroup of a $K$-group is a direct product of minimal normal subgroups. We prove a more general result.

3.1.7 Lemma. Let $A$ be an abelian normal subgroup of the group $G$. If every normal subgroup of $G$ that is contained in $A$ has a complement in $G$, then $A$ is a direct product of minimal normal subgroups of $G$.

Proof. We may assume that $A \neq 1$. Clearly, every normal subgroup $B$ of $G$ contained in $A$ satisfies the assumptions of the lemma. Furthermore, if $K$ is a complement to $B$ in $G$, then $A = A \cap BK = B(A \cap K)$ so that $A \cap K$ is a complement to $B$ in $A$. Since $A$ is abelian, $A \cap K \leq A$ and as $A \leq G$, $A \cap K \leq K$. Thus $A \cap K \leq AK = G$ and it follows that $A = B \times (A \cap K)$ is a completely reducible $G$-module.

We want to show that $A$ contains a minimal normal subgroup of $G$. Take $1 \neq a \in A$ and consider $\mathcal{S} = \{N \leq G| a \notin N \leq A\}$. Clearly $\mathcal{S}$ is not empty and it contains the join of any chain in $\mathcal{S}$. By Zorn's Lemma there exists a maximal element $M$ in $\mathcal{S}$. Since $A$ is completely reducible, $A = M \times C$ for some normal subgroup $C$ of $G$. And if $C$ were not a minimal normal subgroup of $G$, then $C = C_1 \times C_2$ with $1 \neq C_i \leq G$. The maximality of $M$ would imply that $M \times C_i \notin \mathcal{S}$ for $i = 1, 2$; hence $a \in (M \times C_1) \cap (M \times C_2) = M$, a contradiction. Thus $C$ is a minimal normal subgroup of $G$ contained in $A$.

Now if $A^*$ is the subgroup generated by all the minimal normal subgroups of $G$ contained in $A$, then again $A = A^* \times D$ where $D \leq G$. If $D \neq 1$, then $D$ would contain a minimal normal subgroup $N$ of $G$, as we have just shown; but then $N \leq A^* \cap D = 1$, a contradiction. Thus $D = 1$ and $A$ is generated by minimal normal subgroups of $G$. By another straightforward application of Zorn's Lemma $A$ is a direct product of minimal normal subgroups of $G$ (see Robinson [1982], p. 83).

Conversely, we have the following results.

3.1.8 Lemma. Let $A$ be an abelian subgroup of $G$ generated by minimal normal subgroups $A_i (i \in I)$ of $G$ and let $B \leq A$. If either $B \leq G$ or all the $A_i$ are cyclic, then there exists a complement $C$ to $B$ in $A$ that is normal in $G$. 

\[\square\]
Proof. Consider \( \mathcal{S} = \{ N \trianglelefteq G \mid N \leq A \text{ and } N \cap B = 1 \} \). Again \( \mathcal{S} \) is not empty and contains the join of any chain in \( \mathcal{S} \) so that by Zorn's Lemma there is a maximal element \( C \) in \( \mathcal{S} \). Suppose that \( A \neq BC \). Then since \( A \) is generated by the \( A_i \), there is an \( i \in I \) such that \( A_i \leq BC \). If \( B \trianglelefteq G \), then \( BC \trianglelefteq G \) and \( BC \cap A_i = 1 \) since \( A_i \) is a minimal normal subgroup of \( G \); if \( B \) is not normal in \( G \), then \( A_i \) is cyclic of prime order and again \( BC \cap A_i = 1 \). In both cases, \( BCA_i = B \times C \times A_i \) and therefore \( C \times A_i \in \mathcal{S} \), contradicting the maximality of \( C \). Thus \( A = BC \) and \( C \) is a complement to \( B \) in \( A \) that is normal in \( G \).

3.1.9 Lemma. If \( G \) contains an abelian subgroup \( A \) generated by minimal normal subgroups of \( G \) and a complement \( K \) to \( A \) that is a \( K \)-group, then \( G \) is a \( K \)-group.

Proof. Let \( H \leq G \). Since \( K \) is a \( K \)-group, there is a complement \( C \) to \( H \cap K \) in \( K \). Since \( A \) is abelian, \( B = (H \cup K) \cap A \leq A \) and as \( A \leq G \), \( B \leq H \cup K \). Hence \( B \leq AK = G \) and by 3.1.8 there is a complement \( D \) to \( B = (H \cup K) \cap A \) in \( A \) that is normal in \( G \). By 3.1.4, \( CD = DC \) is a complement to \( H \) in \( G \).

We summarise the results proved so far in the following.

3.1.10 Theorem (Zacher [1953], Emaldi [1969]). The group \( G \) is a \( K \)-group if and only if its Fitting subgroup \( F(G) \) is a direct product of abelian minimal normal subgroups of \( G \) and has a complement \( K \) that is a \( K \)-group.

Proof. If \( G \) is a \( K \)-group, then \( F(G) \) by 3.1.6 is abelian and by 3.1.7 is a direct product of minimal normal subgroups of \( G \). Clearly, \( F(G) \) has a complement \( K \) in \( G \) and by 3.1.3, \( K \cong G/F(G) \) is a \( K \)-group. Conversely, if \( G \) satisfies the conditions of the theorem, it is a \( K \)-group by 3.1.9.

Soluble \( K \)-groups

It is clear that Theorem 3.1.10 tells us nothing about the structure of semi-simple \( K \)-groups. In soluble groups, however, \( F(G) \neq 1 \) and the Fitting series, defined inductively by \( F_0(G) = 1 \) and \( F_{i+1}(G)/F_i(G) = F(G/F_i(G)) \) for \( i \geq 0 \), reaches \( G \). Therefore we get the following characterization of soluble \( K \)-groups.

3.1.11 Theorem (Zacher [1953], Emaldi [1969]). The soluble group \( G \) is a \( K \)-group if and only if for all \( i \geq 0 \), \( F_{i+1}(G)/F_i(G) \) is a direct product of minimal normal subgroups of \( G/F_i(G) \) and has a complement in \( G/F_i(G) \).

Proof. If \( G \) is a \( K \)-group, then 3.1.3 shows that also \( G/F_i(G) \) is a \( K \)-group. Therefore by 3.1.10, its Fitting subgroup \( F_{i+1}(G)/F_i(G) \) has the stated properties. Conversely, if \( G \) satisfies the conditions of the theorem, we prove by induction on the Fitting length \( n \) that \( G = F_n(G) \) is a \( K \)-group. For \( n = 0 \), there is nothing to prove. And if the assertion is true for \( n - 1 \), then \( G/F_1(G) \) is a \( K \)-group. Since the complement to \( F_1(G) \) in \( G \) is isomorphic to this group, \( G \) is a \( K \)-group by 3.1.10.
It is a well-known theorem of Gaschütz (see Robinson [1982], p. 131) that for a finite group $G$, the factor group $F(G)/\Phi(G)$ of the Fitting subgroup modulo the Frattini subgroup is the product of all the abelian minimal normal subgroups of $G/\Phi(G)$. We use this to give the following more elegant characterization of finite soluble $K$-groups.

3.1.12 Theorem (Zacher [1953]). The finite soluble group $G$ is a $K$-group if and only if $\Phi(G/F_i(G)) = 1$ for all $i \geq 0$.

Proof. If $G$ is a $K$-group, then 3.1.3 shows that $G/F_i(G)$ is a $K$-group and by 3.1.1, $\Phi(G/F_i(G)) = 1$. Conversely, suppose that $\Phi(G/F_i(G)) = 1$ for all $i \geq 0$. Then again by induction, $G/F(G)$ is a $K$-group and by Gaschütz's theorem, $F(G)/\Phi(G) = F(G)$ is a direct product of abelian minimal normal subgroups of $G$. It remains to be shown that $F(G)$ has a complement in $G$: this will be isomorphic to $G/F(G)$ and Theorem 3.1.10 will yield that $G$ is a $K$-group. For this purpose we take a subgroup $L$ of $G$ which is maximal with the properties that it is contained in $F(G)$ and possesses a complement $H$ in $G$. We want to show that $L = F(G)$, so suppose that $L \neq F(G)$. Then $F(G) \cap H \neq 1$ and $F(G) \cap H \trianglelefteq F(G)H = G$ since $F(G)$ is an abelian normal subgroup of $G$. Let $N$ be a minimal normal subgroup of $G$ contained in $F(G) \cap H$. Since $\Phi(G) = 1$, there is a maximal subgroup $M$ of $G$ with $N \lhd M$ and as $N$ is abelian, it follows that $N \cap M = 1$ and $NM = G$. Now $N$ is a modular subgroup of $G$ and hence

$$(N \cup L) \cap (M \cap H) = ((N \cup L) \cap H) \cap M = (N \cup (L \cap H)) \cap M = N \cap M = 1,$$

$$(N \cup L) \cup (M \cap H) = L \cup (N \cup (M \cap H)) = L \cup ((N \cup M) \cap H) = L \cup H = G.$$ 

Thus $M \cap H$ is a complement to $NL$ in $G$. This contradicts the maximality of $L$. Hence $L = F(G)$ and $F(G)$ has a complement in $G$.

Zacher's theorem has some rather surprising consequences.

3.1.13 Corollary. Every normal subgroup of a finite soluble $K$-group is a $K$-group.

Proof. Let $G$ be a finite soluble $K$-group and suppose that $N \lhd G$. Then it is well-known that $F_i(N) = F_i(G) \cap N$ and hence $N/F_i(N) \cong NF_i(G)/F_i(G) \lhd G/F_i(G)$. Since $\Phi(G/F_i(G)) = 1$ and the Frattini subgroup of a normal subgroup is contained in the Frattini subgroup of the whole group, $\Phi(NF_i(G)/F_i(G)) = 1$. It follows that $\Phi(N/F_i(N)) = 1$ and by 3.1.12, $N$ is a $K$-group.

It is not known whether the assertion of the corollary is also true for infinite soluble groups or arbitrary finite groups; nor is it known if it is true for an arbitrary $K$-group. Another easy consequence of Zacher's theorem is that in order to find out if a finite soluble group $G$ is a $K$-group, it suffices to know that every normal subgroup of $G$ has a complement, or even that every characteristic subgroup of $G$ has a complement in $G$. Here is a more general statement.
Complements and special elements in the subgroup lattice of a group

3.1.14 Theorem (Napolitani [1967b], Emaldi [1970]). The following properties of a soluble group $G$ are equivalent.

(a) Every subgroup of $G$ has a complement in $G$, that is, $G$ is a $K$-group.
(b) Every normal subgroup of $G$ has a complement in $G$.
(c) Every characteristic subgroup of $G$ has a complement in $G$ and for every pair of normal subgroups $N$, $M$ of $G$ with $N < M$ there exists a minimal normal subgroup of $G/N$ contained in $M/N$.

Proof. That (a) implies (b) and (b) implies the first part of (c) is trivial. To show that (c) follows from (b), we therefore have to consider a pair of normal subgroups $N$, $M$ of $G$ with $N < M$. Since $G$ is soluble, there exists a nontrivial abelian normal subgroup $A/N$ of $G/N$ contained in $M/N$. By 3.1.3, every normal subgroup of $G/N$ has a complement in $G/N$ and hence Lemma 3.1.7 yields that $A/N$ contains a minimal normal subgroup of $G/N$. Thus (c) holds.

It remains to show that (c) implies (a), which will be proved by induction on the derived length $k$ of the soluble group $G$. If $k = 0$, then $G = 1$ and (a) holds. So we may assume $k > 1$ and take $A = G^{(k-1)}$, the penultimate term of the derived series of $G$. Then $A$ is a nontrivial abelian characteristic subgroup of $G$ and, by assumption, $A$ has a complement $K$ in $G$. Since both conditions in (c) are preserved by factor groups with respect to characteristic subgroups, by induction, $K \cong G/A$ is a $K$-group. Finally, if $B$ is the subgroup generated by all the minimal normal subgroups of $G$ contained in $A$, then $B$ is characteristic in $G$ and therefore has a complement $C$ in $G$. Since $A$ is an abelian normal subgroup of $G$, $A \cap C \leq AC = G$. Thus if $A \cap C \neq 1$, there would exist a minimal normal subgroup $N$ of $G$ contained in $A \cap C$ and it would follow that $N \leq B \cap C = 1$. This is impossible. Thus $A \cap C = 1$ and $A = B(A \cap C) = B$, that is, $A$ is generated by minimal normal subgroups of $G$. By 3.1.9, $G$ is a $K$-group and (a) holds.

The second assumption in (c) clearly holds if $G$ satisfies the minimal condition on normal subgroups. That the condition cannot be omitted from the theorem is shown by the additive group $\mathbb{Q}$ of rational numbers. This has only trivial characteristic subgroups since multiplication by an arbitrary nonzero rational number is an automorphism; hence every characteristic subgroup has a complement. On the other hand, $\mathbb{Q}$ is not a $K$-group since any two nontrivial subgroups of $\mathbb{Q}$ have nontrivial intersection.

Exercises

1. (Previato [1982]) (a) Let $G$ be a finite group and suppose that $H \leq G$ is a $K$-group. If $H$ is contained in exactly one maximal subgroup $M$ of $G$ and if $M_G = \bigcap_{x \in G} M^x = 1$, show that $G$ is a $K$-group.
(b) Taking for $H$ a Sylow $p$-subgroup, deduce that $PSL(2, p^n)$ is a $K$-group for all $p \in \mathbb{P}$, $n \in \mathbb{N}$. 
2. (Emaldi [1969]) Show that every soluble $K$-group is periodic. (Hint: use the fact that an abelian group $A$ with a locally finite subgroup of Aut $A$ operating irreducibly on $A$ is periodic (see Baer [1964]).)

3. (Curzio [1960]) If $G$ is a soluble group such that $L(G)$ is complemented and satisfies the maximal condition, show that $G$ is finite.

4. (Christensen [1964]) Show that $G$ is a finite metabelian $K$-group if and only if $G$ is the semidirect product of two abelian groups and has elementary abelian Sylow subgroups.

5. (Dinerstein [1968]) Let $G$ be a finite group (it suffices to assume that $L(G)$ satisfies the minimal condition) in which every characteristic subgroup has a complement. Show that every normal subgroup of $G$ has a complement in $G$.

3.2 Special complements

Much more can be said about $K$-groups in which the complements have additional properties. The most natural of these is that they permute with the given subgroups. We call $G$ a $C$-group if to every subgroup $H$ of $G$ there is a subgroup $K$ of $G$ such that

1. $G = HK$ and $H \cap K = 1$;

we also say that $H$ is permutably complemented by $K$ in $G$ if (1) holds. The structure of $C$-groups is well-known, and will be presented in this section. First of all we have the following simple inheritance properties.

3.2.1 Lemma. (a) Subgroups and epimorphic images of $C$-groups are $C$-groups.

(b) The direct product of two $C$-groups is a $C$-group.

Proof. (a) Let $H \leq X \leq G$. If $K$ satisfies (1), then $X = X \cap HK = H(X \cap K)$ and $H \cap (X \cap K) = 1$. Thus $X \cap K$ is a complement to $H$ in $X$ that permutes with $H$. If $N \trianglelefteq G$, $N \leq H \leq G$ and $K$ again satisfies (1), then by 3.1.3, $NK/N$ is a complement to $H/N$ in $G/N$ and clearly $(H/N)(NK/N) = HK/N = G/N$.

(b) Let $H \leq G = A \times B$ with $C$-groups $A$ and $B$. Then there exists a subgroup $C$ of $A$ such that $A = (H \cap A)C$ and $(H \cap A) \cap C = 1$ and a subgroup $D$ of $B$ with the property that $B = (HA \cap B)D$ and $(HA \cap B) \cap D = 1$. By 3.1.4, $CD$ is a complement to $H$ in $G$ and

$$HCD = H(H \cap A)CD = HAD = HA(HA \cap B)D = HAB = G.$$ Thus $G$ is a $C$-group.

Another natural property a complement $K$ to a subgroup $H$ of $G$ might have is the following.

(2) If $H \leq X \leq G$, then $X \cap K$ is a complement to $H$ in $X$. 
We call a subgroup \( K \) of \( G \) with this property a sectional complement, or \( S \)-complement for short, to \( H \) in \( G \). And a group in which every subgroup has an \( S \)-complement is called an \( SC \)-group. The proof of Lemma 3.2.1 (a) shows that if \( G = HK \) and \( H \cap K = 1 \), then \( K \) is an \( S \)-complement to \( H \) in \( G \). Hence

(3) every \( C \)-group is an \( SC \)-group.

The structure of \( SC \)-groups is not known. We shall, however, show that the classes of \( C \)-groups and of locally finite \( SC \)-groups coincide.

3.2.2 Lemma. Subgroups and epimorphic images of \( SC \)-groups are \( SC \)-groups.

Proof. Let \( G \) be an \( SC \)-group, \( H \leq X \leq G \) and suppose that \( K \) is an \( S \)-complement to \( H \) in \( G \). Then clearly \( X \cap K \) is an \( S \)-complement to \( H \) in \( X \). And if \( N \leq G \) such that \( N \leq H \), then by 3.1.3, \( N(X \cap K)/N \) is a complement to \( H/N \) in \( X/N \). Since \( N(X \cap K) = X \cap NK \), it follows that \( NK/N \) is an \( S \)-complement to \( H/N \) in \( G/N \).

The main property of \( SC \)-groups which we shall require is the following.

3.2.3 Lemma. If \( N \) is an abelian minimal normal subgroup of an \( SC \)-group \( G \), then \( N \) is cyclic of prime order.

Proof. Suppose that \( M \) is a proper subgroup of \( N \) and take an \( S \)-complement \( K \) to \( M \) in \( G \). Then \( N \cap K \) is a complement to \( M \) in \( N \) and hence \( 1 < N \cap K \leq N \). Since \( N \) is an abelian normal subgroup of \( G \), \( N \cap K \leq NK = G \) and the minimality of \( N \) implies that \( N \cap K = N \). Thus \( M = 1 \) and \( N \) is cyclic of prime order.

As early as 1937 P. Hall proved that the finite \( C \)-groups and the finite supersoluble \( K \)-groups coincide and determined their structure. He did not consider \( S \)-complements but his proof also works for \( SC \)-groups.

3.2.4 Theorem (P. Hall [1937]). The following properties of the finite group \( G \) are equivalent:

(a) \( G \) is a \( C \)-group,
(b) \( G \) is an \( SC \)-group,
(c) \( G \) is a supersoluble \( K \)-group,
(d) \( G \) is isomorphic with a subgroup of a direct product of groups of squarefree order.

Proof. That (a) implies (b) follows from (3). If \( G \) is an \( SC \)-group, then it clearly is a \( K \)-group and we use induction on \( |G| \) to prove that \( G \) is supersoluble. By 3.2.2, every proper subgroup of \( G \) is supersoluble and a well-known result of Huppert's (see Robinson [1982], p. 287) shows that \( G \) is soluble. So if \( N \) is a minimal normal subgroup of \( G \), then by 3.2.3, \( N \) is cyclic and 3.2.2 yields that \( G/N \) is an \( SC \)-group. By induction \( G/N \) and hence also \( G \) is supersoluble. Thus (b) implies (c).
Now let \( G \) be a supersoluble \( K \)-group and for every maximal subgroup \( M \) of \( G \), let \( M_G = \bigcap_{x \in G} M^x \) be the core of \( M \) in \( G \). By 3.1.1, the intersection of all these \( M_G \) is trivial so that \( G \) is isomorphic with a subgroup of the direct product of the groups \( G/M_G \). To prove that (c) implies (d), we therefore show that every such group \( G/M_G \) has squarefree order. By 3.1.3, \( G/M_G \) is a supersoluble \( K \)-group and hence we may assume that \( M_G = 1 \) and \( M \neq 1 \). Then a minimal normal subgroup \( N \) of \( G \) is cyclic of prime order \( p \), furthermore \( G = NM \) and \( C_M(N) = 1 \) since \( M_G = 1 \). So \( M \) is isomorphic to a subgroup of Aut \( N \) and hence cyclic of order dividing \( p - 1 \). Therefore every Sylow subgroup of \( M \cong G/N \) is an epimorphic image of \( G \); hence it is a \( K \)-group and so has prime order. It follows that \( |G| = p|M| \) is squarefree.

Finally suppose that (d) holds. We want to show that \( G \) is a \( C \)-group, and since direct products and subgroups of \( C \)-groups are \( C \)-groups, we may assume that \( G \) has squarefree order. It is well-known that groups of squarefree order are soluble (see Robinson [1982], p. 281). Every subgroup \( H \) of \( G \) is a Hall \( \pi \)-subgroup for some set \( \pi \) of primes and if \( \pi' = \mathbb{P}\setminus\pi \), any Hall \( \pi' \)-subgroup \( K \) of \( G \) satisfies \( H \cap K = 1 \) and \( HK = G \). Thus \( G \) is a \( C \)-group.

It is now not difficult to give the exact structure of a finite \( C \)-group \( G \). By (c) or (d) of Hall's theorem, \( G \) is metabelian and 3.1.7 then shows that \( G' = A_1 \times \cdots \times A_s \), with minimal normal subgroups \( A_i \) of \( G \). Since \( G \) is supersoluble, these \( A_i \) have prime order. Clearly \( G' \) has a complement \( B \) in \( G \). And since \( B \cong G/G' \) is an abelian \( K \)-group, again 3.1.7 yields that \( B = B_1 \times \cdots \times B_s \) where the \( B_j \) also have prime order. It was proved by Cernikova in 1953 that infinite \( C \)-groups have exactly the same structure; the other two properties in Theorem 3.2.4 were later generalized to infinite groups by Emaldi. We remind the reader that a group \( G \) is called hypercyclic if every nontrivial epimorphic image possesses a nontrivial cyclic normal subgroup. Equivalent is that \( G \) has an ascending normal series with cyclic factors (see Robinson [1972a], p. 14); thus hypercyclic groups are a natural generalization of supersoluble groups. If \( N \) and \( M \) are normal subgroups of \( G \) such that \( N < M \), it follows from Zorn's Lemma that there exists a normal subgroup \( K \) of \( G \) maximal with the property that \( M \cap K = N \). Then \( K \neq G \) and if \( G \) is hypercyclic, there exists a nontrivial cyclic normal subgroup \( Z/K \) of \( G/K \). The maximality of \( K \) implies that \( H = M \cap Z > N \) and clearly \( H/N \) is cyclic. Thus:

(4) If \( G \) is hypercyclic and \( N < M \) are normal subgroups of \( G \), then there exists \( H \leq G \) such that \( N < H \leq M \) and \( H/N \) is cyclic. In particular, chief factors of hypercyclic groups are cyclic.

3.2.5 Theorem (Cernikova [1956], Emaldi [1969, [1978]). The following properties of a group \( G \) are equivalent:

(a) \( G \) is a \( C \)-group,
(b) \( G \) is a locally finite \( SC \)-group,
(c) \( G \) is a hypercyclic \( K \)-group,
(d) \( G \) is the semidirect product of \( A = \bigoplus_{i \in I} A_i \) by \( B = \bigoplus_{j \in J} B_j \) where all the \( A_i \) and \( B_j \) have prime order and \( A_i \leq G \) for all \( i \in I \).
Proof. Suppose first that $G$ is a $C$-group. Then $G$ is an $SC$-group by (3) and we want to show that $G$ is locally finite. Every subgroup of $G$ is a $C$-group and, since the subgroup lattice of an infinite cyclic group is not complemented, $G$ is a torsion group. Let $1 \neq x \in G$ and take $C \leq G$ such that $\langle x \rangle \cap C = 1$ and $G = \langle x \rangle C$. Then $|G : C| = |\langle x \rangle|$ is finite. Therefore by 3.2.1, $G/C_G$ is a finite $C$-group and Hall's theorem shows that $G/C_G$ is metabelian. It follows that $G'' \leq C$ and hence $x \notin G''$. Since $x$ was arbitrary, $G'' = 1$. So $G$ is a soluble torsion group and therefore locally finite (see Robinson [1982], p. 147). Thus (b) holds.

Now suppose that $G$ is a locally finite $SC$-group. Then $G$ is a $K$-group and we want to show that $G$ is hypercyclic. If $a, b, c, d \in G$, then by 3.2.2, $H = \langle a, b, c, d \rangle$ is a finite $SC$-group and Hall's theorem shows that $H$ is metabelian. It follows that $[[a, b], [c, d]] = 1$ and hence $G'' = 1$. So if $N \leq G$ with $G/N \neq 1$, then there exists a nontrivial abelian normal subgroup $A/N$ of $G/N$. By 3.2.2, $G/N$ is an $SC$-group. Therefore 3.1.7 implies that $A/N$ contains a minimal normal subgroup of $G/N$ which is cyclic by 3.2.3. Thus $G$ is hypercyclic and (c) holds.

Next suppose that $G$ is a hypercyclic $K$-group. We want to show that (d) holds, and again we first claim that $G$ is metabelian. To prove this, we show that $G''$ is contained in every maximal subgroup of $G$; then 3.1.1 will imply that $G'' = 1$. So let $M$ be a maximal subgroup of $G$ and suppose that $G' \leq M$. Then $G = G'M$ and $G' \cap M \leq M$. Consider $N = (G' \cap M)_G$. By (4) there exists a nontrivial cyclic normal subgroup $H/N$ of $G/N$ contained in $G''/N$. If $W/N = C_{G/N}(H/N)$, then $G/W$ is isomorphic to a subgroup of $\text{Aut} H/N$ and therefore abelian. Hence $G' \leq W$ and $H/N$ centralizes $G' \cap M/N$. Thus $H$ normalizes $G' \cap M$ and since $H \leq M$ and $M$ is maximal in $G$, it follows that $G' \cap M \leq G$ and $G'/G' \cap M$ is a chief factor of $G$. By (4), $G'/G' \cap M$ is cyclic and hence $G'' \leq G' \cap M \leq M$. Thus $G'' = 1$. Now $A = G'$ is an abelian normal subgroup of $G$ and by 3.1.7, $A = \text{Dr} A_i$ with minimal normal subgroup $A_i$ of $G$. By (4), every $A_i$ is cyclic of prime order. Clearly $A$ has a complement $B$ in $G$. And since $B \simeq G/G'$ is an abelian $K$-group, again 3.1.7 yields that $B = \text{Dr} B_j$ where the $B_j$ also have prime order. Thus (d) holds.

Finally suppose that (d) is satisfied and let $H \leq G = AB$. By 3.1.8 there exist a complement $C$ to $H \cap A$ in $A$ that is normal in $G$, and a complement $D$ to $HA \cap B$ in $B$. By 3.1.4, $CD$ is a complement to $H$ in $G$ and, as in the proof to (b) of 3.2.1, $HCD = G$. Thus (a) holds.

Note that by Exercise 1.2.8, property (b) of Theorem 3.2.5 is a lattice-property so that the class of $C$-groups is invariant under projectivities, a result not obvious from the definition.

Property (d) of Hall's theorem can also be generalized to infinite groups: every $C$-group is isomorphic with a subgroup of a cartesian product of finite groups of squarefree order. However, it is not possible to replace "cartesian" by "direct" in this statement and it is also not true that every periodic subgroup of such a cartesian product is a $C$-group. For details see Exercises 3 and 4 or Cernikova [1956].

As for $K$-groups, to prove that a soluble group $G$ is a $C$-group it is not necessary to show that every subgroup of $G$ is permutably complemented; it suffices to look at the subnormal subgroups. In fact one need only consider the subnormal subgroups
of defect at most 2, that is subgroups $H$ of $G$ such that $H \leq N \leq G$ for some $N$. This was shown for finite groups, using Hall's theorem, by Bechtell [1969] and for arbitrary groups, using Cernikova's theorem, by Kochendorfer [1969]. However, there is a simple direct proof by induction on the derived length of $G$.

3.2.6 Theorem (Kochendorfer [1969]). The group $G$ is a C-group if and only if $G$ is soluble and every subnormal subgroup of defect at most 2 is permutably complemented in $G$.

Proof: If $G$ is a C-group, then by 3.2.5, $G$ is soluble and, clearly, every subnormal subgroup of defect at most 2 is permutably complemented in $G$. Assume conversely that $G$ has these properties. If $G$ is abelian, then every subgroup is complemented and $G$ is a C-group. So suppose that the derived length of $G$ is $n \geq 2$ and that the assertion is true for soluble groups of smaller derived length. Then $A = G^{(n-1)}$ is an abelian normal subgroup of $G$. And if $S/A$ is subnormal at most 2 in $G/A$, then there exists a subgroup $T$ of $G$ such that $S \cap T = 1$ and $ST = G$ and $S/A$ is permutably complemented by $AT/A$ in $G/A$; the induction assumption yields that $G/A$ is a C-group. Let $H \leq G$. Then there exists a subgroup $C/A$ of $G/A$ such that $HA \cap C = A$ and $HAC = G$. Hence $H \cap C \leq A$ and since $A$ is abelian, $H \cap C \leq A \leq G$. By assumption there exists a subgroup $D$ of $G$ such that $(H \cap C) \cap D = 1$ and $(H \cap C)D = G$; it follows that $C = (H \cap C)(C \cap D)$. So if we put $K = C \cap D$, then

$$H \cap K = H \cap C \cap D = 1$$

and

$$HK = H(C \cap D) = H(H \cap C)(C \cap D) = HC = HAC = G.$$

Thus $G$ is a C-group.

Further topics

Since C-groups have such a restricted structure, it seems reasonable to weaken the condition of complementability. This has mainly been done in two directions and there is a vast literature on this subject. But all these results are far too special to be presented here; we shall only give some hints for further reading. First of all, one studies groups $G$ such that for a certain class $\mathcal{X}$ of groups, every $\mathcal{X}$-subgroup of $G$ is permutably complemented in $G$ and tries to prove that $G$ then (nearly) is a C-group. This was initiated by Cernikov [1954] who took for $\mathcal{X}$ the class of abelian groups. In the meantime many other classes have been considered, among them the classes of primary groups (Gorcakov [1960]), elementary abelian groups (Sysak [1977]), infinite abelian groups (Cernikov [1980]), nonabelian groups (Barysovec [1977], [1981a], [1981b]), infinite groups (Cernikov [1967]), and finite groups (de Giovanni and Franciosi [1987]). The second possibility is to assume that, again for a certain class $\mathcal{X}$ of groups, to every subgroup $H$ of $G$ there exists a subgroup $K$ such that
Complements and special elements in the subgroup lattice of a group

\( G = HK \) and \( H \cap K \in \mathcal{X} \). This has been done in particular where \( \mathcal{X} \) is the class of finite groups (Sergeev [1964]; Tsybanev [1973], [1980]) and of cyclic groups (Mozarovskaja [1978]).

**Exercises**

1. (Hall [1937]) Show that a finite group is a \( C \)-group if and only if it is supersoluble and its Sylow subgroups are all elementary abelian.

2. (Cernikova [1956]) Show that every group having an ascending normal series with cyclic factors of nonrepeating prime orders is a \( C \)-group.

3. Let \( G \) be an infinite nonabelian \( P \)-group. Show that \( G \) is a \( C \)-group which is not isomorphic with a subgroup of a direct product of finite groups of squarefree order.

4. Let \( I \) be an infinite set, \( G_i \) a nonabelian group of order 6 for every \( i \in I \) and let \( G = \bigvee_{i \in I} G_i \). Show that \( G \) is periodic but not a \( C \)-group. (Hint: determine the normal subgroups of order 3 in \( G \) and use 3.1.7.)

5. (Emaldi [1970]) Show that \( G \) is a \( C \)-group if and only if \( G \) is a hypercyclic torsion group in which every characteristic subgroup has a complement. (Hint: first show that \( G' \) is abelian.)

6. (Emaldi [1985a]) Show that a finite group is a \( C \)-group if and only if every subgroup of prime order has an \( S \)-complement.

7. (Emaldi [1985a]) Show that \( G \) is a \( C \)-group if and only if every subgroup \( H \) of \( G \) has an \( S \)-complement \( K \) such that \( K \) has finite index in \( G \) if \( H \) is finite.

### 3.3 Relative complements

In this section we shall study groups that satisfy various stronger complementary conditions.

**SK-groups**

A group \( G \) is called an \( SK \)-group if every subgroup of \( G \) is a \( K \)-group, that is if \( L(G) \) is sectionally complemented. By 3.2.2, every \( SC \)-group is an \( SK \)-group but the converse does not hold, the alternating group \( A_4 \), or even \( A_5 \), is an example. Clearly, every \( SK \)-group is periodic and has all its elements of squarefree order, however the structure of \( SK \)-groups is not known. For finite groups, at least, we have the following characterization.

**3.3.1 Theorem** (Bechtell [1965]). *The following properties of the finite group \( G \) are equivalent.*
3.3 Relative complements

(a) \( G \) is an SK-group.
(b) \( \Phi(H) = 1 \) for every subgroup \( H \) of \( G \).
(c) Every Sylow subgroup of \( G \) is elementary abelian.

**Proof.** That (a) implies (b) follows from 3.1.1. And since a finite \( p \)-group with trivial Frattini subgroup is elementary abelian, (b) implies (c). So we finally have to show that a finite group \( G \) with elementary abelian Sylow subgroups is an SK-group. By induction, every proper subgroup of \( G \) is a \( K \)-group and it remains to be shown that \( G \) is a \( K \)-group. For this we first note that \( \Phi(G) = 1 \). For, if \( \Phi(G) \neq 1 \), there would exist a minimal normal subgroup \( N \) of \( G \) contained in \( \Phi(G) \). As \( \Phi(G) \) is nilpotent, \( N \) would be a \( p \)-group and since the Sylow \( p \)-subgroups of \( G \) are elementary abelian, a well-known theorem of Gaschütz (see Huppert [1967], p. 121) would yield a complement \( C \) to \( N \) in \( G \). But then \( \Phi(G)C = G \) would imply \( C = G \) and \( N = 1 \), a contradiction. Thus \( \Phi(G) = 1 \). So if \( 1 \neq H \leq G \), there exists a maximal subgroup \( M \) of \( G \) such that \( H \leq M \). Since \( M \) is a \( K \)-group, there is a complement \( K \) to \( H \cap M \) in \( M \). Clearly, \( H \cap K = H \cap M \cap K = 1 \) and \( H \cup K = H \cup (H \cap M) \cup K = H \cup M = G \). Thus \( K \) is a complement to \( H \) in \( G \) and \( G \) is an SK-group.

**RK-groups**

The group \( G \) is called an **RK-group** if its subgroup lattice is relatively complemented, that is if for all \( L, H, M \in L(G) \),

1. \( L \leq H \leq M \) implies the existence of \( K \leq G \) such that \( H \cap K = L \) and \( H \cup K = M \).

It is easy to see that this property implies that normality is transitive in \( G \). Recall that \( G \) is called a **T-group** if \( L \trianglelefteq H \trianglelefteq M \leq G \) implies \( L \trianglelefteq G \), and that \( G \) is a **T*-group** if \( L \trianglelefteq H \trianglelefteq M \trianglelefteq G \) implies \( L \trianglelefteq M \), that is every subgroup of \( G \) is a T-group.

**3.3.2 Lemma.** Every RK-group is a T*-group.

**Proof.** If \( L \trianglelefteq H \trianglelefteq M \leq G \) and \( K \) is as in (1), then \( L = H \cap K \trianglelefteq K \) since \( H \leq M \) and \( K \leq M \). It follows that \( L \leq H \cup K = M \).

Every simple group is a T-group and every Tarski group is a T*-group, so the structure of these groups is not known. But clearly, every subgroup of a T*-group is a T*-group. So to prove that

3. every finite T*-group \( G \) is supersoluble,

we may use induction on \( |G| \) and get that every proper subgroup of \( G \) is supersoluble. By Huppert's theorem (see Robinson [1982], p. 287), \( G \) is soluble. If \( H/N \) is a chief factor of \( G \) and \( N \trianglelefteq L \leq H \), then \( L \trianglelefteq H \trianglelefteq G \) and hence \( L \trianglelefteq G \). Thus \( H/N \) is of prime order and \( G \) is supersoluble. Now we can prove the following characterization of finite RK-groups.
3.3.3 Theorem (Zacher [1952]). A finite group is an RK-group if and only if it is a $T^*$-group with elementary abelian Sylow subgroups.

Proof. That these conditions are necessary follows from 3.3.2 and 3.3.1. Conversely suppose that $G$ is a $T^*$-group with elementary abelian Sylow subgroups. We use induction on $|G|$ to show that $G$ is an RK-group. First of all, since the assumptions are inherited by subgroups and epimorphic images, every proper subgroup and every proper factor group of $G$ is an RK-group. Therefore (1) holds for subgroups $L$, $H$, $M$ of $G$ such that $M \neq G$ or $L_G \neq 1$, and it remains to show (1) in the case that

$$M = G \text{ and } L_G = 1.$$ 

Let $p$ be the largest prime dividing $|G|$. Since $G$ is supersoluble, there exists a normal subgroup $N$ of order $p$ in $G$ (see Robinson [1982], p. 145) and $N \nleq L$ as $L_G = 1$. Since $G/N$ is an RK-group, there exists $K \leq G$ such that

$$HN \cap K = LN \text{ and } HN \cup K = G.$$ 

If $N \nleq H$, then $H \cup K = H \cup N \cup K = G$ and $L \leq H \cap K \leq HN \cap K = LN$. Since $N \nleq H$ and $|LN : L| = p$, it follows that $H \cap K = L$ and $K$ is the desired relative complement. So suppose that $N \leq H$. Then (5) yields that $H \cap K = LN$ and $H \cup K = G$. If $K \nleq G$, then $K$ is an RK-group and there exists $R \leq K$ such that $LN \cap R = L$ and $LN \cup R = K$. It follows that $H \cap R = H \cap K \cap R = LN \cap R = L$ and $H \cup R = H \cup N \cup L \cup R = H \cup K = G$, thus $R$ has the desired properties. It remains to consider the case where $N \leq H$ and $K = G$. Here (5) yields that $H = LN$.

![Figure 13](image_url)

Case 1: $N \nleq H$  
Case 2: $N \leq H, K \nleq G$  
Case 3: $N \leq H, K = G$

Every Sylow subgroup of $G$ is elementary abelian and hence by 3.3.1 (or Gaschütz's theorem) there exists a complement $S$ to $N$ in $G$. It follows that $H = (S \cap H)N$, that is $L$ and $S \cap H$ are complements to $N$ in $H$. Now $G$ is supersoluble and $p$ is the largest prime dividing $|G|$. Therefore the Sylow $p$-subgroup $P$ of $G$ is normal in $G$. And if $Q$ is any $p$-subgroup of $G$, then $Q \leq P \leq G$ and hence $Q \leq G$ as $G$ is a $T$-group. Since $L_G = 1$, it follows that $|L|$ is prime to $p$ and $N$ is a normal Hall subgroup of $H$. By the Schur-Zassenhaus Theorem, $L$ and $S \cap H$ are conjugate in $H$, that is there exists an $x \in H$ such that $L = (S \cap H)^x = S^x \cap H$. Clearly $S^x \cap H = S^x \cup N \cup H = G$ and hence $S^x$ is a complement to $H$ in $[G/L]$.

The structure of infinite RK-groups is not known. However, it is possible to extend Zacher's theorem to infinite soluble groups. Using Zacher's theorem, it is not
3.3 Relative complements

(6) if $L, H, M \in L(G)$ and $L \leq H \leq M$, then there exists $K \leq G$ such that $H \cap K = L$ and $HK = M$.

This property is slightly stronger than (1). We call groups of this type RC-groups and we shall show that the RC-groups are precisely the soluble or locally finite RK-groups, and these have a similar structure to the finite RK-groups. It is difficult to attribute this result correctly. There are two slightly erroneous versions of it in Emaldi and Zacher [1965] and Abramovskii [1967]; they were corrected by Menegazzo [1970a]. Emaldi [1971] added the characterization of RC-groups. For the proof we shall need the following technical results.

3.3.4 Lemma. If $G$ is a metabelian periodic $T$-group with all Sylow subgroups elementary abelian, then $G'$ is a Hall subgroup of $G$ (that is $\pi(G') \cap \pi(G/G') = \emptyset$).

Proof. Suppose that $p \in \pi(G') \cap \pi(G/G')$. If $N$ is the $p$-complement in $G'$, then $G/N$ satisfies the assumptions of the lemma. Therefore we may assume that $N = 1$. Let $P$ be a Sylow $p$-subgroup of $G$. Then $G' \leq P$ and hence $P \leq G$. Since $G$ is a $T$-group and $P$ is elementary abelian, every subgroup of $P$ is normal in $G$ and $P = G' \times K$ where $1 < K < P$. By 1.5.6, every $g \in G$ induces a universal power automorphism in $P$ and if $x^p = x'$ for $x \in P$, then $x^{-1} = [x, g] \in G' \cap K = 1$ for every $x \in K$. It follows that $r \equiv 1 \pmod p$ and hence $P \leq Z(G)$. There exist $u, v \in G$ of prime power order such that $[u, v] \neq 1$. Then $1 = [u, v]^p = [u^p, v]$ by 2 of 1.5. Since $P \leq Z(G)$, $u \notin P$ and hence $u \in \langle u^p \rangle \leq C_G(v)$, a contradiction. Thus $G'$ is a Hall subgroup of $G$.

3.3.5 Lemma. Let $G$ be a locally finite $T^*$-group with all Sylow subgroups elementary abelian. Then $G'$ is an abelian $K$-group and every subgroup of $G'$ is normal in $G$. Let $\pi = \pi(G/G')$ and suppose that every maximal $\pi$-subgroup of $G$ is a complement to $G'$ in $G$.

(a) If $N \leq G'$, then every maximal $\pi$-subgroup of $G/N$ is a complement to $G'/N$ in $G/N$.

(b) If $H \leq G$, then every maximal $\pi$-subgroup of $H$ is a complement to $G' \cap H$ in $H$.

Proof. Since finite supersoluble groups with elementary abelian Sylow subgroups are metabelian, also $G$ is metabelian. Hence $G'$ is a direct product of its elementary abelian $p$-components and therefore an abelian $K$-group. Since $G$ is a $T$-group, every subgroup of $G'$ is normal in $G$.

(a) Let $S/N$ be a maximal $\pi$-subgroup of $G/N$, choose a maximal $\pi$-subgroup $S_1$ of $S$ and a maximal $\pi$-subgroup $T$ of $G$ containing $S_1$. By assumption, $T$ is a complement to $G'$ in $G$ and since $G'$ is an abelian $K$-group, $G' = M \times N$ for some $M \leq G'$. Then $MT \cap S \cap G' = M \cap S = 1$ and $MT \cap S$ is a $\pi$-group. From $S_1 \leq MT \cap S \leq S$ and the maximality of $S_1$ it follows that $MT \cap S = S_1$ and $NS_1 = N(MT \cap S) = NMT \cap S = S$. Thus $S/N$ is contained in the $\pi$-group $NT/N$. The maximality of $S/N$ yields that $S/N = NT/N$ and so by 3.1.3, $S/N$ is a complement to $G'/N$ in $G/N$.

(b) Let $S$ be a maximal $\pi$-subgroup of $H$ and choose a maximal $\pi$-subgroup $T$ of $G$ containing $S$. Then once again $T$ is a complement to $G'$ in $G$, and hence
Complements and special elements in the subgroup lattice of a group

(G’ ∩ H) ∩ S = 1. From S ≤ T ∩ H and the maximality of S it follows that S = T ∩ H. Hence if G’ ≤ H, then H = G’T ∩ H = G’(T ∩ H) = G’S and S is a complement to G’ in H. Now suppose that G’ ≤ G and let N ≤ G’ such that G’ = N × (G’ ∩ H). Then by (a), G/N satisfies the assumptions of the lemma and NH/N = G’H/N is a subgroup of G/N containing G’/N = (G/N). Since N ∩ H = 1, NS/N is a maximal π-subgroup of NH/N; therefore, as we have just shown, it is a complement to G’/N in G’H/N. In particular, G’H = G’NS = G’S and then H = (G’ ∩ H)S. Thus S is a complement to G’ ∩ H in H.

3.3.6 Theorem (Menegazzo [1970a], Emaldi [1971]). The following properties of a group G are equivalent:
(a) G is an RC-group,
(b) G is a soluble RK-group,
(c) G is a locally finite RK-group,
(d) G is a locally finite T*-group with all Sylow subgroups elementary abelian such that for π = π(G/G’), the set of primes dividing the order of an element of G/G’, every maximal π-subgroup of G is a complement to G’ in G.

Proof. Every RC-group is a C-group and hence soluble by 3.2.5. Thus (a) implies (b). Since every RK-group is periodic and a soluble periodic group is locally finite, (c) follows from (b). Now suppose that (c) holds. Then by 3.3.2, G is a T*-group. By 3.3.3, every finite subgroup of G is supersoluble with elementary abelian Sylow subgroups and hence metabelian. Since G is locally finite, G is metabelian and has elementary abelian Sylow subgroups. By 3.3.4, G’ is a Hall subgroup of G. So if S is a maximal π-subgroup of G, then S ∩ G’ = 1. Since G is an RK-group, there exists a subgroup T of G such that G’S ∩ T = S and G = G’S ∪ T = G’T. Hence T ∩ G’ = T ∩ G’S ∩ G’ = S ∩ G’ = 1 and therefore T ≅ TG’/G’ is a π-group. The maximality of S implies that S = T is a complement to G’ in G.

Finally suppose that (d) holds. We want to show (6) and take L, H, M ∈ L(G) such that L ≤ H ≤ M. By 3.3.5, L ∩ G’ ≤ G and G/L ∩ G’ satisfies (d). Therefore we may assume that L ∩ G’ = 1 so that L is a π-group. Let S be a maximal π-subgroup of H containing L and let T be a maximal π-subgroup of M containing S. Then Lemma 3.3.5 (b) shows that H = (G’ ∩ H)S and M = (G’ ∩ M)T. Furthermore, since T ≅ G’T/G’ and G’ ∩ M are abelian K-groups, there exist subgroups N, Q, R of G such that G’ ∩ M = (G’ ∩ H) × N, S = L × Q and T = S × R = L × Q × R. We claim that K = N(L × R) is the relative complement we are looking for. Since N ≤ G,

HK = (G’ ∩ H)SN(L × R) = (G’ ∩ H)NS(L × R) = (G’ ∩ M)T = M

and if x ∈ H ∩ K = (G’ ∩ H)S ∩ N(L × R), that is x = as = bt where a ∈ G’ ∩ H, s ∈ S, b ∈ N, t ∈ L × R, then b⁻¹a = ts⁻¹ ∈ (G’ ∩ M)T = 1. Hence a = b ∈ (G’ ∩ H) ∩ N = 1 and x = s = t ∈ S ∩ (L × R) = L. Thus H ∩ K = L as desired.

IM-groups

A group G is called an IM-group if every proper subgroup of G is the intersection of maximal subgroups of G. Clearly, every RK-group is an IM-group (see also 3.3.12),
3.3 Relative complements

but one can show (see Exercise 6) that the converse is wrong. A basic property of IM-groups is the following.

3.3.7 Lemma. If \( N \) is a normal subgroup of the IM-group \( G \), then \( N \) and \( G/N \) are IM-groups.

Proof. That \( G/N \) is an IM-group is trivial. Suppose that \( H \) is a proper subgroup of \( N \) and take \( x \in N \backslash H \). Then by Zorn's Lemma, the set of all subgroups \( R \) of \( G \) such that \( H \leq R \leq N \) and \( x \notin R \) has a maximal element \( S \). Since \( x \notin S \), we have \( T = \langle S, x \rangle > S \), and for every subgroup \( X \) of \( N \) containing \( S \) properly, the maximality of \( S \) implies that \( x \in X \) and hence \( T \leq X \). Thus

\[
(7) \quad T = \bigcap \{X | S < X \leq N\}
\]

and \( S \) is a maximal subgroup of \( T \). Since \( G \) is an IM-group, there exists a maximal subgroup \( M \) of \( G \) such that \( S \leq M \) but \( T \not< M \). Then (7) implies that \( M \cap N = S \). Thus \( N \) and \( S \), and therefore also \( T \), are normalized by \( M \). It follows that \( G = TM \) and hence \( N = TM \cap N = T(M \cap N) = T \), that is, \( S \) is maximal in \( N \). We have shown that to every \( x \in N \backslash H \) there exists a maximal subgroup \( S \) of \( N \) containing \( H \) such that \( x \notin S \). In particular, \( x \) is not contained in the intersection \( K \) of all the maximal subgroups of \( N \) containing \( H \). It follows that \( K = H \) and \( N \) is an IM-group.

By the lemma the existence of a finite nonsoluble IM-group implies that of a finite nonabelian simple IM-group. But Bianchi and Tamburini Bellani [1977] and Di Martino and Tamburini Bellani [1980], [1981] checked the list of finite nonabelian simple groups and proved that none of them is an IM-group. Thus, modulo the classification of finite simple groups (see Gorenstein [1982]), we have the following result.

3.3.8 Theorem. Every finite IM-group is soluble.

The structure of soluble IM-groups was determined by Menegazzo [1970b]. First of all we have the following general result.

3.3.9 Lemma. Every IM-group is a T-group.

Proof. Suppose that \( G \) is an IM-group and let \( L \leq H \leq G \). If \( \mathcal{S} \) is the set of all maximal subgroups of \( G \) containing \( L \) but not \( H \), then \( L = H \cap \left( \bigcap_{M \in \mathcal{S}} M \right) = \bigcap_{M \in \mathcal{S}} (H \cap M) \). Every \( M \in \mathcal{S} \) satisfies \( G = MH \) and \( H \cap M \leq M \). So for every \( x \in G \), if we write \( x = mh \) with \( m \in M \) and \( h \in H \), it follows that \( (H \cap M)^x = (H \cap M)^h \geq L^h = L \) and hence \( L^x = \bigcap_{M \in \mathcal{S}} (H \cap M)^x \geq L \). Thus \( L \leq G \).

Let us call a group elementary abelian if it is an abelian torsion group with all \( p \)-components elementary abelian. Then we can state Menegazzo's theorem in the following form.
3.3.10 Theorem (Menegazzo [1970b]). The following properties of a group $G$ are equivalent:

(a) $G$ is a soluble IM-group,
(b) $G$ is a metabelian periodic $T$-group with all Sylow subgroups elementary abelian,
(c) $G$ contains a normal elementary abelian Hall subgroup $N$ with elementary abelian factor group such that every subgroup of $N$ is normal in $G$.

Proof. Suppose first that $G$ is a soluble IM-group. Then by 3.3.9, $G$ is a $T$-group and a well-known theorem of Robinson’s (see Robinson [1982], p. 389) yields that $G$ is metabelian. So by 3.3.7, $G'$ and $G/G'$ are abelian IM-groups. Since every subgroup of an abelian IM-group is an IM-group and the infinite cyclic group clearly is not an IM-group, $G'$ and $G/G'$ and hence also $G$ are periodic. If $P$ is a Sylow $p$-subgroup of $G$, then $P \cong PK/K$ where $K$ is the $p$-complement in $G'$. Then $PK/K \leq G/K$, and again by 3.3.7, $PK/K$ is an IM-group. In particular, $\Phi(P) = 1$. But a metabelian $p$-group is locally nilpotent and therefore has all its maximal subgroups normal (see Robinson [1982], p. 345). Hence $P$ is elementary abelian and (b) holds.

If $G$ satisfies (b), then 3.3.4 shows that $N = G'$ is a Hall subgroup of $G$; clearly it also has the other properties in (c). Finally, suppose that (c) holds. Then $G$ certainly is soluble. Let $H$ be a proper subgroup of $G$. We have to show that $H$ is the intersection of maximal subgroups of $G$. Since $H \cap N \leq G$ and $G/H \cap N$ also satisfies (c), we may assume that $H \cap N = 1$. We shall prove that for every $x \in G \setminus H$ of prime order $p$ there exists a maximal subgroup $M$ of $G$ that contains $H$ but not $x$; since all the Sylow subgroups of $G$ are elementary abelian, the assertion will then follow. Suppose first that $x \in N$ and let $P$ be a Sylow $p$-subgroup of $G$. Since $G$ is locally finite, every pair $x, y$ of $p'$-elements of $C_G(P)$ generates a finite subgroup of $C_G(P)$ in which $P \cap \langle x, y \rangle$ is a direct factor; thus $xy^{-1}$ is a $p'$-element. Therefore the set $L$ of $p'$-elements in $C_G(P)$ is a subgroup and $C_G(P) = P \times L$. Since $G$ induces power automorphisms in $P$, $\lvert G/C_G(P) \rvert$ is finite and clearly prime to $p$. So Gaschütz’s theorem (see Huppert [1967], p. 121) shows that $P$ has a complement $K$ in $G$ and all the complements to $P$ in $G$ are conjugate. Then $H$ and $PH \cap K$ are complements to $P$ in $PH$ and hence there exists $g \in G$ such that $H \leq K^g$. So if $P = \langle x \rangle \times Q$, then $M = QK^g$ is a maximal subgroup of $G$ that contains $H$ but not $x$. Now suppose that $x \notin N$ but $xN \in HN$; let $x = hy$ where $h \in H$ and $1 \neq y \in N$. As we have just shown, there is a maximal subgroup $M$ of $G$ containing $H$ but not $y$; then $x = hy \notin M$. Finally, if $xN \notin HN$, then since $G/N$ is elementary abelian, $G/N = \langle xN \rangle \times M/N$ for some subgroup $M$ of $G$ containing $HN$. Again $M$ is a maximal subgroup of $G$ containing $H$ but not $x$. Thus $G$ is an IM-group.

3.3.11 Corollary. A finite group is a (soluble) IM-group if and only if it is an RK-group.

Proof. By a theorem of Gaschütz (see Robinson [1982], p. 392), every finite soluble $T$-group is a $T^*$-group. Therefore the conditions in Theorem 3.3.3 and (b) in Theorem 3.3.10 are equivalent for finite groups.
3.3 Relative complements

A lattice $L$ is called *weakly join-complemented* if it contains a greatest element $I$ and for every pair $x, y$ of elements of $L$ such that $x < y$ there exists an element $z \in L$ such that $x \cup z \neq I$ and $y \cup z = I$. A complement $z$ to $y$ in the interval $[I/x]$ would clearly satisfy this, so that every relatively complemented lattice is weakly join-complemented.

3.3.12 Theorem (de Giovanni and Franciosi [1981]). The subgroup lattice of a group $G$ is weakly join-complemented if and only if $G$ is an IM-group.

*Proof.* If $G$ is an IM-group and $H < K \leq G$, then there exists a maximal subgroup $M$ of $G$ such that $H \leq M$ but $K \nleq M$. It follows that $K \cup M = G$ and $H \cup M = M < G$. Thus $L(G)$ is weakly join-complemented. Conversely, assume that $L(G)$ is weakly join-complemented and let $H$ be a proper subgroup of $G$. Let $K$ be the intersection of all the maximal subgroups of $G$ containing $H$ and suppose for a contradiction that $H < K$. Then there exists a subgroup $L$ of $G$ such that $K \cup L = G$ and $H \cup L \neq G$; take $x \in G \setminus (H \cup L)$. By Zorn's Lemma there exists a subgroup $M$ maximal with the properties $H \cup L \leq M$ and $x \notin M$. Every subgroup of $G$ containing $M$ properly contains $x$ and so $M$ is a maximal subgroup of $\langle M, x \rangle$. Again since $L(G)$ is weakly join-complemented, there exists a subgroup $N$ of $G$ such that $M \cup N \neq G$ and $\langle M, x \rangle \cup N = G$. If $N \nleq M$, then $M \subset M \cup N$ and the maximality of $M$ would imply that $x \in M \cup N$ and $M \cup N = \langle M, x \rangle \cup N = G$, a contradiction. Hence $N \leq M$ and $\langle M, x \rangle = G$. Thus $M$ is a maximal subgroup of $G$ containing $H$. The definition of $K$ implies that $K \leq M$; since also $L \leq M$, it follows that $M$ contains $K \cup L = G$. This contradiction shows that $K = H$ and $G$ is an IM-group. \qed

A subgroup $H$ of a group $G$ is called *maximal sensitive* in $G$ if every maximal subgroup of $G$ that does not contain $H$ intersects $H$ in a maximal subgroup of $H$ and, conversely, every maximal subgroup of $H$ is the intersection of $H$ with a suitable maximal subgroup of $G$.

3.3.13 Theorem (Venzke [1972]). Let $G$ be a finite soluble group. Then every normal subgroup of $G$ is maximal sensitive in $G$ if and only if $G$ is an IM-group.

*Proof.* First assume that every normal subgroup of $G$ is maximal sensitive. We want to show that $G$ is a T-group. So let $L \leq H \leq G$ and suppose for a contradiction that $L$ is not normal in $G$. Then $L \leq L^G$, the normal closure of $L$ in $G$, and $L^G/L$ is a nontrivial finite soluble group. Hence there exists a normal subgroup $N/L$ of prime index in $L^G/L$. Since $L^G$ is maximal sensitive in $G$, there is a maximal subgroup $M$ of $G$ such that $N = L^G \cap M$. It follows that $N \leq L^G \cup M = G$, a contradiction since $L^G$ is the smallest normal subgroup of $G$ containing $L$. Thus $G$ is a soluble T-group and hence metabelian (see Robinson [1982], p. 389). Let $P$ be a Sylow $p$-subgroup of $G$ and let $N$ be the $p$-complement of $G$. Then $P \simeq P/N$ and $PN \leq G$; let $Q/N = \Phi(P/N)$. If $Q > N$, then since $Q$ is maximal sensitive in $G$, there exists a maximal subgroup $M$ of $G$ such that $Q \cap M$ is a maximal subgroup of $Q$ containing $N$. Since
Complements and special elements in the subgroup lattice of a group

$PN$ is maximal sensitive in $G$, $PN \cap M$ is maximal in $PN$ and it follows that $Q \leq PN \cap M \leq M$, a contradiction. Thus $Q = N$ and $P \cong PN/N$ is elementary abelian. By 3.3.10, $G$ is an IM-group.

Conversely assume that $G$ is an IM-group and take a normal subgroup $H$ of $G$. If $M$ is a maximal subgroup of $G$ that does not contain $H$, then $G = HM$ and $|H : H \cap M| = |G : M|$ is a prime since $G$ is supersoluble. Thus $H \cap M$ is a maximal subgroup of $H$. On the other hand, every maximal subgroup $K$ of $H$ is the intersection of maximal subgroups of $G$ and hence there exists a maximal subgroup $M$ of $G$ such that $K \leq M$ but $H \not\leq M$. It follows that $K = H \cap M$ and $H$ is maximal sensitive in $G$.

Emaldi [1985b] generalized Venzke's theorem to infinite groups. A number of interesting results on chief factors and the socle of an IM-group are contained in Curzio and Rao [1981].

Exercises

1. (Bechtell [1965]) Show that a finite group $G$ satisfies $\Phi(H) \leq \Phi(G)$ for every subgroup $H$ of $G$ if and only if $G/\Phi(G)$ is an SK-group.

2. Find a supersoluble $K$-group that is not an RK-group.

3. (Di Martino and Tamburini Bellani [1980]) Let $n \geq 7$ and $G = A_n$ be the alternating group of degree $n$. Show that if $H = \langle (123) \rangle$, then $[G/C_G(H)]$ is a chain of length 2; thus $G$ is not an IM-group. (Hint: show that a transitive subgroup of $G$ containing $C_G(H)$ is primitive and use the fact that a primitive permutation group of degree $n$ containing a 3-cycle contains $A_n$.)

4. (Di Martino and Tamburini Bellani [1980]) Suppose that $G$ contains proper subgroups $B$ and $N$ such that $G = BNB$, $H = B \cap N \leq N$ and $B = UH$ where $H \leq N_G(U)$. If $G$ is simple, show that every maximal subgroup of $G$ containing $U$ also contains $H$; thus if $H \neq 1$, $G$ is not an IM-group. (Note that all simple Chevalley groups and all twisted groups over a field $K$ have subgroups $B, N$ with the given property and that $H = 1$ only if $K$ is the field with 2 elements or $G = PSU(3, 4)$.)

5. (Menegazzo [1970a]) Let $G$ be a periodic group and $\omega$ a set of primes. A Sylow $\omega$-basis of $G$ is a collection $\mathcal{S}$ of subgroups of $G$ consisting of a maximal $\omega$-subgroup and some Sylow $p$-subgroups of $G$ for primes $p \notin \omega$ such that $ST = TS$ for all $S, T \in \mathcal{S}$ and $\bigcup_{S \in \mathcal{S}} S = G$. Show that $G$ is a soluble RK-group if and only if $G$ is a locally finite $T^\ast$-group with all Sylow subgroups elementary abelian such that for every set $\omega$ of primes, every maximal $\omega$-subgroup of $G$ is a member of a suitable $\omega$-basis of $G$.

6. (Menegazzo [1970a]) For every $i \in \mathbb{N}$ let $p_i, q_i$ be odd primes such that $q_i | p_i - 1$ and $\{p_i, q_i\} \cap \{p_j, q_j\} = \emptyset$ if $i \neq j$; let $H_i = \langle a_i, b_i \rangle$ be a nonabelian group of order $p_i q_i$ where $o(a_i) = p_i$ and $o(b_i) = q_i$. Let $H = Dr H_i$ and $G = H \langle z \rangle$ where $o(z) = 2$ and $za_i z = a_i^{-1}, zb_i z = b_i$ for all $i \in \mathbb{N}$. Show that
3.4 Neutral elements and related concepts

(a) $G$ is a locally finite $T^*$-group such that every Sylow $p$-subgroup of $G$ is elementary abelian and is a member of a suitable Sylow $\{p\}$-basis of $G$, in particular,
(b) $G$ is an IM-group, but
(c) $G$ is not an RK-group.

7. (de Giovanni and Franciosi [1981]) Show that the subgroup lattice of a group $G$ is weakly meet-complemented (that is, for every pair $H$, $K$ of subgroups of $G$ such that $H < K$ there exists a subgroup $L$ of $G$ such that $H \cap L = 1$ and $K \cap L \neq 1$) if and only if $G$ is periodic and every element of $G$ has squarefree order.

8. Show that every subgroup of a group $G$ is maximal sensitive if and only if $G$ is an IM-group and every maximal subgroup of $G$ is modular in $G$.

3.4 Neutral elements and related concepts

Distributive, standard and neutral elements were introduced into lattice theory by Ore, Grätzer and Birkhoff. We shall study these and some further related concepts in subgroup lattices of groups.

An element $a$ of a lattice $L$ is called neutral if every triple $a$, $x$, $y$ of elements in $L$ generates a distributive sublattice. The reader can easily verify that greatest and least elements of $L$ are neutral and that if $L$ is a direct product of lattices $L_1$ and $L_2$, then an element $a = (a_1, a_2)$ of $L$ is neutral if and only if both $a_i$ are neutral in $L_i$.

3.4.1 Theorem. The element $a$ of the lattice $L$ is neutral if and only if for all $x, y \in L$,

1. $a \cup (x \cap y) = (a \cup x) \cap (a \cup y),$

that is the map $\varphi_a: L \to [I/a]; x \mapsto a \cup x$ is an epimorphism,

2. $a \cap (x \cup y) = (a \cap x) \cup (a \cap y),$

that is the map $\psi_a: L \to [a/0]; x \mapsto a \cap x$ is an epimorphism, and

3. $a \cup x = a \cup y$ and $a \cap x = a \cap y$ implies that $x = y$.

Proof. Since (1) and (2) are just distributive laws involving only $a$, $x$ and $y$, they clearly are satisfied if $a$ is neutral; in addition, $a \cup x = a \cup y$ and $a \cap x = a \cap y$ together with the distributive laws imply that

\[ x = x \cap (a \cup x) = x \cap (a \cup y) = (x \cap a) \cup (x \cap y) \]
\[ = (a \cap y) \cup (x \cap y) = (a \cup y) \cap y = y. \]

Conversely, suppose that (1)–(3) hold. Then the map $\sigma: L \to [I/a] \times [a/0]$ defined by $x^\sigma = (a \cup x, a \cap x)$ for $x \in L$ is a monomorphism. For, (1) implies that

\[ (x \cap y)^\sigma = (a \cup (x \cap y), a \cap (x \cap y)) = ((a \cup x) \cap (a \cup y), (a \cup x) \cap (a \cap y)) \]
\[ = (a \cup x, a \cap x) \cap (a \cup y, a \cap y) = x^\sigma \cap y^\sigma, \]
Complements and special elements in the subgroup lattice of a group

similarly (2) yields \((x \cup y)^\sigma = x^\sigma \cup y^\sigma\), and \(\sigma\) is injective by (3). Now \(a\) is neutral in \([I/a]\) and in \([a/0]\). Therefore \(a^\sigma = (a, a)\) is neutral in \([I/a] \times [a/0]\) and hence also in the sublattice \(L^\sigma\) of this direct product. It follows that \(a\) is neutral in \(L\).

All the properties (1)–(3) in Theorem 3.4.1 have been studied separately. An element \(a\) of the lattice \(L\) is called \(join\)-distributive if it satisfies (1), \(meet\)-distributive if (2) holds, and \(uniquely\ complemen\)ted if (3) is satisfied for all \(x, y \in L\). Furthermore, \(a\) is called \(join\)-quasi-distributive if (1) holds for all \(x, y \in L\) such that \(a \cup x = a \cup y\); dually, \(a\) is \(meet\)-quasi-distributive if (2) is satisfied whenever \(a \cap x = a \cap y\). Finally, \(a\) is a \(standard\ element\) if it is join-distributive and uniquely complemented, that is, it satisfies (1) and (3).

**General properties of distributive elements**

In arbitrary lattices there are only the obvious interrelations between the concepts introduced above. For subgroup lattices, however, we have some unexpected results.

3.4.2 Theorem (Ivanov [1969]). Every \(join\)- or \(meet\)-distributive element in the subgroup lattice of a group \(G\) is normal in \(G\) and uniquely complemented in \(L(G)\).

**Proof.** Let \(N \leq G\), \(z \in G\) and \(Z = \langle z \rangle\). Then \(N^z \cup Z = N \cup Z\) and \(N^z \cap Z = z^{-1}(N \cap Z)z = N \cap Z\). Therefore if \(N\) is \(join\)-distributive, then

\[
N = N \cup (N^z \cap Z) = (N \cup N^z) \cap (N \cup Z) = N \cup N^z
\]

and hence \(N^z \leq N\). Similarly, if \(N\) is \(meet\)-distributive, then

\[
N = N \cap (N^z \cup Z) = (N \cap N^z) \cup (N \cap Z) = N \cap N^z
\]

and hence \(N \leq N^z\). Since \(z\) is arbitrary, it follows in both cases that \(N \leq G\).

Now let \(X, Y \leq G\) such that \(N \cup X = N \cup Y\) and \(N \cap X = N \cap Y\). If \(N\) is \(join\)-distributive, then since \(N \leq G\), \(NX = NY = N(X \cap Y)\) and therefore

\[
X = NX \cap X = N(X \cap Y) \cap X = (N \cap X)(X \cap Y) = (N \cap Y)(X \cap Y)
\]

\[
= N(X \cap Y) \cap Y = NY \cap Y = Y.
\]

If \(N\) is \(meet\)-distributive, then \(N \cap (X \cup Y) = N \cap X = N \cap Y \leq X \cap Y\) and therefore since \(N \leq G\),

\[
X = (N \cap (X \cup Y))X = NX \cap (X \cup Y) = NY \cap (X \cup Y) = (N \cap (X \cup Y))Y = Y.
\]

In both cases, \(N\) is uniquely complemented in \(L(G)\).
3.4.3 Theorem (Curzio [1964a], Napolitani [1965]). Let $N$ be a subgroup of the group $G$. Then $N$ is join-quasi-distributive in $\mathcal{L}(G)$ if and only if $N$ is join-distributive in $\mathcal{L}(G)$.

Proof. Clearly every join-distributive element is join-quasi-distributive. So suppose that $N$ is join-quasi-distributive in $\mathcal{L}(G)$. We want to show first that $N \leq G$. If $x \in N$ and $g \in G \setminus N$, then $N \cup \langle g \rangle = N \cup \langle xg \rangle = N \cup (\langle g \rangle \cap \langle xg \rangle)$ as $N$ is join-quasi-distributive. Hence there exists an integer $r$ such that

$$(4) \quad \langle g \rangle \cap \langle xg \rangle = \langle g^r \rangle \leq N \quad \text{and} \quad N \cup \langle g \rangle = N \cup \langle g^r \rangle; \quad \text{furthermore} \quad g^r \in C_G(x)$$

since $\langle g \rangle \cap \langle xg \rangle$ is centralized by $g$ and $xg$ and hence also by $x$. We use the first assertion in (4) to show that if $N$ contains an element of finite order $n$, then every element of $G$ of this order is contained in $N$. For, if this were false this statement would fail for a smallest integer $n$; choose $x \in N$ and $g \in G \setminus N$ such that $o(x) = n = o(g)$. Then every proper subgroup of $\langle g \rangle$ would be contained in $N$ and therefore by (4), $\langle g \rangle \cap \langle xg \rangle = \langle g \rangle$. It would follow that $g \in \langle xg \rangle$, hence also $x \in \langle xg \rangle$ and since the cyclic group $\langle xg \rangle$ contains only one subgroup of order $n$, $\langle g \rangle = \langle x \rangle = \langle x \rangle \leq N$, a contradiction.

The result just proved implies that $N$ is normal in $G$ if it is periodic. So suppose now that $N$ contains an element $x$ of infinite order and take $g \in G \setminus N$. Then by (4), $N \cup \langle g \rangle = N \cup \langle g^r \rangle$ and $g^r x = x g^r$ for some integer $r$. Again by (4), $\langle g^r \rangle \cap \langle x g^r \rangle \leq N$ and hence there exist nonzero integers $s, t$ such that $g^{r} = (x g^{t})^s = x^s g^{r t}$. Since $x$ has infinite order, $1 \neq x^t = g^{r (s - t)}$ and therefore $|\langle g \rangle : N \cap \langle g \rangle|$ is finite. Now choose $g_1 \in \langle g \rangle$ satisfying $N \cup \langle g_1 \rangle = N \cup \langle g \rangle$ for which $|\langle g_1 \rangle : N \cap \langle g_1 \rangle|$ is minimal. If $y \in N$, then again by (4) there exists $g_2 \in \langle g_1 \rangle$ such that $N \cup \langle g_2 \rangle = N \cup \langle g_1 \rangle = N \cup \langle g \rangle$ and $y g_2 = g_2 y$. The choice of $g_1$ implies that

$$|\langle g_1 \rangle : N \cap \langle g_1 \rangle| \leq |\langle g_2 \rangle : N \cap \langle g_2 \rangle| = |\langle g_2 \rangle (N \cap \langle g_1 \rangle) : N \cap \langle g_1 \rangle|$$

and it follows that $\langle g_1 \rangle = \langle g_2 \rangle (N \cap \langle g_1 \rangle)$. Thus $g_1 = g_2 z$ with $g_2 \in \langle g_2 \rangle$, $z \in N$ and hence $y^{g_1} = y^{g_2 z} = y^z \in N$. Since $y$ was arbitrary, $N^{g_1} \leq N$. Similarly $N^{g_1} \leq N$ so that $g_1 \in N_G(N)$. Therefore $g \in N \cup \langle g_1 \rangle \leq N_G(N)$ and since $g$ was arbitrary, $N \leq G$.

Thus $N \leq G$ in all cases. For arbitrary subgroups $X$ and $Y$ of $G$ therefore, by Dedekind's law, $N X \cap N Y = N (N X \cap Y) \leq N X$ and hence

$$N (N X \cap Y) = N (X \cap N (N X \cap Y)) = N (N X \cap Y \cap N (N X \cap Y)) = N (X \cap Y)$$

since $N$ is join-quasi-distributive. Thus $N X \cap N Y = N (X \cap Y)$ and $N$ is join-distributive. □

3.4.4 Corollary. In the subgroup lattice of a group, the join-quasi-distributive elements, the join-distributive elements and the standard elements coincide.
Note that the nonmodular lattice with 5 elements contains an element that is join- and meet-distributive but not uniquely complemented, another one that is join-quasi-distributive but not join-distributive, and a third one that is meet-quasi-distributive but not meet-distributive. This last situation also occurs in subgroup lattices so that the dual to Theorem 3.4.3 does not hold.

3.4.5 Example. Let $G = \langle a, b, c | a^7 = b^3 = c^4 = 1, ab = ba, c^{-1}ac = b, c^{-1}bc = a^{-1} \rangle$. Then $c$ operates fixed-point-freely on $P = \langle a, b \rangle$ and hence $G$ is a Frobenius group of order $7^2 \cdot 4$. We claim that $N = P \langle c^2 \rangle$ is meet-quasi-distributive in $L(G)$. To show this let $X, Y \leq G$ such that $N \cap X = N \cap Y$. If $X \cup Y \leq N$, then $N \cap (X \cup Y) = X \cup Y = (N \cap X) \cup (N \cap Y)$. And if $X$, say, is not contained in $N$, then $X$ contains a Sylow 2-subgroup $\langle c \rangle^9$ of $G$. Since $c$ operates irreducibly on $P$, $\langle c \rangle^9$ is a maximal subgroup of $G$ and hence $X = G$ or $X = \langle c \rangle^9$. In the first case, clearly $X \cup Y = X$; in the second, $N \cap Y = N \cap X = \langle c^2 \rangle$ implies that $\langle c^2 \rangle \leq Y \leq \langle c \rangle^9 = X$ and therefore also $X \cup Y = X$. In both cases $N \cap (X \cup Y) = N \cap X = N \cap Y$ and $N$ is meet-quasi-distributive. Since $\langle a \rangle \cup \langle c \rangle = G$ and $a^2 = a^{-1}$,

$$N \cap (\langle a \rangle \cup \langle c \rangle) = N \neq \langle a \rangle \cup \langle c^2 \rangle = (N \cap \langle a \rangle) \cup (N \cap \langle c \rangle)$$

and hence $N$ is not meet-distributive in $L(G)$.

Uniquely complemented elements

We want to determine these elements in the subgroup lattice of a finite group. So in the sequel, let $G$ be a finite group and $N \leq G$ a uniquely complemented element in $L(G)$. In the first place the following is evident:

(5) if $M \leq N$ and $M \leq G$, then $N/M$ is uniquely complemented in $L(G/M)$.

Furthermore, if $H \leq G$ and $X, Y \in L(H)$ such that $(N \cap H) \cup X = (N \cap H) \cup Y$ and $(N \cap H) \cap X = (N \cap H) \cap Y$, then $N \cup X = N \cup (N \cap H) \cup X = N \cup (N \cap H) \cup Y = N \cup Y$ and $N \cap X = N \cap H \cap X = N \cap H \cap Y = N \cap Y$; since $N$ is uniquely complemented in $L(G)$, it follows that $X = Y$. We have now shown the following which, of course, also holds more generally in arbitrary lattices.

(6) If $H \leq G$, then $N \cap H$ is uniquely complemented in $L(H)$.

If $X \leq G$ and $z \in N_X(N \cap X)$, then $N \cap X = (N \cap X)^z = N \cap X^z$ and $N \cup X = (N \cup X)^z = N \cup X^z$. Since $N$ is uniquely complemented, $X = X^z$ and we have shown that

(7) $N_X(N \cap X) \leq N_G(X)$ for all $X \leq G$.

In particular, if $p$ is a prime dividing $|N|$ and $X$ is a subgroup of order $p$ in $G$ that is not contained in $N$, then $N \cap X = 1$; hence $P \leq N_G(X)$ for every subgroup $P$ of order $p$ of $N$. It follows that $PX$ is elementary abelian of order $p^2$ and $PX \cap N = P$. Therefore every minimal subgroup $Y$ of $PX$ different from $P$ and $X$ satisfies $N \cap Y =$
1 = N ∩ X and N ∪ Y = N ∪ X. This contradiction shows that there is no such X, another important property of N.

(8) If X ≤ G such that |X| = p is a prime dividing |N|, then X ≤ N.

It follows easily that

(9) N is a characteristic subgroup of G.

For, if we choose a prime p dividing |N| and let M = ⟨P ≤ G|P| = p⟩, then M is a characteristic subgroup of G contained in N and by (5) and induction, N/M is characteristic in G/M. Thus N is characteristic in G. Finally (7) and (9) yield that

(10) N ≤ C_G(X) for all X ≤ G such that N ∩ X = 1;

for, N normalizes X and X normalizes N and therefore [N, X] ≤ N ∩ X = 1.

Note that if N is a Hall subgroup of G, then (9), (10) and the Schur-Zassenhaus Theorem imply that G = N × K where K is a complement to N in G; therefore N is neutral in L(G) since it is the greatest element of a direct factor of L(G). On the other hand, the following lemma will show that if G is a p-group and 1 < N < G, then G is cyclic or generalized quaternion and again N is neutral in L(G).

3.4.6 Lemma. Let N be a uniquely complemented element in the subgroup lattice of a finite group G and suppose that p is a prime dividing |N| and |G/N|. Then every Sylow p-subgroup S of G is cyclic or a generalized quaternion group, and in the latter case |N| ≡ 2 (mod 4). Furthermore, \( N_N(S) ≤ C_G(S) \) and N has a normal p-complement.

Proof. By (6), R = N ∩ S is uniquely complemented in L(S). Since N ≤ G, R is a Sylow p-subgroup of N and therefore 1 < R < S. Hence there exists H ≤ S such that R is a maximal subgroup of H, and as R is uniquely complemented in L(S) it is the only maximal subgroup of H. Thus H is cyclic, but by (8), its subgroup R contains every minimal subgroup of S. It follows that S has only one minimal subgroup and therefore is cyclic or a generalized quaternion group (see Robinson [1982], p. 138). In the latter case, (5) shows that R/Z(S) is uniquely complemented in L(S/Z(S)) and therefore is trivial since S/Z(S) is a dihedral group; thus R = Z(S) and |N| ≡ 2 (mod 4).

To prove that \( N_N(R) ≤ C_G(S) \) take \( z ∈ N_N(R) \). If \( z \) is a p-element, then \( z \) is contained in R, the only Sylow p-subgroup of \( N_N(R) \). Since \( R = Z(S) \) if \( S \) is generalized quaternion, it follows that \( z ∈ C_G(S) \). Now suppose that \( z \) is a p'-element. By (7), \( z \) normalizes S and as \( N ≤ G \), \([z, S] ≤ N ∩ S = R\). Since \( R ≤ \Phi(S) \), it follows that \( z \) centralizes \( S/\Phi(S) \) and hence also S. Thus \( z ∈ C_G(S) \) in this case also and so, finally, \( N_N(R) ≤ C_G(S) \). In particular, \( N_N(R) = C_N(R) \) and by Burnside's theorem (see Robinson [1982], p. 280) there exists a normal p-complement in N.

Now we can give the desired characterization of uniquely complemented elements in the subgroup lattice of a finite group.

3.4.7 Theorem (Napolitani [1968]). Let N be a subgroup of a finite group G. Then N is a uniquely complemented element in L(G) if and only if there exist subgroups L and K of G with the following properties.
(a) $G = LK$, $L \trianglelefteq G$, $(|L|, |K|) = 1$, that is, $L$ is a normal Hall subgroup of $G$ with complement $K$.

(b) $N = L(N \cap K)$ and $N \cap K \leq Z(K)$.

(c) For every prime $p$ dividing $|N \cap K|$, the Sylow $p$-subgroups of $G$ are cyclic or generalized quaternion groups.

(d) For every Sylow subgroup $S$ of $K$, $C_L(N \cap S) = C_L(S)$.

Proof. Suppose first that $N$ is uniquely complemented in $L(G)$. Then by (9), $N \trianglelefteq G$ and Lemma 3.4.6 shows that $N$ has a normal $p$-complement for every prime $p$ dividing $|N|$ and $|G/N|$. Let $L$ be the intersection of these normal $p$-complements of $N$ or $L = N$ if there is no such prime $p$. Then $L$ is a characteristic subgroup of $N$ and hence normal in $G$. Furthermore the construction of $L$ shows that a prime $q$ dividing $|L|$ cannot divide $|G/N|$. It follows that $L$ is a normal Hall subgroup of $G$ and by the Schur-Zassenhaus Theorem there exists a complement $K$ to $L$ in $G$. We claim that $L$ and $K$ satisfy (a)-(d). Clearly (a) holds and $N = L(N \cap K)$. Furthermore $N/L$ is nilpotent and has cyclic Sylow subgroups by 3.4.6. Thus $N/L \cong N \cap K$ is cyclic. Let $S$ be a Sylow subgroup of $K$. If $N \cap S \neq 1$, then $N \cap K \leq N_0(N \cap S) \leq C_G(S)$ by 3.4.6, since every prime dividing $|N \cap K| = |N/L|$ also divides $|G/N|$. And if $N \cap S = 1$, (10) shows that $N \cap K < C_G(S)$. Thus $N \cap K$ centralizes every Sylow subgroup of $K$ and hence $K$. Therefore (b) holds and (c) follows again from 3.4.6. Finally, for every subgroup $X$ of $K$, $C_L(N \cap X) = C_L(S)$ by (7). Hence $[C_L(N \cap X), X] \leq L \cap X = 1$ and $C_L(N \cap X) = C_L(X)$. In particular, (d) holds.

Suppose conversely that $G$ contains subgroups $L$ and $K$ satisfying (a)-(d). By (b), $N \trianglelefteq G$ and we claim that

(11) $K$ is the only complement of $L$ in $G$ intersecting $N$ in $N \cap K$.

To show this, suppose that $H$ is such a complement. Let $p$ be a prime dividing $|K| = |H|$ and take Sylow $p$-subgroups $S_0$ and $T$ of $K$ and $H$, respectively. By (a), $S_0$ and $T$ are Sylow $p$-subgroups of $G$ and there exist $x \in L$, $y \in K$ such that $T = S_0^y = S^x$ for $S = S_0^x$, a Sylow $p$-subgroup of $K$. Now $N \cap S$ and $N \cap T$ are Sylow $p$-subgroups of the abelian group $N \cap K = N \cap H$. It follows that $N \cap S = N \cap T = N \cap S^x = (N \cap S)^x$ and therefore $[x, N \cap S] \leq L \cap S = 1$. By (d), $S = S^x = T$ and so $T = K$. Since $p$ was arbitrary, $H \leq K$ and hence $H = K$. This proves (11).

Now consider subgroups $X$ and $Y$ of $G$ such that $N \cap X = N \cap Y$ and $NX = NY$. We have to show that $X = Y$ and may assume that

(12) $NX = G = NY$

since $L$ and $K_0 = K \cap NX$ satisfy (a)-(d) in $G_0 = NX$. If $p$ is a prime dividing $|N \cap K|$ but not $|G/N|$ and $P$ is a Sylow $p$-subgroup of $N \cap K$, then by (b), $P$ is a central Sylow subgroup of $K$ and hence $K = P \times K^*$ where $K^*$ is a $p'$-group. It follows that $L^* = LP$ is a normal Hall subgroup of $G$ with complement $K^*$ satisfying (a)-(d). We may therefore also assume that

(13) every prime dividing $|N \cap K|$ also divides $|G/N|$.

Since $L \cap X$ is a normal Hall subgroup of $X$, we can write $X = (L \cap X)X_1$ where $X_1$ is a complement to $L \cap X$ in $X$; similarly, $Y = (L \cap Y)Y_1$ with a complement $Y_1$ to
3.4 Neutral elements and related concepts

\( L \cap Y \) in \( Y \). Then \( L \cap X = L \cap N \cap X = L \cap N \cap Y = L \cap Y \) and hence

\[(14) \quad X = Mx_1 \text{ and } Y = My_1 \]

where \( M = L \cap X = L \cap Y \). Since \( N \cap X = N \cap Mx_1 = M(N \cap x_1) \) and \( N \cap Y = M(N \cap y_1) \), \( N \cap x_1 \) and \( N \cap y_1 \) are complements to the normal Hall subgroup \( M \) in \( N \cap X = N \cap Y \). By (b), \( N/L \) and hence also \( N \cap X/M \) is abelian. Therefore by the Schur-Zassenhaus Theorem there exists \( z \in M \) such that \( N \cap x_1 = (N \cap y_1)z = N \cap y_1 \). Since also \( N \cap x_1 = G = Ny_1 \), and, in view of (14), it is sufficient to show that \( x_1 = y_1 \), we may finally assume that

\[(15) \quad L \cap X = 1 = L \cap Y. \]

We claim that \( X \) and \( Y \) then are complements to \( L \) in \( G \). For, since \( G/N \cong X/N \cap X \), it follows from (13) that there exists a \( p \)-element \( x \in X \setminus N \) for every prime \( p \) dividing \( |N \cap K| \). By (c), a Sylow \( p \)-subgroup \( S \) of \( G \) containing \( x \) is cyclic or generalized quaternion, and in the latter case, \( |N \cap S| = 2 \) since \( N \cap S \leq Z(S) \). Hence \( N \cap S \leq \langle x \rangle \leq X \) and therefore the normal subgroup \( Lx \) of \( N \) contains every Sylow \( p \)-subgroup of \( N \). It follows that \( N \cap K \leq Lx \) and \( G = N \cap K \leq L(N \cap x) \). Together with (15) this shows that \( X \) is a complement to \( L \) in \( G \); similarly for \( Y \). It follows that \( N \cap K \) and \( N \cap X = N \cap Y \) are complements to \( L \) in \( N \) and the Schur-Zassenhaus Theorem implies that there exists \( z \in L \) such that \( N \cap K = (N \cap x)z = N \cap x^z = N \cap y^z \). By (11), \( x^z = K = y^z \) and hence \( X = Y \) as desired. \(\square\)

No characterization of uniquely complemented elements in the subgroup lattice of an arbitrary group is known.

Join-distributive elements

3.4.8 Theorem (Zappa [1949]). Let \( N \) be a subgroup of a finite group \( G \). Then \( N \) is a join-distributive (or standard) element in \( L(G) \) if and only if there exist subgroups \( L \) and \( K \) of \( G \) with the following properties.

(a) \( G = L \times K \) and \( (|L|, |K|) = 1 \).

(b) \( N = L \times (N \cap K) \) and \( N \cap K \leq Z(G) \).

(c) For every prime \( p \) dividing \( |N \cap K| \), the Sylow \( p \)-subgroups of \( G \) are cyclic or generalized quaternion groups.

Proof. First suppose that \( N \) is join-distributive in \( L(G) \). Then by 3.4.2, \( N \) is uniquely complemented in \( L(G) \) and hence there exist subgroups \( L \) and \( K \) with properties (a)–(d) of Theorem 3.4.7. As in the proof of this theorem, if \( p \) is a prime dividing \( |N \cap K| \) but not \( |G/N| \) and \( P \) is a Sylow \( p \)-subgroup of \( N \cap K \), then \( K = P \times K^* \) for some \( p' \)-subgroup \( K^* \) and \( L^* = LP \) is a normal Hall subgroup of \( G \) with complement \( K^* \) satisfying (a)–(d) of 3.4.7. So we may assume that every prime dividing \( |N \cap K| \) also divides \( |G/N| \); in addition we want to show that under this assumption \( K \leq G \). Then it will follow that \( G = L \times K \), \( N = L \times (N \cap K) \) and \( L \leq C_G(N \cap K) \) so that \( N \cap K \leq Z(G) \); thus (a)–(c) will be satisfied.
Let $p$ be a prime and $S$ a Sylow $p$-subgroup of $K$. If $N \cap S = 1$, then (d) of 3.4.7 shows that $S$ is centralized by $L$. So suppose that $N \cap S \neq 1$. Then $p$ divides $|G/N|$ and therefore $S \leq N$. For $x \in L$, $NS = (NS)^x = NS^x$ and since $N$ is join-distributive, $N(S \cap S^x) = NS \cap NS^x = NS$. In particular, $S \cap S^x \leq N$. By (c) of 3.4.7, $S$ is cyclic or generalized quaternion and in the latter case, $|N \cap S| = 2$ since $N \cap S \leq Z(S)$. It follows that $N \cap S \leq S \cap S^x \leq S$. But then $N(S \cap S^x) = NS$ implies that $S \cap S^x = S$ and hence $S = S^x$. This shows that $L$ normalizes every Sylow subgroup of $K$. Thus $K \leq LK = G$.

Suppose conversely that $G$ contains subgroups $L$ and $K$ satisfying (a)-(c) and let $X \leq G$.

(16) If $g \in NX$ is an element of prime power order, then $g \in N$ or $g \in X$.

To prove this, suppose that $o(g) = p^n$ and let $g \notin N$. Let $a \in N$, $x \in X$ such that $g = ax$ and write $a = bc$ with commuting $p$-element $b$ and $p'$-element $c$. Since $g \notin N$, $p$ divides $|K|$ and hence $g \in K$ and $b \in N \cap K \leq Z(G)$. Hence $\langle b, g \rangle$ is a $p$-group and (c) shows that $\langle b \rangle < \langle g \rangle$. It follows that $\langle g \rangle = \langle b^{-1}g \rangle$. Now $x = a^{-1}g = c^{-1}b^{-1}g$ where $c^{-1} \in N$ is a $p'$-element and $b^{-1}g \in K$ is a $p$-element. Since $[N, K] = 1$, $b^{-1}g$ therefore is a power of $x$. Thus $\langle g \rangle = \langle b^{-1}g \rangle \leq X$ and (16) holds.

Now we prove that $N$ is a join-distributive element in $L(G)$. Since $N \leq G$, we have to show that $N(X \cap Y) = NX \cap NY$ for all $X, Y \leq G$. Let $g \in NX \cap NY$ be an element of prime power order. If $g \in N$, then $g \in N(X \cap Y)$; on the other hand, if $g \notin N$, then by (16), $g \in X$ and $g \in Y$, so that again $g \in N(X \cap Y)$. It follows that $NX \cap NY \leq N(X \cap Y)$. The other inequality is obvious. Hence $N(X \cap Y) = NX \cap NY$, as desired.

The join-distributive elements in the subgroup lattice of an infinite group were characterized by D.G. Higman [1951] in the case of a torsion group and by Sato [1956] for groups with elements of infinite order. We also refer the reader to Suzuki [1956], Chapter IV for a systematic treatment of lattice-homomorphisms of groups. Since any join-distributive element $N$ in $L(G)$ is normal in $G$, the map sending every subgroup $X$ of $G$ to $NX/N$ is a homomorphism from $L(G)$ to $L(G/N)$ induced by the natural group-homomorphism from $G$ to $G/N$. So Suzuki is able to use his general theory of lattice-homomorphisms to give shorter proofs of Zappa's, Higman's and Sato's results.

Neutral elements

3.4.9 Theorem (Suzuki [1951b], Zappa [1951c]). Let $N$ be a subgroup of a finite group $G$. Then $N$ is a neutral element in $L(G)$ if and only if there exist subgroups $L, H$ and $M$ of $G$ with the following properties.

(a) $G = L \times HM$, $M \leq G$ and $(|L|, |H|) = (|L|, |M|) = (|H|, |M|) = 1$ (so that $L$, $H$ and $M$ are Hall subgroups of $G$).

(b) $N = L \times (N \cap H)$ and $N \cap H \leq Z(G)$.

(c) $H$ is nilpotent with Sylow subgroups cyclic or generalized quaternion groups.
Proof. First suppose that $N$ is neutral in $L(G)$. Then by 3.4.1, $N$ is join-distributive in $L(G)$ and hence there exist subgroups $L$ and $K$ with properties (a)–(c) of Theorem 3.4.8. Let $M = \{x \in G|o(x),|N| = 1\}$. If $x, y \in M$, then $N \cap \langle x \rangle = 1 = N \cap \langle y \rangle$ and, since $N$ is meet-distributive, also $N \cap (\langle x \rangle \cup \langle y \rangle) = 1$. It follows from (8) that $\langle |N|,|\langle x,y \rangle| \rangle = 1$. In particular, $o(xy^{-1}),|N| = 1$ and hence $xy^{-1} \in M$. This shows that $M$ is a subgroup, and it is clearly a normal Hall subgroup of $G$. Now $M \leq K$ and by the Schur-Zassenhaus Theorem there is a complement $H$ to $M$ in $K$. Since $N \leq G$ and $LH$ is a Hall subgroup of $G$, $N \leq LH$ and $N \cap H = N \cap K$. Thus (a) and (b) are satisfied and since every prime dividing $|H|$ also divides $|N \cap H|$, it remains to be shown that $H$ is nilpotent. So let $p$ be a prime and suppose for a contradiction that $S$ and $T$ are different Sylow $p$-subgroups of $H$. Since $N \leq G$, $N \cap S$ and $N \cap T$ are Sylow $p$-subgroups of $N \cap H$. An abelian group has only one Sylow $p$-subgroup, hence $N \cap S = N \cap T$. Since $N$ is meet-distributive, $N \cap (S \cup T) = (N \cap S) \cup (N \cap T) = N \cap S$ is a $p$-group. But as $S \neq T$, there exists a subgroup $Q$ of prime order $q \neq p$ in $S \cup T \leq H$. The definition of $M$ implies that $q$ divides $|N|$ and therefore $Q \leq N$ by (8). Thus $Q \leq N \cap (S \cup T)$, a contradiction. It follows that $H$ contains only one Sylow $p$-subgroup for every prime $p$ and hence is nilpotent.

Suppose conversely that $G$ contains subgroups $L, H, M$ satisfying (a)–(c) and let $X, Y \leq G$. We have to show that

\[(17) \quad N \cap (X \cup Y) = (N \cap X) \cup (N \cap Y).\]

Then $N$ will be meet-distributive in $L(G)$; by 3.4.8, $N$ is join-distributive, and 3.4.2 and 3.4.1 will imply that $N$ is a neutral element of $L(G)$. If $L(G)$ is a direct product and (17) is true for the components of $N, X$ and $Y$, then it certainly also holds for the subgroups themselves. By 1.6.4, $L(G) \simeq L(L) \times L(HM)$ and since $L \leq N$, we may therefore assume that $L = 1$. Then $N \leq Z(H)$ and (17) holds for $X, Y \leq H$ since $H$ is nilpotent and (17) is satisfied for the Sylow subgroups of $N, X$ and $Y$. Now $G/M \simeq H$ and it follows that $MN$ is meet-distributive in $[G/M]$. Furthermore $\langle |M|,|N| \rangle = 1$ and therefore for every subgroup $Z$ of $G$,

\[M(N \cap Z) = M((M \cap Z) \times (N \cap Z)) = M(MN \cap Z) = MN \cap MZ.\]

Hence for arbitrary $X, Y \leq G$,

\[M(N \cap (X \cup Y)) = MN \cap M(X \cup Y) = MN \cap (MX \cup MY) = (MN \cap MX) \cup (MN \cap MY) = M(N \cap X) \cup M(N \cap Y) = M((N \cap X) \cup (N \cap Y)).\]

It follows that $N \cap (X \cup Y) = (N \cap X) \cup (N \cap Y)$ as required. \qed

No characterization of neutral elements in the subgroup lattice of an arbitrary group is known, for torsion groups they were determined by Martino [1973]. The meet-distributive and meet-quasi-distributive elements in subgroup lattices of finite groups were characterized by Zappa [1951a] and Napolitani [1968], respectively.
Complements and special elements in the subgroup lattice of a group

(see Exercises 2 and 4 or Suzuki [1956], Chapter IV). Ivanov [1969] showed that meet-distributivity is a local property and thus extended Zappa's result to locally finite groups. Meet-distributive elements in subgroup lattices of non-periodic locally soluble groups have been considered by Ivanov [1985], Stonehewer and Zacher [1990a], [1990b], [1991b]. A characterization of meet-distributive or meet-quasi-distributive elements in subgroup lattices of arbitrary groups is not known.

Modular elements

It is natural to look for elements \( m \) of a lattice \( L \) that stand in the same relation to modularity as neutral elements do to distributivity; thus we introduce:

(18) every triple \( m, x, y \) of elements in \( L \) generates a modular sublattice.

This was done by Zacher [1955a], [1955b], [1956] who used the slightly stronger condition that \( m \) generates a modular sublattice with every modular sublattice of \( L \). Clearly, if \( m \) satisfies (18), then

\[
x \cup (m \cap y) = (x \cup m) \cap y \quad \text{for all } x, y \in L \text{ with } x \leq y, \text{ and}
\]

\[
m \cup (x \cap y) = (m \cup x) \cap y \quad \text{for all } x, y \in L \text{ with } m \leq y,
\]

that is, \( m \) is a modular element of \( L \) in the sense of Section 2.1. The converse is not true; in fact, if \( G \) is the nonabelian group of order \( p^3 \) and exponent \( p \) and \( X \) and \( Y \) are subgroups of order \( p \) of \( G \) with \( G = \langle X, Y \rangle \), then the sublattice of \( L(G) \) generated by \( Z(G) \), \( X \) and \( Y \) is not modular. We shall study modular elements in the subgroup lattice of a finite group \( G \) in Section 5.1 and will get a fairly good description of these modular subgroups. While characterizations of subgroups of \( G \) satisfying either (18) or Zacher's stronger condition in \( L(G) \) are not known, Zacher [1956] determined the Hall subgroups of finite groups with the second property.

Exercises

1. Let \( L \) be a lattice.
   (a) Show that greatest and least elements of \( L \) are neutral.
   (b) Show that if \( L \) is a direct product of lattices \( L_1 \) and \( L_2 \), then an element \( a = (a_1, a_2) \) of \( L \) is neutral if and only if both \( a_i \) are neutral in \( L_i \).

2. (Zappa [1951a]) Show that a subgroup \( N \) of a finite group \( G \) is meet-distributive in \( L(G) \) if and only if there exist subgroups \( L, H \) and \( M \) of \( G \) with the following properties.
   (a) \( G = LHM, L \leq G, M \leq G \) and \( (|L|, |H|) = (|L|, |M|) = (|H|, |M|) = 1 \).
   (b) \( N = L(N \cap H) \) and \( N \cap H \leq Z(HM) \).
   (c) \( H \) is nilpotent with Sylow subgroups cyclic or generalized quaternion.
(d) For every Sylow subgroup $S$ of $H$, $C_L(N \cap S) = C_L(S)$.
(e) For every Sylow subgroup $S$ of $H$, every subgroup of $L$ that is normalized by $N \cap S$ is normalized by $S$.

Using the classification of finite simple groups, Stonehewer and Zacher [1991a] showed that the group $[L, H]$ in Exercise 2 is nilpotent.

3. (Stonehewer and Zacher [1991a]) If $M = 1$ in Exercise 2 and the Sylow 2-subgroup $Q$ of $H$ is a generalized quaternion group, show that $Q$ is a direct factor of $G$.

4. (Napolitani [1968]) Show that a subgroup $N$ of a finite group $G$ is meet-quasi-distributive in $L(G)$ if and only if it satisfies properties (a)–(d) of Exercise 2.

5. Show that a subgroup $N$ of a finite group $G$ is neutral in $L(G)$ if and only if it is both join- and meet-quasi-distributive.

3.5 Finite groups with a partition

A partition of a group $G$ is a set $\Sigma$ of nontrivial subgroups of $G$ such that every nonidentity element of $G$ is contained in a unique subgroup $X \in \Sigma$. Equivalent to this condition clearly is that

1. $X \cap Y = 1$ for all $X, Y \in \Sigma$ such that $X \neq Y$, and

2. for every cyclic subgroup $C$ of $G$ there exists $Z \in \Sigma$ such that $C \leq Z$.

The elements of $\Sigma$ are termed components of the partition; $\Sigma$ is called nontrivial if $X \neq G$ for all $X \in \Sigma$. By 1.2.5, a subgroup $C$ of $G$ is cyclic if and only if $[C/1]$ is distributive and satisfies the maximal condition. Therefore (1) and (2) show that for a group $G$ to possess a nontrivial partition is a lattice-theoretic property. We give examples for partitions of finite groups.

3.5.1 Examples. Let $G$ be a finite group, $p$ a prime, $n \in \mathbb{N}$.

(a) If $1 < N < G$ such that every element in $G \setminus N$ has order $p$, then any partition of $N$ together with the set of cyclic subgroups of $G$ not contained in $N$ is a nontrivial partition of $G$.

(b) In particular, if $N$ is a nontrivial normal subgroup of index $p$ in $G$ such that every element in $G \setminus N$ has order $p$, then $N$ together with the set of cyclic subgroups of $G$ not contained in $N$ is a partition of $G$.

(c) A Frobenius group is a group $G$ containing a proper nontrivial subgroup $H$ such that $H \cap H^x = 1$ for all $x \in G \setminus H$. It is well-known (see Robinson [1982], pp. 243 and 299) that the set $N$ of all elements of $G$ not contained in the conjugates of $H$ together with 1 is a nilpotent normal subgroup of $G$. This is called the Frobenius kernel and $H$ a Frobenius complement. Clearly, $N$ together with the set of conjugates of $H$ is a nontrivial partition of $G$.

(d) If $G$ is the symmetric group on 4 letters, then the set $\Sigma$ of maximal cyclic subgroups of $G$ is a partition; for in any finite group this set satisfies (2). And if $X, Y \in \Sigma$ such that $X \neq Y$ and $X \cap Y \neq 1$, then, since every element in $S_4$ has order...
at most 4, it would follow that $|X| = |Y| = 4$ and $|X \cap Y| = 2$. But $S_4$ has only 3 cyclic subgroups of order 4 and any two of them intersect trivially. Thus (1) also holds and $\Sigma$ is a partition of $G$.

(e) Also for $G = PGL(2, p^n)$, the projective general linear group of dimension 2 over the field with $p^n$ elements, $p^n > 3$, the set of maximal cyclic subgroups is a partition. It consists of groups of order $p$, $p^n + 1$ and $p^n - 1$. The Sylow $p$-subgroups (of order $p^n$), together with these maximal cyclic subgroups of order $p^n + 1$ and $p^n - 1$, form another partition $\Sigma$ of $G$, and $\Sigma' = \{X \cap H | X \in \Sigma\}$ is a partition for the subgroup $H = PSL(2, p^n)$ of $G$ (see Huppert [1967], p. 193).

(f) There is another class of finite simple groups with a nontrivial partition, the Suzuki groups $Sz(q)$, $q = 2^{2n+1}$. This consists of the Sylow 2-subgroups and cyclic subgroups of order $q - 1$, $q + 2^{2n+1} + 1$ and $q - 2^{2n+1} + 1$ (see Huppert and Blackburn [1982b], p. 190).

Our aim in this section is to show that every finite group with a nontrivial partition is one of the examples given in 3.5.1. This was proved in 1961 for soluble groups by Baer and in the general case by Suzuki. The main problem in Suzuki's proof was to show that a finite nonsoluble group with a nontrivial partition has even order. We shall use the Feit-Thompson Theorem to achieve this, and then the classification of Zassenhaus groups to identify the group. In this section, all groups considered are finite.

Elementary results

A partition $\Sigma$ of $G$ is called normal if $X^g \in \Sigma$ for every $X \in \Sigma$ and $g \in G$. If $\Sigma$ and $\Delta$ are partitions of $G$, $1 \neq H \leq G$ and $g \in G$, then clearly

$$\Sigma_H := \{H \cap X | X \in \Sigma, H \cap X \neq 1\}$$

is a partition of $H$, and $\Sigma \cap \Delta := \{X \cap Y | X \in \Sigma, Y \in \Delta, X \cap Y \neq 1\}$ and $\Sigma^g := \{X^g | X \in \Sigma\}$ are partitions of $G$. Thus if $\Sigma$ is a nontrivial partition of $G$, then

$$\Sigma_G := \bigcap_{x \in G} \Sigma^x$$

is a nontrivial normal partition of $G$.

Therefore we may usually assume that the partitions we consider are normal. The following simple results will be used over and over again.

3.5.2 Lemma. Let $\Sigma$ be a partition of $G$ and let $a, b \in G$ such that $ab = ba$ and either

(i) $o(a) \neq o(b)$ or

(ii) $o(a) = o(b)$ is not a prime.

Then there exists a component $X$ of $\Sigma$ containing $a$ and $b$.

Proof. We may assume that $a \neq 1 \neq b$ and take $X, Y \in \Sigma$ such that $a \in X$ and $b \in Y$; we have to show that $X = Y$. Suppose first that (i) holds and take $Z \in \Sigma$ such that $ab \in Z$. Then $o(a) > o(b)$, say, and since $ab = ba$, $1 \neq a^{o(b)} = (ab)^{o(b)} \in X \cap Z$. By (1), $X = Z$. So $Z$ contains $a$ and $ab$ and therefore also $b$; thus $X = Z = Y$ as desired.
Now suppose that (ii) holds and take a prime \( p \) dividing \( o(a) \). Then \( p \neq o(a) \) and hence \( a^p \neq 1 \), \( a^p b = ba^p \) and \( o(a^p) \neq o(b) \). Thus (i) holds for \( a^p \) and \( b \) and, as we have just shown, this implies that \( a^p \) and \( b \) lie in the same component of \( \Sigma \). Since \( a^p \in X \), it follows from (1) that \( X = Y \).

The lemma shows that a finite abelian group has a nontrivial partition only if it is an elementary abelian \( p \)-group. More generally, if \( \Sigma \) is a partition of \( G \) and \( 1 \neq a \in X \) such that \( o(a) \) is not a prime, then every element \( b \in C_G(a) \) satisfies (i) or (ii) of 3.5.2 and hence \( C_G(a) \leq X \). In particular, we have the following.

3.5.3 Corollary. If \( \Sigma \) is a partition of \( G \) and \( H \) is a nilpotent subgroup of \( G \) that is not contained in a component of \( \Sigma \), then \( H \) is a \( p \)-group for some prime \( p \).

3.5.4 Lemma. Let \( \Sigma \) be a normal partition of \( G \) and let \( X \in \Sigma \). If \( 1 \neq H \leq X \), then \( N_G(H) \leq N_G(X) \). In particular, \( C_G(x) \leq N_G(X) \) for every \( 1 \neq x \in X \).

Proof. Let \( g \in N_G(H) \). Then \( 1 \neq H = H^g \leq X \cap X^g \) and \( X^g \in \Sigma \) since \( \Sigma \) is normal. By (1), \( X = X^g \) and hence \( g \in N_G(X) \). In particular, \( C_G(x) \leq N_G(\langle x \rangle ) \leq N_G(X) \) for \( 1 \neq x \in X \).

Admissible subgroups

Let \( \Sigma \) be a partition of \( G \). A subgroup \( H \) of \( G \) is called \( \Sigma \)-admissible if for every \( X \in \Sigma \), either \( X \leq H \) or \( X \cap H = 1 \). Clearly, every component of \( \Sigma \) is \( \Sigma \)-admissible. We want to show that every \( \Sigma \)-admissible subgroup of a finite group \( G \) is either self-normalizing or nilpotent. For this we consider the Hughes subgroup \( H_p(G) \) of \( G \) defined by

\[
(5) \quad H_p(G) = \langle x \in G | o(x) \neq p \rangle.
\]

Suppose that \( H_p(G) < G \). Then every element in \( G \setminus H_p(G) \) has order \( p \). So if \( a \in G \setminus H_p(G) \) and \( x \in H_p(G) \), then

\[
1 = (xa^{-1})^p = xx^a \ldots x^{ap-1} a^{-p} = xx^a \ldots x^{ap-1}.
\]

By a well-known theorem of Hughes, Kegel and Thompson (see Huppert [1967], p. 502), a finite group with such an automorphism is nilpotent. Thus

\[
(6) \quad H_p(G) \text{ is nilpotent if } H_p(G) < G.
\]

We shall also need the following result due to Hughes and Thompson [1959].

3.5.5 Lemma. If \( H_p(G) < G \) and \( G \) is not a \( p \)-group, then \( |G : H_p(G)| = p \).

Proof. We use induction on \( |G| \). Let \( H = H_p(G) \) and \( P \) be a Sylow \( p \)-subgroup of \( G \). Then \( G = HP \) and by (6), \( H = Q \times (H \cap P) \) where \( Q \neq 1 \) is a \( p \)-complement in \( G \). If \( x \in P \) and \( 1 \neq y \in C_Q(x) \), then \( o(xy) \neq p \) and hence \( xy \in H \); since also \( y \in H \), it fol-
Complements and special elements in the subgroup lattice of a group

allows that \( x \in H \cap P \). Thus if \( H \cap P = 1 \), then \( P \) operates fixed-point-freely on \( H \) and by a well-known theorem of Burnside (see Robinson [1982], p. 298), \( P \) is cyclic or generalized quaternion. Since every element in \( G \setminus H \) has order \( p \), it follows that \( |P| = p \) and \( |G : H| = p \). If \( H \cap P \neq 1 \), there exists a subgroup \( N \) of order \( p \) in \( H \cap Z(P) \). Clearly \( N \leq G \) and every element in \( G/N \) that is not contained in \( H/N \) has order \( p \). Thus \( H_p(G/N) \leq H/N \) and by induction, \( |G/N : H_p(G/N)| = p \). It follows that \( H_p(G/N) = H/N \) and \( |G : H| = p \).

It was conjectured, and then proved for \( p = 2 \) and \( 3 \), that \( |G : H_p(G)| \leq p \) if \( G \) is a \( p \)-group; however Wall [1965] gave a counterexample for \( p = 5 \). The reader can find further results on the Hughes subgroup and on partitions of \( p \)-groups in the book by Khukhro [1993]. In any case, Lemma 3.5.5 suffices to prove the result on admissible subgroups announced earlier.

\[\text{3.5.6 Lemma (Kegel [1961])}.\] If \( \Sigma \) is a partition and \( H \) a \( \Sigma \)-admissible subgroup of \( G \), then \( H = N_G(H) \) or \( H \) is nilpotent.

**Proof.** Suppose that \( H < N_G(H) \). Then there exists a subgroup \( M \) of \( N_G(H) \) such that \( |M : H| = p \) for some prime \( p \). Let \( x \in M \setminus H \) and take \( X \in \Sigma \) such that \( x \in X \). Since \( H \) is \( \Sigma \)-admissible, \( X \cap H = 1 \). As \( M = H \langle x \rangle \), it follows that \( \langle x \rangle \cong M/H \) and hence \( o(x) = p \). Thus \( H_p(M) \leq H \). If \( H \) is a \( p \)-group, it is nilpotent. And if \( H \) is not a \( p \)-group, then by 3.5.5, \( |M : H_p(M)| \leq p \). Thus \( H_p(M) = H \) and by (6), \( H \) is nilpotent.

In our first main result on a finite group with a partition we deal with the situation that \( G \) has a nontrivial admissible normal subgroup. This clearly holds in Examples 3.5.1, (b) and (c). The following theorem shows the converse.

\[\text{3.5.7 Theorem (Baer [1961a])}.\] Let \( G \) be a finite group with a normal partition \( \Sigma \) and suppose that \( N \) is a nontrivial proper \( \Sigma \)-admissible normal subgroup of \( G \). Then one of the following holds.

\begin{enumerate}
\item \( G \) is a Frobenius group, the Frobenius complements are components of \( \Sigma \) and \( N \) is contained in the Frobenius kernel of \( G \).
\item There exists a prime \( p \) such that all elements in \( G \setminus N \) have order \( p \), and if \( G \) is not a \( p \)-group, then \( N = H_p(G) \), \( |G : N| = p \) and \( N \) is a component of \( \Sigma \).
\end{enumerate}

**Proof.** Suppose first that there exists \( X \in \Sigma \) such that \( X \nsubseteq N \) and \( C_N(X) = X \). Then as \( N \) is \( \Sigma \)-admissible, \( N \cap X = 1 \) so that \( N \cap N_G(X) \) and \( N \) are normal subgroups of \( N_G(X) \) intersecting trivially. Therefore \( N \cap N_G(X) \leq C_N(X) = 1 \) and by Dedekind,

\[N_{nx}(X) = N \times C_N(X) = (N \cap N_G(X)) \times X = X.\]

Thus \( N \times X \) is a Frobenius group with complement \( X \) and kernel \( N \). It follows that \( N \times X \) is the set-theoretic union of \( N \) and all the \( X^g \) where \( g \in N \times X \), and hence is \( \Sigma \)-admissible since all these \( X^g \) are components of \( \Sigma \). Furthermore \( N \times X \) is not nilpotent and by 3.5.6, \( N_G(NX) = NX \). But as \( N \leq G \), \( N_G(X) \leq N_G(NX) \) and then (7) shows that \( N_G(X) = X \). Thus \( G \) is a Frobenius group with complement \( X \), \( N \) is
3.5 Finite groups with a partition

contained in the Frobenius kernel and (a) holds. So we may assume that

(8) \( C_N(X) \neq 1 \) for every \( X \in \Sigma \) such that \( X \not\leq N \)

and want to show that then (b) is satisfied. If \( 1 \neq a \in C_N(X) \) and \( 1 \neq b \in X \), then \( a \) and \( b \) lie in different components of \( \Sigma \). By 3.5.2, \( o(a) = o(b) \) is a prime \( p \) and every nontrivial element in \( C_N(X) \) and in \( X \) has order \( p \). In particular,

(9) \( p \) divides \( |N| \) and \( \text{Exp} \ X = p \).

It follows that every element in \( G \setminus N \) has prime order. Therefore (b) holds if \( G \) is a \( p \)-group and we may assume that \( G \) is not of prime power order. Then (9) shows that \( N \) too is not of prime power order. If \( p \) is a prime dividing \( |G : N| \) and \( P \) is a Sylow \( p \)-subgroup of \( G \), then \( |NP : N| \) is a power of \( p \) and hence every element in \( NP \setminus N \) has order \( p \). Thus \( H_p(NP) \leq N < NP \). By 3.5.5, \( |NP : H_p(NP)| = p \) and hence \( H_p(NP) = N \) and \( |NP : N| = p \). It follows that all Sylow subgroups of \( G/N \) are cyclic of prime order and by a well-known theorem of Zassenhaus (see Robinson [1982], p. 281), \( G/N \) is soluble. Hence there exists a normal subgroup \( M/N \) of \( G/N \) of prime index \( p \). Again every element of \( G \setminus M \) has order \( p \) and hence \( H_p(G) = M \) by 3.5.5. By (6), \( M \) is nilpotent and not of prime power order since \( N \leq M \). But then 3.5.3 shows that \( M \) is a component of \( \Sigma \) and the \( \Sigma \)-admissibility of \( N \) implies that \( M = N \). Thus (b) holds.

3.5.8 Remark. If \( p = 2 \) in (b) of Theorem 3.5.7, then \( G \) is either an elementary abelian 2-group or a generalized dihedral group, that is, \( N \) is abelian, \( G = N \langle t \rangle \) where \( o(t) = 2 \) and \( tat = a^{-1} \) for all \( a \in N \). For, if we take \( t \in G \setminus N \) and \( a \in N \), then \( at \notin N \) and hence \( t^2 = 1 \) and \( ata = a^{-1} \); it follows that \( tat = a^{-1} \) for all \( a \in N \) and this implies that \( N \) is abelian. If \( \text{Exp} \ N = 2 \), then every element in \( G \) has order at most 2 and \( G \) is elementary abelian. And if \( \text{Exp} \ N \neq 2 \), then \( t \notin C_G(N) \). Since \( t \) was arbitrary, it follows that \( C_G(N) = N \) and that the automorphism group induced by \( G \) in \( N \) has order 2. Thus \( |G : N| = 2 \) and \( G = N \langle t \rangle \) as desired.

A characterization of \( S_4 \)

In view of Theorem 3.5.7 we may assume in the remainder of this section that our groups do not possess admissible normal subgroups. We first establish the following nice characterization of the symmetric group on four letters.

3.5.9 Theorem (Baer [1961b]). Let \( \Sigma \) be a nontrivial normal partition of the finite group \( G \) and suppose that there is no nontrivial proper \( \Sigma \)-admissible normal subgroup of \( G \). If the Fitting subgroup \( F(G) \neq 1 \), then \( G \simeq S_4 \) and \( \Sigma \) consists of the maximal cyclic subgroups of \( G \).

Proof. Since \( F(G) \neq 1 \), there exists a prime \( p \) such that \( G \) contains a nontrivial normal elementary abelian \( p \)-subgroup \( P \). We shall show in a number of steps that \( p = 2 \) and \( |P| = 4 \) for any such \( P \); it will follow easily that \( G \simeq S_4 \). First of all,

(10) \( Z(G) = 1 \).
For, if $1 \neq z \in Z(G)$ and $Z \in \Sigma$ such that $z \in Z$, then $Z \leq G$ by 3.5.4. Since $\Sigma$ is nontrivial, $Z$ would be a proper nontrivial $\Sigma$-admissible normal subgroup of $G$, a contradiction. Similarly, if $P \leq X \in \Sigma$, then $X \leq G$ by 3.5.4, the same contradiction. Thus

(11) $P$ is not contained in a component of $\Sigma$.

But if $1 \neq c \in C_G(P)$ and $o(c) \neq p$, then by 3.5.2, $P \leq X$ where $X$ is the component of $\Sigma$ containing $c$. Thus (11) implies that

(12) $\text{Exp } C_G(P) = p$.

Let $X$ be a component of $\Sigma$. Suppose first that $P \cap X \neq 1$. Then by 3.5.4, $P \leq N_G(P \cap X) \leq N_G(X)$ so that $X \leq H = PX$. By (11), $X < H$ and hence 3.5.6 implies that $X$ is nilpotent. Thus $H = PX$ is the product of nilpotent normal subgroups and therefore, by Fitting's theorem, is nilpotent. Hence every $p'$-element of $H$ centralizes $P$ and (12) implies that $H$ is a $p$-group. Furthermore $X$ is a component of the normal partition $H \cap \Sigma$ of $H$ and Theorem 3.5.7 and Remark 3.5.8 yield the remainder of the following assertion.

(13) If $X \in \Sigma$ such that $P \cap X \neq 1$, then $PX$ is a $p$-group, $X < PX$ and every element in $PX \setminus X$ has order $p$; if $p = 2$, then $PX$ is elementary abelian or $|PX : X| = 2$.

Now suppose that $P \cap X = 1$ and that $p$ divides $|X|$. Let $S$ be a Sylow $p$-subgroup of $X$. Then $S \neq 1$ and since $P$ is a nontrivial normal subgroup of the $p$-group $PS$, there exists $t \in P \cap Z(PS)$ such that $o(t) = p$. By 3.5.4, $t \in C_G(S) \leq N_G(X)$ and hence $[t, X] \leq P \cap X = 1$. Since $t \notin X$, 3.5.2 shows that every nontrivial element in $X$ has order $p$. We have thus proved:

(14) If $X \in \Sigma$ such that $P \cap X = 1$ and $p$ divides $|X|$, then $\text{Exp } X = p$.

In particular, $X$ is a $p$-group, and (13) and (14) show that

(15) every component of $\Sigma$ is either a $p$-group or a $p'$-group.

We want to show next that $G$ contains elements of order $p^2$. So suppose that this is false. Then every nontrivial $p$-element of $G$ has order $p$ and by (15), the set $\Delta$ of subgroups of order $p$ of $G$ and of components of order prime to $p$ of $\Sigma$ is a nontrivial normal partition of $G$. Clearly, $P$ is a $\Delta$-admissible normal subgroup of $G$ and by (10), $G$ is not a $p$-group. It follows from 3.5.7, that either $G$ is a Frobenius group with complement $X \in \Delta$ and kernel $K$ containing $P$, or $P$ is a component of $\Delta$. In the first case, since $K$ as a Frobenius kernel is a normal Hall subgroup of $G$, $X$ is a $p'$-group and hence $X \in \Sigma$; this implies that $K$ is $\Sigma$-admissible, contradicting our assumption. In the second case, $|P| = p$ and hence $P$ is contained in a component of $\Sigma$, contradicting (11). This contradiction shows that

(16) $G$ contains elements of order $p^2$.

In the remainder of the proof let $x \in G$ be an element of order $p^2$, $X \in \Sigma$ such that $x \in X$ and $H = PX$. We want to study the automorphism $\sigma$ induced by $x$ in $P$ which is given by $a^x = x^{-1}ax$ for $a \in P$. By (14), $P \cap X \neq 1$ and (13) then yields that $X \leq H$. It follows that $[P, X] \leq P \cap X$. If $a, b \in P$, then since $P$ is abelian, by (1) of 1.5,
\[ [ab, x] = [a, x][b, x] \]

so that the map \( \alpha : P \to P \cap X \) defined by \( a^\alpha = [a, x] = a^{\sigma - 1} \) for \( a \in P \) is a homomorphism. If \( a \in \text{Ker} \alpha \), then \( ax = xa \) and by 3.5.2, \( a \in X \). Thus \( \text{Ker} \alpha \leq P \cap X \) and the homomorphism theorem yields that

\[ |P| = |P^\sigma||\text{Ker} \alpha| \leq |P \cap X|^2. \tag{17} \]

If \( P \cap X \leq G \), then by 3.5.4, \( X \leq G \), a contradiction. So there exists \( g \in G \) such that \( P \cap X \neq (P \cap X)^g = P \cap X^g \) and since \( X \) and \( X^g \) are components of \( \Sigma \), \( (P \cap X) \cap (P \cap X)^g = \{1\} \). But as \( P \leq G \), \( (P \cap X)(P \cap X)^g \leq P \) and hence \( |P| \geq |P \cap X|^2 \). Thus

\[ |P| = |P \cap X|^2 \tag{18} \]

and since \( P^\sigma \) and \( \text{Ker} \alpha \) are contained in \( P \cap X \), it also follows from (17) that \( P^\sigma = P \cap X = \text{Ker} \alpha \). Hence \( a^{\sigma^2} = 1 \) for all \( a \in P \), that is \( (\sigma - 1)^2 = 0 \) in the endomorphism ring of \( P \). On the other hand, by (11) there exists \( a \in P \) such that \( a \notin X \).

Then \( ax^{-1} \in H \setminus X \) so that \( o(ax^{-1}) = p \) by (13). It follows that

\[ 1 = (ax^{-1})^p = aax \ldots a^{x^{p-1}}x^{-p} = a^{1+\sigma+\cdots+\sigma^{p-1}}x^{-p}. \]

Since \( x^{-p} \neq 1 \), we have \( a^{1+\sigma+\cdots+\sigma^{p-1}} \neq 1 \) and hence \( \sum_{i=0}^{p-1} \sigma^i \neq 0 \). In the polynomial ring \( GF(p)[z] \), the identity \( (z - 1)^p = z^p - 1 = (z - 1)\sum_{i=0}^{p-1} z^i \) implies that \( (z - 1)^{p-1} = \sum_{i=0}^{p-1} z^i \). Now there is an obvious ring epimorphism from \( GF(p)[z] \) to the commutative subring of \( \text{End} \ P \) generated by 1 and \( \sigma \) in which \( z \) maps to \( \sigma \); hence \( (\sigma - 1)^{p-1} = \sum_{i=0}^{p-1} \sigma^i \). Thus \( (\sigma - 1)^{p-1} \neq 0 \) and, because \( (\sigma - 1)^2 = 0 \), it follows that \( p = 2 \). Since \( o(x) = 4 \), \( X \) is not elementary abelian and by (13), \( |P : P \cap X| = |PX : X| = 2 \). On the other hand, (18) shows that \( |P : P \cap X| = |P \cap X| \). It follows that \( |P \cap X| = 2 \) and

\[ |P| = 4. \tag{19} \]

By (12), \( C_G(P) \) has exponent 2 and therefore is an elementary abelian normal 2-subgroup of \( G \). So we may apply our result (19) to \( C_G(P) \) instead of \( P \), obtaining \( |C_G(P)| = 4 \). Hence

\[ 20) \quad P = C_G(P) \]

and \( G/P \) is isomorphic to a subgroup of \( \text{Aut} \ P \cong S_3 \). Since \( G \) has elements of order 4, \( |G/P| \) is even and since \( Z(G) = 1 \), \( G \) is not a 2-group. Thus \( G/P \cong S_3 \) and \( |G| = 24 \). Let \( Y \) be a component of \( \Sigma \) containing an element of order 3; by (15), \( |Y| = 3 \). Hence \( G \) does not contain elements of order 6 and it follows that \( Y = C_G(Y) \). If \( Y = N_G(Y) \), then \( G \) is a Frobenius group and its Frobenius kernel is a \( \Sigma \)-admissible normal subgroup of \( G \), a contradiction. Thus \( |N_G(Y)| = 6 \) and since \( G \) operates faithfully on the set of its Sylow 3-subgroups, \( G \cong S_4 \). By (15) and (11), all cyclic subgroups of order 3 and 4 of \( G \) belong to \( \Sigma \) and a noncyclic component \( W \) of \( \Sigma \) has
Complements and special elements in the subgroup lattice of a group

to be elementary abelian of order 4. But since the Sylow 2-subgroups of \( G \) are dihedral, there would exist a cyclic subgroup of order 4 intersecting \( W \) nontrivially, a contradiction. Thus \( \Sigma \) consists of the maximal cyclic subgroups of \( G \).

The main theorem

We collect the results proved so far to give the structure of a finite soluble group with a partition.

3.5.10 Theorem (Baer). Let \( \Sigma \) be a nontrivial partition of the finite soluble group \( G \). Then one of the following holds.

(a) \( G \) is a \( p \)-group for some prime \( p \) and \( \Sigma \) contains a component \( X \) such that every element in \( G \backslash X \) has order \( p \); furthermore \( |\Sigma| \equiv 1 \pmod{p} \).

(b) \( G \) possesses a nilpotent normal subgroup \( N \) such that \( N \in \Sigma \), \( |G : N| \) is a prime \( p \) and every element in \( G \backslash N \) has order \( p \).

(c) \( G \) is a Frobenius group.

(d) \( G \simeq S_4 \).

Proof. First suppose that \( G \) is a \( p \)-group. If \( 1 \neq x \in Z(G) \) and \( X \in \Sigma \) such that \( x \in X \), then by 3.5.2, \( X \) contains every element of order different from \( p \) in \( G \); thus \( o(g) = p \) for all \( g \in G \backslash X \). Every subgroup of order \( p \) of \( G \) is contained in a unique component of \( \Sigma \). Since \( k(G) \equiv 1 \pmod{p} \) if \( k(G) \) is the number of subgroups of order \( p \) in \( G \) (see Huppert [1967], p. 33), it follows that \( 1 \equiv k(G) = \sum_{X \in \Sigma} k(X) \equiv |\Sigma| \pmod{p} \).

Now suppose that \( G \) is not a \( p \)-group. By (4), \( \Sigma_G \) is a nontrivial normal partition of \( G \). Therefore 3.5.7 and 3.5.9 show that (c) or (d) is satisfied or there is a prime \( p \) such that \( N = H_p(G) \in \Sigma_G \) and \( |G : N| = p \). Since every component of \( \Sigma_G \) is contained in a component of \( \Sigma \), \( N \in \Sigma \) in this case. By (6), \( N \) is nilpotent and (b) holds.

Note that there are nonnormal partitions of \( S_4 \) and of many Frobenius groups. Finally we determine the nonsoluble groups with a partition.

3.5.11 Theorem (Suzuki [1961]). Let \( G \) be a nonsoluble finite group with a nontrivial partition. Then one of the following holds.

(a) \( G \) is a Frobenius group.

(b) \( G \simeq PGL(2, q) \), \( q \) a prime power, \( q \geq 4 \).

(c) \( G \simeq PSL(2, q) \), \( q \) a prime power, \( q \geq 4 \).

(d) \( G \simeq Sz(q) \), \( q = 2^{2n+1} \), \( n \in \mathbb{N} \).

Proof. We cannot give a complete proof of this beautiful theorem here since some classification theorems are required to identify the groups. As a matter of fact, Suzuki's theorem is a consequence of the classification of finite simple groups; however, a proof using this result might not be appropriate. We decided to use the Feit-Thompson Theorem on the solubility of groups of odd order, the classification
of Zassenhaus groups (a complete proof of which can be found in Huppert and Blackburn [1982b], pp. 160–286) and elementary parts of Bender's classification of groups with a strongly embedded subgroup and of the Brauer-Suzuki-Wall Theorem (both to be found in Suzuki [1986], pp. 391–404 and 494–504, respectively). Thus by consulting these books, the reader can find a complete proof of Theorem 3.5.11 modulo the Feit-Thompson Theorem; this is avoided in the original paper of Suzuki by the use of the theory of exceptional characters to prove that the order of the group is even.

So let $G$ be a finite nonsoluble group with a nontrivial partition $\Sigma$. By (4), we may assume that $\Sigma$ is normal and we may clearly also assume that $G$ is not a Frobenius group. It follows that for every $X \in \Sigma$,

(21) $X < N_G(X)$ and $X$ is nilpotent

by 3.5.6. Furthermore, 3.5.7 and the nilpotency of $H_p(G)$ imply that there is no nontrivial proper $\Sigma$-admissible normal subgroup of $G$. By 3.5.9,

(22) $F(G) = 1$.

Let $S$ be a Sylow 2-subgroup of $G$; the Feit-Thompson Theorem implies that $S \neq 1$. We divide the remainder of the proof into four parts.

(I) If there exists a component $X \in \Sigma$ such that $S \leq X$, then $G$ is isomorphic to $\text{PSL}(2, 2^n)$ or $\text{Sz}(2^n)$ for some $n \in \mathbb{N}$.

Proof. Recall that a subgroup $H$ of $G$ is called strongly embedded in $G$ if $H < G$, $|H|$ is even and $|H \cap H^g|$ is odd for every $g \in G \setminus H$. Now if $H = N_G(S)$, then $H < G$ by (22), and clearly $|H|$ is even. By 3.5.4, $N_G(S) \leq N_G(X)$ and since $X$ is nilpotent, $N_G(X) \leq N_G(S)$. So if $g \in G \setminus H$, then $X^g \neq X$ so that $S \cap S^g \leq X \cap X^g = 1$. But the Sylow 2-subgroup of $H \cap H^g$ is contained in $S \cap S^g$ and hence is trivial. Thus $|H \cap H^g|$ is odd and

(23) $H = N_G(S) = N_G(X)$ is strongly embedded in $G$.

If $S$ were cyclic or generalized quaternion, then $H$ would centralize the involution in $S$ and since $S \leq X < H$, 3.5.2 would imply that every element in $H \setminus X$ would be contained in $X$; this is impossible. Thus $S$ is not cyclic or generalized quaternion and it follows (see Suzuki [1986], p. 396) that the action of $G$ on the cosets of $H$ is doubly transitive and that a maximal $p$-subgroup $P$ of $H$, $p$ an odd prime, stabilizing three points is contained in a conjugate $L$ of $H$ for which $|N_L(P)|$ is even. We want to show that $P = 1$; then the stabilizer of three points will be trivial and since, by (22), $G$ has no regular normal subgroup, $G$ will be a Zassenhaus group.

So suppose that $P \neq 1$ and that $T$ is a nontrivial 2-subgroup of $N_L(P)$; let $L = H^u$ where $u \in G$. Since $P$ is contained in three different conjugates of $H$, we may assume that $H^u \neq H$; let $D = H \cap H^u$. Then $T \leq S^u \leq H^u$ and hence $[T,P] \leq S^u \cap P = 1$. Since $T \leq S^u \leq X^u$, it follows from 3.5.2 that $P \leq X^u$. By (23), $X \neq X^u$ and therefore $P \cap X = 1$. Thus $p$ divides $|X|$ and $|H : X|$. Clearly, $X$ is an $(H \cap \Sigma)$-admissible proper normal subgroup of $H$. If $H$ were a Frobenius group containing $X$ in its kernel $K$, then $2p$ would divide $|K|$ and since $K$ is nilpotent, $K \leq X$ by 3.5.3. Thus $K = X$ and
this would contradict the fact that a Frobenius kernel is a normal Hall subgroup. Therefore 3.5.7 shows that $|H : X| = p$. Since $P \cap X = 1$, $|P| = p$ and $H = PX$. It follows that $D = H \cap H^u = P(X \cap H^u)$ and $|X \cap H^u|$ divides $|H^u : X^u| = p$. We may assume that $u$ is an involution (see Suzuki [1986], p. 395). Then $P^u \leq (H \cap H^u)^u = H \cap H^u$ and $P \neq P^u$ since otherwise $P \leq X \cap X^u = 1$. Thus

$$D = H \cap H^u = PP^u$$

is elementary abelian of order $p^2$ and the involution $u$ interchanges the subgroups $P$ and $P^u$. It follows that $D = A \times B$ where $|A| = |B| = p$, $A$ is centralized and $B$ is inverted by $u$. Let $Y$ be the component of $\Sigma$ containing $B$. Then $D < Y$ and so 3.5.7 shows that either $N_G(Y)$ is a Frobenius group containing $Y$ in its kernel or there exists a prime $q$ such that $|N_G(Y) : Y| = q$. In the first case, the Frobenius kernel is a nilpotent normal Hall subgroup of $N_G(Y)$ and therefore contains $D$ and does not contain $u$; this contradicts the fact that $A$ is centralized by $u$. In the second case, again $u \notin Y$ since $Y$ is nilpotent and contains $B$. Hence $q = 2$ and $D = PP^u \leq Y$. Since $P \leq X^u$ and $P^u \leq X$, it follows that $X \cap Y \neq 1 \neq X^u \cap Y$ and hence $X = Y = X^u$. This contradiction shows that $P = 1$ and that $G$ is a Zassenhaus group of degree $|G : H| \equiv 1 \pmod 2$. It follows (see Huppert and Blackburn [1982b], p. 286) that $G \cong PSL(2, 2^n)$ or $G \cong Sz(2^n)$ for some $n \in \mathbb{N}$.

(II) If $C_G(x)$ is nilpotent for every involution $x \in Z(S)$, then either

(a) $G$ is isomorphic to $PSL(2, 2^n)$ or $Sz(2^n)$ for some $n \in \mathbb{N}$, or

(b) $S$ is dihedral of order at least 8 and if $Z(S) = \langle x \rangle$ and $X \in \Sigma$ is the component containing $x$, then $S = C_G(x) = N_G(X) = X\langle t \rangle$ where $o(t) = 2$ and $tat = a^{-1}$ for all $a \in X$.

Proof. Let $x \in Z(S)$ be an involution and let $X \in \Sigma$ such that $x \in X$. If $C_G(x)$ is not a 2-group, then by 3.5.3, $C_G(x) \leq X$; it follows that $S \leq X$ and by (I), (a) holds. So we may assume that

$$C_G(x) = S$$

for every involution $x \in Z(S)$. Since $X$ is nilpotent, its 2'-component centralizes $x$ and hence is trivial; thus $X$ is a 2-group. By 3.5.4, $S = C_G(x) \leq N_G(X)$ and hence $XS$ is a 2-group. It follows that $XS \leq S$ and therefore

$$(26) \ X \leq S.$$ 

If $X = S$, we are done by (I); so we may assume that $X < S$. Then $X$ is a proper $(S \cap \Sigma)$-admissible normal subgroup of $S$ and by 3.5.7 and 3.5.8, either $S$ is elementary abelian or

$$(27) \ S = X\langle t \rangle$$

where $X$ is abelian, $\text{Exp} \ X \geq 4$, $o(t) = 2$ and $tat = a^{-1}$ for every $a \in X$.

If $S$ is elementary abelian, (25) and (26) show that $X \leq S = C_G(x)$ for every $1 \neq x \in S$ and this implies that $S \cap S^g = 1$ for all $g \in G \setminus N_G(S)$. Therefore the conjugates of $S$ together with the 2'-subgroups in $\Sigma$ form a nontrivial normal partition of $G$ which satisfies the assumptions of (I), and again (a) is satisfied. So we may assume that (27) holds.
Then $Z(S) = \Omega(X)$ and every element of $S \setminus X$ is an involution. If none of these is conjugate to an element of $X$, then they all operate as odd permutations on the set of cosets of $X$ in $G$ (see Suzuki [1986], p. 128). It follows that $G$ has a normal subgroup $N$ of index 2 such that $N \cap S = X$. Then $N \cap \Sigma$ is a normal partition of $N$ having a Sylow 2-subgroup $X$ of $N$ as a component. By (I), $N \cong PSL(2, 2^n)$ or $N \cong Sz(2^n)$ for some $n \in \mathbb{N}$. Since $X$ is abelian, $N \cong PSL(2, 2^n)$ and then $X$ is elementary abelian, contradicting (27).

Thus there exist $s \in S \setminus X$ and $g \in G$ such that $s^g \in X$. Then $s \in \Omega(X^g) = Z(S^g)$ and therefore $\Omega(X) = Z(S) \leq C_G(s) = S^g$ by (25). Since $|S^g : X^g| = 2$ and $\Omega(X) \cap X^g = 1, |\Omega(X)| = 2$. Hence $X$ is cyclic, $S$ is dihedral and $N_G(X) \leq C_G(x) = S$; thus (b) holds.

(III) If there exists an involution $x \in Z(S)$ such that $H = C_G(x)$ is not nilpotent, then $S$ is a dihedral group and if $X \in \Sigma$ is the component containing $x$, then $H = C_G(x) = N_G(X) = X \langle t \rangle$ where $X$ is abelian, $o(t) = 2$ and $tat = a^{-1}$ for all $a \in X$.

Proof. First let $x$ be any involution in $S$ such that $C_G(x)$ is not nilpotent, let $X \in \Sigma$ be the component containing $x$ and put $H = N_G(X)$; by 3.5.4, $C_G(x) \leq H$. Again (21) shows that $X$ is a proper $(H \cap \Sigma)$-admissible normal subgroup of $H$ and by 3.5.7, either $C_G(x) \leq K$, a contradiction since $K$ is nilpotent. Thus the second alternative holds. Since $X$ is nilpotent, $C_G(x) \notin X$ and for $z \in C_G(x) \setminus X$, also $xz \notin X$ so that $1 = (xz)^p = x^p z^p = x^p$. Thus $p = 2$ and 3.5.8 shows that

(28) $H = X \langle t \rangle$ where $X$ is abelian, $o(t) = 2$ and $tat = a^{-1}$ for all $a \in X;

in particular, $H = C_G(x)$. We now choose an involution $x \in Z(S)$ such that $C_G(x)$ is not nilpotent. Then $S \leq H = X \langle t \rangle$ and we have to show that $X \cap S$ is cyclic; then $S = (X \cap S) \langle t \rangle$, say, will be a dihedral group.

Since $H$ is not nilpotent, $X$ is not a 2-group and $Z(H) = \Omega(X \cap S)$. Let $Z = Z(H)$ and suppose for a contradiction that $|Z| \geq 4$; let $y \in Z$ such that $1 \neq y \neq x$ and take $g \in G \setminus H$. If $x^u \in Z$ for some $u \in G$, then $x^u \in X \cap X^u$ and hence $X = X^u$; it follows that $u \in N_G(X) = C_G(x)$ and $x^u = x$. This shows that $x$ is not conjugate to $y$ and to $y^g$. Therefore $\langle x, y^g \rangle$ is a dihedral group of order divisible by 4 and there exists an involution $z \in \langle x, y^g \rangle$ that centralizes $x$ and $y^g$. Thus $z \in C_G(x) = H$ and $z \in C_G(y^g) = H^g$ and hence $\langle Z, Z^g \rangle \leq C_G(z)$. If $C_G(z)$ is nilpotent, then $Z$ and $Z^g$ are contained in the Sylow 2-subgroup of $C_G(z)$ and hence in a Sylow 2-subgroup $S^e$ of $G$. Since $(X \cap S)^e$ is a normal subgroup of index 2 in $S^e$ and $|Z| \geq 4$, $Z \cap X^v \neq 1 \neq Z^g \cap X^v$. It follows that $X = X^v = X^g$, a contradiction since $g \notin H$. If $C_G(z)$ is not nilpotent and $W \in \Sigma$ such that $z \in W$, then by (28), $W \leq C_G(z)$ of index 2. It follows that $W \cap Z \neq 1 \neq W \cap Z^g$ and $X = W \in X^g$, the same contradiction as before. Thus $|Z| = 2$, $X \cap S$ is cyclic and $S$ is a dihedral group.

(IV) $G$ is isomorphic to $PGL(2, q)$, $PSL(2, q)$ or $Sz(q)$ for some prime power $q$.

Proof. Suppose first that $G$ has no normal subgroup of index 2. Then by (II) and (III), either $G$ is isomorphic to $PSL(2, 2^n)$ or $Sz(2^n)$ for some $n \in \mathbb{N}$, or an involu-
Complements and special elements in the subgroup lattice of a group

tion \(x \in Z(S)\) and its centralizer satisfy the assumptions of the essential part of the Brauer-Suzuki-Wall Theorem (see Suzuki [1986], p. 497). It follows that \(G\) is a Zassenhaus group of degree \(q + 1\) and order \((q + 1)q(q - 1)/2\) for some prime power \(q\). This implies (see Huppert and Blackburn [1982b], p. 286) that \(G \cong PSL(2, q)\).

In general, let \(N\) denote the smallest normal subgroup of \(G\) such that \(|G : N|\) is a power of 2 and suppose that \(N \neq G\). Then \(N\) is a nonsoluble group with a nontrivial normal partition \(N \cap \Sigma\). Clearly, \(N\) has no normal subgroup of index 2 and \(F(N) = 1\) so that \(N\) is not a Frobenius group. Thus \(N \cong PSL(2, q)\) or \(N \cong Sz(q)\) for some prime power \(q\), as we have just shown. By (II) and (III), the Sylow 2-subgroup \(S\) of \(G\) is dihedral and \(N \cap S\) is a proper noncyclic normal subgroup of \(S\). Therefore \(N \cap S\) is a dihedral group and \(|S : N \cap S| = 2\). Thus \(|G : N| = 2\), \(N \cong PSL(2, q)\) and \(G\) is isomorphic to a subgroup of \(\text{Aut } N \cong PGL(2, q)\). Since \(G\) has dihedral Sylow 2-subgroups, it follows that \(G \cong PGL(2, q)\) (see Suzuki [1986], pp. 507–510). This completes the proof of Theorem 3.5.11.

3.5.12 Corollary. The only finite simple groups with a nontrivial partition are the groups \(PSL(2, p^n)\), \(p^n > 3\), and \(Sz(2^{2n+1})\), \(n \in \mathbb{N}\).

Exercises

1. (Baer [1961a]) Show that a partition is trivial if it consists of the conjugates of one subgroup.
2. Show that a \(p\)-group has a nontrivial partition if and only if it has order at least \(p^2\) and is not generated by its elements of order different from \(p\).
3. Show that a 2-group has a nontrivial partition if and only if it is a generalized dihedral group of order at least 4.
4. Determine all partitions of \(S_4\).
5. Let \(G\) be a \(P\)-group of order \(p^2q\), with \(p\) and \(q\) primes, \(p > q\). Find a nonnormal partition of \(G\). (Note that \(G\) is a Frobenius group.)
6. Show that any of the groups \(PGL(2, p^n)\), \(PSL(2, p^n)\) and \(Sz(2^n)\), where \(p^n > 3\) for the linear groups, is determined by its subgroup lattice.
In this chapter we investigate the influence of the subgroup lattice on the arithmetic structure of a finite group $G$. By this we understand first of all the order of $G$, the number, structure and embedding of Sylow subgroups, and the number of Hall subgroups or, more generally, of subgroups of any given order in $G$.

Finite groups with proper normal Hall subgroups occur in abundance. For example, every Sylow subgroup that is not self-normalizing is a proper normal Hall subgroup in its normalizer. Therefore in §4.1 we describe the subgroup lattice of a finite group $G$ with a normal Hall subgroup $N$ in terms of $L(N)$, $L(G/N)$ and conjugation by elements of $N$. This description is used to construct projectivities between finite groups with isomorphic normal Hall subgroups that will be used quite often.

A projectivity $\varphi$ from $G$ to $\bar{G}$ is called index preserving if it satisfies $|H^\varphi : K^\varphi| = |H : K|$ for all subgroups $K < H$ of $G$. It is easy to see that if $\varphi$ is not index preserving, then there exist a prime $p$ and a Sylow $p$-subgroup $P$ of $G$ such that $|P^\varphi| \neq |P|$. By 2.2.6, $P$ then is cyclic or elementary abelian and we show in §4.2 that $G$ either is a direct product of a $P$-group with a group of coprime order ($P$-decomposable) such that $P$ is contained in the $P$-group, or has a normal $p$-complement $N$ such that $N^\varphi$ is a normal and, most often, a Hall subgroup of $G$. This result was proved by Suzuki in 1951 and is one of the fundamental theorems on subgroup lattices of groups. First of all, it shows that many groups only possess index preserving projectivities. And secondly, it reduces most problems on projectivities of finite groups to index preserving ones since, using the results of §4.1, it is usually not difficult to handle the exceptional situations described above.

Many characteristic subgroups of finite groups can be defined by arithmetic conditions. We show in §4.3 that a projectivity between $P$-indecomposable groups $G$ and $\bar{G}$ maps the maximal normal $p$-subgroup $O_p(G)$ to $O_q(\bar{G})$ for some prime $q$ and hence the Fitting subgroup $F(G)$ to $F(\bar{G})$. This, of course, is not true for $P$-groups; however, for $k \geq 2$, $F_k(G)^\varphi = F_k(\bar{G})$ for every projectivity $\varphi$ between arbitrary finite groups $G$ and $\bar{G}$. The corresponding result for the iterated nilpotent residuals is also true, but we will not be able to prove this until §5.4. The theorem on the Fitting groups is due to Schmidt [1972b]; as a consequence we get the fact, proved independently in 1951 by Suzuki and Zappa, that projective images of finite soluble groups are soluble. We shall give other proofs of this theorem in Chapter 5. Finally we show that index preserving projectivities map the hypercentre of $G$ to that of $\bar{G}$.

In §4.4 we study images of abelian Sylow $p$-subgroups under projectivities and prove two theorems due to Menegazzo [1974] on the image of the centre of a Sylow $p$-subgroup $P$ under an index preserving projectivity $\varphi$ of a finite group $G$ generated
Projectivities and arithmetic structure of finite groups

by $p'$-elements where $p > 2$: If $G$ is $p$-normal, then $Z(P)^p \leq Z(P^p)$; if $G$ is $p$-soluble, then $Z(P)^p = Z(P^p)$. These are the only general results that are known about the projectivities induced in the Sylow subgroups of a finite group.

4.1 Normal Hall subgroups

In this section we study the subgroup lattice of a finite group $G$ with a normal Hall subgroup $N$. Basic for this is the Schur-Zassenhaus Theorem which asserts that $N$ has a complement $H$ in $G$ and that all the complements of $N$ in $G$ are conjugate under $N$. To prove this last assertion the Feit-Thompson Theorem on the solubility of groups of odd order is necessary. This can be avoided if one assumes that $N$ or $G/N$ is soluble. This will always be the case in our applications of the results of this section. Therefore, for these applications, the Feit-Thompson Theorem is not needed. However, we state our results without the assumption that $N$ or $G/N$ is soluble, that is we freely use the Feit-Thompson Theorem in this section.

Normalizers, centralizers and commutator subgroups

We want to describe group-theoretic concepts in the subgroup lattice of $G$ and we start with the core $H_G = \bigcap_{x \in G} H^x$ and the normal closure $H^G = \bigcup_{x \in G} H^x$ of a complement $H$ to $N$ in $G$. For this we do not need that $(|N|, |H|) = 1$.

4.1.1 Lemma. Let $N \leq G$ and $H \leq G$ such that $G = NH$ and $N \cap H = 1$.

(a) If $H_1, H_2 < H$ and $x \in N$ such that $H_1 \leq H_2$, then $H_1 \leq H_2$ and $x \in C_N(H_1)$.

(b) For $x \in N$, $H \cap H^x = C_H(x)$ and $H \cup H^x = [x, H]H$.


Proof. (a) Let $a \in H_1$. Then $a^x \in H_2$ and hence $[a, x] = a^{-1}a^x \in H \cap N = 1$ since $x \in N \leq G$. It follows that $x \in C_H(H_1)$ and $H_1 = H_1^x \leq H_2$.

(b) Clearly, $C_H(x) = C_H(a^x) \leq H \cap H^x$. Conversely, $(H \cap H^x)^{x^{-1}} \leq H$ and hence (a) yields that $x \in C_H(H \cap H^x)$, that is, $H \cap H^x \leq C_H(x)$. This proves the first assertion. By (6) of § 1.5, $H$ normalizes $[x, H]$ so that $[x, H]H$ is a subgroup of $G$ containing $H$. The trivial identities $[x, a^{-1}]a = a^x$ and $[x, a] = (a^{-1})^xa$ show that $[x, H]H$ also contains $H^x$ and that $[x, H] \leq H \cup H^x$. Thus $[x, H]H = H \cup H^x$ and (b) holds.

(c) Now (b) and $G = HN$ yield that $H_G = \bigcap_{x \in G} H^x = \bigcap_{x \in N} H^x = \bigcap_{x \in N} C_H(x) = C_H(N)$ and, similarly, $H^G = \bigcup_{x \in N} [x, H]H = [N, H]H$. By Dedekind, $H^G \cap N = [N, H](H \cap N) = [N, H]$.

4.1.2 Theorem. Let $G$ be a finite group, $N$ a normal Hall subgroup and $H$ a complement to $N$ in $G$. Suppose that $\varphi$ is a projectivity from $G$ to a group $\overline{G}$ such that $N^\varphi$ is a normal Hall subgroup of $\overline{G}$. Then for all $N_1 \leq N$ and $H_1 \leq H$,
4.1 Normal Hall subgroups

(a) \( H_1 \leq N_G(N_1) \) if and only if \( H_1^\circ \leq N_G(N_1^\circ) \).

(b) \( C_N(H_1)^\circ = C_{N^\circ}(H_1^\circ) \) and \( C_H(N_1)^\circ = C_{H^\circ}(N_1^\circ) \).

(c) \( |N : C_N(H_1)| = |N^\circ : C_{N^\circ}(H_1^\circ)| \).

(d) \( [N_1, H_1]^\circ = [N_1^\circ, H_1^\circ] \) if \( H_1 \leq N_G(N_1) \).

Proof. (a) If \( H_1 \leq N_G(N_1) \), then \( N_1 H_1 \) is a subgroup of \( G \) and \( N_1 H_1 \cap N = N_1 \); conversely, if \( N_1 = (N_1 \cup H_1) \cap N \) then \( N_1 \triangleleft N_1 \cup H_1 \) since \( N \triangleleft G \). Thus \( H_1 \leq N_G(N_1) \) if and only if \( N_1 = (N_1 \cup H_1) \cap N \). This is equivalent to \( N_1^\circ = (N_1^\circ \cup H_1^\circ) \cap N^\circ \) and hence to \( H_1^\circ \leq N_G(N_1^\circ) \).

(b) By 1.6.7, \( H_1^\circ \) is centralized by \( C_N(H_1)^\circ \), that is, \( C_N(H_1)^\circ \leq C_{N^\circ}(H_1^\circ) \). The corresponding assertion for \( \varphi^{-1} \) yields the other inclusion. Similarly, \( C_H(N_1)^\circ = C_{H^\circ}(N_1^\circ) \).

(c) By the Schur-Zassenhaus Theorem, \( |N : C_N(H_1)| = |N : C_N(H_1)| \) is the number of complements to \( N \) in \( N H_1 \). This implies (c).

(d) Since \( H_1 \leq N_G(N_1) \), \( N_1 \) is a normal Hall subgroup of \( N_1 H_1 \) and by (a), \( N_1^\circ \) is a normal Hall subgroup of \( N_1^\circ H_1^\circ \). By (c) of 4.1.1 and the Schur-Zassenhaus Theorem, \( [N_1, H_1] \) is the intersection of \( N_1 \) with the join of the complements to \( N_1 \) in \( N_1 H_1 \), and is therefore mapped by \( \varphi \) to the intersection of \( N_1^\circ \) with the join of the complements to \( N_1^\circ \) in \( N_1^\circ H_1^\circ \), that is, to \([N_1^\circ, H_1^\circ]\). \(\square\)

The subgroup lattice of a finite group with a normal Hall subgroup

To construct the subgroup lattice, we need some further properties of a group with a normal Hall subgroup.

4.1.3 Lemma. Let \( N \) be a normal Hall subgroup and \( H \) a complement to \( N \) in \( G \).

(a) For every \( U \leq G \) satisfying \(|U|, |N| = 1\), there exists \( x \in N \) such that \( U^x \leq H \).

(b) \( N = [N, H] C_N(H) \) and \( [N, H, H] = [N, H] \).

(c) If \( N \) is abelian, then \( N = [N, H] \times C_N(H) \).

(d) For every prime \( p \), there exists an \( H \)-invariant Sylow \( p \)-subgroup of \( N \).

Proof. (a) Since \( NU = N(NU \cap H) \), \( U \) and \( NU \cap H \) are complements to \( N \) in \( NU \). By the Schur-Zassenhaus Theorem there exists \( x \in N \) such that \( U^x = NU \cap H \leq H \).

(b) By 4.1.1, \([N, H] \) is a normal Hall subgroup in \( H^G = [N, H] H \). For \( x \in N \), \( H \) and \( H^x \) are complements to \( [N, H] \) in \( H^G \) and hence there exists \( y \in [N, H] \) such that \( H^x = H^y \). Then \( x = (xy^{-1})y \in N_H(N)[N, H] \) and, since \( x \) was arbitrary, \( N = [N, H]N_H(N) = [N, H]C_N(H) \). Furthermore, again by 4.1.1,

\[ [N, H, H]H = \bigcup_{x \in [N, H]} H^x = \bigcup_{x \in N} H^x = [N, H]H \]

and hence \([N, H, H] = [N, H] \).

(c) By (b), we only have to show that \([N, H] \cap C_N(H) = 1\). For this we study the endomorphism \( \tau \) of \( N \) defined by \( x^\tau = \prod_{k \in H} x^k \) for \( x \in N \). If \( a \in H \) and \( x \in N \), then \((x^a)^\tau = \prod_{k \in H} x^{ka} = \prod_{b \in H} x^b = x^\tau \) and hence \([x, a]^\tau = (x^{-1})^\tau(x^a)^\tau = (x^\tau)^{-1}x^\tau = 1\). Since \([N, H] \) is generated by these \([x, a] \) and \( \tau \) is a homomorphism, \( y^\tau = 1 \) for all
Projectivities and arithmetic structure of finite groups

Let $x \in [N, H]$. So if $x \in [N, H] \cap C_N(H)$, then $1 = x^r = x^{[H]}$ and $x = 1$ since $(o(x), |H|) = 1$. Thus $[N, H] \cap C_N(H) = 1$ and (c) holds.

(d) Let $P \in \text{Syl}_p(N)$. By the Frattini argument, $G = N_G(P)N$ and hence $N \cap N_G(P)$ is a normal Hall subgroup of $N_G(P)$ having a complement $K$ isomorphic to $H$. By (a) there exists $x \in N$ such that $K^x \leq H$ and it follows that $H = K^x \leq N_G(P^x) = N_G(P^x)$. Thus $P^x$ is an $H$-invariant Sylow $p$-subgroup of $N$.

4.1.4 Theorem (Paulsen [1975]). Let $G$ be a finite group, $N$ a normal Hall subgroup and $H$ a complement to $N$ in $G$. Then $L(G) = \{N^xH^y | x \in N, N_1 \leq N, H_1 \leq N_H(N_1)\}$ and $N_1^xH_1^y \leq N_2^xH_2^y$ (for $x \in N, N_1, N_2 \leq N, H_1 \leq N_H(N_1)$) if and only if $H_1 \leq H_2, N_1^x \leq N_2$ and $xy^{-1} \in C_N(H_1)N_2$. (Note that, in general, $C_N(H_1)N_2$ is not a subgroup of $N$.)

Proof. If $H_1 \leq N_H(N_1)$, then $N_1^xH_1^y = (N_1H_1)^x$ is a subgroup of $G$. Conversely, suppose that $U \leq G$. Then $U \cap N$ is a normal Hall subgroup of $U$ and therefore possesses a complement $K$ in $U$. Since $|K| = |U : U \cap N| = |UN : N|$ is prime to $|N|$, it follows from 4.1.3(a) that there exists $v \in N$ such that $K^v \leq H$. So if we put $N_1 = (U \cap N)^v, H_1 = K^v$ and $x = v^{-1}$, then $U = (U \cap N)K = N_1^xH_1^y$ as desired.

To prove the second assertion of the theorem, assume first that $N_1^xH_1^y \leq N_2^xH_2^y$, that is, $N_1^{xy^{-1}}H_1^{xy^{-1}} \leq N_2H_2$. Then clearly $N_1^{xy^{-1}} \leq N_2H_2 \cap N = N_2$. Furthermore, applying 4.1.3(a) to the subgroup $H_1^{xy^{-1}}$ of $N_2H_2$, we see that there is $z \in N_2$ such that $H_1^{xy^{-1}z} \leq H_2$. Then 4.1.1(a) shows that $H_1 \leq H_2$ and $xy^{-1}z \in C_N(H_1)$, that is, $xy^{-1} \in C_N(H_1)N_2$. Conversely, suppose that $H_1 \leq H_2, N_1^{xy^{-1}} \leq N_2$ and $xy^{-1} \in C_N(H_1)N_2$. Then there are $s \in C_N(H_1)$ and $t \in N_2$ such that $xy^{-1} = st$. It follows that

$$N_1^{xy^{-1}}H_1^{xy^{-1}} = N_1^{xy^{-1}}H_1^y \leq N_2H_2$$

and hence $N_1^xH_1^y \leq N_2^xH_2^y$.

4.1.5 Remark. In certain situations our description of $L(G)$ in 4.1.4 becomes simpler. For example, if $N$ is abelian or hamiltonian, then $N_1^x = N_1$ for all $x \in N$. Therefore in this case, $L(G) = \{N_1H_1^x | x \in N, N_1 \leq N, H_1 \leq N_H(N_1)\}$ and $N_1^xH_1 \leq N_2H_2^y$ if and only if $H_1 \leq H_2, N_1 \leq N_2$ and $xy^{-1} \in C_N(H_1)N_2$; here $C_N(H_1)N_2$ is a subgroup of $N$.

Projectivities of finite groups with normal Hall subgroups

We use Theorem 4.1.4 to construct projectivities between groups with isomorphic normal Hall subgroups.

4.1.6 Theorem. Let $G = NH$ and $\bar{G} = MK$ be finite groups with normal Hall subgroups $N$ and $M$ and complements $H$ and $K$, respectively. Suppose that $\sigma: N \to M$ is an isomorphism and $\tau: L(H) \to L(K)$ is a projectivity such that for every $N_1 \leq N$ and for every cyclic subgroup $H_1$ of prime power order of $H$,
(1) \(C_N(H_1)^\sigma = C_M(H_1^\tau)\) and

(2) \(H_1 \leq N_H(N_1)\) if and only if \(H_1^\tau \leq N_K(N_1^\sigma)\).

Then the map \(\varphi: L(G) \to L(\overline{G})\) defined by \((N_1^x H_1^\tau)^\varphi = (N_1^x)^\sigma (H_1^\tau)^\tau\) for \(x \in N, N_1 \leq N, H_1 \leq N_H(N_1)\) is a projectivity from \(G\) to \(\overline{G}\).

**Proof.** Since \(\tau\) is a projectivity, it is clear that if (1) and (2) hold for two subgroups \(H_1\) and \(H_2\) of \(H\), then they also hold for \(H_1 \cup H_2\). Therefore our assumptions imply that (1) and (2) are satisfied for every subgroup \(H_1\) of \(H\). Now suppose that \(x, y \in N, N_1, N_2 \leq N\) and \(H_1 \leq N_H(N_i)\). Then by (2), \(H_1^\tau \leq N_K(N_1^\sigma)\) so that \((N_1^x H_1^\tau)^\tau = (N_1^x H_1^\tau)^\tau\) is a subgroup of \(\overline{G}\). And by 4.1.4, \(N_1^x H_1^\tau \leq N_2^x H_2^\tau\) if and only if \(H_1 \leq H_2, N_1^x H_1^\tau \leq N_2^x H_2^\tau\) and \(x^{-1} y^{-1} \in C_N(H_1) N_2\). Since \(\sigma\) is an isomorphism and \(\tau\) a projectivity satisfying (1), this is the case if and only if \(H_1^\sigma \leq H_2^\sigma, (N_1^x)^{\sigma(y^\tau)} = (N_1^x)^{\sigma(y^\tau)}\leq N_2^x\) and \(x^{\sigma(y^\tau)} = x^{\sigma(y^\tau)} \in C_N(H_1)^\sigma N_2^\tau = C_M(H_1^\tau) N_2^\tau\), that is if and only if \((N_1^x)^{\sigma(y^\tau)}(H_1^\tau)^{\sigma(y^\tau)} \leq (N_2^x)^{\sigma(y^\tau)}(H_2^\tau)^{\sigma(y^\tau)}\). This shows that \(\varphi\) is well-defined and preserves inclusion. The same holds for the map \(\psi: L(\overline{G}) \to L(G)\) defined with respect to \(\sigma^{-1}\) and \(\tau^{-1}\) in the same way as \(\varphi\) with respect to \(\sigma\) and \(\tau\). Of course, \(U^{\sigma \psi} = U\) for all \(U \leq G\) and \(V^{\psi \sigma} = V\) for all \(V \leq \overline{G}\). Thus \(\varphi\) is bijective and, by 1.1.2, it is a projectivity from \(G\) to \(\overline{G}\). \(\square\)

To illustrate Theorems 4.1.4 and 4.1.6, we study the simple but interesting situation where \(N\) is elementary abelian and \(H\) is cyclic of prime order.

**4.1.7 Example.** Let \(p\) and \(q\) be different primes, \(F = GF(p)\) and suppose that \(|H| = q\).

(a) Let \(G = NH\) where \(N\) is an elementary abelian normal \(p\)-subgroup of \(G\). Then it is well-known that we can regard \(N\) as an \(FH\)-module and by Maschke's Theorem (see Robinson [1982], p. 209), this \(FH\)-module is completely reducible. Thus

(3) \(N = C_N(H) \times N_1 \times \cdots \times N_t\)

where the \(N_i\) are nontrivial irreducible \(FH\)-modules.

(b) It is also well-known (see Huppert [1967], p. 166) that all nontrivial irreducible \(FH\)-modules \(N\) have the same order \(p^m\), where \(m\) is the smallest natural number such that \(q | p^m - 1\), and all these modules lead to isomorphic semidirect products \(G = NH\). By 4.1.5, the subgroups of \(G\) are of the form \(N_1 H_1^x\) where \(x \in N, N_1 \leq N\) and \(H_1 \leq N_H(N_1)\). Since \(|H| = q\), only \(H_1 = 1\) or \(H_1 = H\) is possible. If \(H_1 = 1\), then

\[L(G)\] for \(p = 5, q = 3, m = 2\]

**Figure 14**
Projectivities and arithmetic structure of finite groups

For $H_1 = H$, since $N$ is $FH$-irreducible, either $N_1 = N$ or $N_1 = 1$, and then $N_1 H_1^i = NH_1^i = G$ or $N_1 H_1^i = H^i$. Therefore $L(G)$ consists of $G$, the subgroups of $N$ and the $|N|$ conjugates of $H$. In particular, this lattice does not depend on the prime $q$. Therefore, if we take another prime $r$ such that $r | p^m - 1$ and $r | p^j - 1$ for $j < m$, a group $K$ of order $r$ and a nontrivial irreducible $FK$-module $M$, then the semidirect product $\bar{G} = MK$ is lattice-isomorphic to $G$. For $m = 1$, $G$ and $\bar{G}$ are nonabelian groups in $P(2, p)$. But for $m \geq 2$ we get, in addition to the cyclic groups and the $P$-groups, another class of examples of lattice-isomorphic groups with different orders. The smallest primes are $p = 29$, $q = 3$, $r = 5$ for $m = 2$ and $p = 11$, $q = 7$, $r = 19$ for $m = 3$.

(c) In the case $m = 1$, that is, $q | p - 1$, a fixed generator $a$ of $H$ induces power automorphisms $x \rightarrow x^a$ in the irreducible $FH$-modules $N_i$. Since $\text{Exp } N = p$, we may regard these $\lambda$ as (nonzero) elements of the field $F = \mathbb{Z}/(p)$ and by (3), $N$ is the direct product of the eigenspaces

$$E(\lambda) = E(\lambda, a, N) = \{x \in N | x^a = x^\lambda\}$$

of $a$. In general, for an automorphism $\sigma$ of $N$ of order dividing $p - 1$, we define the type of $\sigma$ to be $(d_0; d_1, \ldots, d_k)$ if $p^{d_0} = |E(1, x, N)| = |C_N(x)|$ and $d_1 \geq \cdots \geq d_k$ are the dimensions of the eigenspaces of $\sigma$ to eigenvalues $\lambda_i \neq 1$. We shall show in 4.1.8 that two groups $N(a)$ and $N(b)$ of the form considered are lattice-isomorphic if the automorphisms induced by $a$ and $b$ in $N$ have the same type. It is not so easy to decide whether they are isomorphic; this is the case if and only if $\langle a \rangle$ and $\langle b \rangle$ induce automorphism groups in $N$ that are conjugate in $\text{Aut } N$ (see Exercise 3).

(d) If there are two different primes $q$ and $r$ dividing $p - 1$, then we can construct groups $N(a)$ and $N(b)$ with $o(a) = q$ and $o(b) = r$ such that $a$ and $b$ induce automorphisms of the same type in $N$. So we get many further examples of lattice-isomorphic groups having different orders of the form $p^nq$ and $p^n$. The following table shows all types for $n \leq 2$ and the resulting groups of order $p^nq$; in these small cases it is also often clear from earlier results, for example 1.2.8, 1.6.4 or 2.2.3, that all groups of the given type are lattice-isomorphic.

<table>
<thead>
<tr>
<th>type</th>
<th>group</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1; 0)</td>
<td>$C_p \times C_q$</td>
</tr>
<tr>
<td>(0; 1)</td>
<td>nonabelian group of order $pq$</td>
</tr>
<tr>
<td>(2; 0)</td>
<td>$C_p \times C_p \times C_q$</td>
</tr>
<tr>
<td>(1; 1)</td>
<td>$C_p \times F$ where $F$ is nonabelian of order $pq$</td>
</tr>
<tr>
<td>(0; 2)</td>
<td>nonabelian $P$-group of order $p^2q$</td>
</tr>
<tr>
<td>(0; 1, 1)</td>
<td>$\langle x, y, a</td>
</tr>
</tbody>
</table>

The last groups in the table are the Rottländer groups which we shall study more closely in 5.6.8. There are $(q - 1)/2$ nonisomorphic groups of this type and order $p^2q$. \[\square\]
4.1 Normal Hall subgroups

4.1.8 Theorem. Let \( p \) and \( r \) be (not necessarily distinct) primes dividing \( p - 1 \) and suppose that \( G = N\langle a \rangle \) and \( \bar{G} = M\langle b \rangle \) with normal elementary abelian \( p \)-subgroups \( N, M \) and \( o(a) = q, o(b) = r \). Then there exists a projectivity \( \varphi \) from \( G \) to \( \bar{G} \) satisfying \( N^\varphi = M \) and \( \langle a \rangle^\varphi = \langle b \rangle \) if and only if the automorphisms induced by \( a \) on \( N \) and by \( b \) on \( M \) have the same type.

Proof. Let \( \alpha \) and \( \beta \) be the automorphisms induced by \( a \) and \( b \) in \( N \) and \( M \), respectively. Suppose that the type of \( \alpha \) is \( (d_0; d_1; \ldots; d_k) \), that of \( \beta \) is \( (e_0; e_1; \ldots; e_l) \), and let \( N = D_0 \times \cdots \times D_k \) and \( M = E_0 \times \cdots \times E_l \) be the decompositions of \( N \) and \( M \) into eigenspaces of \( \alpha \) and \( \beta \), respectively, such that \( D_0 = C_N(a), E_0 = C_M(b), |D_i| = p^{d_i} \) and \( |E_i| = p^{e_i} \) for all \( i \).

Suppose first that \( \varphi \) is a projectivity from \( G \) to \( \bar{G} \) satisfying \( N^\varphi = M \) and \( \langle a \rangle^\varphi = \langle b \rangle \). Then \( C_N(a)^\varphi = C_M(b) \) by 4.1.2(b). If \( D \) is an eigenspace of \( \alpha \), then \( a \) normalizes every subgroup of \( D \). Conversely, if \( F \) is a subgroup of \( N \) such that \( a \) normalizes every subgroup of \( F \), then by 1.5.4, \( a \) induces a universal power automorphism on \( F \), that is, \( F \) is contained in an eigenspace of \( \alpha \). Thus the eigenspaces of \( \alpha \) are precisely the subgroups of \( N \) maximal with the property that all their subgroups are normalized by \( a \). By 4.1.2, these subgroups are mapped by \( \varphi \) to the corresponding subgroups of \( M \) with respect to \( \beta \), that is, to the eigenspaces of \( \beta \). It follows that \( d_i = e_i \) for all \( i \) and \( \alpha \) and \( \beta \) have the same type.

Conversely, if \( \alpha \) and \( \beta \) have the same type, then \( k = l \) and \( |D_i| = |E_i| \) for all \( i \). Hence there exists an isomorphism \( \sigma: N \to M \) such that \( D_0 = E_0 = C_M(b) \) and, as we have seen in 4.1.7, a subgroup \( F \) of \( N \) is normalized by \( a \) if and only if \( F \) is a direct product of subgroups of the eigenspaces of \( \alpha \), that is, of the \( D_i \). These subgroups are mapped by \( \sigma \) onto the direct products of subgroups of the \( E_i \), that is, onto the \( b \)-invariant subgroups of \( M \). By 4.1.6 there is a projectivity \( \varphi \) from \( G \) to \( \bar{G} \) satisfying \( N^\varphi = M \) and \( \langle a \rangle^\varphi = \langle b \rangle \). \( \square \)

As another application of Theorem 4.1.4, we show how a projectivity of \( G/C_H(N) = G/H_G \) can be lifted to a projectivity of \( G \).

4.1.9 Theorem. Let \( G = NH \) and \( \bar{G} = MK \) be finite groups with normal Hall subgroups \( N \) and \( M \) and complements \( H \) and \( K \), respectively. Let \( \mu \) be a projectivity from \( G/C_H(N) \) to \( \bar{G}/C_K(M) \) satisfying \( (NC_H(N)/C_H(N))^\mu = MC_K(M)/C_K(M) \), let \( \tau \) be a projectivity from \( H \) to \( K \) such that \( C_H(N)^\tau = C_K(M) \) and suppose that \( \mu \) and \( \tau \) induce the same projectivity in \( H/C_H(N) \). Then there exists a projectivity \( \varphi \) from \( G \) to \( \bar{G} \) inducing \( \mu \) in \( G/C_H(N) \) and \( \tau \) in \( H \).

Proof. For \( X \leq G \) let \( \tilde{X} = XC_H(N) \) and let \( \tilde{\mu} \) be the map induced by \( \mu \) in the interval \([G/C_H(N)], \) that is, \( (X/C_H(N))^\mu = X^{\tilde{\mu}}/C_K(M) \) for \( C_H(N) \leq X \leq G \).

Let \( U \leq G \). Then by 4.1.4 there exist \( x \in N, N_1 \leq N, H_1 \leq N_H(N_1) \) and \( \tilde{x} \in M, M_1 \leq M, K_1 \leq N_K(M_1) \) such that

\[ U = N_1^x H_1^\tilde{x}, \quad \tilde{U} = N_1^x (H_1 C_H(N))^\tilde{x} = N_1^x \tilde{H}_1^x \quad \text{and} \quad \tilde{U}^{\tilde{\mu}} = M_1^x \tilde{K}_1^x. \]
We want to define $U^\varphi$ as $(M_1 H_1^x)^x$. In the first place this is a subgroup of $\widetilde{G}$; indeed $C_K(M) \leq K_1$ since $C_K(M) \leq \widetilde{U}$; therefore

$$\tilde{H}_1^x = \tilde{H}_1 = (\tilde{N} \tilde{H}_1 \cap H)^x = (\tilde{N} \tilde{U} \cap H)^x = \tilde{N}^x \tilde{U}^x \cap H^x = M C_K(M) M_1^x K_1^x \cap K$$

that is,

$$(5) \quad H_1^x \leq \tilde{H}_1 = K_1 \leq N_K(M_1).$$

Furthermore, $N_1^x H_1^x = U \leq V = N_2^x H_2^x$ ($y \in N, N_2 \leq N, H_2 \leq N_N(N_2)$) implies that $(M_1 K_1)^x = \tilde{U}^x \leq \tilde{V}^x = (M_2 K_2)^x$ and, by 4.1.4, $H_1 \leq H_2, K_1 \leq K_2, M_1^{x^{-1}} \leq M_2$ and $x y^{-1} \in C_M(K_1) M_2$. It follows that $H_1^x \leq H_2^x$ and $x y^{-1} \in C_M(H_1^x) M_2$ since $H_1^x \leq K_1^x$. Again by 4.1.4, $(M_1 H_1^x)^x \leq (M_2 H_2^x)^x$. So if we put $U^\varphi = (M_1 H_1^x)^x$, then $\varphi$ is well-defined and preserves inclusion. The same holds for the map $\psi: L(\widetilde{G}) \rightarrow L(\tilde{G})$ defined with respect to $\mu^{-1}$ and $\tau^{-1}$ in the same way as $\varphi$ with respect to $\mu$ and $\tau$. Now $C_{H}(M)^x = C_K(M)$ and (5) imply that

$$(6) \quad U^\varphi C_K(M) = M_1^x (H_1^x C_K(M))^x = M_1^x (\tilde{H}_1^x)^x = M_1^x K_1^x = \tilde{U},$$

hence $(U^\varphi C_K(M))^{-1} = \tilde{U} = N_1^x \tilde{H}_1^x$ and therefore, finally, $(U^\varphi)^x = (N_1^x \tilde{H}_1^x)^{x^{-1}} = U$. Since the situation is symmetric in $\varphi$ and $\psi$, it follows that also $(W^\psi)^\varphi = W$ for all $W \leq \widetilde{G}$. Thus $\varphi$ is bijective and, by 1.1.2, it is a projectivity from $G$ to $\widetilde{G}$. If $C_{H}(N) \leq U$, then $U = \tilde{U}$ and, by (6), $U^\varphi = U^\tilde{\varphi}$. Hence $\varphi$ induces $\mu$ in $G/C_{\tilde{H}}(N)$ and it trivially induces $\tau$ in $\tilde{H}$.

**Autoprojectivities**

The group $P(G)$ of autoprojectivities of a group $G$ with normal Hall subgroup $N$ and complement $H$ was studied by Paulsen [1975]. His results are rather technical. Since $N$ is the only subgroup of its order, every autoprojectivity $\psi$ of $G$ that does not fix $N$ satisfies $|N^\psi| \neq |N|$; in the next section we shall study this rare situation to obtain complete information about autoprojectivities of this type. If $N^\psi = N$, then $\psi$ induces autoprojectivities in $N$ and in $G/N$ and operates on the set $\mathcal{X}$ of complements to $N$ in $G$. And $\psi$ is determined by its action on these three subsets of $L(G)$, that is on $L(N)$, $[G/N]$ and $\mathcal{X}$; for, if $x \in N$ and $H_1 \leq H$, then $H_1^x = NH_1 \cap H^x$. There is not much more that can be said in general. If $C_N(H) = 1$, the operation of $\psi$ on $\mathcal{X}$ yields via the Schur-Zassenhaus Theorem a permutation of $N$ which we study for two special cases in the last theorem of this section and in Exercise 5.

**4.1.10 Theorem.** Let $G$ be a finite group, $N$ a normal Hall subgroup and $H$ a complement to $N$ in $G$ such that $C_N(H) = 1$. Suppose that $\psi$ is an autoprojectivity of $G$ which satisfies $N^\psi = N$ and induces the trivial autoprojectivity in $H$; define $\rho: N \rightarrow N$ by $(H^x)^\psi = H^x$ for $x \in N$.

(a) Then $\rho$ is a permutation of $N$ and $1^\rho = 1$.

(b) For every $H_1 \leq H$ and $x \in N$, $(H_1^x)^\psi = H_1^x$; thus $\psi$ is determined by $\rho$ and its action on $L(N)$. 

4.1 Normal Hall subgroups

(c) If \(H_1 \leq H\) and \(L\) is an \(H_1\)-invariant normal subgroup of \(N\) such that \(C_N(H_1) \leq L\) and \(L^\varphi = L\), then \((xL)^\varphi = x^\varphi L\) for all \(x \in N\); in particular, \(L^\varphi = L\).

Proof. (a) For \(x, y \in N\), \(H^x = H^y\) if and only if \(xy^{-1} \in N_N(H) = C_N(H) = 1\), that is, \(x = y\). Since \(\psi\) maps complements of \(N\) onto complements of \(N\), the Schur-
Zassenhaus Theorem shows that \(\psi\) is well-defined and bijective. As \(H^\varphi = H\), \(1^\varphi = 1\).

(b) Since \(N^\varphi = N\) and \(H_i^\varphi = H_i\) we have \((H_i^\varphi) = (NH_i \cap H^x)^\varphi = NH_i \cap H^x = H_i^x\); by 4.1.4, \(\psi\) is determined by \(\varphi\) and its action on \(L(N)\).

(c) For \(x \in N\), let \(S(x) = \{y \in N \mid L \cap H^x = H_i \}\). Then \(y \in S(x)\) if and only if \((L \cap H^x)^\varphi = (H_i^x)^\varphi\) and (b) shows that this is the case if and only if \(L \cap H^x = H_i^x\), that is, \(y^\varphi \in S(x^\varphi)\). Hence \(S(x)^\varphi = S(x^\varphi)\), and it suffices to show that \(S(x) = xL\).

If \(y \in S(x)\), then \(H_i \leq L \cap H^x\) and hence \(L \cap H^x \leq L_i^x\); by the Schur-Zassenhaus Theorem there exists \(z \in L\) such that \(H_i^z = H_i\). It follows that \(xzy^{-1} \in C_N(H_1) \leq L\) and therefore \(y \in xL\) since \(L \leq N\). Conversely, if \(y = xz\) where \(z \in L\), then \(L \cap H^x = (L \cap H^x)z = L \cap H^x = H_i^x\) and hence \(y \in S(x)\). Thus \(S(x) = xL\) and (c) holds. \(\square\)

Exercises

1. Let \(G\) be a finite group, \(N\) a normal Hall subgroup and \(H\) a complement to \(N\) in \(G\). Show that \(L(G) = \{N, H_i \mid x \in N, N_i \leq N, H_i \leq H, H_i^x \leq N_G(N_i)\}\) and \(N_i H_i^x \leq N_2 H_2^x\) (for \(x \in N, N_1, N_2 \leq N, H_1, H_2 \leq H, H_i^x \leq N_G(N_i)\) and \(H_2 \leq N_G(N_2)\)) if and only if \(H_1 \leq H_2, N_1 \leq N_2\) and \(x \in C_N(H_1)\).

2. For \(p > 2\), let \(N = \langle x, y \mid x^p = y = [x, y] = 1 \rangle\) be the abelian group of type \((p^2, p)\) and \(M = \langle u, v \mid u^p = v^p = 1, uv^p = u^{1+p} \rangle\) the nonabelian group of order \(p^3\) lattice-isomorphic to \(N\). Let \(G = N \langle a \rangle\) and \(\overline{G} = M \langle b \rangle\) be semidirect products of \(N\) and \(M\) by cyclic groups of order 2 with respect to the automorphisms given by \(x^a = x^{-1}, y^a = y\) and \(u^b = u^{-1}, v^b = v\). Show that there are projectivities \(\sigma\) from \(N\) to \(M\) and \(\tau\) from \(H = \langle a \rangle\) to \(K = \langle b \rangle\) satisfying (1) and (2), but that \(G\) and \(\overline{G}\) are not lattice-isomorphic. (This shows that we cannot replace the isomorphism \(\sigma\) in Theorem 4.1.6 by a projectivity.)

3. Let \(N\) be a group, \(H\) and \(K\) subgroups of \(\text{Aut}\ N\) and \(G = NH\) and \(\overline{G} = NK\) the corresponding semidirect products. Show that there exists an isomorphism \(\sigma: G \rightarrow \overline{G}\) satisfying \(N^\sigma = N\) and \(H^\sigma = K\) if and only if \(H\) and \(K\) are conjugate in \(\text{Aut}\ N\).

4. Let \(G = NH\) and \(\overline{G} = MK\) be finite groups with normal Hall subgroups \(N\) and \(M\) and complements \(H\) and \(K\), respectively, and suppose that \(C_N(H) = 1 = C_M(K)\). Show that there exists a projectivity \(\varphi\) from \(G\) to \(\overline{G}\) satisfying \(N^\varphi = N\) if and only if there are projectivities \(\sigma\) from \(N\) to \(M\) and \(\tau\) from \(H\) to \(K\) and a bijective map \(\pi: N \rightarrow M\) such that for all \(x, y \in N, N_1 \leq N\) and \(H_1 \leq H\),
(a) \(H_1 \leq N_M(N_1)\) if and only if \(H_i^x \leq N_K(N_i^x)\), and
(b) if \(H_1 \leq N_M(N_1)\), then \(xy^{-1} \in C_N(H_1)N_1\) if and only if \(x^\sigma(y^\sigma)^{-1} \in C_M(H_1)N_1^\sigma\).

5. Let \(G\) be a finite group, \(N\) an abelian normal Hall subgroup, \(H\) a complement to \(N\) in \(G\) and suppose that \(C_N(H) = 1\).
(a) Let \( \pi \) be a permutation of \( N \) such that if \( N_i \leq N \) and \( H_1 \leq N_H(N_i) \) then \( xy^{-1} \in C_N(H_1)N_1 \) if and only if \( x^s(y^s)^{-1} \in C_N(H_1)N_1 \). Show that \( \varphi_\pi : L(G) \rightarrow L(G) \) defined by \( (N_i H_1^s)^{\varphi_\pi} = N_i H_1^s \) is an autoprojectivity of \( G \). Denote the group of all these autoprojectivities by \( \Gamma \).

(b) Let \( \tau \) be an autoprojectivity of \( H \) such that for all \( H_1 \leq H \), \( C_N(H_1^s) = C_N(H_1) \) and \( H_1^s \) and \( H_1 \) normalize the same subgroups of \( N \). Show that \( \psi_\tau : L(G) \rightarrow L(G) \) defined by \( (N_i H_1^s)^{\psi_\tau} = N_i (H_1^s)^\tau \) is an autoprojectivity of \( G \). Denote the group of all these autoprojectivities by \( \Delta \).

(c) Let \( \Lambda = \{ \psi \in P(G) | U^\psi = U \text{ for all } U \leq N \} \). Show that \( \Lambda = \Gamma \times \Delta \).

4.2 Singular projectivities

We already know many projectivities that map a group \( G \) onto a group of different order; this may happen, for example, if \( G \) is cyclic (see 1.2.8), a \( P \)-group (see 2.2.3), or for the groups in 4.1.7. On the other hand, Theorem 2.2.6 states that for a projectivity \( \varphi \) of a nonabelian \( p \)-group \( G \), \( |G^\varphi| = |G| \) and then also \( |H^\varphi| = |H| \) for every subgroup \( H \) of \( G \). In this section we want to show that this last property holds for projectivities of many more groups and, in fact, reflects the normal behaviour of a projectivity. We first of all give it a name.

**Index preserving and singular projectivities**

A projectivity \( \varphi \) of a group \( G \) is called **index preserving** if it satisfies \( |H^\varphi : K^\varphi| = |H : K| \) for every pair \( H, K \) of subgroups of \( G \) such that \( K \leq H \); \( \varphi \) is called **singular** if it is not index preserving. An index preserving projectivity in particular satisfies \( |H^\varphi| = |H| \) for every subgroup \( H \) of \( G \), and from Lagrange's Theorem it is clear that for a finite group \( G \) the converse holds: \( \varphi \) is index preserving if \( |H^\varphi| = |H| \) for all \( H \leq G \). But we can say a little more.

**4.2.1 Lemma.** If \( \varphi \) is a projectivity of a finite group \( G \) satisfying \( |S^\varphi| = |S| \) for every Sylow subgroup \( S \) of \( G \), then \( \varphi \) is index preserving.

**Proof.** Assume that \( K \leq H \leq G \), let \( p \) be a prime and let \( P \in Syl_p(H) \); take \( S \in Syl_p(G) \) such that \( P \leq S \). Since \( S^\varphi \) is a \( p \)-group, \( |P^\varphi| = |P| \). If \( P^\varphi \) would be properly contained in a \( p \)-subgroup \( T^\varphi \) of \( H^\varphi \), then \( P < T \leq H \) and \( T \) would contain an element \( x \) of prime order \( q \neq p \). For a Sylow \( q \)-subgroup \( Q \) of \( G \), \( x = \langle x \rangle^\varphi \) would divide \( |Q^\varphi| = |Q| \), a contradiction. Thus \( P^\varphi \) is a Sylow \( p \)-subgroup of \( H^\varphi \) and hence the \( p \)-part of \( |H^\varphi| \) is the same as that of \( |H| \). Since this holds for all primes \( p \), it follows that \( |H^\varphi| = |H| \). Similarly, \( |K^\varphi| = |K| \) and by Lagrange's Theorem, \( |H^\varphi : K^\varphi| = |H^\varphi|/|K^\varphi| = |H|/|K| = |H : K| \).

The above lemma suggests the introduction of the following concepts.
4.2 Singular projectivities

Let $p$ be a prime and $G$ a finite group. A projectivity $\varphi$ from $G$ to a group $\overline{G}$ is called $p$-singular or singular at $p$ if there exists a $p$-subgroup (or, equivalently, a Sylow $p$-subgroup) $P$ of $G$ such that $|P^p| \neq |P|$; $\varphi$ is called $p$-regular or regular at $p$ if it is not $p$-singular. Lemma 4.2.1 shows that if $\varphi$ is not index preserving, then there exists a prime $p$ such that $\varphi$ is singular at $p$. By 2.2.6 the Sylow $p$-subgroups of $G$ are then cyclic or elementary abelian and we are looking for further restrictions on the structure of $G$ and $\overline{G}$ if $G$ has composite order. However, if $T$ is any group of order prime to $|G|$ and $|\overline{G}|$, then by 1.6.4 there exists a projectivity from $G \times T$ to $\overline{G} \times T$ which induces $\varphi$ in $G$ and therefore is singular at $p$. Hence there is no global restriction on the structure of a group with a $p$-singular projectivity. We can only hope for restrictions on its $p$-structure, for example on the embedding of its Sylow subgroups. We distinguish two kinds of singularities at $p$.

4.2.2 Lemma. Let $\varphi$ be a projectivity from $G$ to $\overline{G}$ and suppose that $P$ is a Sylow $p$-subgroup of $G$ such that $|P^p| \neq |P|$. Assume further that there is no $P$-group $S < G$ containing $P$ as a proper normal subgroup (we call $\varphi$ singular of the first kind at $p$ in this case). Then $P < Z(N_G(P))$ and hence $G$ has a normal $p$-complement.

Proof. We have to show that $P \leq Z(N_G(P))$; then Burnside’s theorem (see Robinson [1982], p. 280) yields that $G$ has a normal $p$-complement. So we suppose that this assertion is wrong and take a counterexample $G'$ of minimal order. If $P \leq H < G'$, then $H$ and the projectivity induced by $\varphi$ in $H$ satisfy the assumptions of the lemma; the minimality of $G$ implies that $P \leq Z(N_H(P))$. In particular, if $N_G(P) < G'$, then $P \leq Z(N_{N_G(P)}(P)) = Z(N_G(P))$, contradicting the choice of $G'$. Thus

1. $P \leq G'$,

2. $P \leq Z(H)$ for all $P \leq H < G'$, and

3. $P \not\leq Z(G)$

since $G$ is a counterexample. It follows that there exists a cyclic subgroup $Q$ of prime power order in $G$ such that $Q \not\leq C_G(P)$. By (1) and (2) $G = PQ$, and, by 2.2.6, $P$ is cyclic or elementary abelian. Thus $P \neq G$ and hence $Q$ is a $q$-group for some prime $q \neq p$. We want to show that $|Q| = q$ and assume, for a contradiction, that $|Q| \geq q^2$. If $D$ is the maximal subgroup of $Q$, $PD < G$ and, again by (2), $D$ is centralized by $P$. By 1.6.7, $[D^p, P^p] = 1$ and since $Q$ and $Q^p$ are cyclic, it follows that $D \leq Z(G)$ and $D^p \leq Z(\overline{G})$. Thus $\varphi$ induces a projectivity $\overline{\varphi}$ from $G/D$ to $\overline{G}/D^p$ that maps the Sylow $p$-subgroup $PD/D$ of $G/D$ onto the subgroup $P^pD^p/D^p$ of order $|P^p| \neq |PD/D|$ of $\overline{G}/D^p$. If $G/D$ were a $P$-group and $G/D \in P(m, p)$, then also $\overline{G}/D^p \in P(m, p)$ by 2.2.2. Since $\overline{\varphi}$ is singular at $p$, $\overline{G}/D^p$ would be nonabelian and since the Sylow $p$-subgroup of $G/D$ is not mapped onto the Sylow $p$-subgroup of $\overline{G}/D^p$, there would exist a subgroup $Q_1/D$ of order $q$ in $G/D$ such that $|Q_1^p/D^p| = p$. Since $G/D$ is generated by its subgroups of order $q$, there would also exist $Q_2/D \leq G/D$ of order $q$ such that $|Q_2^p/D^p| \neq p$. Then $Q_1$ and $Q_2$ would be Sylow $q$-subgroups of $G$ and hence $Q_1^p$ and $Q_2^p$ would be cyclic of prime power order. Since $1 \neq D^p \leq Q_1^p \cap Q_2^p$, the primes have
to be the same; but \( |Q_0^p/D^p| = p \neq |Q_0^q/D^q| \). This contradiction shows that \( G/D \) is not a \( P \)-group and the minimality of \( G \) implies that \( PD/D \leq Z(G/D) \). It follows that \( Q \leq G \) and hence \( G = P \times Q \) is abelian, contradicting (3). We have shown that

(4) \( G = PQ \) and \( |Q| = q \) where \( p \neq q \in \mathbb{P} \).

We want to show next that \( P \) is not cyclic. So suppose, for a contradiction, that \( P \) is cyclic. If \( |P| = p \), then \( P \) would be a proper normal subgroup of the \( P \)-group \( G \), contradicting our assumption. Thus \( |P| = p^n \) where \( n \geq 2 \). If \( x \in \overline{G} \) then \( ((P^p)^x)^{p^{-1}} \) is a cyclic subgroup of \( G \) of order \( t^n \) for some prime \( t \). Since \( |G| = p^n q \) and \( n \geq 2 \), \( t = p \) and hence \( ((P^p)^x)^{p^{-1}} = P \), the only Sylow \( p \)-subgroup of \( G \). Thus \( P^p \leq \overline{G} \) and \( \varphi \) induces a projectivity from \( G/\Phi(P) \) to \( \overline{G}/\Phi(P^p) \). Since \( Q \) operates nontrivially on \( P \), the group \( G/\Phi(P) \) is not cyclic; hence \( G/\Phi(P) \in \text{P}(2, p) \) and therefore also \( \overline{G}/\Phi(P^p) \in \text{P}(2, p) \). Now \( P^p \leq \overline{G} \) implies that \( |P^p/\Phi(P^p)| = p^p \) and since \( P^p \) is also cyclic of prime power order, it follows that \( |P^p| = p^n = |P| \), a contradiction. Thus \( P \) is not cyclic and by 2.2.6,

(5) \( P \) is elementary abelian of order \( p^n \) and \( P^p \) is a nonabelian \( P \)-group of order \( p^{n-1} r \) where \( n \geq 2 \) and \( p > r \in \mathbb{P} \).

Let \( P_0^p \) be the Sylow \( p \)-subgroup of \( P^p \). If \( P^p \leq \overline{G} \), then \( P_0^p \leq \overline{G} \) since it is characteristic in \( P^p \). It follows that \( P_0^p = P_0^q Q^p \cap P^p \); hence \( P_0 = (P_0 \cup Q) \cap P \leq P_0 \cup Q \) and therefore \( P_0 \leq G \). If \( P^p \) is not normal in \( \overline{G} \), then there exists \( x \in \overline{G} \) such that \( P^p \neq P^p x \). By 2.2.5, \( P^{p^{x^{-1}}} \) lies in \( \text{P}(n, p) \) and since it is different from \( P, |P^{p^{x^{-1}}}| = p^{n-1} q \). Then \( |P \cap P^{p^{x^{-1}}}| = p^{n-1} \) and \( P \cap P^{p^{x^{-1}}} \leq P \cup P^{p^{x^{-1}}x} = G \). Therefore, in both cases, there is a maximal subgroup \( M \) of \( P \) such that \( M \leq G \). By Maschke’s theorem (see Robinson [1982], p. 209) there exists a \( Q \)-invariant subgroup \( T \) of \( P \) such that \( P = M \times T \); clearly, also \( T \leq G \). Suppose first that \( |T| = p \). Then \( T \leq P_0 \), hence \( M \leq P_0 \) and therefore \( M^p \) is not a \( P \)-group. Thus \( \varphi \) induces a \( p \)-singular projectivity from \( MQ < G \) to \( (MQ)^p \) and the minimality of \( G \) implies that \( MQ \) is a \( P \)-group or \( M \leq Z(MQ) \). In both cases, every subgroup of \( M \) is normalized by \( Q \) and hence is a normal subgroup of \( G \). Since \( r \) divides \( |M^p| \),

(6) there exists a normal subgroup \( R \) of \( G \) contained in \( P \) such that \( |R^p| = r \).

This is trivial if \( |T^p| \neq p \), since we can take \( R = T \) in that case; thus (6) holds in general. Now if \( X \) is any subgroup of \( P \) such that \( |X^p| = r \), then by Sylow’s Theorem there exists \( z \in P^p \) such that \( R^z = X^p \). Since \( R \leq G \), either \( RQ \in \text{P}(2, p) \) or \( RQ \) is cyclic; hence also \( (RQ)^{p^{x^{-1}}} = X \cup Q^{p^{x^{-1}}} \) in \( \text{P}(2, p) \) or this is cyclic. Since \( |X| = p \), it follows that \( X \leq X \cup Q^{p^{x^{-1}}} \). As \( z \in P^p \), \( Q^{p^{x^{-1}}} \) and hence \( X \leq G \). If \( Y \leq P \) such that \( |Y| = p \), then \( (RY)^{p^{x^{-1}}} \) in \( \text{P}(2, p) \) has order \( pr \) and every minimal subgroup of \( RY \) different from \( Y \) is mapped by \( \varphi \) to a subgroup of order \( r \) in \( \overline{G} \). These groups are normalized by \( Q \), as we have just shown, and hence also \( RY \) and \( Y \) are normalized by \( Q \). Thus \( Q \) induces a power automorphism in \( P \) and, since \( P \leq Z(G) \), it follows that \( G \) is a \( P \)-group. This contradicts our assumption on \( G \).

4.2.3 Lemma. Let \( \varphi \) be a projectivity from \( G \) to \( \overline{G} \) and suppose that \( P \) is a Sylow \( p \)-subgroup of \( G \) such that \( |P^p| \neq |P| \). Assume further that there exists a \( P \)-group \( S \leq G \) containing \( P \) as a proper normal subgroup (we call \( \varphi \) singular of the second kind
at $p$ in this case). Then there exists a subgroup $K$ of $G$ such that $G = S \times K$ and $(|S|, |K|) = 1$.

**Proof.** Again we suppose that the assertion is wrong and consider a counterexample $G$ of minimal order. By 2.2.1, $|S| = p^{n-1}q$ where $n \geq 2$ and $p > q \in \mathbb{P}$. Then $S^o \in P(n, p)$ and, since $|P^o| \neq |P|$, we see that $S^o$ is not abelian and $\varphi$ does not map the Sylow $p$-subgroup of $S$ to that of $S^o$. It follows that there exists a subgroup $Q$ of order $q$ in $S$ such that $|Q^o| = p$. Thus $\varphi$ is singular at $q$ and $\varphi^{-1}$ is singular at $p$, hence the Sylow $q$-subgroups of $G$ and the Sylow $p$-subgroups of $G$ are cyclic or elementary abelian. If $Q$ were contained in a $P$-group $H$ as a normal subgroup, then $H \in P(m, q)$ for some $m \in \mathbb{N}$. Hence also $H^o \in P(m, q)$ and $q$ would be the largest prime dividing $|H^o|$; but $|Q^o| = p > q$ divides $|H^o|$, a contradiction. Thus:

(7) There is no $P$-group $H \leq G$ containing $Q$ as a normal subgroup.

We want to show next that $Q$ is a Sylow $q$-subgroup of $G$. Suppose that this is wrong and take $T \in \text{Syl}_q(G)$ such that $Q < T$. By (7), $T$ is not elementary abelian and hence cyclic. Since $|Q^o| = p$, $T^o$ is a cyclic $p$-group of order at least $p^2$ and therefore the Sylow $p$-subgroups of $G$ are not elementary abelian. It follows that $\varphi^{-1}$ is singular of the first kind at $p$; by 4.2.2 the group $\overline{G}$, and hence also every subgroup of $\overline{G}$, has a normal $p$-complement. But $S^o$ has none, a contradiction. Thus

(8) $Q \in \text{Syl}_q(G)$.

By (7), $\varphi$ is singular of the first kind at $q$ and by 4.2.2 there exists a normal $q$-complement $N$ in $G$, that is

(9) $N \leq G$ such that $G = NQ$ and $N \cap Q = 1$.

Certainly $P \leq N$ and hence $\varphi$ induces a $p$-singular projectivity from $N$ to $N^o$. We want to show that this singularity is of the first kind. So suppose, for a contradiction, that $T \leq N$ is a $P$-group containing $P$ as a proper normal subgroup. Then $T \in P(n, p)$ and $T$ and $S$ are contained in $N_G(P)$. Therefore, if $x \in S^o$ then $T_0^{x_0^{-1}} \leq N_G(P)$ and $T_0^{x_0^{-1}} \in P(n, p)$. Since $P$ is the only Sylow $p$-subgroup of $N_G(P)$, it follows that $P \leq T_0^{x_0^{-1}}$. Furthermore, $S_0^{x_0^{-1}} = S$ and since $S \not\leq N$, $S \cap T = P$. Therefore $P_0^{x_0^{-1}} = S_0^{x_0^{-1}} \cap T_0^{x_0^{-1}} \geq P$, that is, $(P^o)^x = P^o$. Thus $P^o \leq S^o$ and by 2.2.2, $|P^o| = p^{n-1} = |P|$, contradicting the assumption of the lemma. Hence the projectivity induced by $\varphi$ in $N$ is singular of the first kind at $p$ and by 4.2.2 there exists a normal $p$-complement $K$ in $N$. Thus $N = KP$ and $K \cap P = 1$, and since $K$ is characteristic in $N \leq G$, it follows that

(10) $K \leq G$ such that $G = KS$ and $K \cap S = 1$.

If $S \leq G$, then $G = S \times K$ is not a counterexample since $(|S|, |K|) = 1$. Thus

(11) $S$ is not normal in $G$.

Suppose that $K$ is not a primary group, and let $r$ be a prime dividing $|K|$. By 4.1.3(d) there exists an $S$-invariant Sylow $r$-subgroup $R$ of $K$ and $\varphi$ induces a projectivity from $RS$ to $(RS)^o$ that is singular of the second kind at $p$. Since $K$ is not an $r$-group, $RS < G$ and the minimality of $G$ implies that $S \leq RS$. Now $K$ is generated by its
Sylow subgroups and it follows that $K \leq N_G(S)$. Hence $S \subseteq G$, contradicting (11). Thus

(12) $K$ is an $r$-group for some prime $r$.

Let $M$ be a maximal subgroup of $G$ containing $S$. By (10), $M = LS$ where $L = M \cap K$ and the minimality of $G$ implies that $M = L \times S$. Since $K$ is an $r$-group and $L < K$, there exists $g \in N_K(L)/L$. Now $M^g = M$ would imply that $M \leq \langle M, g \rangle = G$ and hence that $S \leq G$ as a characteristic subgroup of $M$; this would contradict (11).

Thus $M^g \neq M$ and $M^g = L^g \times S^g = L \times S^g$ implies that $L \leq M \cup M^g = G$. By 1.6.7, $M^e = L^e \times S^e$ and $(M^g)^e = L^e \times (S^g)^e$; hence also $L^e \leq M^e \cup (M^g)^e = G$. It follows that $\varphi$ induces a projectivity from $G/L$ to $\tilde{G}/L^e$ that maps $PL/L$ to $P^eL^e/L^e \simeq P^e$ and $SL/L$ is a $P$-group containing $PL/L$ as a proper normal subgroup. Therefore if $L \neq 1$, the induction assumption would imply that $SL/L \leq G/L$ and hence that $M = SL \leq G$, contradicting $M^g \neq M$. Thus $L = 1$, that is,

(13) $S$ is a maximal subgroup of $G$.

Let $P^e_1$ be the Sylow $p$-subgroup of $S^e$. Then $P \cap P_0$ is a maximal subgroup of $P$. We want to show that $|P| = p$ and suppose, for a contradiction, that $|P| \geq p^2$. Then there exists a maximal subgroup $D$ of $P$ different from $P \cap P_0$. And since $S \cap D \leq P(2, p)$, there are two different maximal subgroups $S_1$ and $S_2$ of $S$ such that $S_1 \neq S_2$ and $S_1 \cap S_2 = D$. Then $D = S_i \cap P$ is a Sylow $p$-subgroup in $G_i = K S_i$ for $i = 1, 2$. Since $D \leq P_0$, we see that $D^e$ is not a $p$-group and $S_i \leq G_i$ is a $P$-group containing $D$ as a proper normal subgroup. Thus $\varphi$ induces projectivities in the $G_i$ which are singular of the second kind at $p$ and the minimality of $G$ implies that $S_i \leq G_i$ for $i = 1, 2$. Hence $S_1, S_2$ and therefore also $S = S_1 \cup S_2$ are normalized by $K$. It follows that $S \leq G$, a contradiction. Thus $|P| = p$ and

(14) $|S| = pq$.

Let $x \in S^e$ such that $(P^e)^x \neq P^e$. Then $\tau: L(G) \to L(G)$ defined by $X^\tau = X^{\varphi x \varphi^{-1}}$ for $X \leq G$ is an autoprojectivity of $G$ satisfying $P \neq P^\tau \leq S' = S$. By (14), $P^\tau$ is a Sylow $q$-subgroup of $S$ and $S = P \cup P^\tau$. Since $S$ cannot operate fixed-point-freely on $K$ (see Robinson [1982], p. 298), there exist nontrivial subgroups $H$ of $K$ and $U$ of $S$ such that $[H, U] = 1$, that is, $HU = H \times U$. If $P \leq U$, then $P \leq H \cup S = G$ by (13). And if $P \leq U$, then $U$ is a Sylow $q$-subgroup of $S$ and there exists $y \in S$ such that $U^y = P^\tau$. Then $(HU)^y = H^y \times P^\tau$ and, by 1.6.7, $(HU)^{y^{-1}} = H^{y^{-1}} \times P$. Since $C_G(P) = P$, we have $H^{y^{-1}} \not\leq S$ and hence $P \leq H^{y^{-1}} \cup S = G$. Thus in both cases $P \leq G$, hence $PK = P \times K$ and $(PK)^\tau = P^\tau \times K^\tau$. Consequently $K^\tau$ normalizes $P$ and $P^\tau$ and therefore also $P \cup P^\tau = S$. Since $K^\tau \cup S = (K \cup S)^\tau = G$, it follows that $S \leq G$, a final contradiction.

The following terminology will simplify our discussion.

**$P$-decompositions**

A $P$-decomposition of a finite group $G$ is a pair $(S, T)$ of subgroups of $G$ such that $G = S \times T$, $(|S|, |T|) = 1$ and $S$ is a $P$-group. We call $G$ $P$-decomposable if there
exists a $P$-decomposition of $G$; otherwise $G$ is called $P$-indecomposable. Note that $T$ is allowed to be trivial so that a $P$-group is $P$-decomposable. Note further that $P$-decompositions are preserved by projectivities; they are even fixed by autoprojectivities.

4.2.4 Lemma. Let $(S, T)$ be a $P$-decomposition of $G$.

(a) If $\varphi$ is a projectivity from $G$ to $G$, then $(S^\varphi, T^\varphi)$ is a $P$-decomposition of $G$.

(b) If $\sigma$ is an autoprojectivity of $G$, then $S^\sigma = S$ and $T^\sigma = T$.

Proof. (a) By 1.6.6, $G = S^\varphi \times T^\varphi$ where $(|S^\varphi|, |T^\varphi|) = 1$ and, by 2.2.5, $S^\varphi$ is a $P$-group. Thus $(S^\varphi, T^\varphi)$ is a $P$-decomposition of $G$.

(b) Suppose that $S \in P(n, p)$ and let $P$ be the Sylow $p$-subgroup of $S$. By (a), $G = S^\varphi \times T^\varphi$ where $(|S^\varphi|, |T^\varphi|) = 1$ and $S^\varphi \in P(n, p)$. Therefore $p$ divides $|S^\varphi|$ and hence $T^\varphi$ is a $p'$-group and $P \leq S^\varphi$. It follows that $T^\varphi \leq C_G(P) = P \times T$ and, as a $p'$-group, $T^\varphi \leq T$. Since a finite group has no projectivity onto a proper subgroup, $T^\varphi = T$. By 1.6.4, $T$ has only one complement in $G$ and this implies that $S^\varphi = S$.

We show next that autoprojectivities of $P$-indecomposable groups map Sylow subgroups onto Sylow subgroups.

4.2.5 Theorem. Let $p$ be a prime, $G$ a finite group, $P$ a Sylow $p$-subgroup of $G$, $|P| = p^n$ where $n \in \mathbb{N}$ and suppose that there is no $P$-decomposition $(S, T)$ of $G$ such that $P < S$.

(a) Then $P^\sigma$ is a Sylow subgroup of $G$ for every $\sigma \in P(G)$.

(b) Let $\pi$ be the set of primes dividing $|P^\sigma|$ for some $\sigma \in P(G)$. If $\pi \neq \{p\}$, then $P$ is cyclic and there exists a normal $\pi$-complement $D$ in $G$ with cyclic factor group $G/D$ of order $\prod_{q \in \pi} q^{\sigma}$. Furthermore $D = D^\tau$ for all $\tau \in P(G)$ and $P(G)$ operates transitively on the set of normal $\pi$-complements ($q \in \pi$) of $G$.

Proof. We first prove the following assertion.

(15) Let $q$ be a prime, $Q \in \text{Syl}_q(G)$ and $\tau \in P(G)$ such that $P = Q$ or $P \leq Q^\tau$. If $|Q^\tau| \neq |Q|$, then $Q$ is cyclic and has a normal complement in $G$.

For, if $\tau$ were singular of the second kind at $q$, then by 4.2.3 there would exist a $P$-decomposition $(S, T)$ of $G$ such that $Q < S$. Then also $Q^\tau < S^\tau = S$ by 4.2.4. Since $P = Q$ or $P \leq Q^\tau$, it would follow that $P < S$, contradicting our assumption. Thus $\tau$ is singular of the first kind at $q$ and by 4.2.2 there exists a normal $q$-complement in $G$. It follows that $Q^\tau$ also has a normal $q$-complement and therefore cannot be a $P$-group of order $q^mr$ where $q > r \in \mathbb{P}$; by 2.2.6, $Q$ is cyclic. This proves (15).

(a) Suppose, for a contradiction, that $P^\sigma$ is not a Sylow subgroup of $G$. Then, in particular, $|P^\sigma| \neq |P|$ and, by (15), $P$ is cyclic. Hence $P^\sigma$ is a $q$-group for some prime $q$ and there exists a Sylow $q$-subgroup $Q$ of $G$ such that $P^\sigma < Q$. Since $P \in \text{Syl}_p(G)$, the subgroup $Q^{\sigma^{-1}}$ is not of prime power order. In particular, $|Q^{\sigma^{-1}}| \neq |Q|$ and therefore $\tau = \sigma^{-1}$ and $Q$ satisfy the assumptions of (15); it follows that $Q$ is cyclic. But then $Q^{\sigma^{-1}}$ has prime order, a contradiction.
(b) Let \( p \neq q \in \pi \) and let \( \sigma \in P(G) \) such that \( q \) divides \( |P^\sigma| \). By (15), \( P \) is cyclic and has a normal complement \( N_p \) in \( G \). By (a), \( P^\sigma = Q \) is a Sylow \( q \)-subgroup of \( G \) and again (15), applied to \( Q \) and \( \tau = \sigma^{-1} \), shows that \( Q \) is cyclic and has a normal complement \( N_q \) in \( G \). The intersection \( D \) of all these normal \( q \)-complements \( N_q \) where \( q \in \pi \) is a normal \( \pi \)-complement of \( G \) with cyclic factor group \( G/D \) of order \( \prod_{q \in \pi} q^n \).

Suppose, for a contradiction, that \( D^r \neq D \) for some \( \tau \in P(G) \). Then \( D^r D/D \neq 1 \) and hence there exists \( r \in \pi \) dividing \( |D^r| \); let \( R \leq D^r \) such that \( |R| = r \). By (a) and the definition of \( \pi \) there exists \( v \in P(G) \) such that \( P^v \in Syl_q(G) \) and hence \( R \leq (P^v)^x \) for some \( x \in G \). By (a), \( ((P^v)^x)^{-1} \) is a Sylow \( s \)-subgroup of \( G \) for some \( s \in \pi \) and since \( 1 \neq R^x \leq D \cap ((P^v)^x)^{x^{-1}} \), it follows that \( s \) divides \( |D| \). This is a contradiction since \( D \leq N_q \), a normal \( s \)-complement in \( G \). Thus \( D^r = D \) for all \( \tau \in P(G) \).

Therefore every \( \tau \in P(G) \) induces an autoprojectivity \( \bar{\tau} \) in the cyclic group \( G/D \). If \( q \in \pi \) and \( \sigma \in P(G) \) such that \( P^\sigma \in Syl_q(G) \), then \( \bar{\sigma} \) maps the Sylow \( p \)-subgroup \( PD/D \) of \( G/D \) onto the Sylow \( q \)-subgroup \( P^\sigma D/D \) and hence maps the unique complement \( N_p/D \) of \( PD/D \) in \( G/D \) to the unique complement \( N_q/D \) of \( P^\sigma D/D \). It follows that \( N_p^\sigma = N_q \) and \( P(G) \) operates transitively on the set of normal \( q \)-complements \( (q \in \pi) \) of \( G \).

Simple examples for the situation described above can be found in cyclic groups. It is easy to see that if \( m, n \in \mathbb{N} \), \( G = C_m \) and \( \{p_1, \ldots, p_r\} \) is the set of primes \( p \) for which \( p^n \) is the largest power of \( p \) dividing \( m \), then \( P(G) \) induces the full symmetric group \( S_r \) on the set of \( p_i \)-complements of \( G \) (cf. Exercise 1.4.2). Further examples are given in Exercises 2 and 3.

**4.2.6 Theorem (Suzuki [1951a]).** Let \( \varphi \) be a projectivity from the finite group \( G \) to the group \( \widehat{G} \) and suppose that \( P \) is a Sylow \( p \)-subgroup of \( G \) such that \( |P^\sigma| \neq |P| \); let \( |P| = p^n \). Then (a) or (b) holds.

(a) There exists a \( P \)-decomposition \( (S, T) \) of \( G \) such that \( P < S \); that is, \( G = S \times T \) where \( S \) is a \( P \)-group properly containing \( P \) and \( (|S|, |T|) = 1 \).

(b) There exists a subgroup \( N \) of \( G \) with the following properties.

(b1) \( N \leq G \), \( G = NP \) and \( N \cap P = 1 \); that is, \( N \) is a normal \( p \)-complement in \( G \).

(b2) Let \( K = \bigcap_{\sigma \in P(G)} N^\sigma \). If \( P \) is cyclic and \( \pi \) is the set of primes dividing \( |P^\sigma| \) for some \( \sigma \in P(G) \), then \( K \leq G \) and \( G/K \) is cyclic of order \( \prod_{q \in \pi} q^n \). If \( P \) is not cyclic, then \( P \) is elementary abelian, \( P^\sigma \) is a nonabelian \( P \)-group of order \( p^{n-1}q \) where \( p > q \in \mathbb{P} \) and \( K = N \).

(b3) \( N^\sigma \leq \widehat{G} \).

(b4) If \( (|\widehat{G}/N^\sigma|, |N^\sigma|) \neq 1 \), then there exist a \( P \)-group \( S > P \) and a subgroup \( M < N \) satisfying \( MS = G \) and \( M \cap S = 1 \) such that \( M \) and \( M^\sigma \) are normal Hall subgroups of \( G \) and \( G \), respectively, and \( |S| = r^{m-1} \), \( |S^\sigma| = r^m \) where \( p < r \in \mathbb{P} \) and \( 2 \leq m \in \mathbb{N} \).

(b5) If \( |P| > p \) or \( |P| = p > |P^\sigma| \), then \( N^\sigma \) is a normal Hall subgroup of \( \widehat{G} \).
4.2 Singular projectivities

Proof. Suppose that (a) does not hold. Then by 4.2.3 and 4.2.2, \( \varphi \) is singular of the first kind at \( p \) and there exists a normal \( p \)-complement \( N \) in \( G \). Thus \( N \) satisfies (b1) and we want to show that it also has the other properties in (b).

By 2.2.6, \( P \) is cyclic or elementary abelian and, in the latter case, \( P^e \) is a non-abelian \( P \)-group; hence in (b2) we only have to prove the statements on \( K \). These are clearly satisfied if \( N \) is invariant under \( P(G) \); for, in that case, \( |P^e| = |G:N| = |P| \) for all \( \sigma \in P(G) \) and hence \( \pi = \{ p \} \). So suppose that there exists \( \tau \in P(G) \) such that \( N^\tau \neq N \). Then \( p \) divides \( |N^\tau N/N| = |N^\tau : N \cap N^\tau| \) and there exists a Sylow \( p \)-subgroup \( P^x \) of \( G \) such that \( P^x \cap N^\tau \neq 1 \). Therefore \( (P^x)^{x^{-1}} \cap N \neq 1 \), hence \( (P^x)^{x^{-1}} \) is not a \( p \)-group and \( \pi \neq \{ p \} \). Since (a) does not hold, the assumptions of 4.2.5 are satisfied. It follows that \( P \) is cyclic and \( G \) has a normal \( \pi \)-complement \( D \) with cyclic factor group \( G/D \) satisfying \( D^\sigma = D \) for all \( \sigma \in P(G) \). Since \( D \leq N \), this implies that \( D \leq K \). But \( P(G) \) operates transitively on the set of normal \( q \)-complements (\( q \in \pi \)), hence every such complement is of the form \( N^\sigma \) where \( \sigma \in P(G) \) and it follows that \( D = K \). Thus (b2) holds.

If \( \tau \in P(\tilde{G}) \), then \( \varphi \tau \varphi^{-1} \in P(G) \). Since \( K \) is invariant under \( P(G) \), it follows that \( K^\varphi = K^\varphi \); in particular, \( K^\varphi \leq \tilde{G} \). Thus \( N^\varphi \leq \tilde{G} \) if \( K = N \); and if \( K < N \), we have just shown that \( G/K \) is cyclic. Then \( \tilde{G}/K^\varphi \) is cyclic and hence \( N^\varphi \leq \tilde{G} \) in this case also. Thus (b3) holds.

Now let \( r \) be a prime dividing \( (|\tilde{G}/N^\varphi|, |N^\varphi|) \), let \( R^\varphi \in \text{Syl}_r(\tilde{G}) \) and \( |R^\varphi| = r^m \). Then \( R^\varphi \cap N^\varphi \) is a Sylow \( r \)-subgroup of \( N^\varphi \) and hence \( 1 < R^\varphi \cap N^\varphi < R^\varphi \); thus \( 1 < R \cap N < R \). Since \( R \cap N \) is a normal \( p \)-subgroup of \( R \) and \( R/R \cap N \simeq RN/N \) is a \( p \)-group, it follows from 2.2.6 that \( R^\varphi \) is elementary abelian and \( R \in P(m,r) \). By 2.2.2, \( R \cap N \) is an \( r \)-group and \( |R| = r^{m-1} \) where \( r > p \). If \( P_1 \in \text{Syl}_r(G) \) such that \( R \cap P_1 \neq 1 \), then \( r \) divides \( |P_1^\varphi| \). Since \( r > p \), we have \( P_1^\varphi \notin P(n,p) \) and hence \( P_1^\varphi \) is a cyclic \( r \)-group. But the Sylow \( r \)-subgroups of \( \tilde{G} \) are elementary abelian, hence \( |P_1^\varphi| = r \) and \( |P_1| = p \). We have shown:

(16) If \( N^\varphi \) is not a Hall subgroup of \( \tilde{G} \), then \( |P| = p \).

We now apply the results proved so far to \( R^\varphi \) and \( \varphi^{-1} \). Clearly, \( \varphi^{-1} \) is singular at \( r \). If \( (S^e, T^e) \) were a \( P \)-decomposition of \( \tilde{G} \) such that \( R^\varphi < S^e \), then by 4.2.4, \( (S, T) \) would be a \( P \)-decomposition of \( G \) satisfying \( R < S \). Therefore \( p \) would divide \( |S| \) and it would follow that \( P < S \), a contradiction since we assume that (a) is not true for \( P \). Thus (a) does not hold for \( R^\varphi \) and hence \( R^\varphi \) satisfies the parts of (b) we have already proved. In particular, \( \tilde{G} \) has a normal \( r \)-complement \( M^\varphi \) such that \( M \leq G \) and since \( r^2 \) divides \( |R^\varphi| \), (16) shows that \( M \) is a Hall subgroup of \( G \). Now \( p \) divides \( |R| \) and \( R \) is a complement to \( M \) in \( G \). Therefore \( (p, |M|) = 1 \) and hence \( M < N \) and \( P \cap M = 1 \). Thus \( P^\varphi \cap M^\varphi = 1 \) and \( |P^\varphi| = r \); let \( S^e \in \text{Syl}_r(\tilde{G}) \) such that \( P^\varphi \leq S^e \). Then \( R^\varphi \) and \( S^e \) are complements to \( M^\varphi \) in \( \tilde{G} \), hence \( R \) and \( S \) are complements to \( M \) in \( G \) and it follows that \( S \simeq G/M \simeq R \) is a \( P \)-group of order \( r^{m-1}p \) and \( |S^e| = r^m \). Thus (b4) holds and (b5) follows from the fact that \( |P^\varphi| = r > p = |P| \) in (b4). □

We emphasize the following consequences of Suzuki's theorem since they are often sufficient to obtain the applications.

4.2.7 Theorem. If \( \varphi \) is a projectivity from the finite group \( G \) to the group \( \tilde{G} \), then there exists a normal Hall subgroup \( N \) of \( G \) such that
(i) \( N^p \leq \bar{G} \),

(ii) \( G/N \) is a direct product of coprime groups which are P-groups or cyclic \( p \)-groups, and

(iii) for every prime \( p \) dividing \( |N| \), \( \varphi \) is regular at \( p \); in particular, \( \varphi \) induces an index preserving projectivity in \( N \).

Proof. For every prime \( p \) for which \( \varphi \) is \( p \)-singular, we define a subgroup \( N_p \) of \( G \): If (a) of 4.2.6 holds and \((S, T)\) is the P-decomposition appearing there, we put \( N_p = T \); if (a) does not hold, then (b) is satisfied and we let \( N_p \) be the normal p-complement in \( G \). By 4.2.4 and 4.2.6, every \( N_p \) is a normal Hall subgroup of \( G \) such that \( N^p \leq \bar{G} \) and \( G/N_p \) is a P-group of order divisible by \( p \) or a cyclic \( p \)-group. Therefore the intersection \( N \) of all these \( N_p \) is a normal Hall subgroup of \( G \) satisfying \( N^p \leq \bar{G} \), that is, (i) holds. If \( G/N_p \) is a nonabelian P-group and \( q \) the second prime dividing \( |G/N_p| \), then \( G = S \times T \) where \( S \) is a P-group of order \( p^a q \) and \( |S|, |T| \) = 1. Thus \( \varphi \) is also singular at \( q \) but \( N_q = T = N_p \). Therefore the factor groups of \( G \) with respect to different \( N_p \) are coprime and it follows that \( G/N \) is isomorphic to the direct product of the different \( G/N_p \), that is, (ii) holds. Finally, by definition, \( \varphi \) is regular at \( p \) for every prime \( p \) dividing \( |N| \) and hence satisfies \( |S^p| = |S| \) for all Sylow subgroups \( S \) of \( N \). By 4.2.1, \( \varphi \) induces an index preserving projectivity in \( N \) and (iii) holds.

If \( \varphi \) is not index preserving, then the normal Hall subgroup \( N \) constructed in 4.2.7 is different from \( G \) and (ii) shows that there exists a normal Sylow complement in \( G \) with cyclic or elementary abelian factor group. Also by (ii), \( G'' \leq N \). Thus we get the following two corollaries.

4.2.8 Corollary. If \( G \) has no normal Sylow complement with cyclic or elementary abelian factor group, then every projectivity of \( G \) is index preserving.

4.2.9 Corollary. Every projectivity of a finite group \( G \) induces an index preserving projectivity in the second commutator subgroup \( G'' \).

We remark that the results of this section can be generalized to locally finite groups. This is fairly straightforward for the assertions on \( p \)-singular projectivities, but the argument requires the Zacher-Rips Theorem 6.1.7 for the other results. We shall carry this out for Corollary 4.2.9 in 6.5.9.

The structure of a finite group with a \( p \)-singular projectivity

Suzuki's theorem and its consequences are the main tools for handling singular projectivities. In the remainder of this section we are looking for restrictions on the structure of the normal \( p \)-complement \( N \) in (b) of 4.2.6 and the operation of the Sylow \( p \)-subgroup \( P \) on \( N \). The basic result here is that the operating group has to be cyclic.
4.2.10 **Theorem** (Schmidt [1972b]). Let \( \varphi \) be a projectivity from the finite group \( G \) to the group \( \bar{G} \), let \( P \) be a Sylow p-subgroup and \( N \) a normal p-complement in \( G \). Suppose that \( P^\varphi \) is a nonabelian P-group, let \( P^\varphi_0 \) be the Sylow p-subgroup of \( P^\varphi \) and \( Q \) be a subgroup of \( P \) such that \( |Q| = p \neq |Q^\varphi| \), that is, \( P = P_0 \times Q \). Then \( P_0 \leq Z(G) \) and every subgroup of \( P^\varphi_0 \) is normal in \( \bar{G} \); furthermore, \( G = NQ \times P_0 \) and \( \bar{G} = (N^\varphi \times P^\varphi_0)Q^\varphi \).

**Proof.** Since \( P^\varphi \) is a nonabelian P-group, \( P \) is elementary abelian of order at least \( p^2 \). It follows that there is no P-group \( S \) such that \( P < S \leq G \); for, since \( G \) has a normal p-complement, \( p \) must be the smallest prime dividing \( |S| \) and hence \( |P| = p \), a contradiction. We conclude that (b) of 4.2.6 holds for \( P \); in particular, \( N^\varphi \) is a normal Hall subgroup of \( \bar{G} \). By 4.1.2, \( C_N(A)^\varphi = C_{N^\varphi}(A^\varphi) \) for all \( A \leq P \).

Let \( A \) be a maximal subgroup of \( P \) different from \( P_0 \) and take \( B < P \) such that \( P = A \times B \). If \( b \in B \), then \( C_N(A)^\varphi = C_N(A^\varphi) = C_N(A) \), that is \( B \) normalizes \( C_N(A) \). By 4.1.2, \( C_N(A)^\varphi = C_{N^\varphi}(A^\varphi) \) is normalized by \( B^\varphi \). Since \( A^\varphi \) is not a p-subgroup of the P-group \( P^\varphi = A^\varphi \cup B^\varphi \), it is not normalized by \( P^\varphi \) and there exists \( x \in B^\varphi \) such that \( (A^\varphi)^x \neq A^\varphi \). Hence \( P^\varphi = A^\varphi \cup (A^\varphi)^x \) and

\[
C_{N^\varphi}(P^\varphi) = C_{N^\varphi}(A^\varphi) \cap C_{N^\varphi}((A^\varphi)^x) = C_{N^\varphi}(A^\varphi) \cap C_{N^\varphi}(A^\varphi)^x = C_{N^\varphi}(A^\varphi);
\]

it follows that \( C_N(P) = C_N(A) \). It is well-known (see Suzuki [1986], p. 216) that

\[
N = \langle C_N(A) | A \leq P, |P : A| = p \rangle
\]

and we have just shown that \( C_N(A) = C_N(P) \) is contained in \( C_N(P_0) \) if \( A \neq P_0 \). Hence \( N = C_N(P_0) \) and since \( P \) is abelian, it follows that \( P_0 \) is centralized by \( NP = G \). By 1.6.7, \( (NP_0)^\varphi = N^\varphi \times P^\varphi_0 \) and, as every subgroup of \( P^\varphi_0 \) is normal in the P-group \( P^\varphi \), every such subgroup is normalized by \( N^\varphi P^\varphi = \bar{G} \). Finally, since \( P = Q \times P_0 \), we conclude that \( G = NP = NQ \times P_0 \) and \( \bar{G} = N^\varphi P^\varphi = (N^\varphi \times P^\varphi_0)Q^\varphi \). \( \square \)

The above theorem reduces the problem of determining the structure of a group with a p-singular projectivity to the study of groups with cyclic Sylow p-subgroups.

4.2.11 **Theorem.** Let \( G \) be a finite group with elementary abelian Sylow p-subgroups of order \( p^n \), \( n \geq 2 \). Then \( G \) has a p-singular projectivity if and only if either (a) or (b) holds.

(a) \( G = S \times T \) where \( S \) is a P-group of order \( p^q \), \( p > q \in \mathbb{P} \) and \( (|S|, |T|) = 1 \).

(b) There exist subgroups \( G_0 \) and \( P_0 \) of \( G \) satisfying \( G = G_0 \times P_0 \) and \( |P_0| = p^{n-1} \) and then a projectivity \( \psi \) from \( G_0 \) to a group \( G_1 \) and a Sylow p-subgroup \( Q \) of \( G_0 \) such that \( (p, |G_1|) = 1 \) and \( |Q^\psi| \) divides \( p - 1 \).

**Proof.** Let \( \varphi \) be a p-singular projectivity from \( G \) to a group \( \bar{G} \) and let \( P \in \text{Syl}_p(G) \) such that \( |P^\varphi| \neq |P| \). If there exists a P-decomposition \( (S, T) \) of \( G \) such that \( P < S \), then, since \( |P| \geq p^2 \), \( p \) is the larger prime dividing \( |S| \) and (a) holds. If there is no such P-decomposition, then by 4.2.6 there exists a normal p-complement \( N \) in \( G \) such that \( N^\varphi \) is a normal Hall subgroup of \( \bar{G} \). Let \( P^\varphi_0 \) be the Sylow p-subgroup of \( P^\varphi \), and let
Projectivities and arithmetic structure of finite groups

Q ≤ P satisfy |Q| = p ≠ |Q^P| and G_0 = NQ; let G_1 = G^Q and ψ be the projectivity induced by ϕ in G_0. By 4.2.10, G = G_0 × P_0 and, since P^ψ is a nonabelian P-group, |P_0| = p^{n-1} and |Q^P| divides p − 1. Finally, since N^ψ is a normal Hall subgroup of G and p divides |G/N^ψ|, p does not divide |N^ψ| = |G_1|. Thus (b) is satisfied.

Conversely, if (a) holds, then there exist p-singular autoprojectivities of G; for, L(G) ∼ L(S) × L(T) and hence every autoprojectivity of S can be extended to an autoprojectivity of G. So, finally, suppose that G = G_0 × P_0 and ψ is a projectivity from G_0 to a group G_1 with the properties given in (b). Then ψ is singular at p and we show first that we may assume,

(17) there is a normal p-complement N in G_0 such that N^ψ is a normal Hall subgroup in G_1.

This is clear if (b) of 4.2.6 holds for ψ; for, since |Q^ψ| divides p − 1, |Q| = p > |Q^ψ| and the assertion follows from (b5). If (a) if 4.2.6 holds, then G_0 = S × T and G_1 = S^ψ × T^ψ where S is a P-group containing Q and (|S^ψ|, |T^ψ|) = 1 = (|S|, |T|). Since p does not divide |G_1|, p is the smallest prime dividing |S| and hence |S| = r^m p where p < r ∈ P; also |S^ψ| = r^m q since |Q^ψ| = q < p < r. Because L(G) ∼ L(S) × L(T), there exists a projectivity from G_0 to G_1, mapping Q to Q'' the Sylow r-subgroup R of S to the Sylow r-subgroup of S^ψ and inducing ψ in T. We may assume that ψ is this projectivity and then N = R × T is a normal p-complement in G_0 and N^ψ = R^ψ × T^ψ is a normal Hall subgroup of G_1. Thus (17) holds.

Now, clearly, N is also a normal p-complement in G and H = Q × P_0 is a Sylow p-subgroup and hence a complement to N in G. Let G be the semidirect product of an elementary abelian p-group P_1 of order p^{n-1} by G_1 such that P_1 is centralized by N^ψ, and Q^ψ induces a nontrivial power automorphism in P_1. Then K = P_1Q^ψ is a P-group of order p^{n-1}|Q^ψ| and is a complement to the normal Hall subgroup N^ψ of G. If N is centralized by Q, then by 1.6.7, [N^ψ, Q^ψ] = 1 and there exists a projectivity from G = N × H to G = N^ψ × K which satisfies H^ψ = K and therefore is singular at p. So suppose that [N, Q] ≠ 1 and hence also [N^ψ, Q^ψ] ≠ 1. Then C_H(N) = P_0, C_K(N^ψ) = P_1 and G/P_0 ∼ G_0, G/P_1 ∼ G_1. Thus ψ induces a projectivity µ from G/C_H(N) to G/K(N^ψ) mapping NC_H(N)/C_H(N) to N^ψC_k(N^ψ)/C_k(N^ψ) and H/C_H(N) to K/C_K(N^ψ). Of course there is a projectivity τ from H to K mapping P_0 to P_1 and Q to Q'' by 4.1.9 there exists a projectivity φ from G to G which satisfies H^φ = K and therefore is singular at p. □

If p and q are different primes and (|N|, pq) = 1, then by 1.6.4 there exists a p-singular projectivity from G = N × C_ψ to G = N × C_ψ. So it only makes sense to look for restrictions on the structure of the normal p-complement N in 4.2.6(b) if G is not the direct product of N and P. By 4.1.3, N = [N, P]C_N(P) and the examples in 4.1.7(d) show that [N, P] and C_N(P) can be elementary abelian groups of arbitrary order. We give examples of directly indecomposable groups in which C_N(P) is not soluble.

4.2.12 Example (Paulsen [1975]). (a) Let A, F be finite groups and N = AF be a semidirect product of A by F such that F induces power automorphisms on A. Let p and q be primes satisfying (pq, |N|) = 1, let P ∼ C_p and Q ∼ C_q, and suppose that
4.2 Singular projectivities

G = NP and \( \bar{G} = NQ \) are semidirect products of N by P and Q, respectively, such that \( C_N(P) = F = C_N(Q) \) and P and Q also induce power automorphisms on A. Then there exists a projectivity \( \varphi \) from G to \( \bar{G} \) satisfying \( N^\varphi = N \) and \( P^\varphi = Q \).

(b) It is possible to fulfill the assumptions of (a) for the following groups.

(i) \( F = S_n, n < p, n < q, \) A is a nontrivial abelian r-group for some prime r such that \( pq|r - 1 \) (for example \( n = 5, p = 7, q = 11, r = 463 \)), and \( C_F(A) = A_n \).

(ii) \( F = PGL(2, t) \) where \( (pq, (t - 1)t(t + 1)) = 1 \), A is a nontrivial abelian r-group for some prime r satisfying \( pq|r - 1 \) (for example \( t = 7, p = 5, q = 13, r = 131 \)), and \( C_F(A) = PSL(2, t) \).

Proof. If (i) or (ii) is satisfied, then \( p \neq 2 \neq q \) and hence A has fixed-point-free power automorphisms of order 2p and 2q. Therefore \( S_n \times P \) and \( S_n \times Q \) operate on A with kernel \( A_n \) inducing these automorphisms, and the corresponding semidirect products \( G = A(S_n \times P) \) and \( \bar{G} = A(S_n \times Q) \) have the structure described in (a) where \( N = A \), similarly for \( PGL(2, t) \). It remains to prove (a). For this we apply 4.1.6 to the normal Hall subgroups \( N = M \) of \( \bar{G} \) and \( G \), the identity \( \sigma: N \to M \) and the trivial autoprojectivity \( r \) from P to Q. By assumption, \( C_N(P) = F = C_M(Q) \) and hence (1) of 4.1 holds. Moreover, \( C_A(P) \leq C_N(P) = F \) and \( C_A(P) = 1 \) since \( F \cap A = 1 \). By 4.1.3, \( A = [A, P] \) \( C_A(P) = [A, P] \) and hence \( [N, P] = [AF, P] = [A, P] = A \). (Note that since P induces power automorphisms on \( A = [A, P] \), Cooper's theorem implies that \( A \) is abelian.) Therefore if \( U \leq N \) is normalized by P, then \( U = [U, P]C_U(P) \) where \( [U, P] \leq [N, P] = A \) and \( C_U(P) \leq C_N(P) = F \). Conversely, if \( V_1 \leq A \) and \( V_2 \leq F \), then \( V = V_1V_2 \) is a subgroup normalized by P since \( F \) and P normalize every subgroup of \( A \) and P centralizes F. Thus the groups \( V_1V_2 \) where \( V_1 \leq A \) and \( V_2 \leq F \) are precisely the P-invariant subgroups of N. The same holds for \( Q \) and hence also (2) of 4.1 is satisfied. It follows that there is a projectivity from \( G \) to \( \bar{G} \) mapping \( N \) to \( N \) and \( P \) to \( Q \).

Note that in the above examples, \( [N, P] \) is abelian. We can show (see Exercise 6) that in general \( [N, P] \) need not be abelian but leave the question open whether there are any restrictions on the structure of \( [N, P] \).

Exercises

1. Let \( G \) be a finite group and \( \varphi \) be a projectivity from \( G \) to a group \( \bar{G} \). Show that \( \varphi \) is index preserving if

(a) \( |H^\varphi| = |H| \) for every minimal subgroup \( H \) of \( G \), or

(b) \( |\bar{G}:M^\varphi| = |G:M| \) for every maximal subgroup \( M \) of \( G \).

2. Let \( p_1, \ldots, p_r \) be different primes, \( n \in \mathbb{N}, m = (p_1 \ldots p_r)^n, \) \( t \) a prime such that \( m \) divides \( t - 1 \) and suppose that \( G \) is the semidirect product of a cyclic group of order \( t \) by the subgroup of order \( m \) of its automorphism group. Show that \( P(G) \) induces the full symmetric group \( S_t \) on the set of \( p_t \)-complements of \( G \).
3. Let \( t \) be a prime and \( p_1, \ldots, p_4 \) be different primes dividing \( t - 1 \). Let \( N = N_1 \times \cdots \times N_4 \) where \( |N_i| = t \) for all \( i \), suppose that \( H = \langle a_1 \rangle \times \cdots \times \langle a_4 \rangle \) where \( o(a_i) = p_i \) and let \( G \) be the semidirect product of \( N \) by \( H \) in such a way that for all \( i \in \{1, \ldots, 4\} \), \( C_N(a_i) = 1 \) and the eigenspaces of the automorphism induced by \( a_i \) in \( N \) are \( N_i \times N_{i+1}, N_{i+2}, N_{i+3} \) (the indices taken modulo 4). Show that \( P(G) \) operates transitively on the set of \( p_i \)-complements of \( G \) but does not induce the full symmetric group \( S_4 \).

4. Let \( \varphi \) be a projectivity from the finite group \( G \) to the group \( \overline{G} \) and write \( G = S_1 \times \cdots \times S_r \times T \) where the \( S_i \) are \( P \)-groups \((i = 1, \ldots, r; r \geq 0)\), \( T \) is \( P \)-indecomposable and \( (|S_i|, |S_j|) = 1 = (|S_i|, |T|) \) for all \( i, j \in \{1, \ldots, r\} \) such that \( i \neq j \). Show that there exists a normal subgroup \( N \) of \( T \) such that \( T/N \) is cyclic, \( N^\varphi \leq \overline{G} \) and \( \varphi \) induces an index preserving projectivity in \( N \).

5. Let \( \varphi \) be a projectivity from the finite group \( G \) to the group \( \overline{G} \) and suppose that \( P_1, P_2 \in \text{Syl}_p(G) \) such that \( |P_1| \neq |P_2| \). Show that there exist a \( P \)-group \( S \) (containing \( P_1 \) and \( P_2 \)) of order \( r^m p \) where \( r > p \) and a subgroup \( T \) of \( G \) such that \( G = S \times T \) and \( (|S|, |T|) = 1 \).

6. Let \( r \geq 3 \) be a prime, \( N \) the nonabelian group of order \( r^3 \) and exponent \( r \) and let \( p, q \) be different odd primes dividing \( r + 1 \).

(a) Show that there exist automorphisms \( u \) and \( v \) of \( N \) such that \( o(u) = p \), \( o(v) = q \) and \([N, u] = N = [N, v] \).

(b) Show that the semidirect products \( N \langle u \rangle \) and \( N \langle v \rangle \) are lattice-isomorphic.

7. Let \( G \) and \( \overline{G} \) be groups such that \( L(\overline{G}) \cong L(G) \) and recall that for any group \( X \), we denote by \( \pi(X) \) the set of all primes dividing the order of an element of \( X \).

(a) If \( G \) is finite, show that \( |\pi(\overline{G})| \leq 2|\pi(G)| \).

(b) If \( G \) is locally finite and of finite exponent, show that \( \text{Exp} \overline{G} \) is finite.

(Note that there are Tarski groups \( G \) and \( \overline{G} \) such that \( \text{Exp} G \) is finite and \( \text{Exp} \overline{G} \) is infinite.)

8. Generalize 4.2.2, 4.2.3, and 4.2.6 to locally finite groups.

### 4.3 \( O_p(G), O^p(G), \) Fitting subgroup and hypercentre

In this section we study projective images of characteristic subgroups of a finite group \( G \) that are defined, or at least definable, by arithmetic conditions.

**\( O_p(G) \) and the Fitting subgroup**

We begin with \( O_p(G) \), the largest normal \( p \)-subgroup, and \( F(G) = \bigcap_{p \in P} O_p(G) \), the Fitting subgroup of \( G \). Clearly, \( O_p(G) \) is the intersection of all the Sylow \( p \)-subgroups of \( G \) since this intersection is a normal \( p \)-subgroup of \( G \) and any normal \( p \)-subgroup of \( G \) is contained in every Sylow \( p \)-subgroup.

Now let \( \varphi \) be a projectivity from \( G \) to \( \overline{G} \). If \( \varphi \) and \( \varphi^{-1} \) are regular at \( p \), then the Sylow \( p \)-subgroups of \( G \) and \( \overline{G} \) are mapped onto each other by \( \varphi \) and \( \varphi^{-1} \) and hence also every characteristic subgroup of \( G \) that is defined lattice-theoretically by the
Sylow p-subgroups is mapped to the corresponding subgroup of $\overline{G}$. In particular, $O_p(G)^{\varphi} = O_p(\overline{G})$. If $\varphi$ is singular at $p$, we can use the results of §4.2 to see what happens to $O_p(G)$. It remains to consider the case that $\varphi$ is regular and $\varphi^{-1}$ singular at $p$.

4.3.1 Lemma. Let $p$ be a prime dividing $|G|$ and $\varphi$ a projectivity from $G$ to a group $\overline{G}$ such that $\varphi$ is regular at $\varphi^{-1}$ singular at $p$. Then there exist a normal Hall subgroup $N$ and a complement $S$ to $N$ in $G$ such that $S$ is a nonabelian $P$-group of order $p^aq$ for some prime $q < p$, $N^\varphi$ is a normal $p$-complement and $S^\varphi$ an elementary abelian Sylow $p$-subgroup of $G$. Moreover, the Sylow $p$-subgroup $P$ of $G$ is an elementary abelian normal subgroup of $G$, $P^\varphi \in Z(\overline{G})$ and, if $Q \leq S$ satisfies $|Q| = q$, then $G = (N \times P)Q$ and $\overline{G} = N^\varphi Q^\varphi \times P^\varphi$.

**Proof.** Since $\varphi^{-1}$ is singular at $p$, there exists a Sylow $p$-subgroup $T^\varphi$ of $\overline{G}$ such that $|T| \neq |T^\varphi|$. Suppose, for a contradiction, that there is a $P$-decomposition $(U^\varphi, V^\varphi)$ of $\overline{G}$ such that $T^\varphi < U^\varphi$. By 4.2.4, $(U, V)$ is a $P$-decomposition of $G$. Since $\varphi$ is regular at $p$ and $(p, |V^\varphi|) = 1$, $p$ does not divide $|V|$ and hence $p$ divides $|U|$. Suppose first that $U$ and $U^\varphi$ lie in $P(n, p)$ for some $n \in \mathbb{N}$. Then $|U^\varphi| = p^{s-1}q$ for some prime $q < p$ since $T^\varphi$ is a proper subgroup of $U^\varphi$. Now $\varphi$ is regular at $p$ and this implies that $|U| = p^{s-1}r$ for some prime $r < p$ and that the Sylow $p$-subgroup of $U$ is mapped to the Sylow $p$-subgroup $T^\varphi$ of $U^\varphi$. Hence $|T| = |T^\varphi|$, a contradiction. It follows that $p$ is the smaller prime dividing $|U|$ and $|U^\varphi|$; hence $|U| = s^m p = |U^\varphi|$ for some prime $s > p$. Since $\varphi$ is regular at $p$, again the Sylow $p$-subgroups of $U$ have to be mapped onto those of $U^\varphi$ and we get the same contradiction $|T| = |T^\varphi|$ as before. Therefore there is no $P$-decomposition $(U^\varphi, V^\varphi)$ of $\overline{G}$ satisfying $T^\varphi < U^\varphi$ and by 4.2.6 there exists a normal $p$-complement $N^\varphi$ in $\overline{G}$ such that $N \vartrianglelefteq G$.

Let $P \in \text{Syl}_p(G)$. Then $|P^\varphi| = |P|$ since $\varphi$ is regular at $p$; let $S^\varphi$ be a Sylow $p$-subgroup of $G$ containing $P^\varphi$. Then $S^\varphi$ and $T^\varphi$ are complements to $N^\varphi$, hence $S$ and $T$ are complements to $N$ and therefore $|S| = [G : N] = |T| \neq |T^\varphi| = |S^\varphi|$. It follows that $P < S$ so that $S$ is not a primary group. By 4.2.6, $S^\varphi$ is elementary abelian, $S$ is a nonabelian $P$-group of order $p^aq$ for some prime $q < p$ and since $|S^\varphi| > p$, $N$ is a Hall subgroup of $G$. The remaining assertions of the lemma follow from 4.2.10 applied to $\varphi^{-1}$ and the Sylow $p$-subgroup $S^\varphi$ of $\overline{G}$.

It is clear that if $G = S \times T$ and $\overline{G} = \overline{S} \times \overline{T}$ where $S$ and $\overline{S}$ lie in $P(n, p)$, $\overline{S}$ is nonabelian and $(|\overline{S}|, |T|) = (|\overline{S}|, |T|) = 1$, then there exists a projectivity $\varphi$ from $G$ to $\overline{G}$ mapping $O_p(G)$ to a subgroup of $\overline{G}$ which is not nilpotent. In particular, $F(G)^\varphi \neq F(\overline{G})$. If $G$ is $P$-indecomposable, the situation is better.

4.3.2 Lemma. Let $G$ be a $P$-indecomposable finite group and let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$.

(a) For every prime $p$ there exists a prime $q$ such that $O_p(G)^\varphi = O_q(\overline{G})$.

(b) $F(G)^\varphi = F(\overline{G})$.

**Proof.** Clearly, (a) implies that $F(G)^\varphi = \left(\bigcup_{p \in P} O_p(G)\right)^\varphi \leq \bigcup_{q \in P} O_q(\overline{G}) = F(\overline{G})$. By 4.2.4, $\overline{G}$ too is $P$-indecomposable and hence we similarly get that $F(\overline{G})^{\varphi^{-1}} \leq F(G)$.
Thus $F(G)^p = F(\overline{G})$ and (b) holds. For the proof of (a), we may assume that $O_p(G) \neq 1$; otherwise every prime $q$ not dividing $|\overline{G}|$ satisfies $O_q(\overline{G}) = 1 = O_p(G)^p$. Furthermore, if $\phi$ and $\phi^{-1}$ are regular at $p$, then the Sylow $p$-subgroups of $G$ are mapped by $\phi$ onto those of $\overline{G}$ and hence their intersection $O_p(G)$ is mapped to the intersection $O_p(\overline{G})$ of the Sylow $p$-subgroups of $\overline{G}$.

Now let $\phi$ be singular at $p$ and $P \in \text{Syl}_p(G)$ such that $|P^p| \neq |P|$. Since $G$ is not $p$-decomposable, (b) of 4.2.6 is satisfied. In particular, $G$ has a normal $p$-complement $N$ and by 4.1.1, $C_p(N) = P = O_p(G)$.

If $|P| = p$, then, since $1 < O_p(G) \leq P$, $P = O_p(G)$ and hence $G = N \times P$. By 1.6.7, $\overline{G} = N^p \times P^p$ where $(|N^p|, |P^p|) = 1$ and thus $O_p(G)^p = P^p = O_q(\overline{G})$ for some prime $q$. So let $|P| \geq p^2$. Then $N^p$ is a normal Hall subgroup of $\overline{G}$ and therefore by 4.1.2 and 4.1.1, $O_p(G)^p = C_p(N)^p = C_p(N^p) = (P^p)_{\overline{G}}$. If $P$ is cyclic, then $P^p$ is a cyclic $q$-group for some prime $q$ and hence $(P^p)_{\overline{G}} = O_q(\overline{G})$. If $P$ is elementary abelian, then $P^p$ is normal in $\overline{G}$. Therefore $(P^p)_{\overline{G}}$ is contained in the Sylow $p$-subgroup of $P^p$ and hence $(P^p)_{\overline{G}} = O_p(\overline{G})$. (In fact, by 4.2.10, $(P^p)_{\overline{G}}$ is the full Sylow $p$-subgroup of $\overline{G}$.) In both cases, (a) holds.

Finally, let $\phi$ be regular and $\phi^{-1}$ singular at $p$. Then, in the notation of 4.3.1, the Sylow $p$-subgroup $P$ of $G$ is normal in $\overline{G}$, that is, $P = O_p(\overline{G})$, and the Sylow $p$-subgroup $S^p$ of $\overline{G}$ is not normal in $\overline{G}$ since $G$ is $P$-indecomposable. But $P^p \leq Z(\overline{G})$ and hence $O_p(\overline{G}) = P^p = O_p(G)^p$. 

\section*{The Fitting series and soluble groups}

Recall that the Fitting series of a finite group $G$ is defined inductively by $F_0(G) = 1$ and $F_k(G)/F_{k-1}(G) = F(G/F_{k-1}(G))$ for $k \in \mathbb{N}$.

4.3.3 Theorem (Schmidt [1972b]). If $\phi$ is a projection from the finite group $G$ to the group $\overline{G}$, then $F_k(G)^\phi = F_k(\overline{G})$ for all $k \geq 2$.

\textbf{Proof.} Suppose that the theorem is false, let $G$ be a minimal counterexample and take $k \geq 2$ such that $F_k(G)^\phi \neq F_k(\overline{G})$. If $G = S \times T$ where $S$ is a $P$-group and $(|S|, |T|) = 1$, then $\overline{G} = S^p \times T^p$ and the minimality of $G$ would imply that

$$F_k(G)^\phi = (S \times F_k(T))^\phi = S^p \times F_k(T^p) = F_k(\overline{G}),$$

a contradiction. Thus $G$ is $P$-indecomposable.

By 4.3.2, $F(G)^\phi = F(\overline{G})$. Hence if $F(G) = 1$, then $F(\overline{G}) = 1$ and $F_k(\overline{G}) = 1 = F_k(G)^\phi$, a contradiction. Thus $F(G) \neq 1$; put $F(G) = N$ and write $\overline{\phi}$ for the projection induced by $\phi$ in $G/N$.

Then

$$F_{k-1}(G/N)^{\overline{\phi}} = (F_k(G)/N)^{\overline{\phi}} = F_k(G)^{\phi}/N^p \neq F_k(\overline{G})/N^p = F_{k-1}(\overline{G}/N^p)$$

and since the assertion of the theorem is true in $G/N$, it follows that $k = 2$ and $F(G/N)^{\overline{\phi}} \neq F(\overline{G}/N^p)$. By 4.3.2 there exists a $P$-decomposition $(S/N, T/N)$ of $G/N$. Since $F(S)$ and $F(T)$ are nilpotent normal subgroups of $G$, $F(S) = N = F(T)$ and
hence

\[ F_2(G)/N = F(G/N) = F(S/N) \times F(T/N) = F_2(S)/N \times F_2(T)/N, \]

that is, \( F_2(G) = F_2(S)F_2(T) \). By 4.2.4, \((S^\phi/N^\phi, T^\phi/N^\phi)\) is a P-decomposition of \( G/N^\phi \) and hence also \( F_2(G) = F_2(S^\phi)F_2(T^\phi) \). Therefore if \( S < G \), the minimality of \( G \) would imply that \( F_2(S)^\phi = F_2(S^\phi) \) and \( F_2(T)^\phi = F_2(T^\phi) \), and hence \( F_2(G)^\phi = F_2(G) \), a contradiction. Thus \( S = G \), that is, \( G/N \) is a P-group in \( P(n, p) \), say.

Then the Fitting subgroups of \( G/N \) and of \( G/N^\phi \) are their Sylow \( p \)-subgroups and, since \( F(G/N)^\phi \neq F(G/N^\phi) \), \( \phi \) or \( \phi^{-1} \) is singular at \( p \). If \( \phi \) were regular and \( \phi^{-1} \) singular at \( p \), then by 4.3.1, the Sylow \( p \)-subgroup of \( G \) would be normal in \( G \) and hence would lie in \( F(G) \); this is impossible since \( p \) divides \( |G/N| \). Thus \( \phi \) is singular at \( p \) and since \( G \) is not P-decomposable, (b) of 4.2.6 holds. In particular, \( G \) has a normal \( p \)-complement. Then \( G/N \) also has a normal \( p \)-complement and it follows that \( G/N \) is elementary abelian of order \( p^n \) where \( n \geq 2 \). On the other hand, this implies that the Sylow \( p \)-subgroups of \( G \) are not cyclic and then 4.2.10 shows that \( p^2 \) does not divide \( |G/F(G)| \). This is a contradiction.

\[ \square \]

As a consequence of the above theorem we get a classical result that was proved independently by Suzuki and Zappa.

4.3.4 Theorem (Suzuki [1951a], Zappa [1951b]). If \( G \) is a finite soluble group and \( \phi \) a projectivity from \( G \) to a group \( \bar{G} \), then \( \bar{G} \) is soluble.

Proof. Since \( G \) is soluble, there exists \( k \geq 2 \) such that \( F_k(G) = G \). By 4.3.3, \( F_k(\bar{G}) = F_k(G)^\phi = \bar{G} \) and hence \( \bar{G} \) is soluble. \( \square \)

We shall give a simpler proof of this theorem in §5.3, together with a lattice-theoretic characterization of the class of finite soluble groups. Suzuki's proof was also shorter. He only needed 4.2.6 and the following lemma that is often useful; we leave it to the reader to construct a proof of Theorem 4.3.4 from 4.2.6 and 4.3.5.

4.3.5 Lemma. If \( M \) is a normal subgroup of index \( p \) in \( G \) and \( \phi \) a \( p \)-regular projectivity from \( G \) to \( \bar{G} \), then \( M^\phi \trianglelefteq \bar{G} \).

Proof. Let \( X^\phi \) be a \( p' \)-subgroup of \( \bar{G} \). Then \( X^\phi \leq M^\phi \) since otherwise \( p = |XM : M| = |X : X \cap M| \) would divide \( |X| \) and \( \phi \) would be singular at \( p \). Therefore the subgroup \( T \) generated by all the \( p' \)-subgroups of \( \bar{G} \) is contained in \( M^\phi \) and hence \( M^\phi \trianglelefteq \bar{G} \) since \( M^\phi / T \) is a maximal subgroup of the finite \( p \)-group \( \bar{G} / T \). \( \square \)

**O\(p\)(G) and the nilpotent residual**

Recall that \( O\(p\)(G) \) is the intersection of all normal subgroups \( N \) such that \( G/N \) is a \( p \)-group and \( G_\mathfrak{P} = \bigcap_{p \in \mathfrak{P}} O\(p\)(G) \) is the nilpotent residual, the smallest normal subgroup
with nilpotent factor group of $G$. Clearly $O^p(G)$ is the join of all the $p'$-subgroups of $G$; indeed this join is a normal subgroup whose factor group is a $p$-group and it is contained in any such normal subgroup of $G$.

4.3.6 Lemma. Let $\varphi$ be a projectivity from $G$ to $\overline{G}$. If $G/O^p(G)$ is not elementary abelian, then there exists a prime $q$ such that $O^p(G)^q = O^q(\overline{G})$.

Proof. If $\varphi$ is regular at $p$, then $\varphi^{-1}$ also is regular at $p$ since otherwise, by 4.3.1, the Sylow $p$-subgroup of $G$ and hence also $G/O^p(G)$ would be elementary abelian. Since $O^p(G)$ is the join of all the $p'$-subgroups of $G$, it follows that $O^p(G)^q = O^q(\overline{G})$ in this case. So suppose that $\varphi$ is singular at $p$ and let $P \in \text{Syl}_p(G)$ such that $|P^p| \neq |P|$. Again $P$ cannot be elementary abelian and hence $P$ is cyclic of order $p^n$ where $n \geq 2$. Therefore (b) of 4.2.6 holds; in particular, there exists a normal $p$-complement $N$ in $G$ such that $N^p$ is a normal Hall subgroup of $\overline{G}$. Then $|P^p| = q^n$ for some prime $q$ and $O^q(\overline{G}) = N^p = O^p(G)^q$.

4.3.7 Remark. The assumptions in 4.3.6 are stronger than those in 4.3.2, the corresponding result for $O_p(G)$, but they are necessary. It is clear that in certain $P$-decomposable groups, for example $G = S \times T$ where $S$ is a nonabelian $P$-group and $p$ the smaller prime dividing $|S|$, there are even autoprojectivities mapping $O^p(G)$ to a nonnormal subgroup of $G$. But with the hypothesis of Theorem 4.2.10, $O^p(G) = N$ and $\overline{G}/N^p$ is a nonabelian $P$-group; hence $O^p(G)^q \neq O^q(\overline{G})$ for every prime $r$. And $O^q(\overline{G}) = (NP_0)^q$ if $q$ is the smaller prime dividing $|P_0|$; however $NP_0$ is not an $O^p(G)$. That this situation actually occurs is easy to see. If we take primes $p$, $q$, $r$ such that $q \mid p - 1$ and $pq \mid r - 1$, then, by 4.2.11 or 4.1.6, the semidirect product $G = NP$ of a cyclic group $N$ of order $r$ by an elementary abelian group $P$ of order $p^2$ inducing an automorphism of order $p$ in $N$ has a projectivity $\varphi$ onto the semidirect product $\overline{G}$ of $N$ by a nonabelian group $\overline{P}$ of order $pq$ inducing an automorphism of order $q$ in $N$. Here $G$ is $P$-indecomposable, but $O^p(G) = N = G_\pi$ is mapped by $\varphi$ to the normal subgroup $N$ of $\overline{G}$ with nonnilpotent factor group $\overline{G}/N \simeq \overline{P}$, that is, neither to $\overline{G}_\pi$ nor to any $O^t(\overline{G})$ for $t \in \mathcal{P}$.

This example shows that we cannot prove the analogue of 4.3.2 for $O^p(G)$ or the nilpotent residual $G^\pi$. However, we shall show in § 5.4 that nevertheless the iterated nilpotent residuals behave under projectivities like the iterated Fitting subgroups, that is, they are mapped to the corresponding subgroups in the image group.

$O_p(G)$, $O^{p'}(G)$ and $p$-soluble groups

If we replace the prime $p$ in the definition of $O_p(G)$ and $O^p(G)$ by a set $\pi$ of primes, we obtain the largest normal $\pi$-subgroup $O_\pi(G)$ and the smallest normal subgroup $O^\pi(G)$ with factor group a $\pi$-group. Also these are, respectively, the intersection of all the maximal $\pi$-subgroups and the join of all the $\pi'$-subgroups of $G$; thus they are mapped by index preserving projectivities to the corresponding subgroups in the image group. We are mainly interested in the largest normal $p'$-subgroup $O_p(G)$ and
the smallest normal subgroup $O_{p'}(G)$ with factor group a $p'$-group. They are mapped to $O_{p'}(\bar{G})$ and $O_{p'}(\bar{G})$, respectively, by projectivities $\varphi$ from $G$ to $\bar{G}$ such that $\varphi$ and $\varphi^{-1}$ are regular at $p$. Recall that $G$ is $p$-soluble if its upper $p$-series

$$1 = P_0 \leq N_0 \leq P_1 \leq N_1 \leq \cdots \leq P_m \leq N_m \cdots$$

defined by $N_i/P_i = O_{p'}(G/P_i)$ and $P_{i+1}/N_i = O_{p'}(G/N_i)$ reaches $G$; the length of this series, the number of $p$-quotients in it, is called the $p$-length of $G$ and denoted by $l_p(G)$.

**4.3.8 Theorem.** If $G$ is a finite $p$-soluble group and $\varphi$ a projectivity from $G$ to a group $\bar{G}$, then $\bar{G}$ is $p$-soluble and $l_p(\bar{G}) = l_p(G)$ if $l_p(G) > 2$.

**Proof.** Suppose first that $l_p(G) \geq 2$. Then, by 4.2.6, $\varphi$ is regular at $p$ and, by 4.3.1, $\varphi^{-1}$ is also regular at $p$. Therefore every term of the upper $p$-series of $G$ is mapped onto the corresponding term in $\bar{G}$. In particular, $\bar{G}$ is $p$-soluble and $l_p(\bar{G}) = l_p(G)$.

Now suppose that $l_p(G) \leq 1$. Again if $\varphi$ and $\varphi^{-1}$ are regular at $p$, then $\bar{G}$ is $p$-soluble and $l_p(\bar{G}) = l_p(G)$. If $\varphi^{-1}$ is singular at $p$, then, by 4.2.6, $\bar{G}$ is $p$-soluble and $l_p(\bar{G}) = 1$. Finally, if $\varphi^{-1}$ is regular and $\varphi$ singular at $p$, then either $\bar{G}$ is a $p'$-group or we may apply 4.3.1 to $\varphi^{-1}$ and conclude that $\bar{G}$ has a normal Sylow $p$-subgroup. In both cases, $\bar{G}$ is $p$-soluble of $p$-length at most 1.

We shall need the following result that is similar to 4.1.2(a).

**4.3.9 Lemma.** Let $A$ and $B$ be subgroups of $G$ and suppose that $A$ is generated by $p$-elements and $B$ by $p'$-elements. If $\varphi$ is a projectivity from $G$ to a group $\bar{G}$ such that $\varphi$ and $\varphi^{-1}$ are regular at $p$, then $B \leq N_G(A)$ (or $A \leq N_G(B)$) if and only if $B^\varphi \leq N_{\bar{G}}(A^\varphi)$ (resp. $A^\varphi \leq N_{\bar{G}}(B^\varphi)$).

**Proof.** Suppose that $B \leq N_G(A)$, take a $p'$-element $b \in B$ and let $H = \langle A, b \rangle$. Then $A$ is a normal subgroup of $H$ generated by $p$-elements and $H/A$ is a $p'$-group; thus $A = O_{p'}(H)$ and hence $A^\varphi = O_{p'}(H^\varphi)$ since $\varphi$ and $\varphi^{-1}$ are regular at $p$. Therefore $A^\varphi$ is normalized by $\langle b \rangle^\varphi \leq H^\varphi$ and, since $B^\varphi$ is generated by these subgroups $\langle b \rangle^\varphi$, it follows that $B^\varphi \leq N_{\bar{G}}(A^\varphi)$. Now $A^\varphi$ is generated by $p$-elements and $B^\varphi$ by $p'$-elements. Thus if we apply the result just proved to $\varphi^{-1}$, we obtain the opposite implication. The equivalence of $A \leq N_G(B)$ and $A^\varphi \leq N_{\bar{G}}(B^\varphi)$ is proved in an entirely analogous way.

---

**The hypercentre**

Finally we discuss a characteristic subgroup that has not so much to do with the arithmetic structure of a group. It is the hypercentre $Z_\infty(G)$, the final term of the ascending central series of $G$. Unlike the iterated Fitting subgroups $F_1(G)$, the $n$-th centre $Z_n(G)$ in general is not mapped to $Z_n(\bar{G})$ by a projectivity $\varphi$ from $G$ to $\bar{G}$. For example, if $G$ is an abelian $P$-group, then $Z_n(G) = G$ for all $n$, but $Z_n(\bar{G}) = 1$ in a
lattice-isomorphic nonabelian $P$-group $\bar{G}$. Even if $G$ is $P$-indecomposable and $\varphi$ index preserving, the situation is not much better, as is shown by the abelian group $G$ of type $(p^n, p^{n-1})$ and the lattice-isomorphic $M$-group $\bar{G} = \langle a, b | a^{p^n} = b^{p^{n-1}} = 1, a^b = a^{1+p^n} \rangle$; here again $Z_k(G) = G$ for all $k$, but $Z_k(\bar{G}) \neq \bar{G}$ for $k = 1, \ldots, n-1$. So only under rather restrictive assumptions can we expect to be able to prove that $Z_k(G)^\varphi = Z_k(\bar{G})$; an example of such a result is contained in Theorem 5.3.4. But the hypercentre behaves better.

4.3.10 Theorem (Schmidt [1975a]). If $\varphi$ is an index preserving projectivity from the finite group $G$ to the group $\bar{G}$, then $Z_x(G)^\varphi = Z_x(\bar{G})$.

Proof. Let $p$ be a prime and $T = O_p(O_p(C_G(O_p(G))))$. We want to show that $T \leq Z_x(G)$ and $T^\varphi = O_p(O_p(C_{\bar{G}}(O_p(\bar{G})))) \leq Z_x(\bar{G})$. First of all, $T$ is a $p$-group and therefore contained in a Sylow $p$-subgroup $P$ of $G$. Hence there exists $n \in \mathbb{N}$ such that $T \leq Z_n(P)$ and, since $T \leq C_G(O_p(G))$ is centralized by every $p'$-element of $G$, it follows that $T \leq Z_n(G) \leq Z_x(G)$. Now $H = O_p(C_G(O_p(G)))$ and $K = O_p(G)$ satisfy the assumptions of 1.6.8 for $\pi = \{p\}$, and hence $K^\varphi = O_p(\bar{G})$ is centralized by $H^\varphi$. Since $H^\varphi$ is generated by $p$-elements, $O_p(C_G(O_p(G))^\varphi = H^\varphi \leq O_p(C_{\bar{G}}(O_p(\bar{G}))))$. This statement for $\varphi^{-1}$ yields the other inclusion and it follows that $T^\varphi = O_p(O_p(C_{\bar{G}}(O_p(\bar{G}))))$; in particular, $T^\varphi \leq Z_x(\bar{G})$.

To prove the theorem, we use induction on $|G| + |\bar{G}|$ and we may assume that $Z(G) \neq 1$, since otherwise we could consider $\varphi^{-1}$. Let $p$ be a prime dividing $|Z(G)|$. Then the Sylow $p$-subgroup of $Z(G)$ is contained in $T = O_p(O_p(C_G(O_p(G))))$ and hence $T \neq 1$. Since $T^\varphi = O_p(O_p(C_{\bar{G}}(O_p(\bar{G})))) \leq \bar{G}$, $\varphi$ induces a projectivity from $G/T$ to $\bar{G}/T^\varphi$ and, by induction, this projectivity maps $Z_x(G/T) = Z_x(G)/T$ onto $Z_x(\bar{G}/T^\varphi) = Z_x(\bar{G})/T^\varphi$. It follows that $Z_x(G)^\varphi = Z_x(\bar{G})$, as required. □

The example constructed in 4.3.7 shows that even projectivities between $P$-indecomposable groups in general do not map the hypercentres onto each other; in this example, $|Z_x(G)| = p$ whereas $Z_x(\bar{G}) = 1$. Therefore the assumption that $\varphi$ is index preserving cannot be replaced, as in 4.3.2 for the Fitting subgroup, by the $P$-indecomposability of the groups involved.

Exercises

1. If $\varphi$ is an index preserving projectivity from $G$ to $\bar{G}$, show that $F(G)^\varphi = F(\bar{G})$ and $G^\varphi = \bar{G}$.

2. Let $\varphi$ be a projectivity from $G$ to $\bar{G}$.
   (a) If $|G : O_p(G)| \neq p$, show that there exists a prime $q$ such that $O_p(G)^\varphi = O_q(\bar{G})$.
   (b) Show that the assertion in (a) need not hold if $|G : O_p(G)| \neq p$ is replaced by the assumption that $G$ is $P$-indecomposable.

3. If $G$ is $P$-indecomposable and $\varphi$ a projectivity from $G$ to $\bar{G}$, show that $O_p(G)^\varphi \leq \bar{G}$ for all $p \in \mathbb{P}$.

4. Prove Theorem 4.3.4 using only 4.2.6 and 4.3.5.
5. (Suzuki [1951a]) Let \( \varphi \) be a projectivity from \( G \) to \( \bar{G} \).

(a) If \( \varphi \) is index preserving and \( N \) a maximal normal subgroup of \( G \), prove that
\[
N^\varphi \subseteq \bar{G}.
\]

(b) Show that if \( G \) is perfect (that is \( G' = G \)), then \( \bar{G} \) is also perfect.

6. Let \( \pi \) be a set of primes and let \( A \) and \( B \) be subgroups of \( G \) such that \( A \) is generated by \( \pi \)-elements and \( B \) by \( \pi' \)-elements. If \( \varphi \) is an index preserving projectivity from \( G \) to \( \bar{G} \), show that \( B \leq N_G(A) \) if and only if \( B^\varphi \leq N_{\bar{G}}(A^\varphi) \).

7. Show that the assertions of 4.3.9 do not hold without the assumption that \( \varphi \) and \( \varphi^{-1} \) are \( p \)-regular.

4.4 Abelian \( p \)-subgroups and projectivities

In the last section of this chapter we investigate the projectivity induced in a Sylow \( p \)-subgroup \( P \) by an index preserving projectivity \( \varphi \) of \( G \). If \( G = P \times Q \), then \( L(G) \cong L(P) \times L(Q) \) and every projectivity from \( P \) to a \( p \)-group \( \bar{P} \) can be extended to a projectivity of \( G \) (to \( \bar{G} = \bar{P} \times \bar{Q} \)). This will no longer be true if \( P \) is not a direct factor of \( G \) or even if \( G \) is generated by its \( p' \)-elements; but very little is known about this problem. We shall study it first for abelian Sylow \( p \)-subgroups and then go on to show that for arbitrary \( P \), under suitable assumptions on \( p \) and the \( p \)-structure of \( G \), \( Z(P)^\varphi = Z(P^\varphi) \).

Abelian Sylow \( p \)-subgroups

4.4.1 Lemma. Let \( A \) be an abelian \( p \)-subgroup of \( G \), \( B \) a \( p' \)-subgroup of \( N_G(A) \) and suppose that \( \varphi \) is a projectivity from \( G \) to \( \bar{G} \) such that \( A^\varphi \) is a normal Sylow \( p \)-subgroup of \( (AB)^\varphi \). Then

(a) \( A^\varphi = [A^\varphi, B^\varphi] \times C_{A^\varphi}(B^\varphi) \),

(b) \( C_{A^\varphi}(B^\varphi) = C_A(B)^\varphi \),

(c) \([A^\varphi, B^\varphi] = [A, B]^\varphi \) is abelian and hence isomorphic to \([A, B]\).

Proof. By 4.1.3, \( A = [A, B] \times C_A(B) \) and 4.1.2 applied to the projectivity \( \psi \) induced by \( \varphi \) in \( AB \) shows that \([A, B]^\varphi = [A^\varphi, B^\varphi] \) and \( C_A(B)^\varphi = C_{A^\varphi}(B^\varphi) \). Thus \( A^\varphi = [A^\varphi, B^\varphi] \cup C_{A^\varphi}(B^\varphi) \) and \([A^\varphi, B^\varphi] \cap C_{A^\varphi}(B^\varphi) = 1 \). By (6) of §1.5, \([A^\varphi, B^\varphi] \leq A^\varphi \cup B^\varphi \), and we want to show that \( C_{A^\varphi}(B^\varphi) \leq A^\varphi \); then (a) and (b) will hold. Since \( C_A(B) \leq Z(AB) \) we have \([C_A(B), O^p(AB)] = 1 \) and, by 1.6.8, \([C_A(B)^\varphi, O^p((AB)^\varphi)] = 1 \). Our assumption on \( A^\varphi \) implies that \( \psi \) and \( \psi^{-1} \) are regular at \( p \) and hence \( O^p(AB)^\varphi = O^p((AB)^\varphi) \). It follows that \( C_{A^\varphi}(B^\varphi) = C_A(B)^\varphi \leq C_A(O^p((AB)^\varphi)) \leq C_{A^\varphi}(B^\varphi) \) and therefore \( C_{A^\varphi}(B^\varphi) = C_{A^\varphi}(O^p((AB)^\varphi)) \leq A^\varphi \). Thus \( A^\varphi = [A^\varphi, B^\varphi] \times C_{A^\varphi}(B^\varphi) \).

It remains to be shown that \([A^\varphi, B^\varphi]\) is abelian. As a projective image of an abelian group, \([A^\varphi, B^\varphi]\) is a \( p \)-group with modular subgroup lattice in which the quaternion group is not involved, that is, an \( M^* \)-group according to our definition in §2.3. If \([A^\varphi, B^\varphi]\) were not abelian, then, by 2.3.23, there would exist characteristic subgroups \( R > S \) of \([A^\varphi, B^\varphi]\) such that \([R, Aut[A^\varphi, B^\varphi]] \leq S \). It would follow
that \( R \leq A^o B^o \) and hence \( [R, B^o] \leq S \); on the other hand, by 4.1.3, \( R = [R, B^o] C_R(B^o) = [R, B^o] \) since \( C_R(B^o) = R \cap C_{A^o}(B^o) = 1 \). This contradiction shows that \( [A^o, B^o] = [A, B] \) is abelian and therefore isomorphic to \([A, B]\) since the type of a finite abelian \( p \)-group is determined by its subgroup lattice.

4.4.2 Theorem (Paulsen [1975]). Let \( G \) be a finite group with an abelian Sylow \( p \)-subgroup \( P \) and let \( \varphi \) be a \( p \)-regular projectivity from \( G \) to a group \( \tilde{G} \). Then \( P = P_1 \times P_2 \) where \( P_1 = P \cap O^p(G) \) and \( P_2 = P \cap Z(N_G(P)) \), \( P^o = P_1^o \times P_2^o \) and \( P^o \simeq P_1 \) is abelian. If \( P^o \) is not abelian, then \( \text{Exp} P_1 < \text{Exp} P_2 \).

Proof. Since \( P \) is a normal Hall subgroup of \( L = N_G(P) \), there exists a complement \( B \) to \( P \) in \( L \). By 4.1.3, \( P = [P, B] \times C_P(B) \); let \( P_1 = [P, B] \) and \( P_2 = C_P(B) \). Since \( P \) is abelian, \( P_2 = P \cap Z(N_G(P)) \). Furthermore, clearly, \( P_1 \leq P \cap L' \); on the other hand, \( L/B \simeq P/P \cap B^o \) is abelian, hence \( L' \leq B^o \) and therefore \( P \cap L' \leq P \cap B^o = [P, B] \) by 4.1.1. Thus \( P_1 = P \cap L' \). Since \( P \) is abelian, \( G' \leq O^p(G) \) and \( O^p(G)/G' \) is a \( p' \)-group; therefore \( P \cap O^p(G) = P \cap G' \). By Grün's First Theorem (see Robinson [1982], p. 283), \( P \cap G' = P \cap L' \). It follows that \( P_1 = P \cap G' = P \leq O^p(G) \), as desired. Now, by assumption, \( \varphi \) is regular at \( p \) and hence \( P^o \) is a \( p \)-group. If \( \varphi^{-1} \) is singular at \( p \), then the Sylow \( p \)-subgroups of \( \tilde{G} \) are abelian and the remaining assertions of the theorem hold trivially. So suppose that \( \varphi^{-1} \) is regular at \( p \). Then \( P^o \) is a normal Sylow \( p \)-subgroup of \((RB)^o \) and 4.4.1 implies that \( P^o = P_1^o \times P_2^o \), \( P^o \) is abelian and \( P_1^o \simeq P_1 \). Finally, as a projective image of an abelian group, \( P^o \) again is an \( M^* \)-group. Therefore if \( \text{Exp} P_1 \geq \text{Exp} P_2 \), then \( \text{Exp} P_1^o = \text{Exp} P^o \) and, by 2.3.16, \( P^o \) is abelian.

We note some immediate consequences of Paulsen's theorem.

4.4.3 Corollary. If \( G \) is a perfect finite group with an abelian Sylow \( p \)-subgroup \( P \), then \( P^o \simeq P \) for every projectivity \( \varphi \) of \( G \).

Proof. Recall that \( G \) is perfect if and only if \( G = G' \). Thus \( G = O^p(G) \), hence \( P_1 = P \) and, by 4.2.9, \( \varphi \) is index preserving. Now 4.4.2 yields that \( P^o = P_1^o \) is isomorphic to \( P \).

4.4.4 Corollary. Let \( G \) be a \( P \)-indecomposable finite group with an abelian Sylow \( p \)-subgroup \( P \) and let \( \varphi \) be a projectivity from \( G \) to \( \tilde{G} \) such that \( P^o \) is not isomorphic to \( P \). If \( P \) is homocyclic or generated by two elements, then \( G \) has a normal \( p \)-complement.

Proof. If \( \varphi \) is singular at \( p \), then, by 4.2.6, \( G \) has a normal \( p \)-complement; so suppose that \( \varphi \) is regular at \( p \). By 4.4.2, \( P = P_1 \times P_2 \) where \( P_1 = P \cap O^p(G) \), \( P^o = P_1^o \times P_2^o \), \( P_1^o \) is abelian and \( \text{Exp} P_1 < \text{Exp} P_2 \). We have to show that \( P_1 = 1 \); then it will follow that \( G/O^p(G) \simeq P/P \cap O^p(G) = P \) and \( O^p(G) \) is a normal \( p \)-complement in \( G \). If \( P \) is homocyclic of type \((p^n, \ldots, p^n)\), say, then every nontrivial direct factor of \( P \) contains an element of order \( p^n \); since \( \text{Exp} P_1 < \text{Exp} P \), it follows that \( P_1 = 1 \). If \( P \) is generated by two elements and \( P_1 \neq 1 \), then \( P_2 \) and hence also \( P_2^o \) would be cyclic; therefore \( P^o = P_1^o \times P_2^o \) would be abelian and so \( P^o \simeq P \), a contradiction. Thus in this case also, \( P_1 = 1 \).
In general, a finite group $G$ with abelian Sylow $p$-subgroup $P$ need not possess a normal $p$-complement if $P$ is mapped to a nonabelian group by an index preserving projectivity of $G$. This is shown by the following example, that, as Lemma 4.4.1, can be found both in Menegazzo [1974] and in Paulsen [1975].

4.4.5 Example. Let $p$ and $q$ be primes such that $q^p - 1$, $R = \langle a \rangle \times \langle b \rangle$ where $o(a) = p^2$, $o(b) = p$ the abelian group of type $(p^2, p)$, $S = \langle c, d | c^{p^2} = d^p = 1, c^d = c^{1+p} \rangle$ the nonabelian group lattice isomorphic to $R$ and $T$ a nonabelian group of order $pq$. Then there exists a projectivity from $G = R \times T$ to $\overline{G} = S \times T$ mapping the abelian Sylow $p$-subgroup of $G$ to the nonabelian Sylow $p$-subgroup of $\overline{G}$; clearly, $G$ has no normal $p$-complement.

Proof. The map $\sigma : G \to \overline{G}$ defined by $(a^i b^j t)^\sigma = c^i d^j t$ for $i, j \in \mathbb{Z}$ and $t \in T$ is certainly bijective. If $x = a^i b^j t$ and $y = a^k b^l t'$ where $i, j, k, l \in \mathbb{Z}$ and $t, t' \in T$, then

\[
(x^\sigma y^\sigma) \cdot (c^{i+k} d^{j+l} t t') = (xy)^\sigma \cdot (c^{i+k} d^{j+l} t t')^{-1}.
\]

Therefore to see that $(xy)^\sigma \in \langle x^\sigma, y^\sigma \rangle$, we only have to show that $[d^i, c^k] \in \langle x^\sigma, y^\sigma \rangle$. If $k \equiv 0 \pmod{p}$, then $[d^i, c^k] = 1$ and, if $k \not\equiv 0 \pmod{p}$, then $[d^i, c^k] \in \langle c^p \rangle = \langle (c^{k} d^{l})^p \rangle \subseteq \langle x^\sigma, y^\sigma \rangle$. Similarly, $(uv)^\sigma \in \langle u^\sigma, v^\sigma \rangle$ for $u, v \in \overline{G}$ and, by 1.3.1, $\sigma$ induces a projectivity from $G$ to $\overline{G}$ with the desired properties. Since $T$ has no normal $p$-complement, neither does $G$. \qed

Further results on projective images of groups with abelian Sylow $p$-subgroups are contained in Huppert [1960] and Seitz and Wright [1969]. Both papers are concerned with groups $G$ having a Sylow $p$-subgroup $P$ such that $L(P)$ is modular. Corollary 4.4.3, for example, also follows from a theorem of Seitz and Wright which asserts that $O^p(G) \neq G$ if $P$ is a nonabelian $M^*$-group (see Exercise 1).

**Normal abelian $p$-subgroups**

The crucial step in the proof of the main results of this section is to show that if $p > 2$, $G = O^p(G)$ and $Z$ is a normal subgroup of $G$ contained in the centre of a Sylow $p$-subgroup $P$ of $G$, then $Z^P \leq Z(P^p)$ for every index preserving projectivity of $G$. This will then be applied to $N_G(Z(P))$ in place of $G$. The proof of this result is quite long and will be given in the next three lemmas. The first two deal with the structure of $P^p$ and its normalizer in a minimal situation which will emerge in the course of this proof.

4.4.6 Lemma. Let $H$ be a $p$-group with modular subgroup lattice, $Z$ a homocyclic normal subgroup of $H$ of exponent $p^n$, and $Y$ a cyclic subgroup of $H$ that centralizes $Z \Omega(Z)$ and $\Omega(Z)$ but does not normalize every subgroup of $Z$. For $y \in Y$, write $D_Z(y) = \{ z \in Z | z^y = z^{1+p^{n-1}} \}$; note that $D_Z(y)$ is a subgroup of $Z$.

(a) If $Y \cap Z \leq W \leq Z$, then $Y \leq N_H(W)$.

(b) Either
or there exist a generator \( y \) of \( Y \) and an element \( v \in Z \) of order \( p^n \) such that

\[
(2) \quad |Z : D_Z(y)| = p \quad \text{and} \quad v^y = v^{1+\lambda p^{n-1}} \quad \text{where} \quad \lambda \neq 1 \pmod{p},
\]

or

\[
(3) \quad |Z : D_Z(y)| = p \quad \text{and} \quad v^y = v^{1+p^{n-1}w^{p^{n-1}}} \quad \text{where} \quad w \in D_Z(y) \quad \text{and} \quad o(w) = p^n.
\]

Proof. We may assume that \( H = ZY \). If \( Y \cap Z \leq W \leq Z \), then \( W = W \cap (Y \cap Z) = (W \cup Y) \cap Z \leq W \cup Y \), that is, \( Y \leq N_H(W) \), since \( L(H) \) is modular and \( Z \leq H \). Thus (a) holds.

To prove (b), first note that since \( Y \) does not normalize every subgroup of \( Z \) but centralizes \( \Omega(Z) \), \( Z \) is neither cyclic nor elementary abelian. In a direct product of \( Q_8 \) by an elementary abelian 2-group, however, every homocyclic subgroup is cyclic or elementary abelian. Therefore, by 2.3.8, \( Q_8 \) is not involved in \( H \), that is,

\[
(4) \quad H \text{ is an } M^*-\text{group}.
\]

Since \( Z/\Omega(Z) \) is centralized by \( Y, H/\Omega(Z) \) is abelian and since \( \Omega(Z) \) is centralized by \( Z \) and \( Y \),

\[
(5) \quad H' \leq \Omega(Z) \leq Z(H).
\]

Therefore (1) of § 1.5 implies that

\[
(6) \quad [z_1, z_2, y] = [z_1, y] [z_2, y] \quad \text{for all} \quad z_1 \in Z, \quad y \in Y
\]

and hence \( [z^p, y] = [z, y]^p = 1 \), that is, \( (z^p)^y = z^p = (z^p)^{1+p^{n-1}} \) for all \( z \in Z \). Thus

\[
(7) \quad \Phi(Z) \leq C_Z(y) \cap D_Z(y) \quad \text{for all} \quad y \in Y.
\]

Suppose, for a contradiction, that \( |Y| \leq p^n = \text{Exp } Z \). Then \( \text{Exp } H = p^n \) and, by an obvious extension of 2.3.11, there exists a complement \( C \) to \( Z \) in \( H \). For, given \( z \in Z \) with \( o(z) = p^n \), by 2.3.11 there exists a complement \( K \) to \( \langle z \rangle \) in \( H \); hence \( Z = \langle z \rangle \cap (K \cap Z), K \cap Z \) is a homocyclic normal subgroup of \( K \) and, by induction, it has a complement \( C \) in \( K \) such that \( H = \langle z \rangle K = \langle z \rangle (K \cap Z)C = ZC \) and \( Z \cap C = Z \cap K \cap C = 1 \). Now \( C \) in place of \( Y \) satisfies the assumptions of the lemma and, by (a), every subgroup of \( Z \) is normal in \( H \), a contradiction. It follows that

\[
(8) \quad \text{Exp } Z = p^n < p^m = |Y| = \text{Exp } H.
\]

Now suppose first that there exists \( h \in H \) such that \( o(h) = p^m \) and \( \langle h \rangle \leq H \). Then \( h = vy \) where \( v \in Z \), \( y \in Y \) and \( o(y) = p^n \), that is, \( Y = \langle y \rangle \). Thus \( Z \langle h \rangle = H \) and \( H/\langle h \rangle \approx Z/Z \cap \langle h \rangle \) is abelian. Therefore \( H' \leq \langle h \rangle \cap \Omega(Z) \) and hence \( |H'| = p \). By (6), the map \( z \to [z, y] \) is a homomorphism from \( Z \) to \( [Z, y] \leq H' \) with kernel \( C_Z(Y) \). It follows that \( |Z : C_Z(Y)| = p \) and (1) holds.

It remains to consider the case that no cyclic subgroup of maximal order is normal in \( H \). Then by 2.3.18 there exists an abelian normal subgroup \( A \) of \( H \), a generator \( y \) of \( Y \) and an integer \( s \) which is at least 2 in case \( p = 2 \) such that \( H = A \langle y \rangle \) and \( a^y = a^{1+p^r} \) for all \( a \in A \). Then \( \Omega_s(A) = \{a^{p^s} | a \in H \} = H' \leq \Omega(Z) \) and hence \( \text{Exp } A = p^{s+1} \). Therefore, if \( s < n - 1 \), then \( A \leq \Omega_{n-1}(H) \) and \( Z/\Omega_{n-1}(Z) \approx Z/\Omega_{n-1}(H) \) would be cyclic; but \( Z \) has two independent elements of order \( p^n \), a contradiction.
Thus $s \geq n - 1$. If $s > n - 1$, then $\text{Exp } Z = p^n$ implies that $a^y = a^{1+p^n} = a$ for all $a \in Z \cap A$. Hence $Z \cap A \leq C_2(Y)$ and $Z/Z \cap A \cong ZA/A$ is cyclic. Since $\Phi(Z) \leq C_2(Y)$, it follows that $|Z : C_2(Y)| = p$ and again (1) holds. So, finally, let $s = n - 1$, that is,

$$(9) \ a^y = a^{1+p^n-1} \text{ for all } a \in A.$$ 

Now $Z \cap A \leq D_z(y)$, $Z/Z \cap A$ is cyclic and $\Phi(Z) \leq D_z(y)$. It follows that $|Z : D_z(y)| = p$, and we have to find an element $v \in Z$ of order $p^n$ for which the remaining assertions of (2) or (3) hold. If $\mathcal{U}_{n-1}(D_z(y)) \cap Y = 1$, we choose $v \in Z$ such that $o(v) = p^n$ and $Y \cap Z \leq \langle v \rangle$. By (a) and (5), $[v, y] \in \langle v \rangle \cap \Omega(Z) = \langle v^{p^n+1} \rangle$ and hence $v^y = v^{1+\lambda p^n-1}$ where $\lambda \in Z$. Since $y$ does not normalize every subgroup of $Z$, $Y \cap Z \neq 1$, and it follows that $v \notin D_z(y)$. Thus $\lambda \neq 1 \mod p$ and (2) holds. If $\mathcal{U}_{n-1}(D_z(y)) \cap Y \neq 1$, we take $v \in Z \setminus D_z(y)$. Then $o(v) = p^n$, $v = ab$ where $a \in A$, $b \in Y$ and $o(b) \leq p^n$ since $\text{Exp } A = p^n$. By (9) and 2.3.10 applied to $\Omega_n(H)$,

$$[v, y] = [a, y] = a^{p^n-1} = b^{-p^n-1}$$
and since $v \notin D_z(y)$, $b^{-p^n-1} \neq 1$. Now $b^{-p^n-1} \in \Omega(Y) \leq \mathcal{U}_{n-1}(D_z(y))$ and hence there exists $w \in D_z(y)$ such that $w^{p^n-1} = b^{-p^n-1}$. It follows that $o(w) = p^n$ and $v^y = v^{1+p^n w^{-p^n-1}}$, that is, (3) holds. 

4.4.7 Lemma. Let $p > 2$ and $Z$ be a homocyclic group of exponent $p^n$ and order $p^n$ where $n \geq 2$, $r \geq 2$. Let $A = BC \leq \text{Aut } Z$, $B$ a nontrivial elementary abelian normal $p$-subgroup of $A$ and $C = \langle \gamma \rangle$ a cyclic $q$-group where $q \neq p$ is a prime and suppose that

(10) $\gamma$ operates irreducibly on $B$, $[B, \gamma] = B$, $[B, \gamma^q] = 1$,

(11) $\gamma$ operates irreducibly on $\Omega(Z)$,

(12) $[Z, B] \leq \Omega(Z)$, and

(13) every cyclic subgroup $Y \neq 1$ of $B$ satisfies (b) of 4.4.6.

Then $r = 2$, $|B| = p$, $q = 2$ and there exist a generator $\alpha$ of $B$ and a basis $\{u, v\}$ of $Z$ such that $u^2 = u^{1+p^n-1}$, $v^2 = v^{1+p^n-1}$ and $\alpha^2 = \alpha^{-1}$.

Proof. To simplify notation, we write $C_\alpha(x) = C_x$ and $D_\alpha(x) = D_x$ for $x \in B$. If $|Z : C_\alpha| \leq p$, then clearly $\Phi(Z) \leq C_\alpha$. And if $|Z : C_\alpha| > p$, then, by (13) there exists $\beta \in \langle \alpha \rangle$ such that $|Z : D_\beta| = p$; hence $z^\beta = z^{1+p^n-1} = z$ for all $z \in \Phi(Z)$ and again $\Phi(Z) \leq C_\alpha = C_\beta$. It follows that

(14) $\Phi(Z) \leq C_\beta(B)$.

Since $n \geq 2$, (12) implies that $[Z, B]$ is contained in $\Phi(Z)$ and hence is centralized by $B$ and, of course, also by $Z$. Therefore (1) of § 1.5 yields that

(15) $[u, z] = [u, \alpha][v, z]$ and $[z, \alpha \beta] = [z, \alpha][z, \beta]$ for all $u, v, z \in Z$ and $\alpha, \beta \in B$.

In particular, the map $z \to [z, \alpha]$ is an epimorphism from $Z$ to $[Z, \alpha]$ with kernel $C_\alpha$ and hence
(16) $|[Z, x]| = |Z : C_x|$ for $x \in B$;

similarly,

(17) $|[z, B]| = |B : C_B(z)|$ for $z \in Z$.

If $x \in B$ such that $|Z : C_x| = p$, then $1 < \bigcup_{i=1}^{p-1}(C_x) < \Omega(Z)$; furthermore $|[Z, x]| = p$ and hence also $1 < [Z, x] < \Omega(Z)$. Since $\gamma$ operates irreducibly on $\Omega(Z)$, we have $[Z, x] \neq [Z, x]^\gamma = [Z, x^\gamma]$ and $C_x \neq (C_x)^\gamma = C_{x^\gamma}$. For $z \in Z$ and $i = 1, \ldots, p-1$, $[z, x^i] = [z, x][z, x^\gamma] \in [Z, x] \times [Z, x^\gamma]$. If $z \in C_x \setminus C_{x^\gamma}$, then $[z, x^i] = [z, x^\gamma]$ is a nontrivial element in $[Z, x^\gamma]$ and for $z \in C_x \setminus C_{x^\gamma}$, $[z, x^i] = [z, x]^\gamma$ is a nontrivial element in $[Z, x]$. It follows that $[Z, x^i] = [Z, x] \times [Z, x^\gamma]$. In view of (16), we have shown:

(18) If $x \in B$ such that $|Z : C_x| = p$, then $|Z : C_x(x^i)] = p^2$ for $i = 1, \ldots, p - 1$.

If $x \in B$ such that $|Z : D_x| = p$, then every $z \in D_x \cap (D_x)^\gamma$ satisfies $z^x = z^{x^{-1}x^\gamma} = z^{1 + p^{-n-1}} = z^x$, and it follows that $D_x \cap (D_x)^\gamma \leq C_x(x^\gamma^{-1})$. Thus we have:

(19) If $x \in B$ such that $|Z : D_x| = p$, then $|Z : C_x(x^\gamma^{-1})| \leq p^2$.

From (18) and (19) we conclude that there exists $\beta \in B$ such that

(20) $|Z : D_\beta| = p$ and $|Z : C_\beta| = p^2$.

For, if there exists $x \in B$ with $|Z : C_x| = p$, then $|Z : C_x(x^\gamma)] = p^2$, and if there is no such $x$, then by (13) there exists $\delta \in B$ with $|Z : D_\delta| = p$ and hence $|Z : C_z(\delta^\gamma \delta^{-1})| = p^2$. Again (13) implies that a suitable generator $\beta$ of $\langle x^\gamma \rangle$ or $\langle x^\gamma \delta^{-1} \rangle$ satisfies $|Z : D_\beta| = p$ and, of course, $|Z : C_\beta| = p^2$.

By (14) and (20), $\Phi(Z) \leq C_\beta \cap D_\beta$. On the other hand, $z \in C_\beta \cap D_\beta$ implies that $z = z^\beta = z^{1 + p^{-n-1}}$ and hence $z \in \Phi(Z)$. Thus $\Phi(Z) = C_\beta \cap D_\beta$ and, by (20), $p^r = |Z : \Phi(Z)| \leq p^3$, that is, $r \leq 3$. Suppose, for a contradiction, that $r = 3$. Then $Z/\Phi(Z) = C_\beta/\Phi(Z) \times D_\beta/\Phi(Z)$ and hence there exists a basis $\{u, v, w\}$ of $Z$ such that $u^\beta = u, v^\beta = v^{1 + p^{-n-1}}$, and $w^\beta = w^{1 + p^{-n-1}}$. Now $Z$ is a free $\mathbb{Z}/(p^n)$-module and we may consider $A$ as a subgroup of $GL(Z) \cong GL(3, \mathbb{Z}/(p^n))$. The determinant defined there induces a homomorphism from $A$ to the group of units of $\mathbb{Z}/(p^n)$. By (10), $A$ has no normal subgroup of index $p$ and this implies that the determinant is trivial on the $p$-elements of $A$. But det $\beta = 1 + 2p^{-n-1} + (p^n) \neq 1 + (p^n)$ since $p > 2$. This contradiction shows that

(21) $r = 2$.

By assumption, $\gamma$ is irreducible on $\Omega(Z)$. Therefore the order of the operating group divides $p^2 - 1$; in particular, $q|p^2 - 1$. This implies that every irreducible $GF(p)$-module of the cyclic group of order $q$ has order at most $p^2$ (see Huppert [1967], p. 166). Since $\langle \gamma \rangle/\langle \gamma^p \rangle$ operates irreducibly on $B$, it follows that

(22) $|B| \leq p^2$.

Suppose, for a contradiction, that there exists $x \in B$ such that $|Z : C_x| = p$. Then for every $\delta \in \langle \gamma \rangle$, $(C_x)^\delta = C_{x^\delta}$ and hence $|Z : C_{x^\delta}| = p$. By (18), $|Z : C_x(x^\delta)| = p^2$ for $i = 1, \ldots, p - 1$. Therefore $B = \langle x \rangle \times \langle x^\gamma \rangle$ has order $p^2$ and among the $p + 1$
4.4 Abelian $p$-subgroups and projectivities

minimal subgroups of $B$, only $\langle x \rangle$ and $\langle x' \rangle$ have their centralizers of index $p$ in $Z$. Hence $\langle \gamma \rangle$ operates on $\{ \langle x \rangle, \langle x' \rangle \}$ and it follows that $q = 2$; but this contradicts (10) because a group of order 2 cannot operate irreducibly on an elementary abelian group $B$ of order $p^2$. Thus there does not exist $x \in B$ with $|Z : C_x| = p$; since $\Phi(Z)$ is centralized by $B$ and has index $p^2$ in $Z$, it follows that

$$(23) \quad C_x = \Phi(Z) \text{ for all } 1 \neq x \in B.$$ 

Let $B_0$ be a subgroup of order $p$ of $B$. By (13) there exist $x \in B_0$ and $v \in Z$ such that $o(v) = p^n$, $|Z : D_v| = p$ and, either $v^x = v^{1 + \lambda p^{n-1}}$ with $\lambda \not\equiv 1 \pmod p$ or $v^x = v^{1 + p^{n-1} w p^{n-1}}$ with $w \in D_v$, $o(w) = p^n$. In the latter case, $\{v, w\}$ would be a basis of $Z$ and since $w^x = w^{1 + p^{n-1}}$, det $x = 1 + 2p^{n-1} + (p^n) \neq 1 + (p^n)$, a contradiction. Thus $v^x = v^{1 + \lambda p^{n-1}}$ where $\lambda \not\equiv 1 \pmod p$. If $u \in D_x$ with $o(u) = p^n$, then $u^x = u^{1 + p^{n-1}}$ and $\{u, v\}$ is a basis of $Z$. Then $1 + (p^n) = \det x = 1 + (\lambda + 1)p^{n-1} + (p^n)$ implies $\lambda \equiv 1 \pmod p$ and hence our basis $\{u, v\}$ of $Z$ satisfies

$$(24) \quad u^x = u^{1 + p^{n-1}}, \quad v^x = v^{1 - p^{n-1}}.$$ 

Now suppose, for a contradiction, that $|B| = p^2$. Then by (24), any of the $p + 1$ minimal subgroups of $B$ fixes at least 2 cyclic subgroups of order $p^n$ of $Z$. Since $Z$ has only $p + 1$ maximal subgroups, there must exist subgroups $\langle x \rangle \neq \langle x' \rangle$ of order $p$ of $B$, and elements $x, y \in Z$ of order $p^n$ satisfying $[x, x] \in \langle x \rangle$ and $[y, x'] \in \langle y \rangle$ such that $x$ and $y$ lie in the same maximal subgroup $\langle x \rangle \Phi(Z) = \langle y \rangle \Phi(Z)$ of $Z$. By (12), $[x, x]$ and $[y, x']$ are contained in $\Omega(\langle x \rangle) = \Omega(\langle y \rangle)$. Furthermore $x = y^i z$ for some $i \in \mathbb{Z}$, $z \in \Phi(Z)$ and hence (15) and (14) show that $[x, x'] = [y, x'] \in \Omega(\langle x \rangle)$ also. It follows that $[x, B] \leq \Omega(\langle x \rangle)$ and hence $p \geq |[x, B]| = |B : C_B(x)|$ by (17). This implies that $|C_B(x)| \geq p$ and $x \in C_B$ if $1 \neq \delta \in C_B(x)$, contradicting (23). Thus

$$(25) \quad |B| = p.$$ 

Since $\gamma$ does not centralize $B$, $q | p - 1$. And since $\gamma$ operates irreducibly on $\Omega(Z)$, $o(\gamma)$ divides $p^2 - 1$ but not $p - 1$. Therefore $q$ also divides $p + 1$ and it follows that $q = 2$. By (24), there exist a generator $x$ of $B$ and a basis $\{u, v\}$ of $Z$ such that $u^x = u^{1 + p^{n-1}}$ and $v^x = v^{1 - p^{n-1}}$. Finally, $\gamma$ induces an automorphism of order 2 in $B$ and hence $\alpha^x = \alpha^{-1}$.

4.4.8 Lemma. Suppose that $p > 2$, $G$ is a finite group with $O^p(G) = G$, $P \in \text{Syl}_p(G)$, $Z$ is a normal subgroup of $G$ contained in $Z(P)$ and $\varphi$ is an index preserving projectivity from $G$ to a group $\tilde{G}$. Then $Z^{\varphi} \leq Z(P^{\varphi})$.

Proof. Suppose that the lemma is false and consider a counterexample $G$ of minimal order. By 4.3.9,

$$(26) \quad Z^{\varphi} \leq \tilde{G}.$$ 

Furthermore, if $A$ and $B$ are nontrivial normal subgroups of $G$ contained in $Z$ such that $A \cap B = 1$, then $A^{\varphi} \leq \tilde{G}$ and $B^{\varphi} \leq \tilde{G}$, $\varphi$ induces projectivities in $G/A$ and $G/B$, and the minimality of $G$ implies that $[P^{\varphi}, Z^{\varphi}] \leq A^{\varphi} \cap B^{\varphi} = 1$. Hence $Z^{\varphi} \leq Z(P^{\varphi})$, contradicting the choice of $G$. We have shown:
(27) If $A, B \leq Z$ such that $A \leq G, B \leq G$ and $A \cap B = 1$, then $A = 1$ or $B = 1$.

Since $P \leq C_G(Z)$, the group of automorphisms induced by $G$ in $Z$ is a $p'$-group. Therefore $Z = [Z, G] \times C_Z(G)$ (apply 4.1.3 to the semidirect product of $Z$ by this group of automorphisms) and, by (27), $[Z, G] = 1$ or $C_Z(G) = 1$. In the first case, 1.6.8 would imply that $[Z^p, \tilde{G}] = 1$ and hence $Z^p \leq Z(P^o)$, contradicting the choice of $G$. Therefore

(28) $C_Z(G) = Z \cap Z(G) = 1$ and $[Z, G] = Z$.

Furthermore, Maschke's Theorem (see Robinson [1982], p. 209) shows that to every $G$-invariant subgroup $A$ of $\Omega(Z)$, there exists $B \leq G$ such that $\Omega(Z) = A \times B$; then (27) implies that $A = 1$ or $A = \Omega(Z)$. Thus

(29) $G$ operates irreducibly on $\Omega(Z)$.

In particular, $U_{n-1}(Z) = \Omega(Z)$ if $\text{Exp } Z = p^n$ and hence

(30) $Z$ is homocyclic.

Take any $p'$-subgroup $B$ of $G$. By 4.4.1, $Z^p = [Z^p, B^p] \times C_Z(B)^p$ and $[Z^p, B^p]$ is abelian. Therefore $(Z^p)^p \leq C_Z(B)^p$ and hence $((Z^p)^p)^{p^{-1}} \leq C_Z(B)$. Since $G = O^p(G)$ is generated by these $p'$-subgroups $B$, it follows that $((Z^p)^p)^{p^{-1}} \leq C_Z(G) = 1$. Thus $(Z^p)^p = 1$ and

(31) $Z^p$ is abelian.

Put $L = O^p(G)$ and $M = O^p(L)$. Then $P \leq L$ and $MP = L$. Since $\varphi$ is index preserving,

(32) $L^p = O^p(\tilde{G})$ and $M^p = O^p(L^p)$.

Since $G/C_G(Z)$ is a $p'$-group, $L \leq C_G(Z)$. In particular, $[Z, M] = 1$ and, by 1.6.8,

(33) $[Z^p, M^p] = 1$. 
4.4 Abelian p-subgroups and projectivities

Hence $L^o/C_{10}(Z^o)$ is a $p$-group operating on the $p$-group $Z^o$ and therefore it centralizes a nontrivial element in this group. Thus $\Omega(Z^o) \cap Z(L^o) \neq 1$ and, of course, is normal in $\tilde{G}$. By 4.3.9, $(\Omega(Z^o) \cap Z(L^o))^{p^{-1}} \leq G$ and since $G$ operates irreducibly on $\Omega(Z)$, it follows that

$$34 \quad \Omega(Z^o) \leq Z(L^o); \text{ in particular, } \Omega(Z^o) \leq Z(P^o).$$

Since $G$ is a counterexample to the lemma, $\Omega(Z) < Z$ and the minimality of $G$ yields that $Z^o/\Omega(Z^o)$ is contained in the centre of $P^o/\Omega(Z^o)$. Thus

$$35 \quad \text{Exp } Z = p^n > p \text{ and } [P^o, Z^o] \leq \Omega(Z^o).$$

Now (35), (34) and (31) show that for $x \in P^o$ and $z \in Z^o$, $[x, z]$ has order $p$ and commutes with $x$ and $z$. Therefore $1 = [x, z]^p = [x^p, z] = [x, z^p]$, that is, $P^o$ is centralized by $\mathcal{U}(Z^o) = \Phi(Z^o)$ and $Z^o$ is centralized by $\mathcal{U}(P^o)$. Since $[P^o, Z^o, P^o] = 1 = [Z^o, P^o, P^o]$, we have $[\mathcal{U}(P^o), Z^o] = [P^o, P^o, Z^o] = 1$ also (see (7) in § 1.5); hence $Z^o$ is centralized by $\mathcal{U}(P^o)(P^o)' = \Phi(P^o)$. Thus

$$36 \quad [P^o, \Phi(Z^o)] = 1 = [\Phi(P^o), Z^o].$$

Put $G^* = \tilde{G}/M^o$ and $\tilde{G} = \tilde{G}/C_{10}(Z^o)$. For $x \in \tilde{G}$ and $H \leq G$, write $x^* = xM$, $\hat{x} = xC_{10}(Z^o)$, $H^* = H^oM^o/M^o$ and $\hat{H} = H^oC_{10}(Z^o)/C_{10}(Z^o)$ to denote the images of $x$ and $H^o$ under the natural epimorphisms from $\tilde{G}$ to $G^*$ and $\hat{G}$. By (33), $M^o \leq C_{10}(Z^o)$ so that $\hat{G}$ is an epimorphic image of $G^*$. Since $L^o = O_p^o(\tilde{G}) = P^oM^o$, we have $P^o = L^o/M^o \leq G^*$. Hence the Sylow $p$-subgroup $\hat{P}$ of the epimorphic image $\hat{G}$ of $G^*$ is normal in $\tilde{G}$ and $\hat{P} \neq 1$ because $G$ is a counterexample. Since $Z^o$ is centralized by $\Phi(P^o)$, finally,

$$37 \quad \hat{P} \text{ is a nontrivial elementary abelian normal subgroup of } \hat{G}.$$  

The Frattini argument shows that $\tilde{G} = L^oN_{\tilde{G}}(P^o) = M^oN_{\tilde{G}}(P^o)$, and by the Schur-Zassenhaus Theorem there exists a complement $Q^o$ to $P^o$ in $N_{\tilde{G}}(P^o)$. Since $P^o$ and $Q^o$ have relatively prime order, $Q^*$ and $\hat{Q}$ are also complements to $P^*$ and $\hat{P}$, respectively, in the epimorphic images $G^*$ and $\hat{G}$ of $N_{\tilde{G}}(P^o)$. Then $\tilde{G} = O_p^o(\tilde{G})$ implies that $G^* = O_p^o(G^*) = (Q^*)^{p^n}$ and, by 4.1.1, $P^* = P^* \cap (Q^*)^{p^n} = [P^*, Q^*]$. The same applies for $\hat{G}$; since $\hat{P}$ is abelian, 4.1.3 implies that $C_p(\hat{Q}) = 1$. Thus

$$38 \quad [P^*, Q^*] = P^* \cap [\hat{P}, \hat{Q}] = \hat{P} \text{ and } C_p(\hat{Q}) = 1.$$  

Our aim is to show that the assumptions of Lemma 4.4.7 are satisfied for $Z^o$ in place of $Z$, $G = A$, $\hat{P} = B$ and $\hat{Q} = C$. By (30), (31) and (35), $Z^o$ is homocyclic of exponent $p^n$ where $n \geq 2$, and we may regard $\tilde{G} = \tilde{G}/C_{10}(Z^o)$ as a subgroup of $\text{Aut } Z^o$ in which $\hat{P}$, by (37), is a nontrivial elementary abelian normal $p$-subgroup. If $Y \neq 1$ is a cyclic subgroup of $\hat{P}$, then $Y = \langle y \rangle$ for some $y \in P^o$; let $H = \langle y \rangle Z^o$. Since $Z \leq Z(P)$, the subgroup $H^{p^{-1}} = \langle y \rangle^{p^{-1}}Z$ is abelian and hence $L(H)$ is modular. By (35) and (36), $Z^o/\Omega(Z^o)$ and $\Omega(Z^o)$ are centralized by $\langle y \rangle$. If $y$ normalized every subgroup of $Z^o$, then, by 1.5.4, $y$ would induce a universal power automorphism in $Z^o$, which, of course, would centralize every automorphism of $Z^o$; it would follow that $\hat{y} \in C_p(\hat{Q})$, contradicting (38). Thus $Y$ does not normalize every subgroup of $Z^o$; in particular, $Z^o$ is not cyclic, that is, $|Z^o| = p^r$ where $r \geq 2$, and since we shall need it later, we note that we have shown:
(39) If \( y \in P^o \) such that \( y \neq 1 \), then \( H = \langle y \rangle Z^o, Z^o \) and \( \langle y \rangle \) satisfy the assumptions of 4.4.6.

Therefore, by 4.4.6, \( Y \) satisfies (b) of this lemma, that is, (13) holds for \( P = B \) and (12) follows from (35). It remains to be shown that \( \hat{\varphi} \) is a cyclic \( q \)-group for some prime \( q \) satisfying (10) and (11). For this we need:

(40) If \( S \leq G \) such that \( S^o \leq Q^o \) and \( S^* < Q^* \), then \( [L^o, S^o] \leq \text{C}_G(Z^o) \).

To prove (40), first note that \( |S^o|, p \) = 1 and hence \( Z^o = [Z^o, S^o]C_{Z^o}(S^o) \); we show that \( [L^o, S^o] \) centralizes the two factors in this product. Now \( L \leq G \) would imply that \( G^* = L^*S^* = P^*S^* \), contradicting \( S^* < Q^* \). Thus \( L < G \), hence \( G_0 = O_p(\langle L \rangle) < G \) and \( O_p(G_0) = G_0 \). Since \( P \in \text{Syl}_p(\langle L \rangle) \), \( P \cap G_0 \) is a Sylow \( p \)-subgroup of \( G_0 \) containing the normal subgroup \( Z \cap G_0 \) of \( G_0 \) in its centre. The minimality of \( G \) implies that \( (Z \cap G_0)^o \) is centralized by \( (P \cap G_0)^o \) and, by (33), it is also centralized by \( M^o \). Since \( \varphi \) is index preserving, \( G^o \leq O_p(L^oS^o) \) and so,

(41) \( Z^o \cap O_p(L^oS^o) \) is centralized by \( M^p(\langle P^o \cap O_p(L^oS^o) \rangle) \).

Now \( Z^o \leq L^oS^o \) and the \( p^i \)-group \( S^o \leq O_p(L^oS^o) \); hence \( [Z^o, S^o] \leq Z^o \cap O_p(L^oS^o) \). Furthermore \( S^o \leq O_p(L^oS^o) \) implies that \( [L^o, S^o] \leq O_p(L^oS^o) \) and so from \( [L^o, S^o] \leq L^o = M^oP^o \) it follows that \( M^o[L^o, S^o] = M^o(P^o \cap M^o[L^o, S^o]) \leq M^o(P^o \cap O_p(L^oS^o)) \) since \( M^o = O_p(L^o) \leq O_p(L^oS^o) \) also. Thus (41) shows that \( [Z^o, S^o] \) is centralized by \( [L^o, S^o] \).

The other factor of \( Z^o \) is easier to handle. Since \( L \leq C_G(Z), [C_Z(S), LS] = 1 \) and hence, in particular, \( [C_Z(S), O_p(\langle L \rangle)] = 1 \). By 1.6.8, \( [C_Z(S^o), O_p(LS^p)] = 1 \) and, by 4.1.2, \( C_Z(S^o) = C_{Z^o}(S^o) \). Since \( [L^o, S^o] \leq O_p(L^oS^o) = O_p(LS^p) \), it follows that \( [L^o, S^o] \) centralizes \( C_{Z^o}(S^o) \) and hence also \( [Z^o, S^o]C_{Z^o}(S^o) = Z^o \). This proves (40).

We show next that \( \hat{\varphi}^* \) is cyclic of prime power order. If this were not the case, there would exist elements \( s_i \in Q^o \) such that \( \langle s_i^* \rangle < Q^* \) for all \( i \) and \( Q^* \) is generated by the \( s_i^* \). Applying (40) to \( S^o = \langle s_i \rangle \), we obtain \( [L^o, s_i] \leq C_G(Z) \) and hence \( [P^*, s_i] = [L^o/M^o, s_i] \leq C_G(Z)/M^o \). By (38), \( P^* = [P^*, Q^*] \leq C_G(Z^o)/M^o \) and this would contradict (37). Thus \( Q^* \) is cyclic of prime power order and therefore also its epimorphic image.

(42) \( \hat{\varphi} \) is a cyclic \( q \)-group for some prime \( q \).

Let \( s \in Q^o \) such that \( \hat{\varphi} = \langle s \rangle \). We want to show that \( s = \gamma \) satisfies (10) and (11). By (34), \( \Omega(Z^o) \) is centralized by \( \hat{P} \); but, by (29) and 4.3.9, \( \Omega(Z^o) \) is irreducible under \( \hat{\varphi} = \hat{P}\langle s \rangle \). It follows that

(43) \( \hat{\varphi} \) operates irreducibly on \( \Omega(Z^o) \),

that is, (11) holds. By (38), \( [\hat{P}, \hat{s}] = \hat{P} \) and, applying (40) to \( S^o = \langle s^q \rangle \), we obtain \( [P^o, s^q] \leq [L^o, S^o] \leq C_G(Z^o) \). It follows that \( [\hat{P}, \hat{s}^q] = 1 \) and it remains to be shown that \( \hat{s} \) operates irreducibly on \( \hat{P} \). So suppose that \( \hat{P}_1 \) is a \( \hat{Q} \)-invariant subgroup of \( \hat{P} \) such that \( \hat{P}_1 < \hat{P} \). Let \( \hat{T} \leq G \) such that \( T^o/C_G(Z^o) = \hat{P}_1 \hat{Q} \). Then \( \hat{T} < G \), hence \( R = O_p(\hat{T}) < G \) and \( O_p(R) = R \). By 4.1.3, \( Z^o = [Z^o, Q^o] \times C_{Z^o}(Q^o) \); since \( |\Omega(Z^o)| \geq p^2 \) and \( Q^o \) operates irreducibly on \( \Omega(Z^o) \), it follows that \( Z^o = [Z^o, Q^o] \). Since \( Q^o = O_p(T^o) = R^o \) and \( Z^o \leq T^o \), we have \( Z^o = [Z^o, Q^o] \leq R^o \). Now \( |G: R| \) is a power of
4.4 Abelian p-subgroups and projectivities

$p$, hence $G = PR$ and therefore $Z$ is a normal subgroup of $R$ contained in the Sylow p-subgroup $P \cap R$ of $R$. The minimality of $G$ implies that $Z^o$ is contained in the centre of the Sylow p-subgroup $(P \cap R)^o$ of $R^o$. Hence $R^o/R^o \cap C_G(Z^o)$ is a $p'$-group. It follows that $\tilde{R} = R^oC_G(Z^o)/C_G(Z^o)$ is a $p'$-group and since $T^o/R^oC_G(Z^o) = T^o/O^p(T^o)C_G(Z^o)$ is a $p'$-group, $\tilde{R}$ is a normal $p'$-complement in $\tilde{T} = \tilde{P}_1 \tilde{Q}$ and, by (38), $\tilde{P}_1 = 1$. Thus $s$ operates irreducibly on $\tilde{P}$ and all the assumptions of 4.4.7 have been verified. By 4.4.7,

\[(44) \quad r = 2, |\tilde{P}| = p, q = 2 \text{ and there exist } y \in P^o \text{ satisfying } \langle y \rangle = \tilde{P} \text{ and a basis } \{v_1, v_2\} \text{ of } Z^{o}\text{ such that } \langle v_1 \rangle^y = \langle v_1 \rangle, \langle v_2 \rangle^y = \langle v_2 \rangle \text{ and } \dot{y}^4 = y^{-1}.\]

Let $W_i = \Omega(\langle v_i \rangle)$ for $i = 1, 2$. If $x \in P^o \setminus C_{P^o}(Z^o)$, then $\langle x \rangle = \tilde{P} \neq 1$ and therefore, by (39), $H = \langle x \rangle Z^o$ satisfies the assumptions of 4.4.6. If $W_1 \neq \Omega(\langle x \rangle) \neq W_2$, then the cyclic subgroup $\langle x \rangle \cap Z^o$ of the homocyclic group $Z^o$ would be contained in a maximal cyclic subgroup $\langle v \rangle$ of $Z^o$ such that $\langle v_1 \rangle \cap \langle v \rangle = 1 = \langle v_2 \rangle \cap \langle v \rangle$. By (a) of 4.4.6, $\langle v \rangle^{x} = \langle v \rangle$ and since also $\langle v_i \rangle^{x} = \langle v_i \rangle$ for $i = 1, 2$, it would follow from 1.5.4 that $x$ induces a power automorphism in $Z^o$. This is not the case; thus

\[(45) \quad \Omega(\langle x \rangle) \in \{W_1, W_2\} \text{ for every } x \in P^o \setminus C_{P^o}(Z^o).\]

By (44), $(yC_G(Z^o))^y = y^{-1}C_G(Z^o)$ and, since $s$ normalizes $P^o$, it follows that $(yC_{P^o}(Z^o))^y = y^{-1}C_{P^o}(Z^o)$. By (45), $s$ operates on $\{W_1, W_2\}$ and, since $s$ is irreducible on $\Omega(Z^o)$, $W_1 = W_2$ and $W_2 = W_1$. For $i = 1, 2$ define

$$S_i = \{x \in yC_{P^o}(Z^o) | \Omega(\langle x \rangle) = W_i\} \quad \text{and} \quad T_i = \{x \in y^{-1}C_{P^o}(Z^o) | \Omega(\langle x \rangle) = W_i\}.$$ 

Then $S_i^{-1} = \{x^{-1} | x \in S_i\} = T_i$ and hence $|S_i| = |T_i|$ for $i = 1, 2$. If $x \in S_1$, then $W_1 = W_1^x = \Omega(\langle x \rangle)^x = \Omega(\langle x^x \rangle)$ and so $x^x \in T_2$; similarly, $x^x \in T_1$ for $x \in S_2$. By (45), $yC_{P^o}(Z^o) = S_1 \cup S_2$ (disjoint set-theoretic union) and $y^{-1}C_{P^o}(Z^o) = T_1 \cup T_2$, it follows that $S_1^* = T_2$. Therefore $|S_1| = |T_2| = |S_2|$ and hence $|C_{P^o}(Z^o)| = |yC_{P^o}(Z^o)| = 2|S_1|$. But this contradicts the assumption that $p > 2$. \(\square\)

**The centre of a Sylow p-subgroup**

We remind the reader that a finite group $G$ is called $p$-normal if $Z(P)^p \leq P$ implies that $Z(P)^p = Z(P)$ whenever $P \in \text{Syl}_p(G)$ and $g \in G$. In particular, every finite group with abelian Sylow $p$-subgroups is $p$-normal. Therefore the following result is a generalization of Theorem 4.4.2 in the case $p > 2$ and $O^p(G) = G$.

**4.4.9 Theorem (Menegazzo [1974]).** Let $p > 2$ and suppose that the finite group $G$ is $p$-normal and satisfies $O^p(G) = G$. If $\phi$ is an index preserving projectivity from $G$ to a group $\tilde{G}$, then $Z(P)^\phi \leq Z(P^\phi)$ for every Sylow $p$-subgroup $P$ of $G$.

**Proof.** By Grün's Second Theorem (see Robinson [1982], p. 285), the largest abelian $p$-quotient of $G$ is isomorphic to that of $N = N_G(Z(P))$; hence $O^p(G) = G$ implies that $O^p(N) = N$. Now 4.4.8 applied to $Z = Z(P) \leq N$ and the projectivity induced by $\phi$ in $N$ yields that $Z(P)^\phi \leq Z(P^\phi)$. \(\square\)
4.4.10 Theorem (Menegazzo [1974]). Let $p > 2$ and suppose that the finite group $G$ is $p$-soluble and satisfies $O^p(G) = G$. If $\varphi$ is an index preserving projectivity from $G$ to a group $\tilde{G}$, then $Z(P)^\varphi = Z(P^\varphi)$ for every Sylow $p$-subgroup $P$ of $G$.

Proof. Since $\varphi$ is index preserving, $\tilde{G}$ is $p$-soluble (see also 4.3.8) and $O^p(\tilde{G}) = \tilde{G}$. Therefore we only have to show that $Z(P)^\varphi \leq Z(P^\varphi)$; this result for $\varphi^{-1}$ will yield the other inclusion. So suppose that $G$ is a minimal counterexample to the assertion $Z(P)^\varphi \leq Z(P^\varphi)$ and put $Z = Z(P)$. For every nontrivial normal subgroup $N$ of $G$ such that $N^\varphi \leq \tilde{G}$, $\varphi$ induces a projectivity from $G/N$ to $\tilde{G}/N^\varphi$, and $ZN/N$ is contained in the centre of the Sylow $p$-subgroup $PN/N$ of $G/N$. The minimality of $G$ therefore implies that

$$[P^\varphi, Z^\varphi] \leq N^\varphi.$$ (46)

Hence if $O^p_p(G) \neq 1$, it would follow that $[P^\varphi, Z^\varphi] \leq O^p_p(\tilde{G}) \cap P^\varphi = 1$, contradicting the choice of $G$. Thus

$$O^p_p(G) = 1.$$ (47)

Let $Q$ be a complement to $P$ in $N_G(P)$. By 4.1.1, $T = [P, Q]Q$ is the normal closure of $Q$ in $N_G(P)$; in particular, $O^p(T) = T$. Furthermore, $Q$ normalizes $[Z, Q]$ and $[Z, Q] \leq Z$ since $Z \leq N_G(P)$. Therefore $[Z, Q]$ is a normal subgroup of $T$ contained in the centre of the Sylow $p$-subgroup $[P, Q]$ of $T$. By 4.4.8, $[Z, Q]^\varphi \leq Z([P, Q]^\varphi)$. Clearly, $C_Z(Q)$ is centralized by $[P, Q]Q = T$ and, by 1.6.8, $[C_Z(Q)^\varphi, T^\varphi] = 1$; in particular, $[C_Z(Q)^\varphi, [P, Q]^\varphi] = 1$. Since $Z = [Z, Q]C_Z(Q)$, it follows that

$$Z^\varphi$$ is centralized by $[P, Q]^\varphi$. (48)

Let $M$ be a maximal normal subgroup of $G$. Since $O^p(G) = G$, $G/M$ is a $p'$-group; let $H = O^p(M)$. Then $M = PH$ and the Frattini argument yields that $G = N_G(P)M = N_G(P)H$. Now $T = [P, Q]Q \leq N_G(P)$ and hence $[P, Q]QH$ is normalized by $N_G(P)H = G$. Since $QH/H$ contains a $p$-complement of $G/H$, $G/[P, Q]QH$ is a $p$-group. But $O^p(G) = G$ then implies that $G = [P, Q]QH$. By Dedekind's law, $P = P \cap [P, Q]QH = [P, Q](P \cap QH)$ and, since $(|QH : H|, p) = 1$, $P \cap H$ is a Sylow $p$-subgroup of $H$ and of $QH$. Therefore $P \cap QH = P \cap H$ and

$$P = [P, Q](P \cap H).$$ (49)

If $Z \leq H$, then $Z$ would be contained in the centre of the Sylow $p$-subgroup $P \cap H$ of $H$ and, since $O^p(H) = H$, the minimality of $G$ would imply that $[Z^\varphi, (P \cap H)^\varphi] = 1$. But then (48) and (49) would show that $[Z^\varphi, P^\varphi] = 1$, contradicting the choice of $G$. Thus

$$Z \not\leq H.$$ (50)

Since $G$ is $p$-soluble and $O^p_p(G) = 1$, we may conclude that $C_G(O^p_p(G)) \leq O^p_p(G)$ (see Robinson [1982], p. 261). Of course, $Z$ centralizes $O^p_p(G) \leq P$ and hence $Z \leq C_G(O^p_p(G)) = Z(O^p_p(G))$. It follows that

$$Z^G$$ is an abelian normal $p$-subgroup of $G$. (51)
Let $1 = H_0 \leq H_1 \leq \cdots \leq H_n = H$ be part of a chief series of $G$. Then every $H_i/H_{i-1}$ is a $p$-group or a $p'$-group, and we want to show by induction that

$$\text{2.} \quad [Z^G, H_i] = 1 \quad \text{for} \quad i = 0, \ldots, n.$$ 

This is certainly true for $i = 0$. So let $[Z^G, H_{i-1}] = 1$ and suppose first that $H_i/H_{i-1}$ is a $p$-group. Since $H_i \leq G$, $P \cap H_i$ is a Sylow $p$-subgroup of $H_i$ and therefore $H_i = H_{i-1}(P \cap H_i)$. Hence for every $x \in G$, there exists $y \in H_{i-1}$ such that $(P \cap H_i)^{-1} = (P \cap H_i)y$ and $Z^x = Z$ since $[Z^G, H_{i-1}] = 1$. Therefore

$$[Z^G, P \cap H_i] = [Z^G(P \cap H_i)^{yx}] = [Z^{y^{-1}}, P \cap H_i]^{yx} = [Z, P \cap H_i]^{yx} = 1$$

since $Z = Z(P)$. It follows that $[Z^G, P \cap H_i] = 1$ and then also $[Z^G, H_i] = [Z^G, H_{i-1}(P \cap H_i)] = 1$. Now suppose that $H_i/H_{i-1}$ is a $p'$-group. Then, since $[Z^G, H_{i-1}] = 1$, this $p'$-group operates on the abelian $p'$-group $Z^G$, and 4.1.3 applied to the semidirect product of $Z^G$ by the operating group, shows that $Z^G = [Z^G, H_i] \times C_{Z^G}(H_i)$. Both factors are normal $p$-subgroups of $G = O^p(G)$. By 4.3.9, their images are normal in $G$ and one of them has to be trivial since otherwise (46) would yield that $[P^G, Z^G] \leq [Z^G, H_i]^p \cap C_{Z^G}(H_i)^p = 1$, contradicting the choice of $G$. But $C_{Z^G}(H_i) = 1$ would imply that $Z^G = [Z^G, H_i] \leq H_i \leq H$, contradicting (50). Hence $[Z^G, H_i] = 1$, as desired. This proves (52).

Now (52) shows that $[Z^G, H] = [Z^G, H_n] = 1$ and, since $H = O^p(H)$, 1.6.8 yields that $[[Z^{p^*}, H^p]] = 1$; in particular, $[Z^{p^*}, (P \cap H)^{p^*}] = 1$. But then (48) and (49) imply that $[Z^{p^*}, P^{p^*}] = 1$, contradicting the choice of $G$. 

We finally remark that Menegazzo states Theorems 4.4.9 and 4.4.10 without the additional assumption that $p > 2$. Unfortunately his proof is incomplete. In the proof of his main lemma he verifies the assumptions of 4.4.6 and then claims that a suitable generator $y$ of $Y$ has to operate on $Z$ in one of four explicitly given ways that correspond to the assertions (1) and (2) in (b) of 4.4.6. The possibility (3), however, is overlooked. Exercise 4 gives an example for an operation of this type for which (1) and (2) do not hold. Exercise 5 describes the situation that occurs in 4.4.7 for $p = 2$. If one tries to prove Lemma 4.4.8 (and hence Menegazzo's theorems) for $p = 2$, this situation will occur in (44) in addition to the one considered there. One has to decide if it leads to a contradiction or to a counterexample to 4.4.8, and possibly also to Theorems 4.4.9 and 4.4.10 for $p = 2$.

Exercises

1. (Seitz and Wright [1969]) If a Sylow $p$-subgroup of $G$ is a nonabelian $M^*$-group, show that $O^p(G) \neq G$. (Hint: Use 2.3.23.)

2. (Paulsen [1975]) Let $G = NP$ where $P$ is an abelian Sylow $p$-subgroup and $N$ a normal $p$-complement of $G$. If $\phi$ is a projectivity from $G$ to $\overline{G}$, show that $((P^\phi)^*) = Z(G)$ and $(P^\phi)'$ centralizes $N^\phi$. 


3. (Paulsen [1975]) Let $G = NP$ where $P \in \text{Syl}_p(G)$ is an $M^*$-group and $N$ is a normal $p$-complement in $G$. Show that there exists a projectivity from $G$ to a group with abelian Sylow $p$-subgroups if and only if $P' \leq C_P(N)$.

4. Let $N = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle \times \langle b \rangle \times \langle c \rangle$ where $o(a_i) = o(b) = p^n$, $o(c) = p$, $n \geq 2$, and $n \geq 3$ in case $p = 2$. Let $\alpha \in \text{Aut} \ N$ be such that $a_i^\alpha = a_i^{1+p^{n-1}}$ ($i = 1, \ldots, r$), $b^\alpha = b^{1+p^{n-1}}$, and $c^\alpha = ca_i^{-p^{n-1}}$.

   (a) Show that $\alpha$ is an automorphism of order $p$ of $N$ and there exists an extension $H$ of $N$ by $\langle y \rangle$ such that $y^p = a_1 c$ and $x^y = x^\alpha$ for all $x \in N$.

   (b) $H$ is an $M^*$-group and $Z = \langle a_1, \ldots, a_r, b \rangle$ is a homocyclic normal subgroup of $H$.

   (c) Show that $|Z : C_Z(y)| = p^{r+1}$, $|Z : D_Z(y)| = p$ and there is no $v \in Z$ of order $p^n$ and $v \neq 1 \pmod{p}$ such that $v^y = v^{1+2p^{n-1}}$.

5. Show that if $p = 2$ instead of $p > 2$ in the assumptions of 4.4.7, then $r = 2$, $q = 3$, $A \cong A_4$, and there exist a basis $\{u, v\}$ and generators $\alpha$, $\beta$ of $B$ and $\gamma$ of $C$ whose matrices with respect to the basis $\{u, v\}$ are

$$
\alpha = \begin{pmatrix} 1 + 2^{n-1} & 2^{n-1} \\ 0 & 1 + 2^{n-1} \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 + 2^{n-1} & 0 \\ 2^{n-1} & 1 + 2^{n-1} \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.
$$
Many classes of groups are defined via properties of normal subgroups. To decide whether such a class is invariant under projectivities, we have to know something about projective images of normal subgroups; and in order to get lattice-theoretic characterizations of these classes, we have to be able to describe normal subgroups in the subgroup lattice of a group. The basic tools to accomplish this, at least in finite groups, are the modular subgroups introduced in § 2.1. Every normal subgroup \( N \) of \( G \) is modular in \( L(G) \) and for every projectivity \( \varphi \) of \( G \), \( N^{\varphi} \) is a modular subgroup of \( G^{\varphi} \). Therefore we want to find out how far these modular subgroups can deviate from normality. How to measure this? We know that to every subgroup \( H \) of \( G \) there exist two normal subgroups of \( G \) enclosing \( H \), the core \( H_G = \bigcap_{x \in G} H^x \) and the normal closure \( H^G = \bigcup_{x \in G} H^x \) of \( H \) in \( G \). Obviously, \( H_G \) is the largest normal subgroup of \( G \) contained in \( H \), \( H^G \) is the smallest normal subgroup of \( G \) containing \( H \) and the structure of \( H^G/H_G \) and the embedding of this factor in \( G \) describe the deviation of \( H \) from normality.

For this reason we investigate the structure of \( M^G/M_G \) and \( G/M_G \) for a modular subgroup \( M \) of \( G \), and in § 5.1 reduce this problem for finite groups to the case where \( M \) is permutable in \( G \). In § 5.2 we show that then \( M^G/M_G \) is hypercentrally embedded in \( G \) and hence is nilpotent. Together with the results of § 5.1 this yields a structure theorem for \( G/M_G \) for modular subgroups of finite groups which, in particular, implies that \( M^G/M_G \) is hypercyclically embedded in \( G \).

Our first nontrivial result on modular subgroups, Lemma 5.1.2, already leads to lattice-theoretic characterizations of the classes of simple, perfect and soluble finite groups. These we present in § 5.3 together with two characterizations of the class of supersoluble groups. The first of these depends on the main result of § 5.2, the second asserts that a finite group is supersoluble if and only if its subgroup lattice satisfies the Jordan-Dedekind chain condition. This characterization, given by Iwasawa in 1941, and Ore's theorem on cyclic groups are the only results known in which an interesting class of groups is characterized by a property that is important in lattice theory. We finish this section using our results on modular subgroups to determine the finite groups with lower semimodular subgroup lattice.

In § 5.4 we come to the main topic of this chapter. Let \( N \) be a normal subgroup of the finite group \( G \), \( \varphi \) a projectivity from \( G \) to a group \( \bar{G} \), \( H^{\varphi} \) the normal closure and \( K^{\varphi} \) the core of \( N^{\varphi} \) in \( \bar{G} \). We first show that \( H \) and \( K \) are normal subgroups of \( G \), and then use the results of §§ 5.1 and 5.2 to prove a structure theorem due to Schmidt.
[1975a] for $G/K$ and $\overline{G}/K^e$. This theorem, in particular, implies that $H/K$ and $H^e/K^e$ are hypercyclically embedded in $G$ and $\overline{G}$, respectively, and this yields useful criteria for projective images of normal subgroups to be normal in the image group. We mention theorems of Suzuki [1951a] and Schmidt [1972b] which assert that normal subgroups with perfect factor groups or without adjacent cyclic chief factors have this property. Using results in Chapter 4 on singular projectivities, we show that subnormal subgroups of finite groups are mapped by projectivities to subnormal subgroups, modulo the obvious exception of $P$-groups.

The results of §§ 5.2 and 5.4 reduce most problems on projective images of normal subgroups to the study of projectivities between $p$-groups. This, in particular, is the case for the investigation of the finer structure of $H/K$, not only for finite but also for infinite groups, as we shall see in Chapter 6. Therefore in § 5.5 we study this situation; more precisely, we handle the crucial case that $G$ is a finite $p$-group, $G/N$ is cyclic and $K = 1$. In this case we show that $|N'| \leq 2$, $G$ is metabelian and $\overline{G}$ is soluble of derived length at most 3. In § 6.6 we shall use this together with some rather special properties of permutable subgroups, proved in § 6.3, to show that for arbitrary groups, $H/K$ and $H^e/K^e$ are soluble of derived length 4 and 5, respectively. This whole theory was developed in the 1980's by Busetto, Menegazzo, Napolitani and Zacher.

In § 5.6 we show that normalizer preserving projectivities are also centralizer preserving, and present the classic examples, due to Rottländer, Honda, Yff, and Holmes, of projectivities between nonisomorphic groups that preserve indices, conjugacy classes and the isomorphism types of proper subgroups. Finally, we begin to study an important problem that can be regarded as a generalization of the main theme of this chapter: When can we say that a projectivity maps a conjugacy class $\Delta$ of subgroups of $G$ to a conjugacy class of $\overline{G}$? This is interesting because in this case not only $G$ but also $\overline{G}$ operates on $\Delta$. We show that, modulo the obvious exception of $P$-groups, conjugacy classes of maximal subgroups of finite soluble groups are mapped to conjugacy classes by any projectivity.

All groups considered in this chapter are finite except for a few general remarks on modular and permutable subgroups in §§ 5.1 and 5.2, and on normalizer preserving projectivities in § 5.6.

### 5.1 Modular subgroups of finite groups

As already indicated, we shall investigate the structure of $M^G/M_G$ and $G/M_G$ for a modular subgroup $M$ of a finite group $G$. In this section we reduce this problem to the case that $M$ is permutable in $G$. More precisely, we show that if $M$ is not permutable in $G$, then $G/M_G$ is $P$-decomposable.

#### Modularity and permutability

First of all we give a useful criterion for a modular subgroup of a finite group to be permutable; it will be generalized to arbitrary groups in 6.2.10.
5.1 Modular subgroups of finite groups

5.1.1 Theorem. The subgroup $M$ of the finite group $G$ is permutable in $G$ if and only if $M$ is modular and subnormal in $G$.

Proof. First suppose that $M$ is permutable in $G$. Then by 2.1.3, $M$ is modular in $G$. We want to show that $M$ is subnormal in $G$ and use induction on $|G|$. Let $N$ be a maximal permutable subgroup of $G$ containing $M$. We show that $N \trianglelefteq G$; by induction, $M \trianglelefteq N$, and it will follow that $M \trianglelefteq G$. So suppose, for a contradiction, that $N$ is not normal in $G$. Then there exists $x \in G$ such that $N^x \neq N$. For $H \leq G$,

$$HN^x = NHN^x = Nx^{-1}Hx^{-1}N = N^{-1}NH^x = N$$

hence $NN^x$ is permutable in $G$. Since $N$ is a maximal permutable subgroup of $G$, it follows that $NN^x = G$. But then there exist $a \in N$, $b \in N^x$ such that $x = ab$ and we get the contradiction $N = N^x = N^{ab^{-1}} = N^x$. Thus $N \trianglelefteq G$ and $M \trianglelefteq G$.

Conversely suppose that $M$ is modular and subnormal in $G$. We show that $M$ is permutable in $G$, again using induction on $|G|$. Clearly $M$ is modular and subnormal in every subgroup which contains $M$. Let $H \leq G$. If $H \leq M$, then $HM = M = MH$. If $H \not\leq M$, then $M < H \cup M$ and there exists a proper normal subgroup $N$ of $H \cup M$ such that $M \leq N$. It follows that $N < G$ and, by induction, $M(H \cap N) = (H \cap N)M$. The modularity of $M$ implies that $N = (H \cup M) \cap N = M \cup (H \cap N)$ and, since $N \trianglelefteq H \cup M$, we finally get that

$$HM = H(H \cap N)M = HN = NH = M(H \cap N)H = MH.$$ 

Thus $M$ is permutable in $G$.

Since we shall use them constantly, we collect for reference the basic properties of modular subgroups; these were proved more generally for modular elements of lattices in 2.1.5 and 2.1.6. So let $M$ be modular in the (not necessarily finite) group $G$. Then

1. $[H \cup M/M] \simeq [H/H \cap M]$ for all $H \leq G$,
2. $H \cap M \mod H$ for all $H \leq G$.
3. If $N \leq G$, then $M/N$ is modular in $G/N$.
4. If $M \leq M_1 \leq G$ and $M_1 \mod G$, then $M_1 \mod G$. In particular, if $N \leq G$ and $M_1/N \mod G/N$, then $M_1 \mod G$.
5. If $M_1$ and $M_2$ are modular in $G$, then so is $M_1 \cup M_2$.
6. If $\varphi$ is a projectivity from $G$ to a group $\tilde{G}$, then $M \varphi \mod \tilde{G}$.

Permutable subgroups have similar properties. We prove these and also some general results on permutability of subgroups, again for arbitrary groups. So let $H_i (i \in I)$, $H$ and $K$ be subgroups of $G$.

7. If $G$ is finite, then $HK = KH$ if and only if $|H \cup K : K| = |H : H \cap K|$.
Indeed this equation is equivalent to $|HK| = |H \cup K| = |KH|$.

(8) If $H_i K = KH_i$ for all $i \in I$ and $H = \langle H_i | i \in I \rangle$, then $HK = KH$.

For, every $x \in H$ has the form $x = x_1 \ldots x_n$ where $x_i \in H_i$ for some $j \in I$; by induction on $n$, we see that to every $y \in K$ and $x = x_1 \ldots x_n \in H$ there exist $y' \in K$ and $x' \in H$ such that $xy = y'x'$. This is clear by assumption if $n = 1$. And if it is true for $n - 1$, then there exist $y_1, y' \in K$ and $x_n' \in H$ such that

$$xy = x_1 \ldots x_n y = x_1 \ldots x_{n-1} y_1 x_n' = y'x'$$

where $x' = zx_n' \in H$. Thus $HK \subseteq KH$ and the other inclusion is proved in an entirely analogous way. Since every subgroup of $G$ is generated by its cyclic subgroups, an immediate consequence of (8) is the following.

(9) If $X K = K X$ for all cyclic subgroups $X$ of prime power or infinite order of $G$, then $K$ is permutable in $G$.

We come to the basic inheritance properties of permutable subgroups.

(10) If $H_i$ per $G$ for all $i \in I$, then $\langle H_i | i \in I \rangle$ per $G$.

(11) If $H$ per $G$ and $K \leq G$, then $H \cap K$ per $K$.

(12) If $N \trianglerighteq G$ and $H$ per $G$, then $HN/N$ per $G/N$.

(13) If $N \leq G$ and $N \leq H \leq G$ such that $H/N$ per $G/N$, then $H$ per $G$.

Clearly (10) immediately follows from (8). To prove (11), note that for every $X \leq K$, by Dedekind's law, $(H \cap K)X = HX \cap K = XH \cap K = X(H \cap K)$. Finally, (12) and (13) are trivial. We remark that for finite groups (10)--(13) also follow from 5.1.1 and the corresponding properties of modular or subnormal subgroups. Note further that 5.1.1 and Exercise 2.1.3 show that the intersection of two permutable subgroups in general is not permutable.

Maximal modular subgroups

By (5), the join of two modular subgroups of a group is again modular. Therefore, in finite groups, it seems reasonable to study maximal modular subgroups, that is, modular subgroups which are not contained in any larger proper modular subgroup of the group. We are able to show that such a subgroup is nearly normal. This result is basic for everything that follows; for example, it immediately yields the lattice-theoretic characterizations of the classes of simple, perfect and soluble finite groups which will be presented in § 5.3.

5.1.2 Lemma (Schmidt [1969]). If $M$ is a maximal modular subgroup of the finite group $G$, then either $M \leq G$ or $G/M_G$ is nonabelian of order $pq$ for primes $p$ and $q$.

Proof: Let $G$ be a minimal counterexample to the lemma, and take a maximal modular subgroup $M$ of $G$ for which the assertion of the lemma does not hold. By
Let $S$ be a maximal subgroup of $G$ containing $M$. For $x \in S$, $M \leq M \cup M^x \leq S$ and, by (5) and (6), $M \cup M^x \mod G$. The maximality of $M$ implies that $M = M^x$ and hence $M \leq S$. Since $M$ is not normal in $G$, $S$ is the only maximal subgroup of $G$ containing $M$. But then 2.1.5 shows that $S \mod [G/M]$ and, by (4), $S \mod G$. The maximality of $M$ yields $S = M$, that is,

\[(14) \quad M_G = 1.\]

Let $N \neq M$ be a conjugate to $M$ and put $D = N \cap M$. By (1), $[G/M] \cong [N/D]$ and hence $D$ is a maximal subgroup of $N$, and, similarly, of $M$. If $H \neq M$ is a maximal subgroup of $G$ containing $D$, then $H \cup M = G$ and $H \cap M = D$; by (1), $D$ is a maximal subgroup of $H$. Thus

\[(16) \quad [G/D] \setminus \{G, D\} \text{ is an antichain.}\]

We want to show next that $D$ is normal in neither $M$ nor $N$. So suppose, for a contradiction, that $D \triangleleft M$, say. Then $|M : D| = p$ is a prime and every $p'$-element of $M$ is contained in $N$. Since $M$ and $N$ are isomorphic, $N$ cannot contain more $p'$-elements than $M$. It follows that

\[O^p(M) = \langle x \in M | (o(x), p) = 1 \rangle = O^p(N) \leq M \cup N = G.\]

By (14), $O^p(N) = 1$. So $D$ is a maximal subgroup of the $p$-group $N$ and hence $D \leq N$. Therefore $D \leq G$ and, by 2.2.4, $|G/D| = pq$ where $q$ is a prime. This contradicts the choice of $G$. Thus

\[(17) \quad D \text{ is neither normal in } M \text{ nor in } N.\]

By (2) and (6), $D$ is modular in $M$ and in $N$; the minimality of $G$ implies that $M/D_M$ is nonabelian of order $pq$ where $p$, $q$ are primes and $p > q$, say. Since $D$ is not normal in $M$, $|M : D| = p$, hence $|N : D| = p$ and therefore $N/D_N$ is nonabelian of order $pq$.
where \( r < p \) is a prime. Let \( \pi = \{q, r\} \). Then

\[
O^\pi(D) = O^\pi(D_M) = O^\pi(D_N) \leq M \cup N = G
\]

and, by (14), \( O^\pi(D) = 1 \). This shows that \( |M: M \cap N| = p \) is the largest prime dividing \( |M| \) and \( M \cap N \) is a Hall \( p' \)-subgroup of \( M \). This holds for every conjugate \( N \neq M \) of \( M \). The normal \( p' \)-subgroup \( D_M \) of \( M \) is contained in every Hall \( p' \)-subgroup of \( M \), hence in every conjugate of \( M \), and therefore in \( M_G = 1 \). Thus \( D_M = 1 \), that is,

\[
(18) \quad |M| = pq \text{ and } |D| = q < p.
\]

Let \( x \in G \) such that \( N = Mx \). Then \( D \) and \( D^x \) are Sylow \( q \)-subgroups of \( M^x \) and hence there exists \( y \in M^x \) such that \( D = D^{xy} \). Since \( M \neq M^x \), we have \( x \notin M^x \) and therefore \( xy \notin D \). Thus \( T = N_G(D) > D \). By (14), \( T < G \) and then (16) implies that \( D \) is maximal in \( T \), that is,

\[
(19) \quad |T: D| = t \text{ is a prime}.
\]

Since \( M_G = 1 \), there exists a conjugate \( L \neq M \) of \( M \) such that \( D \subseteq T \cap L \). By (1), \( T \cap L \) is maximal in \( T \) and hence of prime order. Since \( D \subseteq T \) of order \( q < p \), \( |T \cap L| = p \) would imply that \( T \) were cyclic of order \( pq \) and hence \( T \cap L \leq T \cup L = G \), contradicting (14). Thus \( |T \cap L| \neq p \) and, since \( |L| = pq \), it follows that \( |T \cap L| = q^2 \). By (1), \( M \) intersects every conjugate of \( T \) in a subgroup of order \( q \). If \( T_1, T_2 \) are different conjugates of \( T \), then \( T_1 \cap M \neq T_2 \cap M \); for, otherwise \( T_1 \cap M = T_2 \cap M \leq T_1 \cup T_2 = G \), contradicting (14). Therefore, since \( M \) has only \( p \) subgroups of order \( q \), \( T \) has at most \( p \) conjugates; on the other hand, \( T \) is a maximal subgroup of \( G \) and \( p \) divides \( |G: T| \). It follows that \( |G: T| = p \) and hence \( |G| = pq^2 \). But then the subgroup of order \( p \) of \( M \) is a Sylow \( p \)-subgroup of \( G \), its normalizer is \( M \), and Sylow's theorem implies that \( q = |G: M| \equiv 1 \pmod{p} \). This contradicts (18).

\[\square\]

The groups \( \langle M, x \rangle \)

In addition to the structure theorem for \( G/M_G \) we want to prove a characterization of modular subgroups in finite groups, due to Previato [1975], that is similar to the useful criterion (9) for permutability. It asserts that \( M \) is modular in the finite group \( G \) if and only if \( M \) is modular in every subgroup \( \langle M, x \rangle \) where \( x \) runs through the elements of prime power order in \( G \). Of course, every modular subgroup has this property, and indeed it is equivalent to modularity. Both results will follow from the fact that a subgroup \( M \) with this property has the desired structure. This we shall prove in a number of steps in the remainder of this section. It should be clear to the reader that all the results we derive in the course of this proof for subgroups having Previato's property, for example (b) of 5.1.5, 5.1.6 and 5.1.12, in particular hold for modular subgroups in finite groups and are useful properties of these.

First of all we have to handle the groups \( \langle M, x \rangle \). By (1) and 1.2.7, the interval \( [M \cup \langle x \rangle, M] \simeq [\langle x \rangle, \langle x \rangle \cap M] \) is a chain if \( M \mod G \) and \( o(x) \) is a prime power. Therefore we shall study this situation.
5.1 Modular subgroups of finite groups

5.1.3 Lemma. If $M$ is modular in the finite group $G$ and $[G/M]$ is a chain, then either $G/M_G$ is a $p$-group or $M$ is a maximal subgroup of $G$ and $G/M_G$ is nonabelian of order $pq$ for primes $p$ and $q$.

Proof. Again let $G$ be a minimal counterexample to the lemma and take a modular subgroup $M$ of $G$ for which the assertion of the lemma does not hold. Then $G/M_G$ is also a counterexample and the minimality of $G$ implies that

$$M_G = 1.$$

By 5.1.2, $[G/M]$ is a chain of length $n \geq 2$; let $H$ be the maximal subgroup of $G$ containing $M$. Then $H \mod [G/M]$, therefore $H \mod G$, by (4), and again 5.1.2 yields that $|G:H| = p$ is a prime. The minimality of $G$, furthermore, implies that either $H/M_H$ is a $q$-group or $M$ is a maximal subgroup of $H$ and $|H:M| = q$ for some prime $q$; in both cases, $|H:M| = q^{n-1}$. Let $P_1 \in \text{Syl}_p(M)$ and take $P \in \text{Syl}_p(G)$ such that $P_1 \leq P$. Since $|G:H| = p$, we have $P \leq H$, and, since $H$ is the only maximal subgroup of $G$ containing $M$, it follows that $P \cup M = G = P \cup H$. If $q \neq p$, then $P_1$ would be a Sylow $p$-subgroup of $H$ contained in the $p$-subgroup $P \cap H$. It would follow that $P \cap H = P_1 = P \cap M$ and then by (1),

$$[G/M] = [P \cup M/M] \simeq [P/P \cap M] = [P/P \cap H] \simeq [P \cup H/H] = [G/H],$$

contradicting $n \geq 2$. Thus $p = q$ and

$$|G:M| = p^n$$

where $n \geq 2$.

Suppose, for a contradiction, that $H$ is not normal in $G$. Then, by 5.1.2, $G/H_G$ is nonabelian of order $pr$ for some prime $r < p$. If $N/H_G$ is the normal subgroup of index $r$ in $G/H_G$, then $MN = G$ and hence $[N/N \cap M] \simeq [G/M]$ is a chain of length $n$. Since $|N/ N \cap M| = |G:M| = p^n$, the minimality of $G$ implies that $N/(N \cap M)_N$ is a $p$-group. It follows that $O^p(N) \leq M$ and, by (20), $O^p(N) = 1$, that is, $N$ is a $p$-group. If $x \in G \setminus H$, then $M \cap M^x \leq H \cap H^x = H_G \leq N$ is a $p$-group and $M \cup M^x = G$ since $M \leq H^x$ and $H^x$ is the only maximal subgroup of $G$ containing $M^x$. As $M^x$ is modular in $G$, $M \cap M^x$ mod $M$ and $[M/(M \cap M^x)] \simeq [G/M^x]$ is a chain of length $n$. Again the minimality of $G$ implies that $M/(M \cap M^x)_M$ is a $p$-group since $r^2$ does not divide the order of $G$. But then $|G:M|, |M:M \cap M^x|$ and $|M \cap M^x|$ are powers of $p$ and hence $G$ is a $p$-group. This contradicts the choice of $G$. Thus we have shown that

$$H \leq G.$$

Since $G$ is not a $p$-group, there exists a prime $s \neq p$ dividing $|G|$; let $S \in \text{Syl}_s(G)$ and $T = N_G(S)$. If $S \leq G$, then (21) would imply that $S \leq M$, contradicting (20). Thus $S$ is not normal in $G$, that is, $T \neq G$. Since $H$ is a normal subgroup of index $p$ in $G$, $S \leq H$ and the Frattini argument yields that $G = HN_G(S) = HT$. It follows that $T \leq H$ and hence $T \cup M^x = G$ for all $x \in G$ since $H$ is the only maximal subgroup of $G$ containing $M^x$. Again $M^x$ mod $G$ implies that $T \cap M^x$ mod $T$ and $[T/T \cap M^x] \simeq [G/M^x]$ is a chain of length $n$; furthermore $|T : T \cap H| = p$ divides $|T : T \cap M^x|$. Therefore the minimality of $G$ implies that $T/(T \cap M^x)_T$ is a $p$-group and it follows that $S \leq (T \cap M^x)_T \leq M^x$ for all $x \in G$. But then $S \leq M_G = 1$, a final contradiction. □
We come back to the groups $\langle M, x \rangle$ for $x$ of prime power order or, more generally, such that

$$o(x, M) = |\langle x \rangle : \langle x \rangle \cap M|$$

is a power of a prime. In particular, we are interested to know when $M$ and $\langle x \rangle$ permute.

5.1.4 Corollary. Let $M$ be modular in the finite group $T$ and suppose that $T = \langle M, x \rangle$ where $o(x, M) = p^n$, with $p$ a prime, and $n \in \mathbb{N}$. Then one of the following holds.

1. $T/M_T$ is a $p$-group and $M$ is permutable in $T$; in particular, $M\langle x \rangle = \langle x \rangle M$.

2. $T/M_T$ is nonabelian of order $pq$ for some prime $q$ and $|M : M_T| = q < p$; here $M\langle x \rangle = \langle x \rangle M$.

3. $T/M_T$ is nonabelian of order $pq$ for some prime $q$ and $|M : M_T| = p < q$; here $M\langle x \rangle \neq \langle x \rangle M$.

Proof. If $x \in M$, (23) holds. So suppose that $x \notin M$. By (1) and 1.2.7, $[T/M] \cong [\langle x \rangle/\langle x \rangle \cap M]$ is a chain and, since $x \notin M_T$, $p$ divides $|T/M_T|$. Therefore 5.1.3 shows that $T/M_T$ is a $p$-group or nonabelian of order $pq$ where $q$ is a prime. In the first case, $M \trianglelefteq T$; therefore, by 5.1.1, $M$ is permutable in $T$ and (23) holds. In the second case, $M$ is not normal in $T$ and hence $|M : M_T|$ is the smaller of the primes $p$ and $q$. So if $p > q$, $|M : M_T| = q$ and hence $|\langle x \rangle \cup M : M| = p = |\langle x \rangle : \langle x \rangle \cap M|$; by (7), $M\langle x \rangle = \langle x \rangle M$ and (24) is satisfied. Finally, if $p < q$, then $|M : M_T| = p$ and $|\langle x \rangle \cup M : M| = q \neq p = |\langle x \rangle : \langle x \rangle \cap M|$; again by (7), $M\langle x \rangle \neq \langle x \rangle M$ and (25) holds.

An immediate consequence of 5.1.4 is the second part of the following useful result.

5.1.5 Lemma. Let $G$ be a finite group and suppose that $M, H \leq G$ such that $(|M|, |H|) = 1$.

(a) If $M$ is permutable in $G$, then $H \leq N_G(M)$.

(b) If $M$ is modular in $\langle M, x \rangle$ for all $x \in H$ of prime power order, then $MH = HM$.

Proof. (a) Clearly, $|MH : M| = |H : H \cap M|$ is prime to $|M|$; on the other hand, for $x \in H$, $|MM^x : M| = |M^x : M \cap M^x|$ divides $|M|$. Since $M \leq MM^x \leq MH$, it follows that $M = MM^x$ and hence $M = M^x$.

(b) If $x \in H$ has prime power order, then $M \mod \langle M, x \rangle$ and, since $(|M|, |H|) = 1$, (25) cannot hold for $T = \langle M, x \rangle$. Therefore 5.1.4 implies that $M\langle x \rangle = \langle x \rangle M$ and, by (8), $MH = HM$.

The structure of $M/M_G$

To determine the structure of $M/M_G$ we need a description of $M_G$ in terms of the groups $M_{\langle M, x \rangle}$ for $x \in G$ of prime power order. To obtain this we define for any
5.1 Modular subgroups of finite groups

(26) \( H^X = \langle H^x | x \in X \rangle \).

If \( Y \subseteq G \), then \( (H^X)^Y = \langle H^x | x \in X \rangle^Y = \langle H^{xy} | x \in X, y \in Y \rangle \) and hence

(27) \( (H^X)^Y = H^{XY} \) for \( H \leq G \) and arbitrary subsets \( X, Y \) of \( G \).

If \( X \) is a subgroup of \( G \), then clearly \( X \leq N_G(H^X) \); furthermore, (27) implies that

(28) \( (H^X)^Y = (H^Y)^X \) for \( X, Y \leq G \) such that \( XY = YX \).

5.1.6 Lemma. Let \( G_0 \) be the set of elements of prime power order in the finite group \( G \). If \( M \) is modular in \( \langle M, x \rangle \) for all \( x \in G_0 \), then \( M_G = \bigcap \{ M_{\langle M, x \rangle} | x \in G_0 \} \).

Proof. Since \( L = \bigcap \{ M_{\langle M, x \rangle} | x \in G_0 \} \) is an intersection of conjugates of \( M \), it clearly contains the intersection \( M_G \) of all these conjugates. We have to prove the other inclusion \( L \leq M_G \), that is, \( L \leq M^g \) for all \( g \in G \). We use induction on the number \( r \) of primes dividing \( o(g) \) to show that if \( 1 \neq x_i \in G_0 \) such that \( \langle g \rangle = \langle x_1 \rangle \times \cdots \times \langle x_r \rangle \), then

(29) \( M_{\langle M, g \rangle} = \bigcap_{i=1}^{r-1} M_{\langle M, x_i \rangle} \).

Since the left hand side of this equation is contained in \( M^g \) and the right hand side contains \( L \), it will follow that \( L \leq M^g \).

For \( r = 1 \), (29) is trivial. So let \( r \geq 2 \) and assume that the assertion is true for \( r - 1 \). For every \( i = 1, \ldots, r \), \( M \) is modular in \( \langle M, x_i \rangle \) and hence, by 5.1.4, any of these groups must have one of the properties (23)–(25). Without loss of generality we may choose the notation in such a way that \( \langle M, x_r \rangle = T \) satisfies (24) or, if there is no such \( x_r \), it satisfies (25) if there is an \( x_i \) with this property. Furthermore write \( \langle M, g \rangle = H, \langle M, x_1, \ldots, x_{r-1} \rangle = S, x_1 \cdots x_{r-1} = x, x_r = y, X = \langle x \rangle \) and \( Y = \langle y \rangle \). Then \( \langle x \rangle = \langle x_1 \rangle \times \cdots \times \langle x_{r-1} \rangle \), hence by our induction assumption,

(30) \( M_S = \bigcap_{i=1}^{r-1} M_{\langle M, x_i \rangle} \)

and we have to show that

(31) \( M_H = M_S \cap M_T \).

This is clear if \( T \leq S \); for, then \( S = H \) and hence \( M_H = M_S = M_S \cap M_T \). Therefore suppose that \( T \not\leq S \) and let \( D = M_S \cap M_T \). Since \( M_H \) is normal in \( S \) and \( T \), \( M_H \leq M_S \) and \( M_H \leq M_T \) and hence

(32) \( M_H \leq D \).

If \( M \) permutes with all the \( \langle x_i \rangle \), then, by (8), \( M \) also permutes with \( \langle x_1 \rangle \cdots \langle x_{r-1} \rangle = X \) and \( Y \). It follows that \( |S : M| = |MX : M| = |X : X \cap M| \) is coprime to \( |Y : Y \cap M| = |T : M| \) and hence \( S \cap T = M \). If \( M \) does not permute with \( \langle x_j \rangle \), say, then, by 5.1.4, \( \langle M, x_j \rangle \) satisfies (25) and our choice of \( x_j \) implies that \( M \) is a maximal subgroup of \( T \). Since \( T \not\leq S \), again it follows that \( S \cap T = M \). Thus in any event
(33) \( S \cap T = M \).

Since \( D \leq M_S \leq S \), we see that \( (D^Y)^x \leq (M_S)^Y \leq T \) and, similarly, \( (D^Y)^x \leq S \). As \( X \) and \( Y \) are contained in \( \langle g \rangle \), they permute and, by (27) and (28), \( D^{XY} = (D^Y)^x = (D^Y)^x \leq S \cap T \); that is,

\[
(34) \quad D^{XY} \leq M.
\]

Now suppose first that \( MY = YM \). Then \( (D^{XY})^M = (D^X)^{YM} \) is invariant under \( YM = T \) and contained in \( M \). Thus \( (D^X)^{YM} \leq M_T \); in particular, \( D^X \leq M_T \). Since \( D \leq M_S \leq S \), it follows that \( D^X \leq M_S \) and hence \( D^X \leq M_S \cap M_T = D \). Thus \( D^X = D \) and \( (D^Y)^x = (D^X)^Y = D^Y \). Since also \( (D^Y)^M = (D^M)^Y = D^Y \), it follows that \( D^X \leq \langle M, X, Y \rangle = H \). This implies that \( D \leq D^Y \leq M_H \) and, by (32), \( D = M_H \), as desired.

So, finally, suppose that \( MY \neq YM \). Then (25) holds for \( T \) and our choice of \( x \), implies that none of the \( \langle M, x_i \rangle \) satisfies (24). Therefore, by 5.1.4, for every \( i \in \{1, \ldots, r\} \), the group \( M/M_{\langle M, x_i \rangle} \) is a p-group if \( x_i \) is a p-element. Since the orders of the \( x_i \) are pairwise coprime, it follows from (30) that \( |M/M_S| \) is prime to \( |M/M_T| \) and hence \( M_S \cup M_T = M \). If \( D^X \neq D \), then \( D < D^X \leq M_S \) and hence \( D^X = M_S \) since \( |M_S : D| = |M : M_T| \) is a prime. By (34), \( M_S \leq D^{XY} \leq M \) and so \( M = D^{XY} \cup M_T \) would be invariant under \( Y \); but \( M \) does not even permute with \( Y \). Thus \( D^X = D \). Again \( (D^Y)^x = (D^X)^Y = D^Y \) and, clearly, \( (D^Y)^M = (D^M)^Y = D^Y \). Since \( D \leq D^Y \leq M_T \) and \( M/D = M_S/D \times M_T/D \), we obtain \( D^Y \leq M \) and hence \( D^Y \leq M \cup X = S \). As \( D^Y \leq M \), it follows that \( D^Y \leq M_S \) and then \( D^Y \leq M_S \cap M_T = D \). Thus \( D^Y = D \) and so, finally, \( D \leq \langle M, X, Y \rangle = H \). This implies that \( D \leq M_H \) and (32) shows that \( D = M_H \), as desired. □

It is clear that \( M_G \leq \bigcap \{ M_{\langle M, x \rangle} | x \in G_0 \} \leq \bigcap \{ M^x | x \in G_0 \} \) holds for arbitrary \( M \leq G \). We remark that for a modular subgroup \( M \) of a finite (or periodic) group \( G \),
the proof of even the assertion $M_G = \bigcap \{ M^x | x \in G_0 \}$ is much easier than that of 5.1.6; one can assume that $G = \langle M, x \rangle$ for some $x \in G$ and then use induction on $o(x, M)$ (see Stonehewer [1976b]). We shall see in 6.2.3 that this result generalizes to modular subgroups of arbitrary groups; also this proof is easier than that of 5.1.6.

If $M \mod <M, x>$ and $x \in G$ is of prime power order, then, by 5.1.4, $M/M_{<M, x>}$ is nilpotent. It follows that $M/\bigcap \{ M_{<M, x>} | x \in G_0 \}$ and therefore, by 5.1.6, that

(35) $M/M_G$ is nilpotent if $M \mod <M, x>$ for every $x \in G_0$.

In particular, we have our first general result on the structure of $M^G/M_G$ for a modular subgroup $M$ of $G$.

5.1.7 **Theorem** (Schmidt [1969]). If $M$ is modular in the finite group $G$, then $M/M_G$ is nilpotent.

By 5.1.7, the proof of our main theorem divides into two parts. We first prove the result for modular subgroups of prime power order, and then show that for an arbitrary modular subgroup $M$ of $G$, the Sylow subgroups of $M/M_G$ are modular in $G/M_G$. The first part, the proof of Lemma 5.1.9, is a combination of ideas of Previato [1975] and Schmidt [1970a]; in the second part we shall mainly follow Previato's paper.

**Modular subgroups of prime power order**

We shall need the following simple lemma to establish the modularity in $G$ of a subgroup $M$ for which $G/M_G$ has the correct structure.

5.1.8 **Lemma.** Let $G = G_1 \times G_2$ and $(\{|G_1|, |G_2|\}) = 1$. If $M_i \mod G_i$ for $i = 1, 2$, then $M_1 \times M_2 \mod G$.

**Proof.** By 1.6.4, $L(G) \cong L(G_1) \times L(G_2)$. Since the modular laws (2) and (3) of § 2.1 hold for $M_i$ in $L(G_i)$, they also hold for $(M_1, M_2)$ in $L(G_1) \times L(G_2)$ and hence for $M_1 \times M_2$ in $L(G)$. \(\square\)

We come to the first part of the program described above.

5.1.9 **Lemma.** If $M$ is a subgroup of prime power order of the finite group $G$, then the following properties are equivalent.

(a) $M$ is modular in $G$.

(b) $M$ is modular in $\langle M, x \rangle$ for all $x \in G$ of prime power order.

(c) $M$ is permutable in $G$ or $G/M_G = M^G/M_G \times K/M_G$ where $M^G/M_G$ is a non-abelian $P$-group of order prime to $|K/M_G|$.

**Proof.** If the first alternative in (c) holds, then, by 2.1.3, $M$ is modular in $G$; if the second one is satisfied, then 5.1.8 shows that $M/M_G$ is modular in $G/M_G$ and, by (4), $M$ is modular in $G$. Thus (a) follows from (c) and, clearly, (b) follows from (a). It remains to be shown that (b) implies (c).
Let $G$ be a minimal counterexample to this assertion and take a $q$-subgroup $M$ of $G$, $q$ a prime, satisfying (b) but not (c). If $N$ is a normal subgroup of $G$ contained in $M$ and $gN \in G/N$ of prime power order, then there exists $g' \in G$ of prime power order such that $gN = g'N$. Because $M \mod \langle M, g' \rangle$, we obtain $M/N \mod \langle M, g' \rangle/N = \langle M/N, gN \rangle$; hence $M/N$ satisfies (b) in $G/N$. The minimality of $G$ implies that

\[(36) \quad M_G = 1.\]

There exists $x \in G$ of prime power order such that $M$ is not permutable in $\langle M, x \rangle$; otherwise, by (9), $M$ would be permutable in $G$. Put $S = \langle M, x \rangle$. Since $M$ is a $q$-group, 5.1.4 shows that $S/M_S$ is nonabelian of order $pq$ where $q < p \in \mathbb{P}$ and we may assume that $o(x) = p$. Then $M \langle x \rangle = \langle x \rangle M$ so that

\[(37) \quad S = MX \text{ where } |X| = p > q \text{ and } S/M_S \text{ is nonabelian of order } pq.\]

It follows that $S \leq M^G$ and hence $M$ is not permutable in $M^G$. Therefore if $M^G \leq H < G$, then (37) implies that $p$ and $q$ divide $|M^H/M_H|$ and the minimality of $G$ yields that $H/M_H = H^M \times L$ where $H^M/M_H$ is a $p$-group of order $p^aq$ ($n \in \mathbb{N}$) and $(|L|, pq) = 1$. Then $M$ is a Sylow $q$-subgroup of $H$, hence of $M^G$, and it follows that the core and the normal closure of $M$ in $M^G$ are characteristic subgroups of $M^G$ and hence normal subgroups of $G$. Now $M^G \leq H \leq G$ trivially implies that

\[M_G \leq M_H \leq M_{M^G} \leq M \leq M^{M^G} \leq M^H \leq M^G\]

and the normality of $M_{M^G}$ and $M^{M^G}$ yields that $M_{M^G} = M_H = M_G = 1$ and $M^{M^G} = M^H = M^G$. Thus we have shown:

\[(38) \quad \text{If } M^G \leq H < G, \text{ then } M^G \text{ is a } P\text{-group of order } p^aq \text{ (} n \in \mathbb{N} \text{) and } H = M^G \times L \text{ where } (|M^G|, |L|) = 1.\]

Now we distinguish two cases.

Case 1: $|M| \geq q^2$.

Then $M_S \neq 1$ and hence $N_G(M_S) \neq G$. If $O^q(G) \leq N_G(M_S)$, there would exist a proper normal subgroup $N$ of $G$ such that $M \leq N_G(M_S) \leq N$. It would follow that $M^G < G$ and (38) would show that $|N| = q$, a contradiction. Therefore $O^q(G)$ is not contained in $N_G(M_S)$, that is, there exist $q'$-elements in $G \setminus N_G(M_S)$ and then also such elements of prime power order.

So let $y \in G \setminus N_G(M_S)$ such that $o(y) = r^n$ where $r \neq q$ is a prime. Since $x \in N_G(M_S)$, also $y^x \in G \setminus N_G(M_S)$ of order $r^m$. And if $y \in N_G(M)$, then $y^x \notin N_G(M)$ since otherwise $y^x$ would normalize $M$ and $M^x$ and hence $M \cap M^x = M_S$. Therefore we may assume without loss of generality that $y \notin N_G(M)$. Then $H = \langle M, x, y \rangle$ is a counterexample to our assertion; for, $M$ is not permutable in $S \leq H$ and, since $M_H < M_S$, we conclude that $|M : M_H| \geq q^2$ so that $H/M_H$ cannot have the structure given in (c). The minimality of $G$ yields that $G = H = \langle M, x, y \rangle$. Now 5.1.5 first of all shows that $\langle y \rangle$ permutes with $M$ and $M^x$ and hence also with $M \cup M^x = S$; thus $G = S\langle y \rangle$. Secondly it yields that $M$ is not permutable in $T = \langle M, y \rangle$ since otherwise $y$ would normalize $M$. By 5.1.4, $T/M_T$ is nonabelian of order $rq$, hence $o(y) = r$ and so, finally,

\[(39) \quad |G| = |S||\langle y \rangle| = |M|pr.\]
Since $M_S$ is not normalized by $y$, $M_S \neq M_T$ and hence $M = M_S \cup M_T$. It follows that

$$T = M \cup M^y = M \cup (M_T)^y \cup (M_S)^y = M \cup (M_S)^y \leq M \cup M^{xy}$$

and $M^x \leq T$ since $S \cap T = M$; therefore also $M^{xy} \leq T$. Thus $T < M \cup M^{xy}$ and since $|G : T| = p$, it follows that

$$40) \quad M \cup M^{xy} = G.$$ 

If $r = p$, we could choose $y$ from a Sylow $p$-subgroup of $G$ containing $x$. Then $o(xy) = p$ and our assumption (b) together with (40) would imply that $M$ is modular in $\langle M, xy \rangle = G$. It would follow that $[G/M] \cong [\langle xy \rangle/1]$ and hence $M$ would be a maximal subgroup of $G$, a contradiction. Thus $r < p$. Now 5.1.5 shows that every subgroup of order $p$ permutes with $M$ and $M^x$, and hence with $M \cup M^x = S$; therefore it is contained in $S$ since $|G : S| = r$. Similarly, every element of order $r$ of $G$ is contained in $T$ and it follows that $S$ and $T$ are the only maximal subgroups of $G$ containing $M$. By (40), $M^{xy} \cap S$ and $M^{xy} \cap T$ are proper subgroups of $M^{xy}$ and hence there exists $z \in M^{xy}$ such that $z \not\in S$ and $z \not\in T$. Since $o(z)$ is a power of $q$, again (b) implies that $M$ mod $\langle M, z \rangle = G$, but $L(\langle z \rangle) \cong [G/M]$ is not a chain. This contradiction shows that Case 1 cannot occur.

**Case 2:** $|M| = q$.

By (37), $|MX| = pq$ and we first want to show that $M^G$ is a $P$-group of order $p^nq$ for some $n \in \mathbb{N}$. For this let $M = M_0, M_1, \ldots, M_k$ be the conjugates of $M$ in $G$. If $R < G$ of prime order $r > q$, then by 5.1.5, $R$ permutes with every $M_i$; hence $|M_i \cup R| = rq$ and $R \leq M_i \cup R$. Thus

$$41) \quad M^G \leq N_G(R) \text{ for every } R \leq G \text{ of prime order } r > q.$$ 

For $i = 1, \ldots, k$, furthermore, $M$ is modular in $M \cup M_i$ and hence, by 5.1.4, $|M \cup M_i| = qr_i$ for $r_i \in \mathbb{P}$. Since $M \cup M_i$ contains two different subgroups of order $q$, $r_i \geq q$. Suppose, for a contradiction, that $r_i = q$ for some $i$. Then, by (41), $H = X(M \cup M_i)$ has order $pq^2$ and $XM$ is the only subgroup of order $pq$ of $H$ containing $M$. Since $M$ is not normal in $XM$, there exists a Sylow $q$-subgroup $Q \neq M \cup M_i$ of $H$ and in $Q$ an element $z$ not contained in any of the two proper subgroups $Q \cap XM$ and $Q \cap (M \cup M_i)$ of $Q$. Then $M$ is modular in $\langle M, z \rangle \neq XM$, hence $|\langle M, z \rangle| = q^2$ and $M \leq \langle M, z \rangle \cup M_i = H$, a contradiction. Thus $r_i > q$ for all $i$. Now suppose, for a contradiction, that $r_i \neq p$ for some $i$; let $r_i = r$. If $R$ is the subgroup of order $r$ in $M \cup M_i$ and again $H = X(RM)$, then $H = XRM$ has order $prq$ and, by (41), $X$ and $R$ are normal in $H$. Therefore $XM$ and $RM$ are the only maximal subgroups of $H$ containing $M$ and it follows that $M = N_H(M)$. Thus $H$ contains $|H : M| = pr$ conjugates of $M$ and all of these have to lie in one of the two maximal subgroups of $H$ containing $M$. But these two groups only contain $p + r - 1$ subgroups of order $q$, a contradiction. So we have shown that $|M \cup M_i| = pq$ for all $i = 1, \ldots, k$. If $P_i$ is the subgroup of order $p$ in $M \cup M_i$, then, by (41), $P_i \leq M^G$ and hence $P = P_1 \cup \cdots \cup P_k$, as a product of normal subgroups of order $p$ of $M^G$, is an elementary abelian normal $p$-subgroup of $M^G$. Furthermore

$$M^G = M \cup M_1 \cup \cdots \cup M_k = M(P_1 \cup \cdots \cup P_k) = MP$$
and, again by (41), every subgroup of \( P \) is normal in \( M^G \). It follows that

(42) \( M^G \) is a \( P \)-group of order \( p^nq \) for some \( n \in \mathbb{N} \).

We want to show next that \( M^G \) is a Hall subgroup of \( G \). For this let \( t \) be a prime and \( g \in G \setminus M^G \) be a \( t \)-element. Every conjugate \( M_i \) of \( M \) is modular in \( \langle M_i, g \rangle = W \). If \( W/(M_i)_w \) were a \( P \)-group, we would have \( g \in W = M_i \cup M_i^g \leq M^G \), a contradiction. Therefore, by 5.1.4, \( M_i \) is permutable in \( W \). Now suppose that \( t \neq q \). Then 5.1.5 implies that \( M_i \) is a \( W \) so that in this case, \( g \) normalizes every subgroup of order \( q \) of \( M^G \). If \( Y \) is a \( p \)-subgroup of \( M^G \), then \( YM \) is a \( P \)-group; hence it is normalized by \( g \) and it follows that \( Y^g = Y \). Thus \( g \) induces a power automorphism in \( M^G \) which, by 1.4.3, has to be trivial since \( Z(M^G) = 1 \). We have shown:

(43) If \( g \in G \setminus M^G \) is of prime power order \( t^m \), then \( M<g> = <g>M \) and, for \( t \neq q \), \( g \in C_G(M^G) \).

Now suppose, for a contradiction, that \( M^G \) is not a Hall subgroup of \( G \). Then there exists a subgroup \( H \) of \( G \) such that \( M^G \leq H \) and \( |H : M^G| = t \) where \( t = p \) or \( t = q \). By (38), \( H = G \) and hence \( |G : M^G| = t \). Let \( T \) be a Sylow \( t \)-subgroup of \( G \) and \( g \in T \setminus M^G \). Then (43) shows that \( g \in C_G(M^G) \) for \( t = p \), and that \( \langle M, g \rangle = M^g \) is abelian for \( t = q \) since it is a \( q \)-group and \( |G| = p^aq^2 \) in that case. Thus in both cases, \( g \in C_G(M) \) and, since \( T \) is generated by the elements in \( T \setminus M^G \), it follows that \( T \leq C_G(M) \). Since \( T \) was an arbitrary Sylow \( t \)-subgroup, this implies that \( M \leq Z(M^G) \) if \( t = p \), and that \( M \leq O_q(G) \) if \( t = q \); both assertions contradict (42).

Thus \( M^G \) is a normal Hall subgroup of \( G \). By the Schur-Zassenhaus Theorem there exists a complement \( K \) to \( M^G \) in \( G \) and, by (43), \( K \leq C_G(M^G) \). But then \( G = M^G \times K \) satisfies (c), a final contradiction.

**The Sylow subgroups of \( M/M_G \)**

We want to show next that for a modular subgroup \( M \) of a finite group \( G \), the Sylow subgroups of \( M/M_G \) are modular in \( G/M_G \). This is quite simple for permutable subgroups; in fact, we prove a more general result for these, which we shall extend in 6.2.16.

5.1.10 Lemma. If \( M \) is a nilpotent permutable subgroup of the finite group \( G \), then every Sylow subgroup of \( M \) is permutable in \( G \).

**Proof.** Let \( q \) be a prime and \( Q \in Syl_q(M) \). By (9), we have to show that \( Q \) permutes with every (cyclic) subgroup \( X \) of \( G \) of prime power order \( p^a \). Let \( H = MX \). If \( p = q \), we consider a Sylow \( p \)-subgroup \( P \) of \( H \) containing \( X \). Since \( |M : M \cap P| = |MP : P| \) is prime to \( p \), \( M \cap P \) is a Sylow \( p \)-subgroup of \( M \), that is, \( M \cap P = Q \). By (11), \( Q \) is permutable in \( P \) and therefore \( QX = XQ \). Now let \( p \neq q \). Then \( |H : M| = |X : X \cap M| = p^m \) for some \( m \in \mathbb{N} \) and hence \( |M : M \cap M'| = |MM' : M| \) is a power of \( p \) for every \( y \in H \). It follows that \( Q \leq M_H \); since it is a Sylow subgroup of the nilpotent normal subgroup \( M_H \) of \( H \), we conclude \( Q \leq H \). Thus \( QX = XQ \) in this case too. 

\( \square \)
5.1 Modular subgroups of finite groups

The corresponding statement for modular subgroups is not true in general (see Exercise 3); however it holds if $M$ is a Hall subgroup of $G$.

5.1.11 Lemma. If $M$ is a nilpotent modular subgroup of the finite group $G$ and $(|G:M|,|M|) = 1$, then every Sylow subgroup of $M$ is modular in $G$.

Proof. Let $G$ be a minimal counterexample to the lemma, let $M$ be a nilpotent modular subgroup of $G$ such that $(|G:M|,|M|) = 1$, and suppose that $Q$ is a Sylow $q$-subgroup of $M$ which is not modular in $G$. By 5.1.9 there exists $x \in G$ of prime power order such that $Q$ is not modular in $\langle Q, x \rangle$ and the minimality of $G$ implies that $\langle M, x \rangle = G$. By 5.1.10, $M$ is not permutable in $G$ and then 5.1.4 shows that $M$ is a maximal subgroup of $G$ and $G/M_G$ is nonabelian of order $pt$ where $p$ and $t$ are primes such that $p > t$, say. It follows that $|G:M| = p$ is prime to $|M|$ and there exists $Y \leq G$ such that $|Y| = p$ and $G = MY$.

Since $Q$ is not modular in $G$ but $L(G/M_G)$ is modular, $M_G \neq 1$; let $N$ be a minimal normal subgroup of $G$ contained in $M_G$. Then $M/N$ is a nilpotent modular Hall subgroup of $G/N$ and the minimality of $G$ implies that $QN/N \mod G/N$. By (4), $QN \mod G$. As a Sylow subgroup of the nilpotent normal subgroup $M_G$ of $G$, $Q \cap M_G \leq G$. So if $Q \cap M_G \neq 1$, we could choose $N \leq Q \cap M_G$ and would get the contradiction $Q = QN \mod G$. Therefore $Q \cap M_G = 1$ and hence $t = q$ and $|Q| = q$.

We want to show next that there exists a subgroup $P$ of order $p$ in $G$ such that $Q$ is not modular in $Q \cup P$. Since $x \notin M_G$ and $|G:M_G| = pq$, $x$ is either a $p$-element or a $q$-element. As $p^2 \nmid |G|$, we may take $P = \langle x \rangle$ if $x$ is a $p$-element. And if $x$ is a $q$-element, there exists a Sylow $q$-subgroup of $G$ containing $x$. Since $Q \in \text{Syl}_q(G)$ and $G = MY$, we can find $a \in M$, $y \in Y$ such that $x = Q^y = Q^y$, and then $\langle Q, x \rangle \leq \langle Q, Q^y \rangle \leq \langle Q, y \rangle$. Thus $Q$ is not modular in $\langle Q, y \rangle$ and we may take $P = \langle y \rangle$ in this case.

Now $QN \mod G$ and $(|QN|,|P|) = 1$. By 5.1.5, $QN$ permutes with $P$ and hence $|QNP : QN| = p$ is prime to $|QN|$. So if $QNP < G$, the minimality of $G$ would imply that $Q \mod QNP$, a contradiction. Thus $QNP = G$ and therefore $N = M_G$ and $M = Q \times N \leq C_G(N) \leq G$. It follows that $C_G(N) = G$ and, since $N$ is a minimal normal subgroup of $G$, $|N| = r$ is a prime and $|G| = pqr$. The subgroup $NP$ of index $q$ in $G$ is normal in $G$ and cyclic since $N \leq Z(G)$. It follows that $P \leq G$ and hence $|Q \cup P| = pq$. But then, of course, $Q \mod Q \cup P$, a final contradiction.

5.1.12 Lemma. Let $G$ be a finite group and $M \leq G$ such that $M$ is modular in $\langle M, x \rangle$ for every $x \in G$ of prime power order. If $Q/M_G$ is a Sylow subgroup of $M/M_G$, then $Q$ is modular in $G$.

Proof. Let $G$ be a minimal counterexample to the lemma, let $M$ be modular in $\langle M, x \rangle$ for every $x \in G$ of prime power order, and suppose that $Q/M_G$ is a Sylow $q$-subgroup of $M/M_G$ such that $Q$ is not modular in $G$. Then $G/M_G$ too is a counterexample since the assumptions on $M$ are also satisfied by $M/M_G$ in $G/M_G$, as we have shown at the beginning of the proof of 5.1.9, and since, by (4), $Q/M_G$ is not modular in $G/M_G$. The minimality of $G$ implies that

$M_G = 1$. 

(44)
Then by (35),

\[(45) \text{M is nilpotent}\]

and, by 5.1.9, there exists $x \in G$ of prime power order such that $Q$ is not modular in $\langle Q, x \rangle$. Again 5.1.10 shows that $M$ is not permutable in $\langle M, x \rangle = S$ and, by 5.1.4, $S/M_S$ is nonabelian of order $p|M:M_S|$ where $p > |M:M_S|$ are primes. Since every Sylow subgroup of the nilpotent normal subgroup $M_S$ is normal in $S$, $Q \not\leq M_S$ and hence $|M:M_S| = q$. Furthermore we claim that we may assume that $o(x)$ is a power of $p$ and $M$ permutes with $\langle x \rangle$, that is, we have the following situation:

\[(46) \text{There exists } x \in G \text{ such that } o(x) = p^n, S = \langle M, x \rangle = M<x>, S/M_S \text{ is non-}\]

abelian of order $pq$, $p > q$ and $Q$ is not modular in $\langle Q, x \rangle$.

Indeed, since $|S:M| = p$ and $|M:M_S| = q \neq p$, there exist cyclic $p$-subgroups $Z$ of $S$ such that $S = M \cup Z$, and 5.1.4 shows that any such $Z$ permutes with $M$. So if $x$ is a $p$-element, then $S = M<x>$ and (46) holds. If $x$ is not a $p$-element, then $x$ is a $q$-element, since $|S/M_S| = pq$, and therefore $x$ is contained in a Sylow $q$-subgroup of $S$. As $S = MZ$, there are $a \in M$, $z \in Z$ such that $x \in Q^a = Q^z$ and hence $\langle Q, x \rangle \leq \langle Q, Q^z \rangle \leq \langle Q, z \rangle$. Then $Q$ is not modular in $\langle Q, z \rangle$ and (46) holds with $x$ replaced by $z$.

Now if $(p, |M|) = 1$, then the assumption of 5.1.11 would be satisfied in $S$ and hence $Q \mod S$, contradicting (46). Thus $p$ divides $|M|$; let $P$ be the Sylow $p$-subgroup of $M$. Now $N_G(P) \neq G$ since $M_G = 1$; let $y \in G \setminus N_G(P)$ of prime power order and put $T = \langle M, y \rangle$. If $P \leq M_T$, then as a Sylow subgroup of the nilpotent normal subgroup $M_T$ of $T$, $P \leq T$, contradicting the choice of $y$. Thus $p$ divides $|M:M_T|$ and, by 5.1.4,

\[(47) \frac{M}{M_T} \text{ is a } p\text{-group.}\]

Suppose, for a contradiction, that $H = \langle M, x, y \rangle < G$ and let $N = M_H$. Then the minimality of $G$ yields that $QN/N$ is modular in $H/N$ and hence $QN \mod H$, by (4). If $QN$ per $H$, then $Q$ per $H$, by 5.1.10; but $Q$ is not even modular in $H$. Therefore $QN/N$ is not permutable in $H/N$ and, by 5.1.9, $H/N = A/N \times B/N$ where $(|A/N|, |B/N|) = 1$ and $A/N = (QN/N)^{H/N}$ is a nonabelian $P$-group. By (47), $p$ divides $|M/N|$. Since $M$ is nilpotent, $QN/N$ is centralized by $PN/N$ and so 2.2.2 implies that $PN/N \leq B/N$. It follows that $|H:B|$ is prime to $p$, hence $x \in B$ and then $(QN)^x = QN$. Since $QN$ is nilpotent, this implies that $Q^x = Q$, contradicting (46). Thus $H = G$, that is,

\[(48) G = \langle M, x, y \rangle = S \cup T.\]

Let $L$ be the $\{p, q\}$-complement of $M$, that is, $M = P \times Q \times L$. Then $L \leq M_S \cap M_T$ and, as a characteristic subgroup of $M_S \leq S$, $L \leq S$; similarly, $L \leq T$ and so $L \leq S \cup T = G$. Since $M_G = 1$, it follows that $L = 1$, that is,

\[(49) M = P \times Q.\]

Now let $R$ be any Sylow subgroup of $G$ and $z \in R$. Then by assumption, $M$ is modular in $\langle M, z \rangle = U$ and, by 5.1.4, $M/M_U$ is a group of prime power order. Therefore either $P \leq M_U$ or $Q \leq M_U$ and, since $M_U$ is nilpotent, this again implies that $P \leq U$ or $Q \leq U$, that is, $z \in N_R(P)$ or $z \in N_R(Q)$. Since $R$ cannot be the set-
5.1 Modular subgroups of finite groups

Theoretic union of two proper subgroups, it follows that \( R = N_R(Q) \) or \( R = N_R(P) \). Thus:

\[ (50) \text{ If } R \text{ is a Sylow subgroup of } G, \text{ then } R \leq N_G(P) \text{ or } R \leq N_G(Q). \]

By (46), \( Q \) and \( Q^x \) are different Sylow \( q \)-subgroups of \( S \). Therefore a Sylow \( q \)-subgroup of \( G \) containing \( Q^x \) cannot normalize \( Q \), nor can a Sylow \( p \)-subgroup of \( G \) containing \( x \). Thus (50) shows that \( N_G(P) \) must contain these two Sylow subgroups of \( G \) and, since \( M_G = 1 \), \( N_G(P) \neq G \). Hence there must exist a prime \( r \) dividing \( |G| \) such that \( p \neq r \neq q \) and a Sylow \( r \)-subgroup \( R \) of \( G \) that is not contained in \( N_G(P) \). Then we may choose \( y \in R \setminus N_G(P) \). For this \( y \), \( M \) is not permutable in \( T = \langle M, y \rangle \) since 5.1.5 (a) would imply that \( M^y = M \) and hence \( P^y = P \) if \( M \) per \( T \). By 5.1.4, \( T/M_T \) is a \( P \)-group and so \( o(y) = |T:M| = r \). Again by 5.1.5, \( \langle y \rangle \) permutes with \( M \) and \( M^x \), hence with \( S \), and (48) yields that \( |G| = |S|\langle y \rangle| = |M|pr \). It follows that \( S \) and \( T \) are maximal subgroups of \( G \) and hence \( S = N_G(P) \) and \( T = N_G(Q) \). Since \( |G:T| = p \), \( T \) cannot contain any Sylow \( p \)-subgroup of \( G \); by (50), all these Sylow \( p \)-subgroups have to lie in \( S \). Since \( P \leq S \), it follows that \( P \) is contained in the intersection \( O_p(G) \) of all the Sylow \( p \)-subgroups of \( G \), and, since \( P \) is a Sylow \( p \)-subgroup of \( T \), we have \( P = O_p(G) \cap T \leq T \). This contradicts the choice of \( y \in G \setminus N_G(P) \).

The main theorems

5.1.13 Theorem (Previato [1975]). The subgroup \( M \) of the finite group \( G \) is modular in \( G \) if and only if \( M \) is modular in \( \langle M, x \rangle \) for every \( x \in G \) of prime power order.

Proof. If \( M \) is modular in \( G \), then it is also modular in every group \( \langle M, x \rangle \). Conversely, if \( M \) is modular in \( \langle M, x \rangle \) for every \( x \in G \) of prime power order and \( Q/M_G \) is a Sylow subgroup of \( M/M_G \), then, by 5.1.12, \( Q \) is modular in \( G \). Since \( M \) is generated by these subgroups \( Q \), it follows from (5) that \( M \) is modular in \( G \).

5.1.14 Theorem (Schmidt [1970a]). The subgroup \( M \) of the finite group \( G \) is modular in \( G \) if and only if

\[ G/M_G = S_1/M_G \times \cdots \times S_r/M_G \times T/M_G \]

where \( 0 \leq r \in \mathbb{Z} \) and for all \( i, j \in \{1, \ldots, r\} \),

(a) \( S_i/M_G \) is a nonabelian \( P \)-group,

(b) \(|S_i/M_G|, |S_j/M_G|\) = 1 = \(|S_i/M_G|, |T/M_G|\) for \( i \neq j \),

(c) \( M/M_G = Q_1/M_G \times \cdots \times Q_r/M_G \times (M \cap T)/M_G \) and \( Q_i/M_G \) is a nonnormal Sylow subgroup of \( S_i/M_G \), and

(d) \( M \cap T \) is permutable in \( G \).

Proof. If \( G/M_G \) has the given structure, then \( L(S_i/M_G) \) is modular and hence \( Q_i/M_G \) mod \( S_i/M_G \) for all \( i \). Furthermore \((M \cap T)/M_G \) mod \( T/M_G \) so that, by 5.1.8, \( M/M_G \) mod \( G/M_G \); by (4), \( M \) is modular in \( G \).
Conversely, we use induction on $|G|$ to show that for a modular subgroup $M$ of $G$, $G/MG$ has the structure given in the theorem. Of course, we may assume that $M_G = 1$ since otherwise $G/MG$ by induction has the right structure. Then, by 5.1.7, $M$ is nilpotent. If all the Sylow subgroups of $M$ are permutable in $G$, then by (10), $M$ is permutable in $G$ and the assertion holds with $r = 0$ and $T = G$. If $Q$ is a Sylow subgroup of $M$ that is not permutable in $G$, then, by 5.1.12, $Q$ is modular in $G$ and 5.1.9 yields that $G = Q^G \times L$ where $Q^G$ is a nonabelian $P$-group of order prime to $|L|$. By (2), $M \cap L$ is modular in $L$ and, clearly, $(M \cap L)_L = 1$. Hence, by induction, $L$ has the right structure. Since $M \cap Q^G$ is nilpotent, 2.2.2 shows that $Q = M \cap Q^G$ is a nonnormal Sylow subgroup of $Q^G$. Thus $G$ has the right structure.

Exercises

1. Show that the subgroup $M$ of the finite group $G$ is a maximal modular subgroup of $G$ if and only if either $M$ is a maximal normal subgroup of $G$ or $M$ is a maximal subgroup of $G$ and $G/MG$ is nonabelian of order $pq$ where $p$ and $q$ are primes.

2. (Schmidt [1969]) Let $M$ be modular in the finite group $G$ and suppose that $|G:M| = p^n$ where $p \in \mathbb{P}$ and $n \in \mathbb{N}$. Show that $G/MG$ is either a $p$-group or a $P$-group of order $p^nq$ where $p > q \in \mathbb{P}$.

3. Let $G = PQ \times R$ where $|P| = |R| = p \in \mathbb{P}$ and $PQ$ is nonabelian of order $pq$, $p > q \in \mathbb{P}$. Show that $M = QR$ is a nilpotent modular subgroup of $G$ whose Sylow $q$-subgroup is not modular in $G$.

4. (Schmidt [1970a]) Show that if $M$ is a nilpotent modular subgroup of the finite group $G$, $q$ the largest prime dividing $|M|$ and $Q$ the Sylow $q$-subgroup of $M$, then $Q$ is modular in $G$.

5. (Whitson [1977]) Let $G$ be a finite group and let $M \leq G$ be such that $(X \cup M) \cap Z = X \cup (M \cap Z)$ for all subgroups $X$ and $Z$ of $G$ satisfying $X \leq Z$, that is, $M$ is semimodular in $L(G)$ as defined in Exercise 2.1.7. Show that if $[G/M]$ is a chain of length 2 and $|G:M| = p^2$ for some prime $p$, then $G/MG$ is a $p$-group.

5.2 Permutable subgroups of finite groups

Since we know the structure of $P$-groups very well, Theorem 5.1.14 reduces our problem of determining the structure of $G/MG$ for a modular subgroup $M$ of a finite group $G$ to the study of the factor $T/MG$ in this theorem, that is, to the case that $M$ is permutable in $G$. Our main result in this section is that $M^G/MG$ is then hypercentrally embedded in $G$, in particular is nilpotent. In the remainder of this section we shall study some special problems on permutable subgroups in order to prepare our investigations on projective images of normal subgroups. We shall not always insist on the finiteness of the groups considered since we shall be able to apply the more general results also in the study of images of normal subgroups under projectivities of infinite groups in Chapter 6. For the same reason we introduce the
concepts of hypercentral and hypercyclic embedding in the most general form, although, at the moment, we are only interested in projectivities between finite groups.

**Hypercentral and hypercyclic embedding**

Let $K \leq H$ be normal subgroups of the group $G$. We say that $H/K$ is **hypercentrally** (respectively **hypercyclically**) embedded in $G$ if to every normal subgroup $N$ of $G$ such that $K \leq N < H$ there exists a subgroup $M$ of $G$ satisfying $N < M \leq H$ such that $[M, G] \leq N$ (respectively such that $M \leq G$ and $M/N$ is cyclic). For groups satisfying the maximal condition for normal subgroups, in particular for finite groups, this is equivalent to the existence of a chain of subgroups $N_i$ of $G$ such that

$$K = N_0 \leq N_1 \leq \cdots \leq N_r = H$$

and $[N_i, G] \leq N_{i-1}$ (respectively $N_i \trianglelefteq G$ and $N_i/N_{i-1}$ is cyclic) for $i = 1, \ldots, r$. In particular, every hypercentrally (respectively hypercyclically) embedded factor of a finite group is nilpotent (respectively supersoluble). Since for $N \leq M \leq G$ the inclusion $[M, G] \leq N$ is equivalent to $N \trianglelefteq G$ and $M/N \leq Z(G/N)$, it is clear that every hypercentrally embedded factor of an arbitrary group is hypercyclically embedded. We shall need the following simple inheritance properties of the concepts introduced above.

**5.2.1 Lemma.** Let $F, H, K, L, M, N$ be normal subgroups of $G$ such that $K \leq M \leq H$, $L \leq H$ and $K \leq F$.

(a) If $H/K$ is hypercentrally (hypercyclically) embedded in $G$, then so are $HN/KN$ and $H \cap N/K \cap N$.

(b) $H/K$ is hypercentrally (hypercyclically) embedded in $G$ if and only if $H/M$ and $M/K$ are hypercentrally (hypercyclically) embedded in $G$.

(c) If $F/K$ and $H/K$ are hypercentrally (hypercyclically) embedded in $G$, then so is $FH/K$.

(d) If $H/K$ and $H/L$ are hypercentrally (hypercyclically) embedded in $G$, then so is $H/K \cap L$.

**Proof.** We sketch the proofs of these properties for hypercentral embedding; the proofs for hypercyclic embedding are similar. First of all, (a) follows from the fact that for normal subgroups $S$, $T$ of $G$ such that $[T, G] \leq S$, (1) of § 1.5 yields $[TN, G] \leq [T, G]^G[N, G] \leq SN$; furthermore, of course, $[T \cap N, G] \leq S \cap N$. To prove (b), observe first that if $H/K$ is hypercentrally embedded in $G$, then from (a) it follows that $HM/KM = H/M$ and $H \cap M/K \cap M = M/K$ are hypercentrally embedded. Conversely, if these two factors are hypercentrally embedded and $S \trianglelefteq G$ such that $K \leq S < H$, then $H/MS$ and $M/M \cap S$ are hypercentrally embedded and therefore, by (a), $MS/S$ is also. Hence there exists $T \leq G$ satisfying $[T, G] \leq S$ such that $S \leq T \leq MS \leq H$ if $S \leq MS$ and such that $S = MS < T \leq H$ in the other case.
Thus (b) holds. In (c), $F/K$ and $FH/FK = FH/F$ are hypercentrally embedded; in (d), $H/K$ and $H \cap K/L \cap K = K/L \cap K$ are hypercentrally embedded. In both cases, (b) yields the desired result.

We need a criterion for a normal subgroup of prime power order to be hypercentrally embedded in a finite group.

5.2.2 Lemma. If $p$ is a prime and $N$ a normal $p$-subgroup of a finite group $G$, then $N$ is hypercentrally embedded in $G$ if and only if $G/C_G(N)$ is a $p$-group.

Proof. First assume that $N$ is hypercentrally embedded in $G$ and let $Q$ be a $q$-subgroup of $G$ for some prime $q \neq p$. Then $N$ and the $q$-group $QN/N$ are hypercentrally embedded in $QN$. Thus $QN$ is hypercentrally embedded in $QN$, that is $QN$ is nilpotent. It follows that $Q \leq C_G(N)$ and, since $q$ was arbitrary, $G/C_G(N)$ is a $p$-group.

Conversely, suppose that $G/C_G(N)$ is a $p$-group and take $S \leq G$ such that $S < N$. Then $G$ operates as a $p$-group on the $p$-group $N/S$ and therefore has a nontrivial centralizer $T/S$ in this group. It follows that $S < T$ and $[T, G] \leq S$. Thus $N$ is hypercentrally embedded in $G$.

The structure and embedding of $M^G/M_G$

5.2.3 Theorem (Maier and Schmid [1973]). If $M$ is permutab in the finite group $G$, then $M^G/M_G$ is hypercentrally embedded in $G$.

Proof. Let $G$ be a minimal counterexample to the theorem and let $M$ be minimal among the permutable subgroups of $G$ for which $M^G/M_G$ is not hypercentrally embedded in $G$. Then $G/M_G$ is a counterexample and the minimality of $G$ implies that

(1) $M_G = 1$.

By 5.1.7 and 5.1.10, $M$ is nilpotent and its Sylow subgroups are permutable in $G$. Hence if $M$ had composite order, the minimality of $M$ would imply that $P^G$ would be hypercentrally embedded in $G$ for every Sylow subgroup $P$ of $M$. By (c) of 5.2.1, the product of these normal closures, that is $M^G$, would also be hypercentrally embedded in $G$, a contradiction. Thus $M$ is a $p$-group for some prime $p$ and therefore also

(2) $M^G$ is a $p$-group

since the product of $p$-groups is a $p$-group. Now $M^G$ is not hypercentrally embedded in $G$ and therefore, by 5.2.2, there exists a prime $q \neq p$ dividing $|G/C_G(M^G)|$. Let $Q \in \text{Syl}_q(G)$ and put $H = N_G(Q)M$. The Frattini argument shows that the Sylow normalizer $N_G(Q)$ cannot be contained in a proper normal subgroup of $G$. Thus $O^p(G)H = G$ and every $x \in G$ can be written in the form $x = yh$ where $y \in O^p(G)$, $h \in H$. Since $O^p(G)$ is generated by $p'$-elements, 5.1.5 shows that $M$ is normalized by
5.2 Permutable subgroups of finite groups

\(O_p(G)\). Therefore \(M^x = M^h\) and hence \(M^H = M^G\) and \(M_H = M_G = 1\). So if \(H\) were a proper subgroup of \(G\), the minimality of \(G\) would imply that \(M^G = M^H/M_H\) would be hypercentrally embedded in \(H\). But then 5.2.2 would imply that \(Q \leq C_H(M^G)\) and this would contradict the fact that \(q\) divides \(|G/C_G(M^G)|\). Thus \(H = G\), that is,

\[(3) \ G = N_G(Q)M.\]

This yields \(Q^G = Q^M \leq QM\) and hence \(Q^G \cap M^G \leq QM \cap M^G = (Q \cap M^G)M = M\) since \(Q\) is a \(q\)-group and \(M^G\) a \(p\)-group. Since \(M_G = 1\), it follows that \(Q^G \cap M^G = 1\) and we get that \(Q \leq C_G(M^G)\), the same contradiction as before.

Recall that if \(K \leq H\) are normal subgroups of a group \(G\), then \(G\) operates by conjugation on \(H/K\) and the kernel of this operation is

\[CG(H/K) = \{x \in G | [H,x] < K\}.\]

Thus \(G/C_G(H/K)\) is isomorphic to the automorphism group induced by \(G\) in \(H/K\); furthermore, \(C_G(H/K)/K = C_G/K(H/K)\).

5.2.4 Corollary. If \(M\) is permutable in the finite group \(G\), then \(G/C_G(M^G/M_G)\) is nilpotent and the primes dividing the order of this group are precisely those dividing \(|M/M_G|\).

Proof. We may assume that \(M_G = 1\) so that \(M^G\) is hypercentrally embedded in \(G\). Then \(M^G\) is nilpotent and a prime divides \(|M^G|\) if and only if it divides \(|M|\). If \(p\) is such a prime and \(P\) the Sylow \(p\)-subgroup of \(M^G\), then \(P \leq G\) and (b) of 5.2.1 shows that \(P\) is hypercentrally embedded in \(G\). By 5.2.2, \(G/C_G(P)\) is a \(p\)-group which is not trivial since otherwise \(P \cap M\) would be a nontrivial normal subgroup of \(G\) contained in \(M\). Since \(C_G(M^G)\) is the intersection of all the \(C_G(P)\), the assertion follows.

Our main results, Theorems 5.1.14 and 5.2.3, yield a rather good but somewhat complicated description of the structure and embedding of \(M^G/M_G\) for a modular subgroup \(M\) of a finite group \(G\). Therefore we prove a handier result that follows immediately from these theorems and that will often suffice for the applications.

5.2.5 Theorem (Schmidt [1975a]). If \(M\) is modular in the finite group \(G\), then \(M^G/M_G\) is hypercyclically embedded in \(G\) and \(G/C_G(M^G/M_G)\) is supersoluble.

Proof. Again we may assume that \(M_G = 1\). Then, by 5.1.14, \(G = S_1 \times \cdots \times S_r \times T\) where the \(S_i\) are nonabelian \(P\)-groups, \(M \cap T\) is permutable in \(G\), and \(M^G = S_1 \times \cdots \times S_r \times (M \cap T)^G\). Clearly, all the \(S_i\) are hypercyclically embedded in \(G\) and so is \((M \cap T)^G\), by 5.2.3; thus (c) of 5.2.1 shows that \(M^G\) is hypercyclically embedded in \(G\). Furthermore \(G/C_G((M \cap T)^G)\) is nilpotent and \(G/C_G(S_i) \simeq S_i\) is supersoluble for every \(i = 1, \ldots, r\). Since \(C_G(M^G)\) is the intersection of all these centralizers, it follows that \(G/C_G(M^G)\) is supersoluble.

5.2.6 Corollary. If \(M\) is modular in the finite group \(G\) and \(G\) or \(M\) is perfect, then \(M \trianglelefteq G\).
Proof. Recall that a group is perfect if it has no proper normal subgroup with soluble factor group. Therefore, if $G$ is perfect, Theorem 5.2.5 implies that $G = C_G(M^G/M_G)$; and if $M$ is perfect, it follows that $M = M_G$. In both cases, $M \trianglelefteq G$. 

The results established so far will suffice to prove a number of important criteria for projectivities of finite groups to map normal subgroups onto normal subgroups; Corollary 5.2.6 is a first example. But they say nothing if the groups considered are nilpotent groups or $p$-groups; rather they reduce the problems to the investigation of $p$-groups. As mentioned before, we shall be able to prove similar reduction theorems also for infinite groups. Therefore, in the remainder of this section, we shall study permutable subgroups of $p$-groups and cyclic permutable subgroups of arbitrary groups as far as necessary for the applications to projective images of normal subgroups.

Elements of infinite order

First of all we show that elements of infinite order cause little trouble in the problems we consider. The reason for this is the following basic result which we shall generalize in 6.2.2.

5.2.7 Lemma. If $M \trianglelefteq G$ and $g \in G$ such that $o(g, M)$ is infinite, then $g \in N_G(M)$.

Proof. We may assume that $M \trianglelefteq \langle g \rangle = G$. Since $o(g, M) = |\langle g \rangle : \langle g \rangle \cap M|$, it follows that $o(g)$ is infinite and $M \cap \langle g \rangle = 1$. If $p$ is a prime, $S = M \langle g^p \rangle$ is a subgroup of index $p$ in $G$; let $N = S_G$. Then $|G/N|$ divides $p!$ and hence $MN/N \leq S/N$ is a $p'$-subgroup of $G/N$. Since $MN/N$ is permutable in $G/N$, we see that $(MN/N)^{G/N} = M^G/N/N$ is a $p'$-group and hence $M^G/N/N \leq S/N$. Thus $M^G \leq S$. This shows that $M^G$ is contained in $M\langle g^p \rangle$ for every prime $p$ and, since, by 2.1.5, the intersection of these subgroups is $M$, it follows that $M = M^G \trianglelefteq G$. 

Permutable subgroups of finite $p$-groups

The structure of $M/M_G$ may be rather complicated even if $M$ is a permutable subgroup of a finite $p$-group. That $M/M_G$ need not be abelian is shown by Exercise 1. Papers by Bradway, Gross and Scott [1971], Gross [1971], [1975b], Stonehewer [1973], [1974], and Berger and Gross [1982] contain examples in which the nilpotency class, derived length and Frattini length of $M/M_G$ are arbitrarily large. Although all these structural complications, by 5.1.6, have to occur in groups of the form $G = M\langle x \rangle$, these groups at least have a decent power structure.

5.2.8 Theorem (Gross [1971]). Let $M$ be a core-free permutable subgroup of the finite $p$-group $G = MX$ and suppose that $X$ is cyclic of order $p^n$. Then the following properties hold.
5.2 Permutable subgroups of finite groups

(a) Every $X$-invariant subgroup of $M$ is trivial.
(b) $M \cap X = 1$, $\Omega(X) \leq Z(G) \leq X$.
(c) $\Omega(G)$ is elementary abelian.
(d) For $r = 1, \ldots, n$, $\Omega_r(G) = \Omega_r(M)(\Omega_r(X))$ has exponent $p^r$ and is soluble of derived length at most $r$; furthermore, the core of $M\Omega_r(G)/\Omega_r(G)$ in $G/\Omega_r(G)$ is trivial.
(e) $\exp G = p^n > \exp M$.
(f) For $p = 2$, $\Omega_2(G)$ is abelian and hence $\Omega_r(G)/\Omega_{r-2}(G)$ is abelian for $r \geq 2$.
(g) If $p = 2$ and $M \neq 1$, then $M \leq \Omega_{n-2}(G)$.

Proof. If $n = 1$, $M \leq G$ and hence $M = 1$. Thus $G = X$ is of order $p$ and all the assertions hold trivially. So assume that $n \geq 2$. If $H$ is an $X$-invariant subgroup of $M$, then $H^G = H^M = M \leq M$ and, since $M_G = 1$, it follows that $H = 1$. In particular, $M \cap X = 1$ and $C_G(X) = X(C_G(X) \cap M) = X$ implies that $Z(G) \leq X$. Therefore $\Omega(X) \leq Z(G)$ since $Z(G) \neq 1$. Thus (a) and (b) hold.

For $g \in G$ with $o(g) = p$, $|M\langle g \rangle : M| \leq p$ and hence $M\langle g \rangle$ is contained in the atom $M\Omega(X)$ of the chain $[G/M] \simeq L(X)$. It follows that $\Omega(G) \leq M\Omega(X)$ and so $\Omega(G) = (M \cap \Omega(G))\Omega(X)$. Therefore $M \cap \Omega(G)$ is of index $p$ in $\Omega(G)$ and $\Omega(G)$ is a normal subgroup of $G$. Since $M_G = 1$, it follows that $\Phi(\Omega(G)) = 1$. Thus $\Omega(G)$ is elementary abelian and (c) holds. This implies that $\Omega(M) = M \cap \Omega(G)$ and hence $\Omega(G) = \Omega(M)\Omega(X)$. If $K/\Omega(G)$ is the core of $M\Omega(G)/\Omega(G)$ in $G/\Omega(G)$, then $|K : M \cap K| = p$ since $M$ is a maximal subgroup of $M\Omega(G) = M\Omega(X)$. So this time $\Phi(K)$ is a normal subgroup of $G$ contained in $M$ and is therefore trivial. Thus $K$ is elementary abelian and hence $K = \Omega(G)$. This shows that (d) holds for $r = 1$.

![Figure 18](image-url)
and the general assertion follows by induction on \( r \). For, if \( N = \Omega(G) \), then \( MN/N \) is a core-free permutable subgroup of \( G/N \), as we have just shown, and \( G/N = (MN/N)(XN/N) \); since \( \Omega(G) \) is elementary abelian, \( \Omega_{r-1}(G/N) = \Omega_r(G)/N \), \( \Omega_{r-1}(MN/N) = \Omega_r(M)/N \) and \( \Omega_{r-1}(XN/N) = \Omega_r(X)/N \). Therefore by induction, \( \Omega_{r-1}(G/N) = \Omega_r(G)/N \) is of exponent \( p^{r-1} \) and soluble of derived length at most \( r - 1 \), and hence \( \Omega(G) \) is of exponent \( p^r \) and soluble of derived length at most \( r \). Furthermore \( \Omega_r(G) = \Omega_r(M)/N \Omega_r(X) = \Omega_r(M) \Omega_r(X) \) and the core of \( (MN/N)\Omega_{r-1}(G/N)/\Omega_{r-1}(G/N) \) in \( G/N \) is trivial. Thus the core of \( M \Omega_r(G)/\Omega_r(G) \) in \( G/\Omega_r(G) \) is also trivial and \( d \) holds.

Since \( M \Omega_{n-1}(X) \leq M \Omega_{n-1}(G) \) is a maximal subgroup of \( G \), we have \( M \Omega_{n-1}(G) \leq G \); on the other hand, by \( d \), \( M \Omega_{n-1}(G)/\Omega_{n-1}(G) \) is core-free. It follows that \( M \Omega_{n-1}(G)/\Omega_{n-1}(G) = 1 \) and hence \( M \leq \Omega_{n-1}(G) \). Again by \( d \), \( \text{Exp} M \leq p^{n-1} \) and \( G = MX = \Omega_n(M) \Omega_n(X) = \Omega_n(G) \) has exponent \( p^n \). Thus \( e \) holds.

To prove \( f \) and \( g \), suppose that \( p = 2 \) and first note that \( |\Omega_2(G):\Omega_2(M)| = |\Omega_2(X)| = 4 \); let \( \Omega_2(M) < T < \Omega_2(G) \). Then \( \Omega_2(M) \leq T \leq \Omega_2(G) \) and \( \Omega_2(M) \) has at most two conjugates in \( \Omega_2(G) \), both contained in \( T \). So if \( \Omega_2(M) \) were not normal in \( \Omega_2(G) \) and \( L \) is the core of \( \Omega_2(M) \) in \( \Omega_2(G) \), it would follow that \( |\Omega_2(G)/L| = 8 \) and, by \( 11 \) of § 5.1, \( \Omega_2(M)/L = (M \cap \Omega_2(G))/L \) would be a nonnormal permutable subgroup of order 2 in \( \Omega_2(G)/L \). But such a group of order 8 does not exist. This shows that \( \Omega_2(M) \leq \Omega_2(G) \) and \( \Omega_2(G)/\Omega_2(M) \) is abelian. Therefore \( \Omega_2(G) \) is a normal subgroup of \( G \) contained in \( M \) and hence is trivial. Thus \( \Omega_2(G) \) is abelian. By \( d \), \( G/\Omega_{r-2}(G) \) satisfies the assumptions of the theorem and hence \( \Omega_2(G/\Omega_{r-2}(G)) = \Omega_r(G)/\Omega_{r-2}(G) \) is also abelian. In particular, \( G/\Omega_{n-2}(G) \) is abelian and, by \( d \), \( M\Omega_{n-2}(G)/\Omega_{n-2}(G) \) is core-free in this group. It follows that \( M \leq \Omega_{n-2}(G) \). Thus \( f \) and \( g \) are satisfied. \( \square \)

There is a vast literature on permutable subgroups of finite groups, especially finite \( p \)-groups. We refer the reader to the papers mentioned above and in addition to Ore [1937], Ito and Szép [1962], Deskins [1963], and Nakamura [1966], [1970], [1979]. However, most of the results in these papers are not relevant to our purposes. For example, Gross [1971], [1975b] exhibits bounds for the nilpotency class and derived length of \( M/M_G \) for a permutable subgroup \( M \) of a finite \( p \)-group \( G \). But all these bounds depend on the exponent of \( G \), tend to infinity with \( \text{Exp} G \), and are best possible as is shown by the examples mentioned above. In contrast to this we shall prove in 6.6.1 that \( M/M_G \) is metabelian if \( M \) is a projective image of a normal subgroup. For this, the bounds of Gross are clearly not usable. In addition, this different behaviour of permutable subgroups and of projective images of normal subgroups shows that the former do not sufficiently approximate the latter. It is clear that images of normal subgroups under projectivities between \( p \)-groups (called “images” for short) have a number of additional properties, for example:

(4) If \( M \) is an image, there exist images \( M_i \) such that \( 1 = M_0 < \cdots < M_k = M < \cdots < M_r = G \) and \( |M_i:M_{i-1}| = p \) for \( i = 1, \ldots, r \).

(5) If \( M \) is an image and \( T \) is a maximal subgroup of \( G \), then \( M \cap T \) is an image.

(6) If \( M \) is an image and \( A \leq M \) is invariant under \( P(M) \), for example \( A = \Phi(M) \) or \( \Omega(M) \), then \( A \) is an image.
It would be desirable to use these or similar simple properties to define a class of subgroups in finite $p$-groups that lies between the projective images of normal subgroups and the permutable subgroups, and to prove that $M/M_G$ is metabelian for any member $M$ of this class. This would suffice to prove the same result for images of normal subgroups under projectivities between arbitrary groups as we shall see in Chapter 6. However, such a theory does not exist.

Cyclic permutable subgroups

We want to show that $M^G/M_G$ is hypercentrally embedded in $G$ if $M$ is a finite cyclic permutable subgroup of an arbitrary group $G$. If $|M|$ is a prime, we can say a little more.

5.2.9 Theorem. Let $M$ be a permutable subgroup of prime order $p$ in the group $G$ and suppose that $M$ is not normal in $G$.

(a) Then $M^G$ is an elementary abelian $p$-group.

(b) If $x \in G$ has infinite order or finite order prime to $p$, then $x \in C_G(M^G)$.

(c) $M^G \leq N(G) \leq Z_2(G)$.

(d) $M^G = M \times (M^G \cap Z(G))$.

(e) $M^G \cap Z(G) \cap \langle x \rangle \neq 1$ for every $x \in G \setminus C_G(M)$.

Proof. (a) Since every conjugate of $M$ is permutable in $G$, the subgroup $\langle M^x, M^y \rangle$ has order $p$ or $p^2$ and is therefore abelian for all $x, y \in G$. It follows that $M^G = \langle M^x | x \in G \rangle$ is abelian and hence elementary abelian as $|M| = p$.

(b) By 5.1.5 or 5.2.7, $x$ normalizes every conjugate of $M$. Since $M$ is not normal in $G$, there exists $y \in G \setminus N_G(M)$ such that $o(y) = p^m$ for some $m \in \mathbb{N}$. Put $H = \langle M, x, y \rangle$ and $T = M^y$. Since $M^T$ is normalized by $x$, we have $M^T = M^H$. Furthermore $M \leq \Omega(T) \leq T$ and $|\Omega(T)| = p^2$. Since $M$ is not normal in $T$, it follows that $M^H = M^T = \Omega(T)$ is elementary abelian of order $p^2$ and $|M^H \cap \langle y \rangle| = p$. Let $N = M^H \cap \langle y \rangle$. Then $y \in C_H(N)$ and, since $H$ has only $p + 1$ subgroups of order $p$, $N$ is the only subgroup of order $p$ of $M^H$ that is normalized by $y$. The other subgroups of order $p$ of $M^H$ are conjugates of $M$, and are therefore normalized by $x$; it follows that $N^x = N$. Since $x \in N_G(M)$ and $y \notin N_G(M)$, clearly $xy \notin N_G(M)$ and hence $o(xy)$ is finite. Let $\langle z \rangle$ be the Sylow $p$-subgroup of $\langle xy \rangle$. Then $M^z \neq M$ and hence $M^H = M^{\langle M^z \rangle}$ and $|M^H \cap \langle z \rangle| = p$ as for $y$. Therefore if $L = M^H \cap \langle z \rangle = M^H \cap \langle xy \rangle$, then $\langle xy \rangle \leq C_H(L)$ and so $y \in N_H(L)$. Since $N$ is the only subgroup of order $p$ of $M^H$ normalized by $y$, $L = N$. Thus $N$ is centralized by $y$ and $xy$ and hence also by $x$. But $x$ normalizes every subgroup of $M^H$ and, by 1.5.4, induces a universal power automorphism in this group. It follows that $x \in C_G(M^H) \leq C_G(M)$. Now $x$ was arbitrary and hence also $x^g = x \in C_G(M^g)$ for all $g \in G$. Thus $x \in C_G(M^G)$, as desired.

(c) If $X$ is a cyclic $p$-subgroup of $G$ and $g \in G$ such that $M^g \nsubseteq X$, then $|M^gX| = p|X|$ and hence $M^g \leq N_G(X)$. Thus $M$ and its conjugates normalize every cyclic $p$-subgroup and centralize every element of infinite order and of finite order prime to $p$. It follows that $M^G$ is contained in the norm $N(G)$ of $G$ and, by 1.5.3, $N(G) \leq Z_2(G)$. 


(d) By (c), \( Z(G) \leq MZ(G) \leq Z_3(G) \) and hence \( MZ(G) \leq G \); it follows that \( M^G \leq MZ(G) \). Then Dedekind's law shows that \( M^G = M(M^G \cap Z(G)) \) and, since \( M \leq Z(G) \), the product is direct.

(e) Let \( X = \langle x \rangle \). Since \( M^G \) normalizes every subgroup of \( G \), \( 1 \neq [M, X] \leq M^G \cap X \). Therefore if \( M^G \cap Z(G) \cap X = 1 \), it would follow that

\[
M \leq M^G = (M^G \cap Z(G))(M^G \cap X) \leq C_G(X),
\]

a contradiction. Thus \( M^G \cap Z(G) \cap X \neq 1 \), as desired. \( \square \)

To prove the result announced above we have to show first that every subgroup of a cyclic permutable subgroup is permutable in \( G \). For this we need the following.

5.2.10 Lemma. Let \( K \leq H \) be permutable subgroups of the \( p \)-group \( G \). If \([H/K]\) is a finite chain and \( K \leq M \leq H \), then \( M \) is permutable in \( G \).

Proof. We use induction on the length of the chain \([H/K]\) and have to show that \( XM = MX \) for every cyclic subgroup \( X \) of \( G \). This is clear if \( M = H \), so assume that \( M < H \). If \( M \leq KX \), then \( XM = XKM = KXM = KX = M(KX) = MX \). So suppose that \( M \leq KX \) and hence \( KX < HX \). Since \([H/K]\) is a finite chain, there exists \( g \in G \) such that \( H = K\langle g \rangle \), and it follows that \( |H : K| = |\langle g \rangle : K \langle g \rangle \cap K| \) and \( |HX : H| = |X : X \cap H| \) are finite. Then \( |HX : K| \) is also finite, thus \( HX/K_{HX} \) is a finite \( p \)-group and hence there exists a normal subgroup \( T \) of index \( p \) in \( HX \) containing \( KX \). Then \( K \leq H \cap T \leq H \) and \( |H : H \cap T| = |HT : T| = |HX : T| = p \). Since \([H/K]\) is a chain, it follows that \( M \leq H \cap T \) and (11) of § 5.1 yields that \( H \cap T \) and \( K \) are permutable subgroups of \( T \). By induction, \( M \) is permutable in \( T \) and hence \( XM = MX \). \( \square \)

It is not difficult to show that the above lemma holds for arbitrary groups \( G \); for a still more general result see Exercise 6.

5.2.11 Lemma. If \( M \) is a cyclic permutable subgroup of the group \( G \), then every subgroup of \( M \) is permutable in \( G \).

Proof. Let \( 1 \neq H \leq M \) and assume first that \( G \) is finite. Let \( p \) be a prime dividing \( |H| \), \( P \in \text{Syl}_p(H) \) and \( S \in \text{Syl}_p(M) \). Then \( P \leq S \) and \( S \) is permutable in \( G \) by 5.1.10. Therefore, if \( X \) is a subgroup of prime power order \( q^n \) of \( G \) and \( p \neq q \), then, by 5.1.5, \( S \leq SX \) and hence \( P \leq SX \); also if \( p = q \), then \( SX \) is a \( p \)-group and \( P \) per \( SX \) by 5.2.10. In both cases, \( PX = XP \). Thus \( P \) is permutable in \( G \) and, since this holds for every prime dividing \( |H| \), it follows that \( H \) is permutable in \( G \).

Now let \( G \) be arbitrary and take \( x \in G \). We have to show that \( \langle x \rangle H = H \langle x \rangle \). If \( x \in N_G(M) \), then also \( x \in N_G(H) \) and we are done; so let \( x \notin N_G(M) \) and consider \( L = M\langle x \rangle \). By 5.2.7, \( |L : M| = o(x, M) \) is finite, hence \( |L : H| \) is also finite and so, finally, \( L/H_L \) is a finite group. Then \( H/H_L \) permutes with \( \langle x \rangle H_L/H_L \), as we have just shown, and it follows that \( \langle x \rangle H = \langle x \rangle H_L H = H \langle x \rangle H_L = HH_L \langle x \rangle = H \langle x \rangle \). \( \square \)
5.2.12 Theorem (Busetto [1980b]). Let $M$ be a finite cyclic permutable subgroup of the group $G$ and suppose that $M_G = 1$; let $|M| = p_1^{n_1} \cdots p_r^{n_r}$ be the prime factor decomposition of $|M|$ and put $n = \max \{n_i | i = 1, \ldots, r \}$. Then $M^G \leq Z_{2n}(G)$.

Proof. By 5.2.11, the Sylow subgroups of $M$ are permutable in $G$ and, clearly, $M^G$ is the product of their normal closures. Therefore we may assume that $M$ is a $p$-group. Then $|M| = p^n$ and we show by induction on $n$ that $M^G$ is a $p$-group of exponent $p^n$ and is contained in $Z_{2n}(G)$. If $n = 1$, this is true by 5.2.9. So assume that $n \geq 2$ and the assertion holds for $n - 1$; let $N = \Omega_{n-1}(M)^G$. Again by 5.2.11, $\Omega_{n-1}(M)$ is permutable in $G$ and the induction assumption yields that $N \leq Z_{2n-2}(G)$ and $\operatorname{Exp} N = p^{n-1}$. Since $M_G = 1$ and $[M/1]$ is a chain, there exists $x \in G$ such that $M \cap M^x = 1$. By 5.2.7 and 5.1.5, $M$ is normalized by elements of infinite order or finite order prime to $p$; therefore we may choose $x$ as a $p$-element. Then $H = M\langle x \rangle$ is a finite $p$-group and $M_H = 1$. By 5.2.8, $\Omega_{n-1}(H) = \Omega_{n-1}(M)\Omega_{n-1}(\langle x \rangle)$ has order at most $p^{2n-2}$; on the other hand, $\Omega_{n-1}(M)\Omega_{n-1}(M^x)$ is contained in $\Omega_{n-1}(H)$ and has this order since $M \cap M^x = 1$. Thus $\Omega_{n-1}(H) = \Omega_{n-1}(M)\Omega_{n-1}(M^x) \leq N \cap H$ and, since $\operatorname{Exp} N = p^{n-1}$, we obtain $\Omega_{n-1}(H) = N \cap H$. Now (d) of 5.2.8 shows that $MN \cap H = M(N \cap H) = M\Omega_{n-1}(H)$ is not normal in $H$ and hence $MN/N$ is a nonnormal permutable subgroup of order $p$ in $G/N$. By 5.2.9, $(MN/N)^{G/N} = M^G/N$ is elementary abelian and $M^G/N \leq Z_2(G/N)$. It follows that $\operatorname{Exp} G = p^n$ and, as $N \leq Z_{2n-2}(G)$, that $M^G \leq Z_{2n}(G)$.

5.2.13 Theorem. The $p$-group $G$ is metacyclic if and only if it is the product of two cyclic subgroups one of which is permutable in $G$.

Proof. If $G$ is metacyclic, it is the product of a cyclic normal subgroup and a cyclic supplement. So assume that, conversely, $G$ satisfies the condition of the theorem. Then, as a product of two cyclic $p$-groups, $G$ is finite and we use induction on $|G|$ to show that $G$ is metacyclic. First of all we note that the assumption on $G$ is equivalent to the following condition.

(7) There exists a modular subgroup $M$ of $G$ such that $[G/M]$ and $[M/1]$ are chains.

For, since $G$ is a $p$-group, a cyclic permutable subgroup $M$ with cyclic supplement clearly satisfies (7); and if (7) holds and $g \in G$ is not contained in the maximal subgroup of $G$ containing $M$, then $G = M\langle g \rangle$, $M$ is permutable in $G$ and $M$ is cyclic. Now (1), (2) and (3) of §5.1 immediately show that property (7) is inherited by subgroups and factor groups; for, if (7) holds and $H \leq G$ or $N \leq G$, then $M \cap H$ and $MN/N$ satisfy (7) in $H$ and $G/N$, respectively. Therefore, by induction,

(8) proper subgroups and factor groups of $G$ are metacyclic.

Metacyclic $p$-groups

A group $G$ is called metacyclic if it has a normal subgroup $N$ such that $N$ and $G/N$ are cyclic. For $p$-groups a seemingly weaker condition suffices.

5.2.13 Theorem. The $p$-group $G$ is metacyclic if and only if it is the product of two cyclic subgroups one of which is permutable in $G$.

Proof. If $G$ is metacyclic, it is the product of a cyclic normal subgroup and a cyclic supplement. So assume that, conversely, $G$ satisfies the condition of the theorem. Then, as a product of two cyclic $p$-groups, $G$ is finite and we use induction on $|G|$ to show that $G$ is metacyclic. First of all we note that the assumption on $G$ is equivalent to the following condition.

(7) There exists a modular subgroup $M$ of $G$ such that $[G/M]$ and $[M/1]$ are chains.

For, since $G$ is a $p$-group, a cyclic permutable subgroup $M$ with cyclic supplement clearly satisfies (7); and if (7) holds and $g \in G$ is not contained in the maximal subgroup of $G$ containing $M$, then $G = M\langle g \rangle$, $M$ is permutable in $G$ and $M$ is cyclic. Now (1), (2) and (3) of §5.1 immediately show that property (7) is inherited by subgroups and factor groups; for, if (7) holds and $H \leq G$ or $N \leq G$, then $M \cap H$ and $MN/N$ satisfy (7) in $H$ and $G/N$, respectively. Therefore, by induction,

(8) proper subgroups and factor groups of $G$ are metacyclic.
We show next that we may assume that $|G'| = p$. If $G' = 1$, then $G$ is clearly metacyclic. So assume that $G' \neq 1$ and let $N$ be a normal subgroup of order $p$ contained in $G'$. By (8), $G/N$ is metacyclic; let $K/N \leq G/N$ such that $K/N$ and $G/K$ are cyclic and let $t \in K$ such that $K = N\langle t \rangle$. If $K$ is cyclic, we are done; so assume that $K$ is not cyclic. Then $N \not\leq \langle t \rangle$ and hence $K = N \times \langle t \rangle$ since $N \leq Z(G)$. If $L = N\langle t^p \rangle = N\Phi(K)$ is the maximal subgroup of $K$ containing $N$, then $K/L \leq Z(G/L)$ and $G/K$ is cyclic. It follows that $G/L$ is abelian and hence $N \leq G' \leq L = N\Phi(K)$. Thus

$$G' = N \times (G' \cap \Phi(K)).$$

Suppose, for a contradiction, that $G' \cap \Phi(K) \neq 1$. Then the minimal subgroup $N_1$ of this cyclic normal subgroup is normal in $G$ and $G'/N_1$ is cyclic as in the case of $N$. It follows that $|G' \cap \Phi(K)| = p$ and hence $G' \leq Z(G)$. It is well-known (see Huppert [1967], p. 258) that for a group $G$ generated by two elements, $G'/[G', G]$ is cyclic; in our case, $[G', G] = 1$ and $G' = N \times N_1$ is not cyclic, a contradiction. Thus $G' \cap \Phi(K) = 1$ and by (9),

$$|G'| = p.$$

Since $G$ is generated by two elements, $G'G' = \langle aG' \rangle \times \langle bG' \rangle$ for suitable $a, b \in G$. Let $o(aG') = p^n$ and $o(bG') = p^m$. If $a^{p^n} \neq 1$, it generates $G'$ and $\langle a \rangle \geq G'$ is a cyclic normal subgroup of $G$ with cyclic factor group. Thus $G$ is metacyclic and we are done. So assume that $a^{p^n} = 1$ and, similarly, $b^{p^m} = 1$. We want to show that then $n = 1 = m$. Suppose that in fact $n > 1$. Of course, $[a, b] = c$ is a generator of $G'$ and, since $G' \leq Z(G)$, we have $[a^p, b] = [a, b]^p = 1 = [a, b^p]$. Thus $H = \langle a^p, b, c \rangle$ is abelian and metacyclic by (8). Hence $|\Omega(H)| \leq p^2$ and since $\langle a^{p^m} \rangle$ and $\langle c \rangle$ are different minimal subgroups of $H$, it follows that $b^{p^m-1} \in \Omega(H) = \langle a^{p^m-1}, c \rangle$. In particular, $b^{p^m-1} \in \langle a \rangle G'$; but $b$ has order $p^m$ modulo $\langle a \rangle G'$. This contradiction shows that $n = 1$. In exactly the same way we get that $m = 1$ and hence $|G| = p^3$. Since $G$ is the product of two cyclic groups, one of these must have order at least $p^2$ and is then a cyclic normal subgroup with cyclic factor group. Thus $G$ is metacyclic.

5.2.14 Corollary (Napolitani and Zacher [1983]). The $p$-group $G$ is a metacyclic $M$-group if and only if it is the product of two cyclic subgroups which are both permutable subgroups of $G$.

Proof. If $G$ is a metacyclic $M$-group, every subgroup is permutable in $G$ and hence $G$ is a product of two cyclic permutable subgroups. Conversely, let $G = AB$ where $A$ and $B$ are cyclic permutable subgroups of $G$. By 5.2.13, $G$ is metacyclic; let $N \leq G$ such that $N = \langle x \rangle$ and $G/N$ are cyclic. Since $G = AB$ and $G/N$ is cyclic, $G = NA$ or $G = NB$; say that $G = NB$ and let $B = \langle b \rangle$. Then, by 2.3.4, $G$ is an $M$-group except when $p = 2, |N| \geq 4$ and $N/\langle x^4 \rangle$ is not centralized by $b$. In this case, $T = \langle x^4, b^2 \rangle \leq G$, $G/T$ would be dihedral of order 8 and $BT/T$ would be a nonnormal permutable subgroup of order 2 in $G/T$. But such a subgroup does not exist in a dihedral group. Thus $G$ is an $M$-group.

We can regard Theorem 5.2.13 as a lattice-theoretic characterization of the class of metacyclic $p$-groups within the class of all finite $p$-groups; this restriction, of
course, is needed since the metacyclic, noncyclic group of order \( p^2 \) is lattice-isomorphic to the nonabelian group of order \( pq \) for any prime \( q \) dividing \( p - 1 \). The lattice-theoretic property (7) appearing in the proof of Theorem 5.2.13, that there exists a modular subgroup \( M \) of \( G \) such that \([G/M]\) and \([M/1]\) are chains, characterizes in the class of finite groups those groups \( G \) which possess a normal subgroup \( N \) such that \( N \) and \( G/N \) are cyclic of prime power order (see Exercise 7). Finally, we remark that the class of finite metacyclic groups is not invariant under projectivities (see Exercise 8).

### Exercises

1. (Thompson [1967], Nakamura [1968]) Let \( p > 2 \) and \( A = \langle a_0, \ldots, a_p \rangle \) be an elementary abelian group of order \( p^{p+1} \).
   (a) Show that there exists an extension \( H = A\langle x \rangle \) of \( A \) by a cyclic group \( \langle x \rangle \) satisfying \( x^{p^2} = a_0, x^{-1}a_0x = a_0 \) and \( x^{-1}a_ix = a_ia_{i-1} \) for \( i = 1, \ldots, p \).
   (b) Show that there exists an extension \( G = H\langle y \rangle \) of \( H \) by a cyclic group \( \langle y \rangle \) satisfying \( y^p = a_1^{-1}, y^{-1}a_by = a_{b_1}^{-1}, y^{-1}a_1y = a_i \) for \( i = 0, \ldots, p - 1 \) and \( y^{-1}xy = x^{1+p} \).
   (c) Show that \( M = \langle y, a_2, \ldots, a_p \rangle \) is a core-free nonabelian permutable subgroup of \( G \).

2. (Nakamura [1979]) If \( G = MX \) is a finite \( p \)-group, \( M \) permutable in \( G \) and \( X \) cyclic, show that there exists a permutable subgroup \( H \) of order \( p \) of \( G \) such that \( H \leq Z(M) \).

3. (Gross [1971]) If \( G = MX \) is a finite \( p \)-group, \( M \) a core-free permutable subgroup of \( G \) and \( X \) cyclic, show that the nilpotency class of \( \Omega_2(G) \) is at most \( p - 1 \) (compare with 5.2.8 (f)).

4. (Gross [1971]) Suppose that \( G = MX \) is a finite \( p \)-group, \( M \) a core-free permutable subgroup of \( G \) and \( X \) cyclic of order \( p^n \), \( n \geq 2 \).
   (a) Show that \(|\Omega(G)| \leq p^{n-2}(p - 1)\) where \( m = p^{n-2}(p - 1) \).
   (b) Show that the nilpotency class of \( G \) is at most \( p^{n-1} - 1 \).

5. Prove properties (4)--(6).

6. (Busetto [1980b]) Let \( H \) and \( K \) be permutable subgroups of the group \( G \) and suppose that there exists \( g \in G \) such that \( H = K\langle g \rangle \). Show that every subgroup \( M \) of \( G \) such that \( K \leq M \leq H \) is permutable in \( G \).

7. Show that a finite group \( G \) contains a normal subgroup \( N \) such that \( N \) and \( G/N \) are cyclic of prime power order if and only if \( L(G) \) contains a modular element \( M \) such that \([G/M]\) and \([M/1]\) are chains.

8. Let \( p \) and \( q \) be primes such that \( 2 < q | p - 1 \), and let \( G = NH \) and \( \overline{G} = NK \) where \(|N| = p \), \( H \) is the abelian and \( K \) the nonabelian group of order \( q^3 \) and exponent \( q^2 \), \( C_H(N) = \Omega(H) \) and \( C_K(N) = \Omega(K) \). Show that
   (a) \( G \) and \( \overline{G} \) are lattice-isomorphic,
   (b) \( G \) is metacyclic, but \( \overline{G} \) is not.
5.3 Lattice-theoretic characterizations of classes of finite groups

A rather natural way of obtaining a lattice-theoretic characterization of a class of groups is to replace concepts appearing in the definition by lattice-theoretic concepts that are equivalent to them or nearly so. For example, we should try to replace "normal subgroup" by "modular subgroup", "cyclic factor group" by "distributive interval in the subgroup lattice", "abelian factor group" by "modular interval in the subgroup lattice", and so on.

We shall show that this method indeed yields lattice-theoretic characterizations for the classes of simple, perfect, soluble and supersoluble finite groups; and we shall use this idea for many other lattice-theoretic characterizations. For the first three classes we only need Lemma 5.1.2 on maximal modular subgroups; in the case of supersoluble groups we shall use 5.2.5, but we remark that it is possible to give a more elementary proof using 5.1.4 and 5.2.3 instead (see Exercise 1). We remark further that in §6.4 we shall extend nearly all these results to infinite groups. Finally, we shall present Iwasawa's characterization of finite supersoluble groups and discuss certain classes of groups that are related to nilpotent groups, the most interesting being the class of groups with lower semimodular subgroup lattice.

Simple groups

5.3.1 Theorem. The finite group $G$ is simple if and only if 1 and $G$ are the only modular elements in $L(G)$.

Proof. If 1 and $G$ are the only modular elements in $L(G)$, then $G$ in particular has no proper nontrivial normal subgroup, that is, $G$ is simple. Conversely, let $G$ be simple and suppose, for a contradiction, that there exists a modular element in $L(G)$ different from 1 and $G$. Then there also exists a nontrivial maximal modular subgroup $M$ in $G$ and, by 5.1.2, $M \unlhd G$ or $G/M_G$ is nonabelian of order $pq$ with primes $p$ and $q$. In both cases, $G$ is not simple, a contradiction.

Since projectivities map modular subgroups onto modular subgroups, Theorem 5.3.1 has the following immediate consequence.

5.3.2 Corollary (Suzuki [1951a]). If $G$ is a finite simple group and $\varphi$ is a projectivity from $G$ to a group $\bar{G}$, then $\bar{G}$ is simple.

Perfect groups

Recall that a group is perfect if it coincides with its commutator subgroup. For finite groups, an equivalent condition is that no maximal subgroup is normal. To this definition we can apply the method described at the beginning of this section.
5.3.3 **Theorem.** The finite group $G$ is perfect if and only if no maximal subgroup of $G$ is modular in $G$.

*Proof.* If no maximal subgroup of $G$ is modular in $G$, then, clearly, no maximal subgroup of $G$ is normal, that is, $G$ is perfect. Conversely, let $G$ be perfect and suppose, for a contradiction, that there exists a maximal subgroup $M$ of $G$ that is modular in $G$. Then again by 5.1.2, $M \trianglelefteq G$ or $G/M_G$ is nonabelian of order $pq$ with primes $p$ and $q$. In both cases there exists a normal subgroup of prime index in $G$, and this contradicts the assumption that $G$ is perfect.

Using 5.2.6, we again obtain as a corollary an older result of Suzuki's.

5.3.4 **Theorem** (Suzuki [1951a]). If $G$ is a finite perfect group and $\varphi$ a projectivity from $G$ to a group $\overline{G}$, then $\overline{G}$ is perfect, $\varphi$ induces an isomorphism from the lattice of normal subgroups of $G$ to that of $\overline{G}$, and $Z_n(G)^\varphi = Z_n(\overline{G})$ for all $n \in \mathbb{N}$.

*Proof.* By 5.3.3, $\overline{G}$ is perfect. If $N \trianglelefteq G$, then $N^\varphi$ is a modular subgroup of $\overline{G}$ and hence $N^\varphi \trianglelefteq \overline{G}$ by 5.2.6. Similarly, preimages of normal subgroups of $\overline{G}$ are normal in $G$ so that $\varphi$ induces an isomorphism from $\mathcal{N}(G)$ to $\mathcal{N}(\overline{G})$. Finally, let $P \in \text{Syl}_p(Z(G))$ for some prime $p$. Then $[P, G] = 1$ and, since $O^p(G) = G$, 1.6.8 yields $[P^\varphi, \overline{G}] = 1$, that is, $P^\varphi \trianglelefteq Z(\overline{G})$. It follows that $Z(G)^\varphi \trianglelefteq Z(\overline{G})$ and this statement for $\varphi^{-1}$ yields the other inclusion. Thus $Z(G)^\varphi = Z(\overline{G})$ and, since $G/Z(G)$ is perfect, a trivial induction yields that $Z_n(G)^\varphi = Z_n(\overline{G})$ for all $n \in \mathbb{N}$.

**Soluble groups**

There are many ways of defining solubility and some of them are suitable for application of the method described at the beginning of this section. We present three lattice-theoretic characterizations of the class of finite soluble groups obtained this way.

5.3.5 **Theorem** (Schmidt [1968]). The following properties of the finite group $G$ are equivalent.

(a) $G$ is soluble.

(b) There are subgroups $G_i$ of $G$ such that $1 = G_0 \leq \cdots \leq G_r = G$, $G_i$ is modular in $G$ and $[G_{i+1}/G_i]$ is modular $(i = 0, \ldots, r - 1)$.

(c) There are subgroups $G_i$ of $G$ such that $1 = G_0 \leq \cdots \leq G_s = G$, $G_i$ is modular in $G_{i+1}$ and $[G_{i+1}/G_i]$ is modular $(i = 0, \ldots, s - 1)$.

(d) There are subgroups $G_i$ of $G$ such that $1 = G_0 < \cdots < G_t = G$, $G_i$ is maximal and modular in $G_{i+1}$ $(i = 0, \ldots, t - 1)$.

*Proof.* That (a) implies (b) is clear since, by 2.1.3 and 2.1.4, the members $G_i$ of a chief series of the soluble group $G$ have the desired properties. Trivially, (b) implies (c) and (4) of §5.1 shows that if (c) holds, then every subgroup between $G_i$ and $G_{i+1}$ is modular in $G_{i+1}$, so that every maximal chain in $L(G)$ containing all the $G_i$ has the
properties required in (d). Finally, we prove by induction on $|G|$ that (d) implies (a). The induction assumption yields that $M = G_{i-1}$ is soluble and, by 5.1.2, either $M \leq G$ and $G/M$ is cyclic of prime order or $|G/M_G| = pq$ with primes $p$ and $q$. In both cases, $M_G$ and $G/M_G$ are soluble and hence $G$ is soluble.

The above theorem yields a second proof of the fact that the class of finite soluble groups is invariant under projectivities; in 4.3.4 we used Suzuki's results on singular projectivities to prove this. Another lattice-theoretic characterization of the class of finite soluble groups was given by Suzuki [1956]. He proved that the finite group $G$ is soluble if and only if there exists a maximal chain $1 = G_0 \leq \cdots \leq G_r = G$ of subgroups $G_i$ invariant under $P(G)$ such that $[G_{i+1}/G_i]$ is modular for all $i = 0, \ldots, r - 1$.

Recall that in every finite group $G$ there exist the soluble residual $G_\geq$ and the soluble radical $G^\triangleleft$. The residual is defined as the intersection of all the normal subgroups with soluble factor group and is therefore the smallest normal subgroup of $G$ with soluble factor group; the radical is the product of all the soluble normal subgroups and hence is the largest soluble normal subgroup of $G$. Let $R = G_\geq$. Then $R'$ is a normal subgroup of $G$ with soluble factor group and hence $R = R'$, that is, $R$ is perfect. On the other hand, if $H$ is any subgroup of $G$, then $R \cap H \leq H$ and $HR/R \cap H \simeq HR/R$ is soluble. It follows that every perfect subgroup of $G$ is contained in $R$. Thus

(1) $G_\geq$ is the largest perfect subgroup of $G$.

Now let $T = G^\triangleleft$. Then if $M$ is a maximal soluble subgroup of $G$, $TM/T \simeq M/M \cap T$ is soluble, hence $TM$ is soluble and the maximality of $M$ implies that $TM = M$. Thus $T$ is contained in every maximal soluble subgroup of $G$ and, since the intersection of all these clearly is a soluble normal subgroup of $G$,

(2) $G^\triangleleft$ is the intersection of all the maximal soluble subgroups of $G$.

By 5.3.3 and 5.3.5, we can detect perfect and soluble subgroups in the subgroup lattice of $G$. Thus (1) and (2) yield lattice-theoretic characterizations of the soluble residual and the soluble radical in finite groups. We only note the usual corollary.

5.3.6 Theorem (Suzuki [1951a]). If $\varphi$ is a projectivity from the finite group $G$ to a group $\overline{G}$, then $(G_\geq)^{\varphi} = \overline{G_\geq}$ and $(G^\triangleleft)^{\varphi} = \overline{G^\triangleleft}$.

Supersoluble groups

The finite supersoluble groups can be characterized like the soluble groups.

5.3.7 Theorem (Schmidt [1968]). The following properties of the finite group $G$ are equivalent.

(a) $G$ is supersoluble.

(b) There are subgroups $G_i$ of $G$ such that $1 = G_0 \leq \cdots \leq G_r = G$, $G_i$ is modular in $G$ and $[G_{i+1}/G_i]$ is distributive ($i = 0, \ldots, r - 1$).
(c) There are subgroups $G_i$ of $G$ such that $1 = G_0 < \cdots < G_s = G$, $G_i$ is modular in $G$ and maximal in $G_{i+1}$ $(i = 0, \ldots, s - 1)$.

**Proof.** That (a) implies (c) is clear since the members $G_i$ of a chief series of the supersoluble group $G$ have the desired properties. And (c) implies (b) since every interval $[G_{i+1}/G_i]$ in (c) is a chain and hence is distributive. We prove by induction on $|G|$ that (b) implies (a). The property (b) is inherited by factor groups $G/N$; for $NG_i/N$ is modular in $G/N$ and (1) of §5.1 shows that

$$[(NG_{i+1}/N)/(NG_i/N)] \cong [NG_iG_{i+1}/NG_i] \cong [G_{i+1}/G_{i+1} \cap NG_i]$$

is an interval in $[G_{i+1}/G_i]$ and is therefore distributive. We may assume that $1 = G_0 < G_1 = M$. Then $M$ is modular in $G$ and $L(M) \cong [G_1/G_0]$ is distributive. By 1.2.4, $M$ is cyclic; in particular, $M_G$ is cyclic. By 5.2.5, $M^G/M_G$ is hypercyclically embedded in $G$ and, since $M^G \neq 1$, the induction assumption yields that $G/M^G$ is supersoluble. Thus $M_G$, $M^G/M_G$ and $G/M^G$ all are hypercyclically embedded in $G$, and (b) of 5.2.1 shows that $G$ is supersoluble. 

5.3.8 **Corollary.** If $G$ is a finite supersoluble group and $\varphi$ is a projectivity from $G$ to a group $\bar{G}$, then $\bar{G}$ is supersoluble.

The first lattice-theoretic characterization of the class of finite supersoluble groups was given by Iwasawa. If $G$ is supersoluble, it is easy to prove by induction on $|G|$ that every maximal subgroup $M$ of $G$ has prime index in $G$. This is clear if $M_G \neq 1$; for then $M/M_G$ is a maximal subgroup of the supersoluble group $G/M_G$ of smaller order than $|G|$. And if $M_G = 1$ and $N$ is a minimal normal subgroup of $G$, then $MN = G$ and $|G:M| = |N|$ is a prime. Since every subgroup of $G$ is supersoluble it follows that for every pair of subgroups $K < H$ of $G$, the length of a maximal chain in $L(G)$ from $K$ to $H$ is the number of prime divisors of $|H:K|$, including multiplicities. Thus $L(G)$ satisfies the Jordan-Dedekind chain condition and this is Iwasawa's characterization.

5.3.9 **Theorem** (Iwasawa [1941]). A finite group is supersoluble if and only if its subgroup lattice satisfies the Jordan-Dedekind chain condition.

**Proof.** It remains to be shown that a finite group $G$ satisfying the Jordan-Dedekind chain condition is supersoluble. We use induction on $|G|$. Then every proper subgroup of $G$ is supersoluble and, by a theorem of Huppert's (see Robinson [1982], p. 287), $G$ is soluble. Therefore a composition series of $G$ is a maximal chain in $L(G)$ and its length is the number $d$ of prime divisors of $|G|$. If $M$ is a maximal subgroup of $G$, the Jordan-Dedekind chain condition implies that $L(M)$ has length $d - 1$ and, since $M$ is supersoluble, $|M|$ has $d - 1$ prime divisors. It follows that $|G:M|$ is a prime and, by another well-known theorem of Huppert's (see Robinson [1982], p. 268), $G$ is supersoluble. 

We remark that Iwasawa's theorem (and the above proof) by now can be found in many textbooks on group theory; see, for example, Robinson [1982], p. 288 or
Huppert [1967], p. 719. Huppert's theorem, used to show that $G$ is soluble, depends on Grün's Second Theorem or a similar transfer argument. The reader can find a direct proof of Iwasawa's theorem, using only Grün's Second Theorem, in Suzuki [1956], p. 9.

Finally we mention that Berkovic [1966] and Fort [1978] study finite groups in which for every $1 \neq H \leq G$ the interval $[G/H]$ satisfies the Jordan-Dedekind chain condition. Both authors determine the structure of soluble groups with this property (see Exercise 4); using the classification of minimal simple groups, Fort, in addition, shows that any group with this property is soluble.

Groups with semimodular subgroup lattice

For the class of finite nilpotent groups, our method of obtaining lattice-theoretic characterizations does not work: the $P$-groups show that this class is not invariant under projectivities. Nevertheless it is interesting to examine the properties that emerge if we apply the usual process to a given characterization of nilpotency. The most suitable one for our purpose is Wielandt's well-known theorem which asserts that a finite group is nilpotent if and only if every maximal subgroup is normal. Using this, we get the following class of groups.

5.3.10 Theorem (Schmidt [1970b]). Every maximal subgroup of the finite group $G$ is modular in $G$ if and only if $G$ is supersoluble and induces an automorphism group of at most prime order in every complemented chief factor of $G$.

Proof. Suppose first that every maximal subgroup $M$ of $G$ is modular in $G$. Then it follows from 5.1.2 that $|G : M|$ is a prime and, by Huppert's theorem (see Robinson [1982], p. 268), $G$ is supersoluble. Let $H/K$ be a complemented chief factor of $G$; we have to show that $|G : C_G(H/K)|$ is a prime or 1. Since $H/K$ is complemented, there exists $M \leq G$ such that $G = HM$ and $H \cap M = K$. Then $|G : M| = |H : K| = p$ is a prime and hence $M$ is a maximal subgroup of $G$. By 5.1.2, $M \trianglelefteq G$ or $|G : M_G| = pq$ for some prime $q \neq p$. In both cases, $HM_G \leq C_G(H/K)$ and thus $|G : C_G(H/K)|$ is $q$ or 1.

Conversely, suppose that $G$ satisfies the conditions of the theorem and take a maximal subgroup $M$ of $G$; we have to show that $M \text{mod} G$. If $M \trianglelefteq G$, we are done; so assume that $M$ is not normal in $G$. Then $G/M_G$ is a primitive soluble group and therefore (see Robinson [1982], p. 192) contains a minimal normal subgroup $N/M_G$ such that $N = C_G(N/M_G)$. Since $G$ is supersoluble, $|N/M_G| = p$ is a prime and, since $N \not\leq M$, $M/M_G$ is a complement to $N/M_G$ in $G/M_G$. Thus $N/M_G$ is a complemented chief factor of $G$ and our assumption yields that $|G : N| = |G : C_G(N/M_G)| = q$ is a prime. Thus $|G/M_G| = pq$ and hence $G/M_G$ has modular subgroup lattice. By (4) of § 5.1, $M$ is modular in $G$.

A condition that appears to be slightly stronger than Wielandt's is that every maximal subgroup of every subgroup $H$ of $G$ is normal in $H$. This clearly is also
equivalent to nilpotency and, if we translate this, we get the condition that every maximal subgroup of every subgroup \(H\) of \(G\) is modular in \(H\). By 2.1.5, a maximal subgroup \(M\) of \(H\) is modular in \(H\) if and only if for every \(K \leq H\) such that \(M \cup K = H\), \(M \cap K\) is maximal in \(K\). This shows that our condition is equivalent to the following: if \(K, M \leq G\) and \(M\) is maximal in \(M \cup K\), then \(M \cap K\) is maximal in \(K\). This is equivalent to \(L(G)\) being lower semimodular as defined in §2.1. These groups were characterized by Ito; they are still closer to nilpotent groups than those in Theorem 5.3.10.

5.3.11 Theorem (Ito [1951]). The subgroup lattice of the finite group \(G\) is lower semimodular if and only if \(G\) is supersoluble and induces an automorphism group of at most prime order in every chief factor of \(G\).

Proof. Suppose first that \(L(G)\) is lower semimodular. Then by 5.3.10 or Iwasawa's theorem, \(G\) is supersoluble. Let \(H/K\) be a chief factor of \(G\); we have to show that \(|G : C_G(H/K)|\) is a prime or 1 and may assume that \(K = 1\). Then \(|H| = p\) is a prime. Since \(G\) is soluble, there exists a Hall \(p'\)-subgroup \(Q\) in \(G\). Then every maximal subgroup of \(HQ\) is modular in \(HQ\) and \(H\) is a complemented chief factor in \(HQ\). By 5.3.10, \(|HQ : C_{HQ}(H)|\) is a prime \(q\) or 1; in particular, \(|Q : C_Q(H)|\) divides \(q\). Every Sylow \(p\)-subgroup \(P\) of \(G\) centralizes \(H\) since \(H\) is a minimal normal subgroup of \(P\). It follows that \(|G : C_G(H)|\) divides \(q\), as desired.

Conversely, suppose that \(G\) is supersoluble and \(|G : C_G(H/K)|\) is a prime or 1 for every chief factor \(H/K\) of \(G\). Let \(S \leq G\) and take a chief series \(1 = G_0 < \cdots < G_r = G\) of \(G\). Then for every \(i\), \(S \cap G_i \leq S\) and \(|S \cap G_i : S \cap G_{i-1}|\) divides \(|G_i : G_{i-1}| \in \mathbb{P}\). By the Jordan-Hölder Theorem, every chief factor of \(S\) is isomorphic to one of the \(S \cap G_i / S \cap G_{i-1}\). Now \(C_G(G_i / G_{i-1}) \cap S\) centralizes \(S \cap G_i / S \cap G_{i-1}\) and has index in \(S\) equal to 1 or a prime. Thus \(S\) satisfies the conditions of the theorem, in particular those of Theorem 5.3.10. It follows that every maximal subgroup of \(S\) is modular in \(S\) and \(L(G)\) is lower semimodular.

It is easy to see that the two classes of groups in Theorems 5.3.10 and 5.3.11 are different (see Exercise 5). An immediate consequence of 5.3.11 is the following result which is a little surprising.

5.3.12 Corollary. If \(H\) and \(K\) are finite groups with lower semimodular subgroup lattice, then so is their direct product \(H \times K\).

Finite groups with upper semimodular subgroup lattice are less important since there is no related class of groups which is significant from the group-theoretic point of view. The structure of these groups was determined by Sato, who also studied infinite groups with this property; see Suzuki [1956], pp. 24–26.

We shall give lattice-theoretic characterizations of certain classes of infinite nilpotent groups in §§7.2–7.4. However, not much is known about infinite groups which satisfy the Jordan-Dedekind chain condition or have lower semimodular subgroup lattice.
Exercises

1. Use 5.1.4 and 5.2.3 instead of 5.2.5 to prove Theorem 5.3.7. (Hint: In a minimal counterexample to the implication (b) ⇒ (a) there is exactly one minimal normal subgroup \( N \), and \( G/N \) is supersoluble; furthermore, \((G_1)_{G} = 1\) for \( G_1 > G_0 \). If \( M \) is maximal with respect to the properties \( G_1 \leq M \mod G \) and \( M_G = 1 \), show the following:
   (a) \( M < NM \leq D(M) = \bigcap \{ M \cup M^x | x \in G \backslash N_G(M) \} \) and \([D(M)/M]\) is a chain;
      let \( F \) be the atom of this chain.
   (b) If \( M \leq F \), then \( M \) per \( G \); by 5.2.3, \(|N|\) is a prime.
   (c) If \( M \) is not normal in \( F \), then \( NM = D(M) = M^G \) is a nonabelian group of
      order \( pq \ (p, q \in \mathbb{P}) \) and hence again \(|N|\) is a prime.)

2. Let us call a lattice \( L \) polymodular if it contains a least element \( 0 \), a greatest
   element \( I \) and elements \( a_i \) such that \( 0 = a_0 < \cdots < a_r = I \), \( a_i \) is modular in \( L \) and
   \([a_i/a_{i-1}]\) is modular \((i = 1, \ldots, r)\). If \( G \) is a finite group, show that
   (a) \( G^0 \) is the largest modular subgroup of \( G \) with polymodular subgroup lattice
      and
   (b) \( G^\circ \) is the smallest modular subgroup \( M \) of \( G \) with polymodular factor interval
      \([G/M]\).

3. Let us say that the element \( a \) of the lattice \( L \) with least element \( 0 \) is polymodular
   in \( L \) if there exist \( a_i \in L \) such that \( 0 = a_0 < \cdots < a_r = a \), \( a_i \) is modular in \( L \) and
   \( a_{i-1} \) is maximal in \( a_i \) \((i = 1, \ldots, r)\). For a finite group \( G \), let \( T(G) \) be the largest
   hypercyclically embedded normal subgroup of \( G \), and \( G_T \) the supersoluble residual,
   the smallest normal subgroup of \( G \) with supersoluble factor group; by 5.2.1, these subgroups exist. Show that
   (a) \( T(G) \) is the largest polymodular element of \( L(G) \) and
   (b) \( G_T \) is the smallest modular subgroup \( M \) of \( G \) for which \( G \) is polymodular in
      \([G/M]\).
   It follows that \( T(G)^\varphi = T(\bar{G}) \) and \((G_T)^\varphi = \bar{G}_T \) for any projectivity \( \varphi \) from \( G \) to a
group \( \bar{G} \).

4. (Berkovic [1966], Fort [1978]) Let \( G \) be a finite soluble group. Show that \([G/H]\)
   satisfies the Jordan-Dedekind chain condition for every nontrivial subgroup \( H \) of
   \( G \) if and only if \( G \) is either supersoluble or is a semidirect product of an elementary
   abelian group \( N \) by a cyclic group \( K \) of odd order such that every nontrivial
   subgroup of \( K \) operates irreducibly on \( N \).

5. Let \( p, q, r \) be primes such that \( q \neq r \) and \( qr | p - 1 \) and let \( 0 < s, t < p \) such that
   \( s^q \equiv t^r \equiv 1 \mod p \). Let \( P = \langle a, b, c | a^p = b^p = c^p = 1, ac = ca, ab = ba, c^{-1}bc = ba \rangle \) be the nonabelian group of order \( p^3 \) and exponent \( p \) and define \( \sigma \in \text{Aut} P \) by
   \( (c^{i-j}a^k)^\sigma = c^{is}b^{jt}a^{kst} \ (0 \leq i, j, k < p) \). Show that every maximal subgroup of the
   semidirect product \( G \) of \( P \) and \( \langle \sigma \rangle \) is modular in \( G \), but that \( L(G) \) is not lower
   semimodular.

6. (Venzke [1972]) Show that every subgroup of a finite group \( G \) is maximal sensitive in \( G \) (for the definition see § 3.3, Further Topics) if and only if \( G \) is isomorphic to a subgroup of a direct product \( S_1 \times \cdots \times S_r \) of \( P \)-groups \( S_i \in P(n_i, p_i) \) such that
   \( p_i \neq p_j \) for \( i \neq j \).
7. (Venzke [1975]) If \( M \cap N \) is maximal in \( M \) (and in \( N \)) for any two different maximal subgroups \( M \) and \( N \) of the finite group \( G \), show that every maximal subgroup \( M \) of minimal order which is not modular in \( G \). If \( G \) is not soluble, use the Feit-Thompson Theorem to get an involution \( t \in G \) such that \( G = \langle M, t \rangle \); show that \( (M \cap M^t) \langle t \rangle \) is a maximal subgroup of \( G \) and hence is modular in \( G \).

### 5.4 Projective images of normal subgroups of finite groups

In the next two sections and in §§ 6.5 and 6.6 we shall study images of normal subgroups \( N \) of a group \( G \) under projectivities \( \varphi \) from \( G \) to groups \( G \). We want to show that \( N^G \) is near to being normal in \( G \). The main result of this section, Theorem 5.4.7, will reduce this problem for finite groups to the case that \( N^G \) is permutable in \( G \). Together with the results of §5.2 this will yield a number of useful criteria for \( N^G \) to be normal in \( G \). In the course of our analysis we shall very often have to consider the core or the normal closure of \( N^G \) and the preimages of these subgroups. Therefore it is worthwhile introducing the following general notation for arbitrary groups.

**5.4.1 Notation.** If \( \varphi \) is a projectivity from \( G \) to \( \bar{G} \), \( H \leq G \) and \( x \in \bar{G} \), we put \( H^\varphi = H^\varphi (x) \) and denote the preimages of the core and the normal closure of \( H^\varphi \) in \( G \) by \( Hz^\varphi \) and \( H^G \), respectively, that is,

\[
Hz^\varphi = ((H^\varphi)^G)^{-1} = (Hz^\varphi)^{-1} \quad \text{and} \quad H^G = ((H^\varphi)G)^{-1} = (H^G)^{-1};
\]

furthermore, as in Chapter 4, we shall write \( H^{\varphi \times \psi^{-1}} = ((H^\psi)^x)^{-1} \).

### Minimal normal subgroups

It seems reasonable to start our investigations with minimal normal subgroups. We shall show that these are mapped to minimal normal subgroups if they are not cyclic and we begin with the cyclic case.

**5.4.2 Lemma.** Let \( p \) be a prime, \( G \) a finite \( p \)-group and \( \varphi \) a projectivity from \( G \) to a group \( \bar{G} \).

(a) Then there exists a normal subgroup \( Z \) of order \( p \) in \( G \) such that \( Z^\varphi \leq \bar{G} \).

(b) If \( N \) is a minimal normal subgroup of \( G \), then \( N^G \leq \Omega(Z(G)) \).

**Proof.** If \( \bar{G} \) is not a \( p \)-group, then, by 2.2.6, \( G \) and \( \bar{G} \) are cyclic or \( P \)-groups and both assertions of the lemma hold trivially. So we may assume that \( \bar{G} \) is a \( p \)-group.

(a) Suppose, for a contradiction, that there is no minimal normal subgroup \( Z \) of \( G \) such that \( Z \leq \bar{G} \). Let \( N \) be a minimal normal subgroup of \( G \) and \( M \leq G \) such that \( M \) is a minimal normal subgroup of \( \bar{G} \). Then \( \bar{N} \) and \( \bar{M} \) are nonnormal permutable
subgroups of order \( p \) in \( \overline{G} \) and \( G \), respectively. Let \( x \in G \setminus C_G(M) \). By (e) of 5.2.9, \( Z(G) \cap \langle x \rangle \neq 1 \). If also \( Z(\overline{G}) \cap \langle x \rangle^\varphi \neq 1 \), then \( Z = \Omega(\langle x \rangle) \leq Z(G) \) and \( \overline{Z} \leq Z(\overline{G}) \); but we assume that such a normal subgroup does not exist. Therefore \( Z(\overline{G}) \cap \langle x \rangle^\varphi = 1 \), and (e) of 5.2.9 now shows that \( \langle x \rangle^\varphi \leq C_{\overline{G}}(N) \). Since \( G \) is generated by the elements \( x \in G \setminus C_G(M) \), \( \overline{G} \) is generated by these \( \langle x \rangle^\varphi \) and it follows that \( \overline{N} \leq Z(\overline{G}) \). This contradiction proves (a).

(b) Let \( G \) be a minimal counterexample and \( N \) a minimal normal subgroup of \( G \) such that \( H = N^G \) is not contained in \( \Omega(Z(G)) \). Then \( H \neq N \) and hence again \( \overline{N} \) is a nonnormal permutable subgroup of order \( p \) in \( \overline{G} \). By 5.2.9, \( H = \overline{N} \times (\overline{H} \cap Z(\overline{G})) \) is elementary abelian. Since \( N \leq Z(G) \) and \( H \not\leq Z(G) \), there exists a subgroup \( M \) of order \( p \) in \( (\overline{H} \cap Z(\overline{G}))^{\varphi^{-1}} \) that is not contained in \( Z(G) \). Therefore \( M \) is a nonnormal permutable subgroup of order \( p \) in \( G \). Finally, by (a) there exists a normal subgroup \( Z \) of order \( p \) in \( G \) such that \( Z \leq \overline{L} \leq G \). Since \( \overline{Z} \leq L \) and hence \( Z \leq \overline{Z} \leq L \). Thus \( MZ \leq G \) and, since \( M \) is not normal in \( G \), it follows that \( MZ = M^G \) and \( M^G \cap Z(G) = \overline{Z} \). For \( x \in G \setminus C_G(M) \), again by (e) of 5.2.9, \( 1 \neq M^G \cap Z(G) \cap \langle x \rangle = Z \cap \langle x \rangle \) and hence \( Z \leq \langle x \rangle \). Then \( Z \neq N \leq Z(G) \) implies that \( N \langle x \rangle = N \times \langle x \rangle \) and \( \Omega(N \langle x \rangle) = NZ \). Since \( \varphi \) is a projectivity,

\[
(NZ)^\varphi = (\Omega(N \langle x \rangle))^\varphi = \Omega((N \langle x \rangle)^\varphi) \leq (N \langle x \rangle)^\varphi,
\]

that is, \( \langle x \rangle^\varphi \) normalizes \( (NZ)^\varphi \). Now \( G \) is generated by these \( x \in G \setminus C_G(M) \) and it follows that \( (NZ)^\varphi \leq \overline{G} \). But then \( H = NZ \leq \Omega(Z(G)) \), a contradiction.

We need the following simple result on projective images of hypercentrally embedded normal \( p \)-subgroups.

5.4.3 Lemma. Let \( \varphi \) be a projectivity from the finite group \( G \) to a group \( \overline{G} \) and suppose that \( H \leq G \) such that \( H^\varphi \) is a normal \( p \)-subgroup of \( \overline{G} \) which is hypercentrally embedded in \( \overline{G} \) but not contained in the centre of \( \overline{G} \).

(a) If \( P^\varphi \in \text{Syl}_p(\overline{G}) \), then \( P \) is a \( p \)-subgroup of \( G \) containing \( H \) and \( G = P \cup C_G(H) \).

(b) If \( H \leq G \), then \( H \) is hypercentrally embedded in \( G \).

Proof. Clearly, \( \overline{G} = \overline{P} \varphi(\overline{G}) \) and \( \overline{H} \leq \overline{P} \) since \( \overline{H} \) is a normal \( p \)-subgroup of \( \overline{G} \). By 5.2.2, \( [\overline{H}, O_p(\overline{G})] = 1 \). Since \( \overline{H} \not\leq Z(\overline{G}) \), \( \overline{P} \) is not abelian and hence \( P \) is a \( p \)-group by 2.2.6. Furthermore, 1.6.8 yields that \( [H, O_p(\overline{G})] = 1 \) and it follows that \( G = P \cup C_G(H) \). Finally, if \( H \not\leq G \), then \( H \leq P \) is a normal \( p \)-subgroup of \( G \) and \( G/C_G(H) \simeq P/P \cap C_G(H) \) is a \( p \)-group. By 5.2.2, \( H \) is hypercentrally embedded in \( G \).

5.4.4 Theorem (Schmidt [1975a]). Let \( N \) be a minimal normal subgroup of the finite group \( G \) and suppose that \( \varphi \) is a projectivity from \( G \) to a group \( \overline{G} \) such that \( N^\varphi \) is not a minimal normal subgroup of \( \overline{G} \). Then \( N \) is cyclic of prime order \( p \) and for \( S = N^G \), one of the following two assertions holds:
(a) $S$ and $S^\circ$ are $P$-groups in $P(n, p)$ for some $n \in \mathbb{N}$ and there exists $T \leq G$ such that $G = S \times T, \overline{G} = S^\circ \times T^\circ$ and $(|S|, |T|) = 1 = (|S^\circ|, |T^\circ|)$.
(b) $S$ and $S^\circ$ are elementary abelian $p$-groups, furthermore $S \leq Z(G)$ and $S^\circ = N^\circ \times (S^\circ \cap Z(\overline{G})) \leq Z_2(\overline{G})$.

**Proof.** Suppose, for a contradiction, that there exists a subgroup $M$ of $G$ such that $1 < M < N$ and $\overline{M} \leq \overline{G}$. Then $M$ is modular in $G$ and, since $N$ is a minimal normal subgroup, $M^G = N$ and $M_\circ = 1$. By 5.2.5, $N$ is hypercyclically embedded in $G$ and hence $|N|$ is a prime, contradicting $1 < M < N$. Thus there is no normal subgroup of $\overline{G}$ lying properly between $1$ and $\overline{N}$. In particular, if $\overline{N} \leq \overline{G}$, then $\overline{N}$ would be a minimal normal subgroup of $\overline{G}$, contradicting our assumption. It follows that $\overline{N}$ is not normal in $\overline{G}$ and $\overline{NG} = 1$.

By 5.1.7, $\overline{N}$ is nilpotent and hence $N$ is a soluble minimal normal subgroup of $G$. Thus $N$ is an elementary abelian $p$-group and, by 2.2.6, its nilpotent projective image $\overline{N}$ is a $q$-group for primes $p$ and $q$. By 5.1.9 (or 5.1.14), either $\overline{N}$ is permutable in $\overline{G}$ or $\overline{S}$ is a $P$-group and $\overline{G} = \overline{S} \times \overline{T}$ where $(|\overline{S}|, |\overline{T}|) = 1$. In the latter case, $|\overline{N}| = q$, hence $N$ is cyclic of prime order $p$ and, by 1.6.6, $G = S \times T$ where $(|S|, |T|) = 1$. By 2.2.5, $S$ and $\overline{S}$ lie in the same class $P(n, r)$ and, since $N$ is a normal subgroup of order $p$ in $S$, $r = p$. Thus (a) holds.

Now suppose that $\overline{N}$ is permutable in $\overline{G}$. As a product of $q$-groups, $\overline{S}$ is a normal $q$-subgroup of $\overline{G}$ and is hypercentrally embedded in $\overline{G}$ by 5.2.3. Then 5.2.2 shows that $\overline{G}/C_{\overline{G}}(\overline{S})$ is a $q$-group and hence $\overline{G} = \overline{P}C_{\overline{G}}(\overline{S})$ for some $\overline{P} \in \text{Syl}_q(\overline{G})$. Furthermore $\overline{S} \leq Z(\overline{G})$ since $\overline{N}$ is not normal in $\overline{G}$. By 5.4.3, $P$ is a $q$-subgroup of $G$ containing $S$, hence $p = q$ as $N \leq S$, and $G = P \cup C_G(S)$. Therefore $1 \neq Z(P) \cap N \leq Z(G)$ and, since $N$ is a minimal normal subgroup of $G$, it follows that $N$ is cyclic of order $p$. Now $\overline{G} = C_{\overline{G}}(\overline{S})\overline{P}$ implies that $\overline{S} = \overline{N}^G = \overline{N}^p$ and 5.4.2, applied to the projectivity induced in $P$, yields that $S \leq \Omega(Z(P))$. Since $G = P \cup C_G(S)$, it follows that $S$ is an elementary abelian $p$-subgroup of $Z(G)$. Finally, $\overline{N}$ is a nonnormal permutable subgroup of order $p$ in $\overline{G}$ and, by 5.2.9, $\overline{S}$ is an elementary abelian $p$-group and $\overline{S} = \overline{N} \times (\overline{S} \cap Z(\overline{G})) \leq Z_2(\overline{G})$. Thus (b) holds.

Our theorem in particular asserts that every projectivity between finite groups maps noncyclic minimal normal subgroups onto minimal normal subgroups. We show that the centralizers of these minimal normal subgroups are also mapped onto each other.

**5.4.5 Theorem.** Let $N$ be a minimal normal subgroup of the finite group $G$ and let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$. If $N$ is cyclic, of order $p$, say, assume further that $N^\varphi \leq \overline{G}$ and that $\varphi$ and $\varphi^{-1}$ are regular at $p$. Then $C_G(N)^\varphi = C_{\overline{G}}(N^\varphi)$.

**Proof.** By 5.4.4, $\overline{N}$ is a minimal normal subgroup of $\overline{G}$ if $N$ is not cyclic. Therefore it suffices to show that $C_G(N)^\varphi \leq C_{\overline{G}}(\overline{N})$; application of this result to $\varphi^{-1}$ and $\overline{N}$ will yield the other inclusion.

First assume that $N$ is not abelian, let $q$ be a prime and $X$ a $q$-subgroup of $C_G(N)$. Since $N$ is a nonabelian minimal normal subgroup, $N = O^q(N)$ and 1.6.8 shows that $\overline{X} \leq C_{\overline{G}}(\overline{N})$. Since $C_G(N)$ is generated by its subgroups of prime power order, it follows that $C_G(N)^\varphi \leq C_{\overline{G}}(\overline{N})$. 

\[\_\]
Now suppose that $N$ is abelian, hence $|N| = p^n$ for some prime $p$. Again by 1.6.8, $[\overline{N}, O^p(C_G(N))^o] = 1$ and we have to show that $\overline{P} \leq C_{\overline{G}}(\overline{N})$ for some $P \in \text{Syl}_p(C_G(N))$. By the Frattini argument, $G = C_G(N)N_G(P)$. This shows that $N$ is a minimal normal subgroup of $H = N_G(P)$ and, by 5.4.4 or assumption, $\overline{N}$ is a minimal normal subgroup of $\overline{H}$. We claim that $\varphi$ and $\varphi^{-1}$ are regular at $p$. This is clear by assumption if $N$ is cyclic; and if $N$ is not cyclic, it follows from the fact, see 4.2.6, that a group with a $p$-singular projectivity has only cyclic $p$-chief factors. Therefore $P^o \leq O_p(H)^o = O_p(H^o)$ and hence $\overline{N} \leq O_p(\overline{H})$. Then $\overline{N} \cap Z(O_p(\overline{H}))$ is a nontrivial normal subgroup of $\overline{H}$ and, since $\overline{N}$ is a minimal normal subgroup of $\overline{H}$, it follows that $\overline{N} \leq Z(O_p(\overline{H}))$. In particular, $\overline{P} \leq O_p(\overline{H})$ centralizes $\overline{N}$, as desired.

The structure of $G/N_G$ and $\overline{G}/\overline{N_G}$

We come to our main theorem on images of normal subgroups under projectivities of finite groups. Our results on modular and permutable subgroups yield the structure of $G/N_G$. To use this efficiently in the study of $G$, we need to know that the preimage $N_G$ of $\overline{N_G}$ is a normal subgroup of $G$ so that $\varphi$ induces a projectivity from $G/N_G$ to $\overline{G}/\overline{N_G}$. In fact we prove a little more than this.

5.4.6 Lemma. Let $N$ be a normal subgroup of the finite group $G$, $\varphi$ a projectivity from $G$ to a group $\overline{G}$, $H = N^\overline{G}$ and $K = N_G$, that is, $H^o$ the normal closure and $K^o$ the core of $N^o$ in $G$.

(a) Then $H$ and $K$ are normal subgroups of $G$.
(b) If $N^o$ is permutable in $\overline{G}$, then $H/K$ and $H^o/K^o$ are hypercentrally embedded in $G$ and $\overline{G}$, respectively.

Proof. (a) We use induction on $|G|$ and show first that $H \leq G$. For this let $M$ be a minimal normal subgroup of $G$ contained in $N$ and put $S = M^\overline{G}$. Then $S \leq H$ and, by 5.4.4, $S \leq G$. Therefore $\varphi$ induces a projectivity $\overline{\varphi}$ from $G/S$ to $\overline{G}/\overline{S}$ and, for $NS/S \leq G/S$, $\overline{H}/\overline{S}$ is the normal closure of $(NS/S)^\varphi$ in $\overline{G}/\overline{S}$. By induction, $H \leq G$.

Now we show that $K \leq G$. This is clear if $K = 1$. So let $K \neq 1$ and take $M \leq G$ such that $M$ is a minimal normal subgroup of $G$ contained in $K$. Then if $S$ is the normal closure of $M$ in $G$, $S \leq N$ since $M \leq N \leq G$. By 5.4.4, $S \leq \overline{G}$ and, as $\overline{K}$ is the core of $\overline{N}$ in $\overline{G}$, it follows that $\overline{S} \leq \overline{K}$. Again $\varphi$ induces a projectivity from $G/S$ to $\overline{G}/\overline{S}$ and by induction, $K \leq G$.

(b) By (a), $\varphi$ induces a projectivity from $G/K$ to $\overline{G}/\overline{K}$ and therefore we may assume that $K = 1$. Then by 5.2.3, $\overline{H}$ is hypercentrally embedded in $\overline{G}$. In particular, $\overline{H}$ is nilpotent and hence $\overline{H} = H_1^o \times \cdots \times H_r^o$ with Sylow $p_i$-subgroups $H_i^o$ of $\overline{H}$. Every $H_i^o$ is characteristic in $\overline{H}$ and hence normal in $\overline{G}$; thus $H_i^o$ is a hypercentrally embedded normal $p_i$-subgroup of $\overline{G}$ that is not contained in $Z(\overline{G})$ since $H_i^o \cap \overline{N} \neq 1$. By 1.6.6, $H = H_1 \times \cdots \times H_r$, where $|H_i|/|H_j|$ = 1 for $i \neq j$; hence $H_i$ is characteristic in $H \leq G$ and thus $H_i \leq G$. By (b) of 5.4.3, every $H_i$ is hypercentrally embedded in $G$, and then (c) of 5.2.1 shows that $H = H_1 \cdots H_r$ is hypercentrally embedded in $G$. \qed
5.4.7 Theorem (Schmidt [1975a]). Let \( N \) be a normal subgroup of the finite group \( G \), \( \phi \) a projectivity from \( G \) to a group \( \overline{G} \), \( H = N^G \) and \( K = N_{\overline{G}} \), that is, \( H^\phi \) the normal closure and \( K^\phi \) the core of \( N^\phi \) in \( \overline{G} \). Then \( H \) and \( K \) are normal subgroups of \( G \) and there are primes \( p_i, q_i \) and \( n_i \in \mathbb{N} \) such that

\[
G/K = \frac{S_1}{K} \times \cdots \times \frac{S_r}{K} \times \frac{T}{K} \quad \text{and} \quad \overline{G}/K^\phi = \frac{S_1^\phi}{K^\phi} \times \cdots \times \frac{S_r^\phi}{K^\phi} \times \frac{T^\phi}{K^\phi}
\]

where \( 0 \leq r \in \mathbb{Z} \) and for all \( i, j \in \{1, \ldots, r\} \),

(a) \( \frac{S_i^\phi}{K^\phi} \) is a \( P \)-group of order \( p_i^{n_i} q_i \), \( p_i > q_i \) and \( (|\frac{S_i^\phi}{K^\phi}|, |\frac{S_j^\phi}{K^\phi}|) = 1 \), for \( i \neq j \),

(b) \( S_i/K \in P(n_i + 1, p_i) \) and \( (|\frac{S_i}{K}|, |\frac{S_j}{K}|) = 1 \) \( (|\frac{S_i}{K}|, |\frac{T}{K}|) \) for \( i \neq j \),

(c) \( N/K = (N \cap S_1)/K \times \cdots \times (N \cap S_r)/K \times (N \cap T)/K, \ |(N \cap S_i)/K| = p_i, \ |(N \cap S_i)^\phi/K^\phi| = q_i \) and \( (N \cap T)^\phi \) is permutable in \( \overline{G} \),

(d) \( H/K = \frac{S_1}{K} \times \cdots \times \frac{S_r}{K} \times \frac{H \cap T}{K}, \ (H \cap T)/K \) and \( (H \cap T)^\phi/K^\phi \) are hypercentrally embedded in \( G \) and \( \overline{G} \), respectively.

Proof. We have just shown that \( H \) and \( K \) are normal subgroups of \( G \). Therefore to prove that \( G/K \) and \( \overline{G}/K \) have the required structure, we may assume that \( K = 1 \). If \( \overline{N} \not\leq \overline{G} \), then all assertions hold trivially for \( H = N = K \) and \( r = 0 \). So assume that \( \overline{N} \) is not normal in \( \overline{G} \). Then by 5.1.14, \( \overline{G} = S_1^\phi \times \cdots \times S_r^\phi \times \overline{T} \) where (a) is satisfied, \( |\overline{N} \cap S_i^\phi| = q_i \) and \( \overline{N} \cap \overline{T} \) is permutable in \( \overline{G} \). By 1.6.6 and 2.2.5, \( G = S_1 \times \cdots \times S_r \times T \) and (b) holds. Furthermore \( |N \cap S_i| = p_i \) since \( N \cap S_i \leq S_i \); thus (c) is also satisfied. Since \( H = S_1^\phi \times \cdots \times S_r^\phi \times (H \cap T) \), \( H \) has the structure required in (d). Finally, \( N \cap T \leq G \) and \( (N \cap T)^\phi \) is permutable in \( \overline{G} \); therefore (b) of 5.4.6 yields that \( H \cap T \) and \( (H \cap T)^\phi \) are hypercentrally embedded in \( G \) and \( \overline{G} \), respectively. \( \square \)

Since all the \( S_i/K, S_i^\phi/K^\phi, (H \cap T)/K \) and \( (H \cap T)^\phi/K^\phi \) in Theorem 5.4.7 are hypercyclically embedded in \( G \) or \( \overline{G} \), (c) of 5.2.1 shows that the same is true for \( H/K \) and \( H^\phi/K^\phi \). Thus we get the following result.

5.4.8 Corollary. Under the assumptions of Theorem 5.4.7, \( H/K \) and \( H^\phi/K^\phi \) are hypercyclically embedded in \( G \) and \( \overline{G} \), respectively.

Furthermore, 5.4.7 and 5.4.8 yield some useful criteria for a projective image of a normal subgroup to be normal in the image group. We collect these in the following theorem. Parts (a) and (b) of it are due to Schmidt who improved similar criteria with “cyclic” replaced by “abelian”; these, as part (c) of the theorem, had been proved by Suzuki using his results on singular projectivities.

5.4.9 Theorem (Suzuki [1951a], Schmidt [1972b]). Let \( N \) be a normal subgroup of the finite group \( G \) and suppose that one of the following is satisfied:

(a) \( G/N \) has no nontrivial cyclic normal subgroup.

(b) There is no normal subgroup \( M \) of \( G \) such that \( M < N \) and \( N/M \) is cyclic.

(c) \( G/N \) is perfect.

Then \( N^\phi \leq \overline{G} \) for every projectivity \( \phi \) from \( G \) to a group \( \overline{G} \).
Proof. By 5.4.8, \( N^G / N \) and hence also \( N^G / N \) are hypercyclically embedded in \( G \). Therefore (a) implies that \( N^G = N \) and (b) yields \( N^G = N \); in both cases, \( \bar{N} \leq \bar{G} \). Finally, if (c) is satisfied and \( R = G_{\infty} \) is the soluble residual of \( G \), then \( G = NR \) since \( G / N \) is perfect. Furthermore, by 5.3.6, \( R \) is the soluble residual of \( G \). By 5.2.5, \( G / C_G(N^G / N^G) \) is supersoluble and hence \( R \) is contained in this centralizer. In particular, \( \bar{N} \) is normalized by \( \bar{R} \) and, since \( \bar{G} = \bar{N} \cup \bar{R} \), it follows that \( \bar{N} \leq \bar{G} \).

Iterated nilpotent residuals

As a first application of our results we prove the theorem on the iterated nilpotent residuals announced in \( \S \) 4.3. Let us write \( G_{\infty} \) for the smallest normal subgroup with nilpotent factor group in the finite group \( G \) and define inductively

\[
N_0(G) = G \quad \text{and} \quad N_k(G) = N_{k-1}(G)_{\infty} \quad \text{for } k \in \mathbb{N}.
\]

Then \( N_k(G) \) is the smallest normal subgroup of \( G \) with factor group soluble of nilpotent length at most \( k \).

5.4.10 Theorem. If \( \phi \) is a projectivity from the finite group \( G \) to the group \( \bar{G} \), then \( N_k(G)^{\phi} = N_k(\bar{G}) \) for all \( k \geq 2 \).

Proof. Let \( N = N_k(G) \) and \( K = N_{\infty} \). By 5.4.7, \( G / K = S_1 / K \times \cdots \times S_r / K \times T / K \) where the \( S_i / K \) are \( P \)-groups and \( N \cap T / K \) is hypercentrally embedded in \( G \). Now \( T / N \cap T \simeq NT / N \) is soluble of nilpotent length at most \( k \). If \( F / N \cap T \) is the Fitting subgroup of \( T / N \cap T \), then \( F / N \cap T \) is nilpotent and \( N \cap T / K \) is hypercentrally embedded in \( F \); by 5.2.1, \( F / K \) is nilpotent. It follows that \( T / K \) is soluble of nilpotent length at most \( k \). Since \( k \geq 2 \), the same holds for all the \( S_i / K \) and hence also for \( G / K \).

The definition of \( N = N_k(G) \) implies that \( N \leq K \) and therefore \( N = K \). This shows that \( \bar{N} \leq \bar{G} \) and \( \phi \) induces a projectivity from \( G / N \) to \( \bar{G} / \bar{N} \). By 4.3.3, \( \bar{G} / \bar{N} \) is soluble of nilpotent length at most \( k \). It follows that \( N_k(\bar{G}) \leq \bar{N} = N_k(G)^{\phi} \), and this result for \( \phi^{-1} \) yields the other inclusion.

Projective images of subnormal subgroups

In the remainder of this section we show that subnormal subgroups of finite groups are mapped by projectivities onto subnormal subgroups, with the obvious exception of \( P \)-groups. Since it is immediate that index preserving projectivities behave well with respect to subnormal subgroups, we use the results of Chapter 4 on singular projectivities and not the methods developed in this section. In this way we also obtain another approach to our results on projective images of normal subgroups.

5.4.11 Lemma. Let \( \phi \) be an index preserving projectivity from the finite group \( G \) to the group \( \bar{G} \).
5.4 Projective images of normal subgroups of finite groups

(a) If \( N \trianglelefteq G \), then \( N^\phi \) is permutable in \( \bar{G} \).
(b) If \( N \trianglelefteq \trianglelefteq G \), then \( N^\phi \trianglelefteq \trianglelefteq \bar{G} \).

Proof. (a) For every \( H \leq G \), \( |H \cup N : N| = |H : H \cap N| \). Since \( \phi \) is index preserving, it follows that \( |\bar{H} \cup \bar{N} : \bar{N}| = |\bar{H} : \bar{H} \cap \bar{N}| \) and, by (7) of § 5.1, \( \bar{H} \bar{N} = \bar{N} \bar{H} \). Thus \( \bar{N} \) is permutable in \( \bar{G} \). (Of course, the assertion also follows from Theorem 5.4.7.)

(b) We use induction on \( |G : N| \). For \( N = G \) there is nothing to prove, so suppose that \( N \neq G \). Then there exists a normal subgroup \( M \) of \( G \) such that \( N \trianglelefteq M < G \). By (a), \( \bar{M} \) is permutable in \( \bar{G} \) and hence, by 5.1.1, \( \bar{M} \trianglelefteq \trianglelefteq \bar{G} \). (In fact, Exercise 4.3.5 shows that \( \bar{M} \trianglelefteq \bar{G} \) if \( M \) is a maximal normal subgroup of \( G \).) Since \( N \trianglelefteq \trianglelefteq M \), the induction assumption yields that \( \bar{N} \trianglelefteq \trianglelefteq \bar{M} \) and it follows that \( \bar{N} \trianglelefteq \trianglelefteq \bar{G} \). \( \square \)

5.4.12 Theorem (Schmidt [1975a]). Let \( N \) be a subnormal subgroup of the finite group \( G \), \( \phi \) a projectivity from \( G \) to a group \( \bar{G} \) and \( K \) the largest normal subgroup of \( G \) contained in \( N \) such that \( K^\phi \trianglelefteq \bar{G} \). Then there exist primes \( p_i, q_i \) and \( n_i \in \mathbb{N} \) such that

\[ G/K = S_1/K \times \cdots \times S_r/K \times T/K \quad \text{and} \quad \bar{G}/K^\phi = S_1^\phi/K^\phi \times \cdots \times S_r^\phi/K^\phi \times T^\phi/K^\phi \]

where \( 0 \leq r \in \mathbb{Z} \) and for all \( i, j \in \{1, \ldots, r\} \),

(a) \( S_i^\phi/K^\phi \) is a P-group of order \( p_i^{\alpha_i} \), \( p_i > q_i \) and \( (|S_i^\phi/K^\phi|, |S_j^\phi/K^\phi|) = 1 = (|S_i^\phi/K^\phi|, |T^\phi/K^\phi|) \) for \( i \neq j \),
(b) \( S_i/K \in P(n_i + 1, p_i) \) and \( (|S_i/K|, |S_j/K|) = 1 = (|S_i/K|, |T/K|) \) for \( i \neq j \),
(c) \( |N/K| = (N \cap S_1)/K \times \cdots \times (N \cap S_r)/K \times (N \cap T)/K \) and \( |N \cap S_i|/K^\phi = q_i \), and
(d) \( (N \cap T)^\phi \trianglelefteq \trianglelefteq \bar{G} \).

Proof. Let \( G \) be a minimal counterexample to the theorem. Then \( G/K \) is also a counterexample and hence

(1) \( K = 1 \).

If \( \bar{N} \trianglelefteq \trianglelefteq \bar{G} \), then all assertions would hold trivially for \( r = 0 \) and \( T = G \). Thus

(2) \( \bar{N} \) is not subnormal in \( \bar{G} \).

If \( G = A \times B \) where \( (|A|, |B|) = 1 \) and \( A \neq 1 \neq B \), then \( N = (N \cap A) \times (N \cap B) \), \( N \cap A \trianglelefteq \trianglelefteq A \) and \( N \cap B \trianglelefteq \trianglelefteq B \). The minimality of \( G \) would imply that \( A \) and \( B \) would have the right structure and so would \( G \), a contradiction. Hence if \( (A, B) \) were a P-decomposition of \( G \), then \( B = 1 \) and \( G \) would be a P-group in \( P(n, p) \), say. As a subnormal subgroup of this P-group, \( N \) would have order \( p^k \) for some \( k \in \mathbb{N} \) and, since \( \bar{N} \) is not subnormal in \( \bar{G} \), \( |\bar{N}| = p^{k-1}q \) for \( p > q \in \mathbb{P} \). But \( K = 1 \) would imply \( k = 1 \), that is, \( |N| = p \) and \( |\bar{N}| = q \), and the assertions of the theorem would hold for \( S_1 = G \) and \( T = 1 \). This would contradict the choice of \( G \). Thus

(3) \( G \) is not P-decomposable.

Since \( \bar{N} \) is not subnormal in \( \bar{G} \), 5.4.11 shows that \( \phi \) is not index preserving. Let \( \pi \) be the set of primes \( p \) for which \( \phi \) is singular at \( p \). Since \( G \) is not P-decomposable, (b) of Theorem 4.2.6 holds for all these primes. In particular, for every \( p \in \pi \),
(4) $G$ has a normal $p$-complement $C_p$ such that $C_p \trianglelefteq G$.

Let $D = \bigcap_{p \in \pi} C_p$. By 4.2.1, $\varphi$ induces an index preserving projectivity from $D$ to $\overline{D}$.

Hence if $N \leq D$, then by 5.4.11, $\overline{N} \trianglelefteq \overline{D}$; therefore $\overline{N} \trianglelefteq \overline{G}$ since $\overline{D} \leq \overline{G}$. This would contradict (2); thus $N \not\leq D$ and

(5) there exists a prime $p \in \pi$ dividing $|N|$.

Let $C = C_p$. Then the Sylow $p$-subgroups of $G$ are just the complements to $C$ in $G$.

Since $\overline{C} \trianglelefteq \overline{G}$, the inner automorphisms of $\overline{G}$ permute the images of the Sylow $p$-subgroups of $G$. Therefore if $V = \langle P | P \in Syl_p(G) \rangle$ and $W = \langle \Omega(P) | P \in Syl_p(G) \rangle$, then

(6) $V \trianglelefteq G$, $W \trianglelefteq G$, $\overline{V} \trianglelefteq \overline{G}$ and $\overline{W} \trianglelefteq \overline{G}$.

If $P \in Syl_p(G)$, then $N \cap P \in Syl_p(N)$ since $N \trianglelefteq \trianglelefteq G$. By (5), $N \cap P \neq 1$. Therefore if the Sylow $p$-subgroups of $G$ were cyclic, it would follow that $\Omega(P) \leq N$ for every $P \in Syl_p(G)$ and hence $W \leq N$. But then (6) would contradict (1). Thus the Sylow $p$-subgroups of $G$ are not cyclic and therefore are elementary abelian since $\varphi$ is singular at $p$. Let $P_1 \in Syl_p(G)$ such that $|P_1^p| \neq |P_1|$ and let $P_0^p$ be the Sylow $p$-subgroup of the $P$-group $P_1^p$. By 4.2.10, $P_0 \leq Z(G)$ and every subgroup of $P_0^p$ is normal in $\overline{G}$; again (1) implies that $N \cap P_0 = 1$. But if $P$ is an arbitrary Sylow $p$-subgroup of $G$, $P_0 \leq P$ of index $p$ and $N \cap P \neq 1$. It follows that $P = P_0(N \cap P) \leq P_0 N$ and this shows that

(7) $V \leq P_0 N$.

Now $P_0 N \cap C$ is the normal $p$-complement in $P_0 N$. Since $P_0 \leq Z(G)$, $N$ is a normal subgroup of $P_0 N$ and therefore contains this normal $p$-complement; in particular, $V \cap C \leq N$. By (4) and (6), $V \cap C \trianglelefteq G$ and $(V \cap C)^p = V^p \cap C^p \trianglelefteq \overline{G}$. Thus by (1), $V \cap C = 1$ and $VC = G$ since $P_1^p \leq V$ and $P_1 C = G$. It follows that $G = V \times C$ and $V = P_1$ is a $P$-group, contradicting (3). \hfill $\Box$

5.4.13 Remark. In 5.4.12, if $N$ is not only subnormal but normal in $G$, then $N \cap T \trianglelefteq G$; hence $(N \cap T)^p$ is subnormal and modular in $\overline{G}$, that is, by 5.1.1, $(N \cap T)^p$ per $\overline{G}$. Thus Theorem 5.4.12, like 5.1.14 for modular subgroups, reduces the study of projective images of normal subgroups of finite groups to the case of permutable subgroups. In particular, via 5.4.12 we can obtain a second proof of the main theorem of this section which does not use Theorem 5.1.14 on modular subgroups. For the first basic step in our discussion was Theorem 5.4.4 on minimal normal subgroups. In the proof of this we need, apart from 5.4.12, just 5.1.1, 5.2.9 and the Maier-Schmid Theorem 5.2.3. The proof of the latter theorem uses 5.1.5(a) and 5.1.10, which are independent of the results on modular subgroups, and 5.1.7. However, it is easy to show directly that $M/M_G$ is nilpotent whenever $M$ is a permutable subgroup of $G$. The proof of 5.4.6 remains unchanged (it uses 5.4.4, 5.4.3 and 5.2.3) and 5.4.6 (a) yields that for $N \trianglelefteq G$, the subgroup $K$ defined in 5.4.12 is just $N_G$. Then 5.4.7 follows from 5.4.12 and 5.4.6 (b). \hfill $\Box$

If $r > 0$ in 5.4.12, that is, if there is a $P$-group $S_1/K$, then neither $G$ nor $N$ is perfect; therefore we get the following corollary.
5.5 Normal subgroups of $p$-groups with cyclic factor group

5.4.14 Corollary. Let $\varphi$ be a projectivity from the finite group $G$ to the group $\bar{G}$ and let $N \trianglelefteq G$. If $G$ or $N$ is perfect, then $N^\varphi \trianglelefteq \bar{G}$.

Incidentally the first assertion in 5.4.14 also follows immediately from 5.4.11 and the fact that projectivities of perfect groups are index preserving; the second assertion follows by induction from 5.4.9(b) (observe that if $N$ is a perfect subgroup of $G$, then $N^G$ is perfect).

**Exercises**

In Exercises 1, 3–5, and 8, $\varphi$ is a projectivity from the finite group $G$ to a group $\bar{G}$.

1. (Schmidt [1975a]) If $G$ is a $p$-group, show that $\Omega(Z(G))^\varphi \trianglelefteq \bar{G}$. (The assertion holds more generally; see Zacher [1982a].)

2. (Schmidt [1975a]) Let $G = \langle x, y, z | x^p = y^p = z^p = 1, [x, y] = z^p, [x, z] = [y, z] = 1 \rangle$ and $\bar{G} = \langle \bar{x}, \bar{y}, \bar{z} | \bar{x}^{p^r} = \bar{y}^{p^r} = \bar{z}^{p^r} = 1, [\bar{x}, \bar{y}] = \bar{z}^p, [\bar{x}, \bar{z}] = \bar{x}^p, [\bar{y}, \bar{z}] = \bar{y}^p \rangle$ where $p > 5$ is a prime. Show that there exists a projectivity $\varphi$ from $G$ to $\bar{G}$ such that $Z(G)^\varphi = \langle z \rangle^\varphi = \langle \bar{z} \rangle$ is not normal in $\bar{G}$.

3. Show that $Z_{x,\varphi}(G)^\varphi \trianglelefteq \bar{G}$. (Hint: $Z_{x,\varphi}(G)$ is the largest hypercentrally embedded normal subgroup of $G$.)

4. If there exists no minimal normal subgroup $N$ of $G$ such that $N^\varphi$ is a minimal normal subgroup of $\bar{G}$, show that $G = S_1 \times \cdots \times S_s$ with nonabelian coprime $p$-groups $S_i$ of order $|S_i| = p_i q_i$ where $p_i, q_i \in \mathbb{P}$. Conversely, if $G$ is such a direct product, show that there exists an autoprojectivity of $G$ mapping every minimal normal subgroup of $G$ to a nonnormal subgroup.

5. For $N \trianglelefteq G$, let $S_G(N)$ be the largest and $T_G(N)$ the smallest normal subgroup of $G$ such that $S_G(N)/N$ and $N/T_G(N)$ are hypercyclically embedded in $G$. Show that $S_G(N)^\varphi$ and $T_G(N)^\varphi$ are normal subgroups of $\bar{G}$ and that $S_G(N)^\varphi/T_G(N)^\varphi$ is hypercyclically embedded in $\bar{G}$.

6. (Ito and Szép [1962]) If $M$ is a permutable subgroup of the finite group $G$, show directly (not using the results of §5.1) that $M/M_G$ is nilpotent.

7. Use 5.4.12, 5.1.1, 5.2.3 and 5.2.9 to prove Theorem 5.4.4.

8. Show that the following properties of $\varphi$ are equivalent.
   (a) $N^\varphi \trianglelefteq \bar{G}$ for every normal subgroup $N$ of prime index in $G$.
   (b) $N^\varphi \trianglelefteq \bar{G}$ for every normal subgroup $N$ of $G$.
   (c) $N^\varphi \trianglelefteq \bar{G}$ for every subnormal subgroup $N$ of $G$.

5.5 Normal subgroups of $p$-groups with cyclic factor group

We continue with the study of the structure of $N^\bar{G}/N_{\bar{G}}$ and $\bar{N}^\bar{G}/\bar{N}_{\bar{G}}$ for a normal subgroup $N$ of a finite group $G$. The main result of the last section, Theorem 5.4.7, reduces this to the case where $\bar{N}$ is permutable in $\bar{G}$ and $\bar{N}_{\bar{G}} = 1$. Then 5.1.6 and 5.1.3, or the corresponding results for permutable subgroups (which are much easier to
prove), reduce the investigation of $N/N_G$ and $\overline{N}/\overline{N}_G$ further to the situation where $G$ is a $p$-group, $G/N$ is cyclic and $N_G = 1$. Moreover the results of § 6.5 will do the same for normal subgroups in arbitrary groups. Therefore we shall now study this situation aiming to show that $N$ is abelian and $G$ and $\overline{G}$ are metabelian if $p > 2$; if $p = 2$, we shall show that $N$ has modular subgroup lattice, $|N'| \leq 2$, $G$ is metabelian and $\overline{G}$ is soluble of derived length at most 3. The results on $N/N_G$ and $\overline{N}/\overline{N}_G$ will be generalized to arbitrary groups in 6.6.1.

**Basic properties of $G$ and $\overline{G}$**

We continue to use the notation introduced in 5.4.1, and throughout this section we assume the following.

5.5.1 Hypothesis. Let $p$ be a prime, $G$ a finite $p$-group, $\varphi$ a projectivity from $G$ to the $p$-group $\overline{G}$, and $N$ a normal subgroup of $G$ such that $G\cap N$ is cyclic and $N_G = 1$; write $\text{Exp}_N = p^r$ and $|\Omega(N)| = p^m$.

Let $a \in G$ be such that $G = N\langle a \rangle$. Then $\langle a \rangle^G = \langle b \rangle$, say, $\overline{N}$ is a core-free permutable subgroup of $\overline{G}$ and $\overline{G} = \overline{N}\langle b \rangle$. Therefore the assumptions of Theorem 5.2.8 are satisfied by $\overline{N}$ and we first of all note the consequences of this theorem for our situation. By (a) and (b) of 5.2.8, we have:

1. Every $b$-invariant subgroup of $\overline{N}$ is trivial; in particular $\overline{N} \cap \langle b \rangle = 1$ and hence also $N \cap \langle a \rangle = 1$.

This immediately implies:

2. If $H$ is an $a$-invariant subgroup of $N$, then $G^* = H\langle a \rangle$, $N^* = H$, and the projectivity induced by $\varphi$ in $G^*$ satisfy Hypothesis 5.5.1.

By (d) of 5.2.8,

3. $\Omega_k(\overline{G})/\Omega_k(\overline{G})$ is core-free in $\overline{G}/\Omega_k(\overline{G})$ for every $k \geq 0$. Therefore $\varphi$ induces projectivities $\varphi_k$ from $G/\Omega_k(G)$ to $\overline{G}/\Omega_k(\overline{G})$ for which the images of $N\Omega_k(G)/\Omega_k(G)$ are core-free; thus $G/\Omega_k(G)$, $N\Omega_k(G)/\Omega_k(\overline{G})$ and $\varphi_k$ satisfy Hypothesis 5.5.1.

4. $\Omega(G)$ and $\Omega(\overline{G})$ are elementary abelian. For $k = 1, \ldots, r$, $\Omega_k(G) = \Omega_k(N)\Omega_k(\langle a \rangle)$ and $\Omega_k(\overline{G}) = \Omega_k(\overline{N})\Omega_k(\langle b \rangle)$ have exponent $p^k$; furthermore, $\Omega_k(N) = \Omega_k(\overline{G}) \cap N$.

**Proof.** The statements about $\overline{G}$ follow directly from 5.2.8(c) and (d). Thus $\Omega(G)$ is elementary abelian and, since the exponent of a subgroup is invariant under $\varphi$ and $\Omega_k(N) \leq G$, we observe that $\Omega_k(G) = \Omega_k(N)\Omega_k(\langle a \rangle)$ has exponent $p^k$. Finally, by Dedekind's law, $\Omega_k(N) \cap N = \Omega_k(N)(\Omega_k(\langle a \rangle) \cap N) = \Omega_k(N)$.

5. If $p = 2$, then $\Omega_k(G)/\Omega_k-2(G)$, $\Omega_k(\overline{G})/\Omega_k-2(\overline{G})$, $\Omega_k(N)/\Omega_k-2(N)$ and $\Omega_k(\overline{N})/\Omega_k-2(\overline{N})$ are abelian for $k \geq 2$; furthermore, $|G : \Omega_4(G)| \geq 4$ if $N \neq 1$.

**Proof.** By (f) of 5.2.8, $\Omega_4(\overline{G})/\Omega_4-2(\overline{G})$ is abelian. As a projective image of this group, $\Omega_k(G)/\Omega_k-2(G)$ is an $M$-group of exponent at most 4 in which the quaternion
5.5 Normal subgroups of $p$-groups with cyclic factor group

$Q_8$ is not involved; by 2.3.7, $\Omega_k(G)/\Omega_{k-2}(G)$ is abelian. By (4), $\Omega_{k-2}(N) = \Omega_{k-2}(G) \cap N = \Omega_{k-2}(G) \cap \Omega_k(N)$ and hence $\Omega_k(N)/\Omega_{k-2}(N)$ is isomorphic to the subgroup $\Omega_k(N)/\Omega_{k-2}(G)/\Omega_{k-2}(G)$ of the abelian group $\Omega_k(G)/\Omega_{k-2}(G)$. Thus $\Omega_k(N)/\Omega_{k-2}(N)$ is abelian, and in the same way one shows that $\Omega_k(N)/\Omega_{k-2}(N)$ is abelian. Finally, by (g) of 5.2.8, $\overline{N} \leq \Omega_{n-2}(G)$ if $2^n = \text{Exp } G$ and $\overline{N} \neq 1$. It follows that $r \leq n - 2$ and hence $|G: \Omega_r(G)| \geq 4$.

In particular, $\Omega_2(G)$ and $\Omega_2(\overline{G})$ are abelian for $p = 2$ and hence the quaternion group $Q_8$ is not a subgroup of $G$ or $\overline{G}$. Therefore if $H$ is a subgroup of $G$ or $\overline{G}$ with modular subgroup lattice, then by 2.3.8, $Q_8$ is not involved in $H$ and so $H$ is an $M^*$-group. Thus we have shown:

(6) Every subgroup of $G$ or $\overline{G}$ having modular subgroup lattice is an $M^*$-group.

As for $M^*$-groups, the commutativity of $\Omega_2(G)$ and $\Omega_2(\overline{G})$ for $p = 2$ implies:

(7) If $p = 2$ and $k \in \mathbb{N}$, the maps $x \rightarrow x^{2^k}$ are endomorphisms of $\Omega_{k+1}(G)$ and $\Omega_{k+1}(\overline{G})$. Hence if $x, y \in G$ such that $1 \neq x^{2^k} = y^{2^k} \in \Omega(G)$, then $x \equiv y \pmod{\Omega_k(G)}$; if in addition $x, y \in N$, then $x \equiv y \pmod{\Omega_k(N)}$. If $X, Y \leq G$ such that $X \cap Y = 1$ and $XY = YX$, then $\Omega_k(XY) = \Omega_k(X)\Omega_k(Y)$.

Proof. We use induction on $|G|$ to prove the first assertion. For $k = 1$, it is trivial since $\Omega_2(G)$ and $\Omega_2(\overline{G})$ are abelian; so suppose that $k \geq 2$. Since $G/\Omega(G)$ satisfies Hypothesis 5.5.1, we may apply the induction assumption to $\Omega_k(G)/\Omega_2(G) = \Omega_k(G)/\Omega_2(G)$ and deduce that for $x, y \in \Omega_{k+1}(G)$ there exists $z \in \Omega(G)$ such that $(xy)^{2^{-k}} = x^{2^{-k}}y^{2^{-k}}z$. Now $x^{2^{-k}}, y^{2^{-k}}$ and $z$ are contained in the abelian group $\Omega_2(G)$ and hence

$$(xy)^{2^k} = (x^{2^{-k}}y^{2^{-k}}z)^{2^k} = x^{2^k}y^{2^k},$$

as desired. The proof for $\Omega_{k+1}(\overline{G})$ is similar. Now if $x, y \in G$ such that $1 \neq x^{2^k} = y^{2^k} \in \Omega(G)$, then $x, y \in \Omega_{k+1}(G)$ and have the same image under the endomorphism $\nu: g \rightarrow g^{2^k}$ of $\Omega_{k+1}(G)$. Therefore $x^{-1}y \in \text{Ker } \nu = \Omega_k(G)$. If in addition $x, y \in N$, then $x^{-1}y \in \Omega_k(G) \cap N = \Omega_k(N)$, by (4). Finally, for $g \in XY$ there exist $x \in X$ and $y \in Y$ such that $g = xy$. If $o(x) = 2^i$, $o(y) = 2^j$, $o(g) = 2^k$ and $h = \max\{i, j, k\}$, then $g^{2^{i-1}} = x^{2^{i-1}}y^{2^{j-1}} \neq 1$ since $\langle x \rangle \cap \langle y \rangle = 1$. This shows that $h = k$ and that $\Omega_k(XY) = \{z \in XY | z^{2^k} = 1\} \subseteq \Omega_k(X)\Omega_k(Y)$. The other inclusion is trivial.

We return to the general situation with arbitrary prime $p$ and assume in addition that $N \neq 1$; for, if $N = 1$, then $G$ and $\overline{G}$ are cyclic $p$-groups and all the assertions we want to prove hold trivially.

(8) Let $\tau$ be an autoprojectivity of $G$ and $T = N \cap N^\tau$. Then $T \leq N^\tau$ with cyclic factor group $N^\tau/T$ and $T$ is permutable in $N$ with $[N/T]$ a chain.

Proof. Clearly, $N \leq G$ and $G/N$ cyclic imply that $T = N \cap N^\tau \leq N^\tau$ with cyclic factor group $N^\tau/T$. Since $N^\tau$ is a projective image of $N$, it is permutable in $G$ and $[G/N^\tau]$ is a chain. It follows from (11) and (1) of §5.1 that $T = N \cap N^\tau$ is permutable in $N$ and $[N/T] \simeq [NN^\tau/N^\tau]$ is a chain.
Since we shall study numerous autoprojectivities $\tau$ of $G$, we shall frequently use the following argument.

(9) Let $H$ be a $p$-group of exponent $p^n$ and $M$ a permutable subgroup of $H$ such that $[H/M]$ is a chain. Then $H = M\langle x \rangle$ for any element $x \in H$ that does not lie in the maximal subgroup of $H$ containing $M$ and hence $|H:M| = |\langle x \rangle : \langle x \rangle \cap M| \leq p^n$. If $z \in H$ such that $o(z) = p^n$ and $M \cap \langle z \rangle = 1$, then $|M\langle z \rangle : M| = |\langle z \rangle| = p^n$ and hence $H = M\langle z \rangle$.

(10) $|C_{Q(N)}(a)| = p$; thus $C_N(a)$ is cyclic.

Proof. Let $H = C_{Q(N)}(a)$. Since $\Omega(N)$ is elementary abelian, $H\langle a \rangle$ is abelian. By (6), $(H\langle a \rangle)^p = \overline{H} \cup \langle b \rangle$ is an $M^*$-group and hence, by Iwasawa's theorem, contains an abelian normal subgroup $A$ with cyclic factor group inducing power automorphisms in $A$. Then $\overline{H} \cap A$ is a $b$-invariant subgroup of $\overline{N}$, hence is trivial by (1) and therefore $\overline{H} \cong \overline{H}/A$ is cyclic. It follows that $H$ is cyclic and elementary abelian, hence $|H| \leq p$; on the other hand, $N \leq G$ implies that $\Omega(N) \cap Z(G) \neq 1$ and hence $|H| = p$. Thus $C_N(a)$ is a $p$-group with only one minimal subgroup and therefore is cyclic since, by (6), $Q_8$ is not a subgroup of $G$.

(11) There exist bases $\{e_0, e_1, \ldots, e_m\}$ of $\Omega(G)$ and $\{f_0, f_1, \ldots, f_m\}$ of $\Omega(G)$ with the following properties:

11(a) $\langle e_0 \rangle = \Omega(\langle a \rangle) \leq Z(G)$, $\langle f_0 \rangle = \Omega(\langle b \rangle) \leq Z(G)$;

11(b) $\Omega(N) = \langle e_1 \rangle \times \cdots \times \langle e_m \rangle$;

11(c) $\langle e_1, \ldots, e_i \rangle$ is the unique $a$-invariant subgroup of order $p^i$ of $\Omega(N)$ ($i = 1, \ldots, m$); in particular,

11(d) $e_i \in H$ for every $a$-invariant subgroup $H$ of $G$ such that $H \cap N \neq 1$;

11(e) $\langle e_i \rangle = Z(G) \cap \Omega(N)$ and $e_i^p = e_i e_{i-1}$ for $i = 2, \ldots, m$;

11(f) $\langle f_i \rangle = \langle e_i \rangle^p$ for $i = 0, \ldots, m$;

11(g) $f_i^p = f_i f_0$ and $\langle f_i f_0 \rangle = \langle e_i e_0 \rangle^p$;

11(h) $\langle f_0, \ldots, f_i \rangle$ is the unique $b$-invariant subgroup of order $p^{i+1}$ of $\Omega(G)$ ($i = 0, \ldots, m$).

Proof. For every $a$-invariant subgroup $L$ of $\Omega(N)$, the map $\tau_L: x \to [x, a]$ ($x \in L$) is an endomorphism of $L$ with kernel $C_L(a)$ and image $[L, a]$; for (1) of § 1.5 shows that for $x, y \in L$, $[xy, a] = [x, a][y, a] = [x, a][y, a]$ since $L$ is abelian. Now let $1 = L_0 < L_1 < \cdots < L_m = \Omega(N)$ be part of a chief series of the group $\Omega(N)\langle a \rangle$ and let $\tau_{L_i} = \tau_{L_{i-1}}$ for $i = 1, \ldots, m$. Then $L_i/L_{i-1}$ is centralized by $a$ and hence $L_i^a = [L_i, a] \leq L_{i-1}$; on the other hand, by (10), $|\ker \tau_i| \leq p$ and the homomorphism theorem yields that $L_i^a = [L_i, a]$. In particular, $L_{m-1} = [\Omega(N), a]$ is uniquely determined by $a$ and, similarly, $L_i = [\Omega(N), a, \ldots, a]$ where $a$ is written $m - i$ times. Since the chief series was chosen arbitrarily, it follows that $L_i$ is the unique $a$-invariant subgroup of order $p^i$ of $\Omega(N)$. In particular, $L_1 = C_{Q(N)}(a) = Z(G) \cap \Omega(N)$; let $L_1 = \langle e_1 \rangle$. For
5.5 Normal subgroups of $p$-groups with cyclic factor group

$i = 2, \ldots, m$, we define inductively elements $e_i \in \Omega(N)$ such that $e_i^a = e_i e_i^{-1}$ and $\langle e_1, \ldots, e_i \rangle = L_i$; if $e_1, \ldots, e_i$ are defined, then since $L_i = L_i^a$ there exists $e_i \in L_i$ such that $e_i^{-1} = [e_i, a]$ and hence $e_i^a = e_i e_i^{-1}$; as $[L_i, a] = L_{i-2}, e_i \notin L_{i-1}$ and hence $L_i = \langle e_1, \ldots, e_i \rangle$. For $i = m$, we get $\Omega(N) = \langle e_1, \ldots, e_m \rangle = \langle e_i \rangle \times \cdots \times \langle e_m \rangle$ and hence (11b), (11c) and (11e) are satisfied. Furthermore, if $H \leq G$ is such that $H^p = H$ and $H \cap N \neq 1$, then $H \cap \Omega(N)$ is a nontrivial $a$-invariant subgroup of $\Omega(N)$, and so, by (11c), it contains $e_i$; thus (11d) holds. Now let $f_i$ be any generator of $\langle e_i \rangle^a$ for $i = 1, \ldots, m$. Since $e_i \in Z(G)$, it is clear that $\langle e_i, a \rangle = \langle e_i \rangle \times \langle a \rangle$ and hence $\langle e_i, \Omega(\langle a \rangle) \rangle = \Omega(\langle e_i, a \rangle)$. Thus $\langle e_1, \Omega(\langle a \rangle) \rangle^a = \langle f_1, \Omega(\langle b \rangle) \rangle$ is invariant under $b$. Furthermore, $\langle b \rangle$ is invariant under $f_1$ and $\langle f_1 \rangle^b \neq \langle f_1 \rangle$ by (1). It follows that $\langle f_1 b \rangle \in \langle f_1, \Omega(\langle b \rangle) \rangle \cap \langle b \rangle = \Omega(\langle b \rangle)$. So if we choose $f_0 = [f_1, b]$, then $f_i^b = f_i f_0$ and $f_0 = \Omega(\langle b \rangle) \leq Z(\tilde{G})$; and for a suitable generator $e_0$ of $\Omega(\langle a \rangle)$, we can write $\langle f_1 f_0 \rangle^a = \langle e_1 e_0 \rangle$. Thus (11f) and (11g) are satisfied. By (1), $\langle f_0 \rangle$ is the only minimal normal subgroup of $\tilde{G}$ and hence 5.4.2 shows that $\langle e_0 \rangle = \langle f_0 \rangle^a$ is a normal subgroup of $G$. Therefore (11a) also holds and, by (4), $\langle e_0, \ldots, e_m \rangle$ and $\langle f_0, \ldots, f_m \rangle$ are bases of $\Omega(G)$ and $\Omega(\tilde{G})$, respectively. Finally, by (11c), $\langle e_0, \ldots, e_i \rangle = \langle e_0, a, e_1, \ldots, e_i \rangle$ and hence $\langle f_0, \ldots, f_i \rangle$ is invariant under $b$ for $i = 0, \ldots, m$. Since $\Omega(\tilde{G})$ is abelian, for every $b$-invariant subgroup $L$ of $\Omega(\tilde{G})$ containing $f_0$, the map $\tau: x \to [x, b]$ ($x \in L$) is an endomorphism with kernel $C_L(b) = \langle f_0 \rangle$, by (1). Therefore $[\tilde{L} : [\tilde{L}, b]] = [L : L^b] = [\ker \tau] = p$ and hence $[\tilde{L}, b]$ is the only $b$-invariant maximal subgroup of $\tilde{L}$. Now starting with $\tilde{L} = \Omega(\tilde{G})$, a trivial induction yields (11h).

(12) If $p > 2$ and $N' \leq \langle e_1 \rangle$, then $(xy)^p = x^p y^p$ for all $x, y \in N$ and $k \in \mathbb{N}$.

Proof. By (11e), $\langle e_1 \rangle \leq Z(G)$ and hence (4) of § 1.5 shows that $(xy)^p = x^p y^p [y, x]^t$ where $t = \left( \frac{p^k}{2} \right) \equiv 0 \pmod{p}$. Since $|N'| \leq p$, it follows that $[y, x]^t = 1$.

(13) If $p = 2$ and $m \geq 2$, the bases $\{e_0, \ldots, e_m\}$ and $\{f_0, \ldots, f_m\}$ can be chosen with the additional property that $f_2 = f_2 f_1$.

Proof. By (11h), $[\langle f_0, f_1, f_2 \rangle, b] = \langle f_0, f_1 \rangle$ and $[\langle f_0, f_1 \rangle, b] = \langle f_0 \rangle$ so that $[f_2, b] \in \langle f_0, f_1 \rangle \setminus \langle f_0 \rangle$. Thus $[f_2, b] = f_1 f_0^a$ where $a \in \{0, 1\}$. If $a = 0$, we are done; so suppose that $a = 1$. If we then put $e_i^* = e_i$ for $i \in \{0, 1\}$, $e_i^* = e_i e_i^{-1}$ for $i \geq 2$ and $\langle f_i^* \rangle = \langle e_i^* \rangle^a$ for $i \in \{0, \ldots, m\}$, it is clear that all the assertions of (11) will hold for the $e_i^*, f_i^*$ in place of $e_i, f_i$ except, possibly, (11e). But for $i \geq 3$,

$$(e_i^*)^a = (e_i e_i^{-1})^a = e_i e_i^{-1} e_{i-1} e_{i-2} = e_i e_i^{-1},$$

furthermore $(e_2^*)^a = e_2 e_1 e_1 = e_2 e_1^*$ and therefore (11e) holds. Since $\langle e_1, e_2 \rangle$ is a four-group, $\langle e_2^* \rangle^a = \langle e_2 e_1 \rangle^a = \langle f_2 f_1 \rangle$. Hence $f_2^* = f_2 f_1$ and so, finally,

$$(f_2^*)^b = (f_2 f_1)^b = f_2 f_1 f_0 f_1 f_0 = f_2 f_1 f_1 = f_2^* f_1^*,$$

as desired.
In the remainder of this section we fix bases \( \{ e_0, \ldots, e_m \} \) and \( \{ f_0, \ldots, f_m \} \) with the properties given in (11) and (13) and study the autoprojectivity \( \sigma \) induced by \( b \) in \( G \), that is, the map \( \sigma : L(G) \to L(G) \) defined by

\[
H^\sigma = H^{\varphi b \varphi^{-1}} \quad \text{for all } H \leq G.
\]

We first note that

\[
H^\sigma = H \quad \text{if } a \in H \leq G;
\]

for, then \( b \in H^\sigma \) and \( H^\sigma = H^{\varphi b \varphi^{-1}} = H \). In particular, \( \langle a \rangle^\sigma = \langle a \rangle \) and so \( G = N\langle a \rangle \) implies

\[
G = N^\sigma \langle a \rangle.
\]

By (11), \( f_0^b = f_0 \) and \( f_1^b = f_1 f_0 \) so that

\[
\langle e_0 \rangle^\sigma = \langle e_0 \rangle \quad \text{and} \quad \langle e_1 \rangle^\sigma = \langle e_1 e_0 \rangle.
\]

Since \( \langle e_1 \rangle \leq N \), therefore \( \langle e_1 e_0 \rangle \leq N^\sigma \); on the other hand, \( \langle e_0 \rangle \leq N \) implies that \( \langle e_0 \rangle^\sigma = \langle e_0 \rangle \leq N^\sigma \). It follows that

\[
N^\sigma \cap \langle e_0, e_1 \rangle = \langle e_1 e_0 \rangle; \quad \text{in particular, } e_1 \notin N^\sigma.
\]

We study the core \( K^\sigma \) of \( N^\sigma \) in \( G \) and the intersection \( Q \) of \( N \) and \( N^\sigma \).

\[
(19) \text{Let } K \leq G \text{ such that } K^\sigma = (N^\sigma)_G. \text{ Then } N \cap K^\sigma = 1, \text{ and } K \text{ and } K^\sigma \text{ are cyclic normal subgroups of } G, \Omega(K) = \langle e_1 \rangle \text{ and } \Omega(K^\sigma) = \langle e_1 e_0 \rangle.
\]

**Proof.** Since \( e_1 \notin N^\sigma \), \( e_1 \notin K^\sigma \leq G \) and hence \( N \cap K^\sigma = 1 \) by (11d). Therefore \( K^\sigma \simeq K^\sigma N/N \) is cyclic, hence also \( K \) is cyclic and, by 5.4.6 applied to the projectivity \( \sigma \), \( K \leq G \). By (11) and (18), \( \langle e_1 e_0 \rangle \leq Z(G) \cap N^\sigma \). It follows that \( \langle e_1 e_0 \rangle = \Omega(K^\sigma) \) and then (17) implies that \( \Omega(K) = \langle e_1 \rangle \).

\[
(20) \text{Let } K = C_N(a) \text{ and } K^\sigma \leq Z(G); \text{ if } p = 2, \text{ then } \Omega_2(K) \leq Z(G).
\]

**Proof.** By (15), \( K \langle a \rangle^\sigma = (K \langle a \rangle)^\sigma = K^\sigma \langle a \rangle^\sigma = K^\sigma \langle a \rangle \) so that both \( K \) and \( K^\sigma \) are normal subgroups of \( K \langle a \rangle \) with cyclic factor groups. Thus \( (K \langle a \rangle)^\sigma \leq K \cap K^\sigma = 1 \), by (19). This shows that \( K \langle a \rangle = K^\sigma \langle a \rangle \) is abelian so that \( K \) and \( K^\sigma \) are centralized by \( a \). On the other hand, by (10), \( C_N(a) \langle a \rangle \) is abelian and invariant under \( \sigma \). Therefore \( C_N(a)^\sigma \leq C_N(a) \langle a \rangle \) is centralized by \( a \). Since \( G = N^\sigma(a) \), every \( g \in G \) can be written in the form \( g = a^i z \) where \( z \in N^\sigma \) and \( (C_N(a)^\sigma)^z = (C_N(a)^\sigma) \leq N^\sigma \). It follows that \( (C_N(a)^\sigma)^G \leq (N^\sigma)_G = K^\sigma \) and hence \( C_N(a) \leq K \). Thus \( C_N(a) = K \), as desired.

If \( x \in N \), then \( G = N \langle xa \rangle \), and we may apply our results with \( xa \) in place of \( a \). Since \( \bar{G} = \bar{N} \langle xa \rangle^\sigma \), there exists \( y \in \bar{N} \) and \( b' \in \langle xa \rangle^\sigma \) such that \( b = y^{-1} b' \); it follows that \( \bar{G} = \bar{N} \langle b' \rangle \) and hence \( b' = y b \) generates \( \langle xa \rangle^\sigma \). So if we let \( \sigma' = \varphi b' \varphi^{-1} \), then \( N^\sigma = N^\varphi \varphi^{-1} = N^\sigma \) and \( (N^\sigma)_G = K^\sigma \) is centralized by \( xa \), as we have just shown. Thus \( K^\sigma \) is centralized by \( a \) and every \( x \in N \) so that \( K^\sigma \leq Z(G) \). In particular, \( \langle xa, K^\sigma \rangle \) is abelian and hence \( \langle xa, K^\sigma \rangle^\sigma = \langle xa \rangle^\sigma \) is an \( M \)-group. If \( p = 2 \), then by (5) and (7), \( o(x) < o(a) = 2^n \) and \( (xa)^{2^n-1} = a^{2^{n-1}} = e_0 \); thus \( \langle xa \rangle \cap K^\sigma = 1 \). By
2.3.6, $\Omega_3(K)$ normalizes $\langle xa \rangle^{q^{-1}}$ and hence $[\langle xa \rangle^{q^{-1}}, \Omega_3(K)] \leq \langle xa \rangle^{q^{-1}} \cap K = 1$. Since $G$ is generated by the $\langle xa \rangle$ ($x \in N$), it follows that $\Omega_3(K) \leq Z(G)$. \hfill $\Box$

(21) Let $Q = N \cap N^e$. Then $Q^G = QQ^e$.

**Proof.** Since $Q \leq N \leq G$, we have $Q \leq Q^G \leq N$ and hence $[Q^G/Q]$ is a chain by (8). Since $Q$ is permutable in $N$, $Q \cup Q^e = QQ^e$; let $|Q^G : QQ^e| = p^t$. Then $QQ^e$ is the unique subgroup of index $p^t$ in $Q$ and $Q^G$ and also between $Q^e$ and $Q^G$. It follows that $(QQ^e)^e = QQ^e$. By (16) and (8), $G = N^e\langle a \rangle$ and $Q \leq N^e$. Thus $Q^G = Q^{(a)} \leq (QQ^e)^{(a)} = QQ^e$ and hence $Q^G = QQ^e$. \hfill $\Box$

(22) If $p = 2$ or $N^e \leq \langle e_1 \rangle$, then $Q^G = \Omega_4(N)$ where $p^t = \text{Exp} \; Q$ and $s$ is the smallest integer such that $N/\Omega_s(N)$ is cyclic.

**Proof.** Let $p^t = \text{Exp} \; Q$. Then $Q \leq \Omega_4(N) \leq G$ so that $Q^G \leq \Omega_s(N)$. By (7) or (12), $\mathcal{U}_{s-1}(Q^G) = \{x^{p^{r-1}} | x \in Q^G\}$ is a nontrivial normal subgroup of $G$ and therefore, by (11d), contains $e_1$. Thus there exists $x \in Q^G$ such that $x^{p^{r-1}} = e_1$. Let $y \in \Omega_s(N)$. Since $Q$ is permutable in $N$, we deduce that $|Q \langle x \rangle : Q| = |\langle y \rangle : \langle y \rangle \cap Q| \leq p^s$; by (18), $e_1 \notin Q$ and hence $\langle x \rangle \cap Q = 1$ so that $|Q \langle x \rangle : Q| = p^s$. Now $[N/Q]$ is a chain and it follows that $Q \langle x \rangle \leq Q^G$. Thus $Q^G = \Omega_s(N)$ and $N/\Omega_s(N)$ is cyclic. Suppose, in order to obtain a contradiction, that $N/\Omega_{s-1}(N)$ is cyclic. Then $|\Omega_s(N) : \Omega_{s-1}(N)| = p$ and therefore $\Omega(N) = Q\Omega_{s-1}(N)$. Hence there exist $z \in Q$, $w \in \Omega_{s-1}(N)$ such that $x = zw$; by (7) or (12), $e_1 = x^{p^{r-1}} = z^{p^{r-1}}w^{p^{r-1}} = z^{p^{r-1}} \in Q$, a contradiction. Thus $s$ is the smallest integer such that $N/\Omega_s(N)$ is cyclic. \hfill $\Box$

(23) If $p = 2$ or $N^e \leq \langle e_1 \rangle$, there exists $u \in N$ such that $u^{p^{r-1}} = e_1$; let $U = \langle u \rangle$ and $V = U^e$. For any such pair $U$ and $V$, we have:

(23a) $N = QU$ and $N^e \cap U = 1$, hence also $Q \cap U = 1$;

(23b) $N^e = QV$ and $N \cap V = 1$, hence also $Q \cap V = 1$;

(23c) $NV = \Omega_s(G) = N^eU$; furthermore

(23d) $N\Omega_s(\langle a \rangle) = \Omega_s(G) = N^s\Omega_s(\langle a \rangle)$.

**Proof.** By (7) or (12), this time $\mathcal{U}_{s-1}(N) = \{x^{p^{r-1}} | x \in N\}$ is a nontrivial normal subgroup of $G$ and therefore, by (11d), contains $e_1$; thus there exists $u \in N$ such that $u^{p^{r-1}} = e_1$. By (18), $\Omega(U) = \langle e_1 \rangle \not\leq N^e$ and hence $N^e \cap U = 1$; in particular, $Q \cap U = 1$. By (17) and (11), $\Omega(V) = \Omega(U^e) = \langle e_1 e_0 \rangle \not\leq N$ and hence $N \cap V = 1$; in particular, $Q \cap V = 1$. By (9), $N = QU$ and $N^e = QV$ so that (23a) and (23b) are satisfied. By (4), $\Omega_s(G) = N\Omega_s(\langle a \rangle)$ and hence $\Omega_s(G) = \Omega_s(G)^e = N^e\Omega_s(\langle a \rangle)^e = N^e\Omega_s(\langle a \rangle)$ since $b$ normalizes $\Omega_s(\langle a \rangle)^e$. Thus (23d) holds and again by (9), $\Omega_s(G) = NV = N^eU$. \hfill $\Box$

(24) If $\Omega_s(\langle a \rangle) \leq N_g(Q)$, then $N$ is abelian.
Proof. By (23d), \( \Omega_r(G) = N^\sigma \Omega_r(\langle a \rangle) \). Since \( Q = N \cap N^\sigma \leq N^\sigma \) and \( \Omega_r(\langle a \rangle) \) normalizes \( Q \), it follows that \( Q \leq \Omega_r(G) \); in particular, \( Q \leq N \). Then \( N/Q \) is cyclic and hence \( N' \leq Q \leq N^\sigma \). Since \( N' \leq G \), we get that \( N' \leq (N^\sigma)G = K^\sigma \). But by (19), \( N \cap K^\sigma = 1 \) and thus \( N' = 1 \).

(25) If \( N' \leq \langle e_1 \rangle \), then \( Q \) is abelian and every subgroup of \( Q \) is normal in \( N^\sigma \); furthermore, \( N \) and \( N^\sigma \) are \( M \)-groups.

Proof. Let \( U \) and \( V \) be as in (23). Since \( N' \leq \langle e_1 \rangle \leq U \), we see that \( U \leq N \) and \( Q \cong N/U \) is abelian. Furthermore, \( U^\sigma = V \) is permutable in \( N^\sigma \). For every \( X \leq Q \),

\[
X = X(V \cap Q) = XV \cap Q \leq XV
\]

since \( Q \leq N^\sigma \); thus \( X \leq QV = N^\sigma \). Finally, as a projective image of the abelian group \( N/\langle e_1 \rangle \), the group \( N^\sigma/\langle e_1 e_0 \rangle \) is an \( M \)-group, and, since \( \langle e_1 e_0 \rangle \leq C_V(X) \), we see that \( XV/C_V(X) \) is an \( M \)-group. Thus if \( p = 2 \), \( \text{Exp} Q \geq 4 \) and \( X \) is cyclic of order 4, then \( X \leq Z(N^\sigma) \) since otherwise \( x^v = x^{-1} \) for \( X = \langle x \rangle \), \( V = \langle v \rangle \) and hence \( XV/C_V(X) \) would be dihedral of order 8 and not an \( M \)-group. By 2.3.4, \( N^\sigma \) is an \( M \)-group and then so is \( N \).

The case \( p > 2 \)

We come to our first main result.

5.5.2 Theorem (Menegazzo [1978]). Suppose that Hypothesis 5.5.1 is satisfied and \( p > 2 \). Then \( N \) is abelian.

Proof. We proceed by induction on \(|N|\) and keep the notation introduced above. If \( m = 1 \), \( N \) is cyclic; if \( r = 1 \), \( N \) is elementary abelian, by (4). Thus we may assume that \( m, r \geq 2 \). We now apply the induction assumption to three different projectivities. First of all, by (2), \( \varphi \) induces a projectivity in \( \Omega_{r-1}(N)<a> \) satisfying Hypothesis 5.5.1; by induction,

\[
(26) \Omega_{r-1}(N) \text{ is abelian.}
\]

By (3), the projectivity induced by \( \varphi \) in \( G/\Omega(G) \) satisfies Hypothesis 5.5.1; thus \( N\Omega(G)/\Omega(G) \) is abelian. Finally, \( \sigma \) induces a projectivity from \( G/K \) to \( G/K^\sigma \) and, by (19), \( \Omega(K) = \langle e_1 \rangle \) so that \( K \neq 1 \). Thus \( N/K \) is abelian and it follows that \( N' \leq \Omega(G) \cap K = \Omega(K) \) since \( K \) is cyclic and \( \Omega(G) \) is elementary abelian. So

\[
(27) N' \leq \langle e_1 \rangle
\]

and all the assertions in (22)–(25) hold for \( N \); let \( p^*= \text{Exp} Q, u \in N \) such that \( u^{p^*-1} = e_1 \), \( U = \langle u \rangle \) and \( V = U^\sigma \). If \( s < r \), then \( Q \leq \Omega_{r-1}(N) \) and, since \( UQ = N \), we have \( U\Omega_{r-1}(N) = N \leq G \). If \( s = r \), then by (12), the map \( v: N \to N \) defined by \( x^v = x^{p^*-1} \) (\( x \in N \)) is an endomorphism of \( N \) with \( \text{Ker} v = \Omega_{r-1}(N) \) and, since \( u^{p^*-1} = e_1 \), the
subgroup $U\Omega_\gamma(N) = \{ x \in N \mid x^{p^{-1}} \in \langle e_1 \rangle \}$ is the preimage of $\langle e_1 \rangle$ with respect to this homomorphism. Since $N$ and $\langle e_1 \rangle$ are normal subgroups of $G$, it follows that $U\Omega_\gamma(N) \leq G$. Thus in any case

(28) $U\Omega_\gamma(N) \leq G$.

To simplify notation, put $T = \Omega_\gamma(G)$. Then $UT = U\Omega_\gamma(N)T \leq G$ and hence $\overline{U}T$ is permutable in $\overline{G}$. Since $o(u) = p'$, $\overline{U}T/\overline{T}$ is a permutable subgroup of order $p$ in $\overline{G}/\overline{T}$ and hence normalizes the cyclic group $\overline{T}\langle b \rangle/\overline{T}$. By (3) and (1) applied to $G/T$, $\overline{N}\overline{T}/\overline{T}$ only contains trivial $b$-invariant subgroups and hence $(\overline{U}\overline{T})^b \neq \overline{U}\overline{T}$; by (14), $\overline{U}^b = U_\phi^{\phi^b} \phi = U_\phi^\phi = \overline{V}$ so that $(\overline{U}\overline{T})^b = \overline{V}\overline{T}$. Therefore if $\overline{S}/\overline{T} = \Omega(\overline{U}\overline{T}\langle b \rangle/\overline{T})$, then

(29) $\overline{S}/\overline{T}$ has order $p^2$ and contains $\overline{U}\overline{T}/\overline{T}, (\overline{U}\overline{T}^b)/\overline{T} = \overline{V}\overline{T}/\overline{T}$ and $\overline{T}\Omega,\langle a \rangle^\phi/\overline{T} = \Omega(\overline{T}\langle b \rangle/\overline{T})$ as three different minimal subgroups.

We want to show that $VT$ normalizes every subgroup of $\Omega_s(N)$. By (4), $|VT : \Omega_\gamma(N)| = |VT : T||T : \Omega_\gamma(N)| = p|\Omega_\gamma(\langle a \rangle)| = p'$ and, by (23), $|V:V\cap\Omega_\gamma(\langle a \rangle)| = |V| = p'$. Since $\Omega_\gamma(N) \leq T$, it follows that

(30) $VT = V\Omega_\gamma(N)$.

We show first that $\Omega_s(N)$ is centralized by $\Omega_\gamma(N)$. This is clear if $s < r$ since then $\Omega_s(N) \leq \Omega_\gamma(N)$ and this group is abelian. So suppose that $s = r$. Then by (25), $N' = QU$ is an $M$-group and since $Q \cap U = 1$, $|N : \Omega_\gamma(N)| \geq p^2$. On the other hand, $N' \leq \Omega(U)$ implies that $\langle u^p \rangle C_Q(U) \leq Z(N)$ and hence $|N : Z(N)| \leq |N : \langle u^p \rangle C_Q(U)| \leq p^2$. By 2.3.16, $N$ is abelian or $Z(N) \leq \Omega_\gamma(N)$ and, in the latter

![Figure 19](image-url)
case, it follows from the above inequalities that \( Z(N) = \Omega^{-1}(N) \). Thus in any event

\[(31) \Omega^{-1}(N) \leq C_G(\Omega_s(N)). \]

Since \( V T = V \Omega^{-1}(N) \), it remains to be shown that \( V \) normalizes every subgroup of \( \Omega_s(N) \). By (25), every subgroup of \( Q \) is normal in the \( M^* \)-group \( N^* = Q V \) and hence by 2.3.13 there exists a generator \( v \in V \) and \( k \in \mathbb{N} \) such that \((Q, v, k)\) is an Iwasawa triple for \( N^* \), that is, \( x^v = x^{1+p^k} \) for all \( x \in Q \). By (29) and (4), \( v \in \Omega_s(\langle a \rangle) \), and hence there exist \( a_1 \in \Omega_s(\langle a \rangle) \) and \( x_1 \in \Omega^{-1}(N) \) such that \( v = a_1 x_1 \). Then \([v, a] = [x_1, a] \in \Omega^{-1}(N) \) since, by (28), \( U \Omega^{-1}(N)/\Omega^{-1}(N) \) is a normal subgroup of order \( p \) in \( G/\Omega^{-1}(N) \). By (31), \( v^{-1}v^a = [v, a] \in C_G(\Omega_s(N)) \) and therefore \( v \) and \( v^a \) induce the same automorphism in \( \Omega_s(N) \). By (21) and (22), \( \Omega_s(N) = QQ^a \). Hence for \( v \in \Omega_s(N) \) there exist \( x, y \in Q \) such that \( z = xy^a \), and, since \( (y^a)^v = (y^a)^v = (y^{1+p^k})^v = (y^a)^{1+p^k} \), it follows that \( z^v = (xy^a)^v = x^{1+p^k}(y^a)^{1+p^k} \).

Since \( p > 2 \), \( \left(1 + \frac{p^k}{2}\right) \equiv 0 \pmod{p} \) so that \( |N'| \leq p \) and (4) of \$1.5$ imply that \( z^{1+p^k} = x^{1+p^k}(y^a)^{1+p^k} \). Thus \( z^v = z^{1+p^k} \), that is, \( v \) induces a power automorphism in \( \Omega_s(N) \). Now (30) and (31) yield that

\[(32) VT \text{ normalizes every subgroup of } \Omega_s(N). \]

All assertions proved so far also hold with \( b \) replaced by \( b^{-1} \). Thus if \( \tau \) is the autoprojectivity of \( G \) induced by \( b^{-1} \), that is, \( H^\tau = H^{\tau b^{-1} \varphi^{-1}} \) for all \( H \leq G \), and \( W = U^\tau \), then by (29), \( \overline{W T}/T \) is a minimal subgroup of \( \overline{S}/T \) and, by (32), every subgroup of \( \Omega_s(N) \) is normalized by \( W T \) where, by (22), \( s \) is still the smallest integer such that \( N/\Omega_s(N) \) is cyclic. If \( V T = W T \), then \((\overline{U T})^\tau = \overline{V T} = \overline{W T} = (\overline{U T})^\tau \) and hence \( (\overline{U T})^k = \overline{U T} \); since \( p > 2 \), it would follow that \( b \notin N_G(\overline{U T}) \), contradicting (29). Thus \( V T /T \) and \( W T /T \) are different minimal subgroups of \( S/T \) and hence generate \( S/T \). Therefore \( U \leq V T W \) normalizes every subgroup of \( \Omega_s(N) \). In particular, \( Q^U = Q \) and so \( N' \leq \langle e_1 \rangle \leq U \), also \( U \leq N \) and, by (23), \( N = Q \times U \). By (25), \( Q \) is abelian and so, finally, \( N \) is abelian.

Since \( N \) is abelian and \( G/N \) is cyclic, \( G \) is clearly metabelian if \( p > 2 \). An example in which \( \overline{N} \) is not abelian is given in Exercise 2. Nevertheless, \( G \) is also metabelian as we are now going to show. In fact, we prove a more general result that will also be used in the case \( p = 2 \).

5.5.3 Lemma. Suppose that Hypothesis 5.5.1 is satisfied and \( N \) is abelian. Then \( \Omega_s(G) \) is an \( M^* \)-group and \( G \) is metabelian; for every \( c \in \Omega_s(G) \) there exists \( k \in \mathbb{N} \) such that \( k \equiv 1 \pmod{4} \) if \( p = 2 \) and \( x^c = x^k \) for all \( x \in N \).

Proof: We keep the notation introduced above and let \( \Omega_s(\langle a \rangle) = \langle c \rangle \). Since \( N' \leq \langle e_1 \rangle \), all the assertions in (22)–(25) hold and we use induction on \(|N|\) to prove first that \( c \) induces a universal power automorphism \( v \to v^k \) in \( N \). By (23) and (25), every subgroup \( X \) of \( Q \) is normal in \( N^* = Q V \). Since \( N \) is abelian, \( X \leq NV = \Omega_s(G) \). By 1.5.4, \( c \) induces a universal power automorphism in the abelian group \( Q \), that is, there exists \( h \in \mathbb{Z} \) such that \( x^c = x^h \) for all \( x \in Q \). Since \( c \in \langle a \rangle \), we obtain \( (x^a)^c = (x^c)^a = (x^a)^h \), so that \( c \) induces the automorphism \( x \to x^h \) in \( QQ^a \). By (21) and
5.5 Normal subgroups of $p$-groups with cyclic factor group

(22), $QQ^s = \Omega_s(N)$ for some $s \in \mathbb{N}$. If $s = r$, then $\Omega_r(N) = N$ and we are done; thus we may assume that $s < r$. By (23), $N = Q \times \langle u \rangle$ where $u^{pr-1} = e_1$. The induction assumption applied to $G/\Omega(G)$ yields $j \in \mathbb{Z}$ such that $c\Omega(G)$ induces the automorphism $v \to v^j$ in $N\Omega(G)/\Omega(G)$; thus $u^c = u^jz$ where $z \in \Omega(G) \cap N = \Omega(N)$. It follows that $(u^{pr-1})^c = (u^c)^{pr-1} = u^{jpr-1}$; on the other hand, $(u^{pr-1})^c = u^{jpr-1}$ since $u^{pr-1} \in \Omega_s(N)$. Thus $h \equiv j (\mod p^r)$ and hence $x^c = x^j$ for all $x \in Q$. Since $u^s \in N = \langle u \rangle \times Q$, there exist $i \in \mathbb{N}$ and $y \in Q$ such that $u^s = u^iy$. It follows that $(u^c)^i = (u^i)^c = (u^i)^jy = (u^jz)^iy = (u^j)^iy^i$; on the other hand, $(u^c)^i = (u^i)^c = (u^iz)^a = (u^a)^i$ since $c \in \langle a \rangle$. Thus $z^a = z^i \in \langle z \rangle$, hence $\langle z^a \rangle = \langle z \rangle$ and (11d) implies that $\langle z \rangle \leq \langle e_1 \rangle$. Since $u^{pr-1} = e_1$, there exists $t \in \mathbb{N}$ such that $z = u^{tp-1}$. It follows that $u^c = u^{j+tp-1}$ and $x^c = x^j = x^{j+tp-1}$ for all $x \in Q$ so that $c$ induces the power automorphism $v \to v^k$ in $N$ where $k = j + tp-1$.

By (5), $\Omega_s(G)/\Omega_{s-2}(G)$ is abelian if $p = 2$ and so $[N, c] \leq \Omega_{s-2}(G) \cap N = \Omega_{s-2}(N)$, by (4); it follows that $k = 1 (\mod 4)$ in this case. By 2.3.4, $\Omega_r(G) = N\langle c \rangle$ is an $M$-group and, by (6), $\Omega_r(G)$ and $\Omega_r(G)$ are $M^*$-groups. Of course, every element of $\Omega_r(G)$ operates on $N$ as a power of $c$ and hence induces an automorphism $v \to v^j$ where $l \equiv 1 (\mod 4)$ if $p = 2$. Finally, $\Omega_{s-1}(G) < \Omega_{s-1}(G) \leq \Omega_r(G)$ and $\Omega_{s-1}(G) / \Omega_{s-1}(G)$ is core-free in $\Omega_r(G)$. It follows that $\Omega_s(G)/\Omega_{s-1}(G) = \Omega_r(G)/\Omega_{s-1}(\Omega_r(G))$ is not cyclic. Since $\Omega_r(G)$ is cyclic, 2.3.21 yields that $G$ is metabelian. \qed

Now 5.5.2 and 5.5.3 immediately imply:

5.5.4 Theorem (Busetto and Menegazzo [1985]). Suppose that Hypothesis 5.5.1 is satisfied and $p > 2$. Then $G$ is metabelian.

The case $p = 2$

In the proof of Theorem 5.5.2, the assumption $p > 2$ is used only in the last few lines. All the assertions up to (32) could be proved similarly for $p = 2$ with simple alterations; but for $p = 2$, of course, $VT = WT$ so that we would not get $U \leq VTW$. Indeed, there is an example of a 2-group satisfying Hypothesis 5.5.1 in which $N$ is nonabelian. We shall describe it briefly since the details are rather complicated and tedious.

5.5.5 Example (Busetto and Stonehewer [1985]). It is easy to see that the group

$$G = \langle a, u, w | a^{64} = u^{16} = w^8 = 1, u^w = u^9, a^u = u^{-1}w^4, w^a = u^2w^{-1} \rangle$$

is the semidirect product of the normal subgroup $N = \langle u, w | u^{16} = w^8 = 1, u^w = u^9 \rangle$ of order $2^7$ by the cyclic group $\langle a \rangle$ of order $2^6$. Clearly, $N$ is metacyclic and $N' = \langle u^8 \rangle$ has order 2.

The group $G$ is best defined in three steps. First take $H = \langle c \rangle \times \langle \bar{u} \rangle$ where $o(c) = o(\bar{u}) = 16$ (note that $H \cong \langle a^4 \rangle \times \langle u \rangle \leq G$). The group $H$ has an automorphism $\beta$ of order 4 satisfying $c^\beta = c^{13}u^8$ and $\bar{u}^\beta = \bar{u}^3$; hence we may form the semidirect product $M$ of $H$ by a cyclic group $\langle \bar{w} \rangle$ of order 8 inducing the automorphism $\beta$ in $H$; thus
Projectivities and normal structure of finite groups

$|M| = 2^{11}$. Finally, there is an automorphism $\varphi$ of $M$ satisfying $e^2 = c, \overline{u}^2 = c^{-1}\overline{u}^7\overline{w}^4$, and $\overline{w}^2 = \overline{u}^{14}\overline{w}^{-1}$; also it is not difficult to show that $\varphi^4$ is conjugation by $c$. Therefore there exists the extension $\overline{G} = M\langle \overline{a} \rangle$ where $M \trianglelefteq \overline{G}, \overline{G}/M$ is cyclic of order 4, $\overline{a}$ operates as $\varphi$ on $M$, and $\overline{a}^4 = c$.

Every element of $G$ can be written uniquely in the form $a^ku^iw^j$ where $0 \leq k \leq 63$, $0 \leq j \leq 15$, $0 \leq i \leq 7$, and every cyclic subgroup $X \trianglelefteq N\langle a^2 \rangle$ is generated by an element of the form $au^iw^j$. Similarly for $G$, and we define $v: G \to \overline{G}$ by

$$(a^ku^iw^j)v = \overline{a}^{(1+4i)k(1+4i)}u^{(1+4i)w^j+i}$$

where $\varepsilon = 2$ if $i$ is odd and $\varepsilon = 4jk$ if $i$ is even. It is easy to check that $v$ is bijective; but it is less obvious—and we refer the reader to the paper of Busetto and Stonehewer—that the map $\tau$ defined by $X^\tau = X^\nu$ for $X \leq N\langle a^2 \rangle$ and $X^\tau = (\langle au^iw^j \rangle)^\tau$ with cyclic $X = \langle au^iw^j \rangle \not\leq N\langle a^2 \rangle$ can be extended to a projectivity $\varphi$ from $G$ to $\overline{G}$. It is clear that $N^\varphi = \overline{N} = \langle \overline{u}, \overline{w} \rangle$ is core-free in $\overline{G}$ since $\Omega(\overline{N}) \cap \Omega(\overline{N})^2 \cap \Omega(\overline{N})^3 = 1$. Therefore Hypothesis 5.5.1 is satisfied. Since $[\overline{u}, \overline{a}] = c^{-1}\overline{u}^6\overline{w}^4$ and $[\overline{w}, \overline{a}] = \overline{u}^6\overline{w}^6$ do not commute, $\overline{G}^\varphi \neq 1$; on the other hand, $M = H\langle \overline{w} \rangle$ is metabelian so that $\overline{G}$ is soluble of derived length 3. Finally, $\overline{N} = \langle \overline{u}^4 \rangle$ is cyclic of order 4.

Busetto and Stonehewer also proved that the above example is the smallest possible one for which Hypothesis 5.5.1 is satisfied and $N$ is nonabelian. But $N$ is still an $M$-group and $|N'| \leq 2$. It was shown by Busetto and Napolitani [1991] that this is true in general. The basic breakthrough, however, had been accomplished by Busetto [1984] who had almost determined generators and relations for $G$ to show that $N$ and $\overline{N}$ have derived length at most 3 and 4, respectively. Busetto and Napolitani improved this argument to obtain the results we shall present here. We start with a preliminary result due to Menegazzo.

5.5.6 Lemma. Suppose that Hypothesis 5.5.1 is satisfied and $p = 2$. Then $\Omega(G) \leq Z(\Omega_2(G))$.

Proof. We use induction on $|N|$ and may assume that $r \geq 3$ since $\Omega_2(G)$ is abelian. By (19), $\sigma$ induces a projectivity from $G/K$ to $G/K^\sigma$ and the induction assumption yields that $\Omega(G/K) \leq Z(\Omega_2(G/K))$ if $2^\sigma = \text{Exp}(N/K)$. Since $\Omega(G)K/K \leq \Omega(G/K)$ and $N/K \leq \Omega(G/K)$, it follows that $[\Omega(G), N] \leq K$ and hence

$$(33) \ [\Omega(G), N] \leq \Omega(G) \cap K = \Omega(K) = \langle e_1 \rangle.$$ Let $U, V$ be as defined in (23). Then $U \leq N$ implies that $[\Omega(G), U] \leq \langle e_1 \rangle \leq U$ and hence $U$ is normalized by $\Omega(G)$. It follows that $|UX : U| \leq 2$ for every minimal subgroup $X$ of $G$; hence $|U^\sigma \cup X^\sigma : U^\sigma| \leq 2$ and therefore $V = U^\sigma$ is normalized by $\Omega(G)$. The same holds for the projective image $N^\sigma$ of the normal subgroup $N$. Thus $[\Omega(G), Q] = [\Omega(G), N \cap N^\sigma] \leq \langle e_1 \rangle \cap N^\sigma = 1$, by (18), and $[\Omega(G), V] \leq G' \cap V \leq N \cap V = 1$, by (23b), so that

$$(34) \ [\Omega(G), N^\sigma] = [\Omega(G), QV] = 1.$$
Since \( \Omega_r(G) = N V = NN^\sigma \), it follows from (33) and (34) that

\[
(35) \quad [\Omega(G), \Omega_r(G)] \leq \langle e_1 \rangle.
\]

To prove the lemma we therefore suppose, for a contradiction, that \([\Omega(G), \Omega_r(G)] = \langle e_1 \rangle\). By (18), \(e_0 \notin N^\sigma\). So if \(W\) is a cyclic subgroup of order \(2^r\) in \(G\) such that \(e_0 \in W\), then \(W \cap N^\sigma = 1\) and \(\Omega_r(G) = N^\sigma W\) since \([\Omega_r(G) : N^\sigma] = 2^r\). If \(W\) were normalized by \(\Omega(G)\), then (35) and (34) would imply that \([\Omega(G), W] \leq W \cap \langle e_1 \rangle = 1\) and \([\Omega(G), \Omega_r(G)] = [\Omega(G), N^\sigma W] = 1\); this would contradict our assumption. Thus

\[
(36) \quad \Omega(G) \not\leq N(G)(W)
\]

for every cyclic subgroup \(W\) of order \(2^r\) of \(G\) containing \(e_0\).

In particular, \(\Omega_r(\langle a \rangle)\) is not normalized by \(\Omega(G)\) so that, by (35),

\[
(37) \quad [\Omega(G), \Omega_r(\langle a \rangle)] = \langle e_1 \rangle.
\]

By induction on \(j \in \mathbb{N}\) we obtain that

\[
(38) \quad e_i^{a_j} = e_i \text{ for } 2 \leq i \leq 2^j \text{ and } e_i^{a_j} = e_i e_{i-2^j} \text{ for } 2^j < i \leq m.
\]

For, if \(j = 0\), this holds by (11e); and if (38) holds for \(j\), then

\[
e_i^{a_{2j+1}} = (e_i^{a_j})^{a_{2j}} = (e_i^{a_{i-2^j}})^{a_{2j}} = e_i e_{i-2^j} e_{i-2^{j+1}} e_i = e_i e_{i-2^{j+1}}
\]

where \(2^{j+1} < i \leq m\). If \(i \leq 2^j\), then \(e_i^{a_{2j+1}} = e_i\); and if \(e_i^{a_{2j+1}} = e_i e_{i-2^j} e_{i-2^{j+1}} = e_i\) where \(2^j < i \leq 2^{j+1}\). Thus (38) holds for \(j + 1\), as desired.

Now let \(\Omega_r(\langle a \rangle) = \langle a^{2^k} \rangle\). By (38), \([e_i, a^{2^k}] = 1\) for \(i \leq 2^k\), and \([e_i, a^{2^k}] = e_i e_{i-2^k}\) for \(2^k < i\). But by (37), \([\Omega(G), \langle a^{2^k} \rangle] = \langle e_1 \rangle\) and it follows that

\[
(39) \quad m = 2^k + 1.
\]

Then \(\langle e_0, \ldots, e_{m-1} \rangle\) is centralized by \(\langle a^{2^k} \rangle = \Omega_r(\langle a \rangle)\) and by \(N^\sigma\), as (34) states, and hence by \(\Omega_r(\langle a \rangle) N^\sigma = \Omega_r(G)\).

Thus

\[
(40) \quad \langle e_0, \ldots, e_{m-1} \rangle = Z(\Omega_r(G)) \cap \Omega(G).
\]

We want to show that, on the other hand, \(\bar{U}\) is not centralized by \(\langle f_0, \ldots, f_{m-1} \rangle\). For this let \(\bar{U} = \langle \bar{u} \rangle\) and \(W = \langle \bar{u} \bar{u}^b \rangle^{x^{-1}}\). By (7), (23), (11f) and (11g),

\[
(\bar{u} \bar{u}^b)^{2r-1} = \bar{u}^{2r-1} (\bar{u} \bar{u}^b)^{2r-1} = f_1 f_1^b = f_1 f_0 = f_0
\]

and hence \(W\) is a cyclic subgroup of order \(2^r\) of \(G\) containing \(e_0\). Since \(f_0 \in Z(\bar{G})\),

\[
(41) \quad \bar{u}^{1+2r-1} (\bar{u} \bar{u}^b)^{1+2r-1} = (\bar{u} \bar{u}^b)^{2r-1} \bar{u}^b = (\bar{u} \bar{u}^b)^{1+2r-1}.
\]

By (33), \(U\) is normalized by \(\Omega(G)\). Thus if \(x \in \Omega(G)\) and \(\langle y \rangle = \langle x \rangle^x\), then \(\bar{U} y = \bar{U}\) and, since \(\Omega_2(\bar{G})\) is abelian, the automorphism induced by \(y\) in \(\bar{U}\) has the form

\[
(42) \quad \bar{u}^y = \bar{u}^l \text{ where } l = 1 \text{ or } l = 1 + 2r-1.
\]

By (11h), \(\langle f_0, \ldots, f_{m-1} \rangle\) is \(b\)-invariant and of index \(p\) in \(\Omega(\bar{G})\); thus \(y^b = yz\) where \(z \in \langle f_0, \ldots, f_{m-1} \rangle\). Therefore if \(\bar{U}\) were centralized by \(\langle f_0, \ldots, f_{m-1} \rangle\), it would follow that \(\bar{u}^{y^b} = \bar{u}^{z^b} = \bar{u}\); since \((\bar{u} b)^{y^b} = (\bar{u} b)^{y z} = (\bar{u} b)^b = (\bar{u} b)^l\), we would get that \((\bar{u} b)^{y^b} = \bar{u}^l (\bar{u} b)^l = (\bar{u} b)^l\) where the last equation is trivial if \(l = 1\) and is (41) for \(l = 1 + 2r-1\).
Thus $\bar{W} = \langle \bar{u}u^b \rangle$ would be normalized by $\langle y^b \rangle = \langle x \rangle^y$ and so $W$ by $\langle x \rangle^{ybr^{-1}} = \langle x \rangle^y$. Since $x \in \Omega(G)$ was arbitrary, it would follow that $W$ would be normalized by $\Omega(G)^y = \Omega(G)$, contradicting (36). Thus, as $f_0 \in Z(\bar{G})$,

(43) $\langle f_1, \ldots, f_{m-1} \rangle \not\subseteq C_{\bar{G}}(\bar{U})$.

Since $\langle e_1, \ldots, e_{m-1} \rangle$ is generated by the elements outside $\langle e_1, \ldots, e_{m-2} \rangle$, there exists $x \in \langle e_1, \ldots, e_{m-1} \rangle \langle e_1, \ldots, e_{m-2} \rangle$ such that $\langle y \rangle = \langle x \rangle^y \not\subseteq C_{\bar{G}}(\bar{U})$. Then $l \neq 1$ in (42) and hence

(44) $[\bar{u}, y] = \bar{u}^{2r-1} = f_1$.

By (40), $\langle a^{2k} \rangle = \Omega_k(\langle a \rangle)$ centralizes $\langle e_1, \ldots, e_{m-1} \rangle$. Thus $\langle x^a | 0 \leq i \leq 2^k - 1 \rangle$ is an $a$-invariant subgroup of $\langle e_1, \ldots, e_{m-1} \rangle$ and hence, by (11c), is equal to $\langle e_1, \ldots, e_{m-1} \rangle$ since $x \notin \langle e_1, \ldots, e_{m-2} \rangle$. It follows that the $2^k = m - 1$ elements $x^a(0 \leq i \leq 2^k - 1)$ form a basis of $\langle e_1, \ldots, e_{m-1} \rangle$. Hence if

$L = \langle x^a | 0 \leq i \leq 2^k - 1, i \text{ even} \rangle,$

then $L^a = \langle x^a | 0 \leq j \leq 2^k - 1, j \text{ odd} \rangle$ and $L \cap L^a = 1$. In particular,

(45) $C_L(a) = 1$ and $L \leq C_G(N)$,

by (40). Since $L$ is generated by the conjugates of $x$ under $\langle a^2 \rangle$, we see that $L$ is normalized by this group. Thus if $h \in N$ and $i \in \mathbb{N}$ is odd, then $L \subseteq \langle x, ha^{2i} \rangle = L\langle ha^{2i} \rangle$. By (5) and (7), $o(a^{2i}) > o(h)$ and $\Omega(\langle ha^{2i} \rangle) = \Omega(\langle a^{2i} \rangle) = \langle e_0 \rangle$. Thus $L \cap \langle ha^{2i} \rangle = 1$ and hence

(46) $\Omega(\langle x, ha^{2i} \rangle) = L \times \langle e_0 \rangle$ for all $h \in N$ and $i \neq 0 \pmod{2}$.

Since $\bar{u}b^2 \in \bar{N}\langle b^2 \rangle = (N\langle a^2 \rangle)^y$, there exist $h \in N$ and $i \in \mathbb{N}$ such that $\langle \bar{u}b^2 \rangle = \langle ha^{2i} \rangle^y$. Again by (5) and (7), $o(\bar{u}) < o(b^2) = o(\bar{u}b^2)$ and hence $i$ is odd. By (46), $\Omega(\langle y, \bar{u}b^2 \rangle) = \Omega(\langle x, ha^{2i} \rangle)^y = (L \times \langle e_0 \rangle)^y$ and $\Omega(\langle y, b^2 \rangle) = \Omega(\langle x, a^{2i} \rangle)^y = (L \times \langle e_0 \rangle)^y$. Since $o(y) = 2$, it follows that $[\bar{u}b^2, y] \in \Omega(\langle y, \bar{u}b^2 \rangle) = (L \times \langle e_0 \rangle)^y$ and $[b^2, y] \in (L \times \langle e_0 \rangle)^y$. By (1) of § 1.5, (44) and (11g),

$$[\bar{u}b^2, y] = [\bar{u}, y]b^2[b^2, y] = f_1b^2[b^2, y] = f_1, [b^2, y]$$

and hence $f_1 = [\bar{u}b^2, y][b^2, y]^{-1} \in (L \times \langle e_0 \rangle)^y$. Thus $e_1 \in (L \times \langle e_0 \rangle) \cap N = L$; but by (45), $C_L(a) = 1$. This is the desired contradiction.

\begin{flushright} \Box \end{flushright}

**Modularity in 2-groups**

We interrupt our investigation of the case $p = 2$ to prove some lemmas on 2-groups with modular subgroup lattices and permutable subgroups in 2-groups; these will be used in the sequel. We start with two rather trivial properties which hold for arbitrary primes $p$.

(47) If $H$ is a $p$-group of exponent $p^n$, $1 \leq k \leq n$, $\Omega_{n-1}(H)$ and $H/\mathcal{U}_k(H)$ are $M$-groups and $\mathcal{U}_k(H)$ is cyclic, then $H$ is an $M$-group.
5.5 Normal subgroups of $p$-groups with cyclic factor group

Proof. By 2.3.2, we have to show that $XY = YX$ for any two subgroups $X, Y$ of $H$. This is clear if $X, Y \leq \Omega_{n-1}(H)$; and if $X \not\subseteq \Omega_{n-1}(H)$, say, then $X$ contains an element $x$ of order $p^n$ and $K = U_k(H) = \langle x^{p^n} \rangle \leq X$. It follows that $XY = XKY = KYX = YKX = YX$.

(48) If $H = M\langle z \rangle$ is a $p$-group with modular subgroup lattice, $M$ abelian, $M \leq H$ and $M \cap \langle z \rangle = 1$, then there exists $k \in \mathbb{N}$, $k \equiv 1 \pmod{4}$ in case $p = 2$, such that $x^z = x^k$ for all $x \in M$.

Proof. If $X \leq M$, then $X = X \cap (\langle z \rangle \cap M) = (X \cap \langle z \rangle) \cap M \leq X \cap \langle z \rangle$. By 1.5.4, $z$ induces a universal power automorphism $x \rightarrow x^k$ in $M$. If $\text{Exp} M \leq 2$, $k = 1$; and if $x \in M$ such that $o(x) = 4$, then by 2.3.6, $x^{k-1} = [x, z] \in \langle x, z \rangle \cap \langle z \rangle = 1$ so that $k \equiv 1 \pmod{4}$.

In the following four assertions let $M$ be a subgroup and $z$ an element of the group $H$ and let $k \in \mathbb{N}$. For short, let us say that $z$ induces the power $k$ in $M$ if $x^z = x^k$ for all $x \in M$.

(49) If $z$ induces the power $k$ in $M$ and $a \in H$ such that $[a^{-1}, z^{-1}] \in C_H(M)$, then $z$ also induces the power $k$ in $M^a$.

Proof. By assumption there exists $c \in C_H(M)$ such that $az = cza$. Hence $(x^a)^z = x^{cz} = (x^k)^z = (x^z)^k$ for every $x \in M$.

(50) Let $H$ be a 2-group and $k \equiv 1 \pmod{4}$. If $|M'| \leq 2$, then $(xy)^k = x^ky^k$ for all $x, y \in M$. So if $z$ induces the power $k$ in subgroups $A, B$ of $M$ and $AB \leq M$, then $z$ also induces the power $k$ in $AB$.

Proof. By (4) of §1.5, $(xy)^k = x^k y^k [y, x]'$ where $t = \binom{k}{2}$ is even, since $k \equiv 1 \pmod{4}$; thus $[y, x]' = 1$. For $a \in A$, $b \in B$, therefore $(ab)^t = a^tb^z = a^kb^k = (ab)^k$.

(51) Let $H = M\langle a \rangle$, $M \leq H$, $z \in \langle a \rangle$ and $L \leq M$ where $L \leq M\langle z \rangle$. If $z$ induces the power $k$ in $M/L$, then it does likewise in $M/LH$.

Proof. By assumption, $x^{-k}x^z \in L$ for every $x \in M$. For $c \in \langle a \rangle$, therefore $L^c$ contains $(x^{-k}x^z)^c = (x^{-k})^c(x^z)^c$ and, since $M \leq H$, it follows that $x^c$ is an arbitrary element of $M$. Thus $y^{-k}y^z \in \bigcap_{c \in \langle a \rangle} L^c = \bigcap_{h \in H} L^h = L_H$ for every $y \in M$.

(52) Let $H$ be a 2-group, $\Omega(M) \leq Z(\langle \langle H, z \rangle \rangle)$ and suppose that $z$ induces the power $k$ in $M/\Omega(M)$. Then $(x^2)^z = (x^2)^k$ and $x^{z^2} = x^{k^2}$ for all $x \in M$; in particular, $z^2$ induces the power $k^2$ in $M$.

Proof. Let $x^z = x^ky$ where $y \in \Omega(M)$. Then $(x^2)^z = (x^2)^k = (x^ky)^z = (x^k)^2y^z = (x^2)^k$ and, since $y^k = y = y^z$, we conclude that $x^{z^2} = (x^ky)^z = (x^ky)^ky^z = x^k y^2 = x^{k^2}$.
We have seen in § 2.3 that elements of order 4 play a special role in 2-groups with modular subgroup lattices. One reason for this is the following more general result.

(53) If \( M \) is a permutable subgroup of the 2-group \( H \) and \( M \leq X \leq H \) such that \( |X : M| \leq 4 \), then \( M \leq X \); in particular, \( M \leq M\Omega_2(H) \).

**Proof.** If \( M \) were not normal in \( X \), then \( |X : M| = 4 \) and \( X/M \) would be isomorphic to a 2-subgroup of order at least 8 of the symmetric group \( S_4 \). But \( D_8 \in \text{Syl}_2(S_4) \) does not possess a nonnormal permutable subgroup of order 2. Thus \( M \leq X \); in particular, every element of order at most 4 of \( H \) normalizes \( M \).

(54) Let \( H = \langle x, y \rangle \) be a 2-group with modular subgroup lattice and suppose that \( o(x) = 4 \) and \( \langle x \rangle \) is core-free in \( H \). Then \( \langle [x, y] \rangle = \Omega_2(\langle y \rangle) \), \( \langle [x, y^2] \rangle = \Omega(\langle y \rangle) \) and \( \langle x^y \rangle \neq \langle x \rangle \).

**Proof.** By 2.3.6 or (53), \( x \) normalizes \( \langle y \rangle \) and hence \( [x, y] \in \langle y \rangle \cap \Omega_2(H) = \Omega_2(\langle y \rangle) \). If \( [x, y] \in \Omega(\langle y \rangle) \), then \( [x^2, y] = [x, y]^2 = 1 \) since \( \Omega(\langle y \rangle) \leq Z(H) \) and hence \( x^2 \in Z(H) \), contradicting \( \langle x \rangle_H = 1 \). Thus \( \langle [x, y] \rangle = \Omega_2(\langle y \rangle) \) and hence \( [x, y^2] = [x, y]^2 \) generates \( \Omega(\langle y \rangle) \). Since \( \langle x \rangle \cap \langle y \rangle = 1 \), therefore \( \langle x \rangle^{y^2} \neq \langle x \rangle \) and hence \( \langle x^y \rangle \neq \langle x \rangle \).

(55) If \( H \) is a 2-group such that \( H' \) is cyclic of order at most 4, then \( [x^2, H] \leq \Phi(H') \) and \( x^4 \in Z(H) \) for every \( x \in H \).

**Proof.** Since \( H' \) is cyclic and \( |H'| \leq 4 \), we have \( [x, y]^s = [x, y]^{-1} \) or \( [x, y]^s = [x, y] \) where \( y \in H \). Then (1) of § 1.5 shows that in the first case \( [x^2, y] = [x, y]^s[x, y] = 1 \) and hence also \( [x^4, y] = 1 \); in the second case, \( [x^2, y] = [x, y]^2 \in \Phi(H') \) and \( [x^4, y] = [x, y]^4 = 1 \).

In the last two lemmas of this subsection, \( H \) again is a p-group with modular subgroup lattice for an arbitrary prime \( p \). And since both assertions trivially hold in a hamiltonian 2-group, that is, in a direct product of \( Q_8 \) with an elementary abelian 2-group, we may assume that \( H \) is an \( M^* \)-group. Then by Iwasawa’s Theorem 2.3.1 there exist \( A \leq H, b \in H \) and an integer \( s \) which is at least 2 in case \( p = 2 \) such that \( H = A\langle b \rangle \), \( A \) is abelian, and \( b^{-1}ab = a^{1+p^s} \) for all \( a \in A \). Clearly, \( H' = \mathcal{U}_s(A) \).

(56) If the \( M^* \)-group \( H \) contains a maximal subgroup \( M \) that is abelian, then \( H' \) is elementary abelian.

**Proof.** We keep the notation introduced above and assume first that \( A \leq M \). Then \( b^p \in M \leq C_H(A) \) so that \((1 + p^s)^p \equiv 1 \pmod{\text{Exp} A} \). But since \( s \geq 2 \) in case \( p = 2 \), \((1 + p^s)^p \equiv 1 + p^{s+1} \pmod{p^{s+2}} \) and hence \( p^{s+1} \geq \text{Exp} A \). It follows that \( H' = \mathcal{U}_s(A) \) is elementary abelian. If \( A \not\leq M \), then \( H' \leq A \cap M \leq Z(AM) = Z(H) \) and \( H = M\langle z \rangle \) for some \( z \in H \). Since \( z^p \in M \), we have \( [x, z]^p = [x, z^p] = 1 \) for every \( x \in M \) and therefore again \( H' \) is elementary abelian.

(57) If \( H \) is an \( M^* \)-group of exponent \( p^r \) such that \( H' \) is cyclic and \( |H/\Omega_{r-1}(H)| \geq p^3 \), then \( H \) is abelian.
Proof. Suppose, for a contradiction, that $H' = \mathcal{U}_s(A) \neq 1$. Then $A = \langle a \rangle \times B$ where $o(a) > \text{Exp } B$. It follows that $|A : \mathcal{O}_{r-1}(A)| \leq p$ and hence also $|A\mathcal{O}_{r-1}(H) : \mathcal{O}_{r-1}(H)| = |A : A \cap \mathcal{O}_{r-1}(H)| \leq p$. Since $H/\mathcal{O}_{r-1}(H)$ is both cyclic and elementary abelian, $|H : \mathcal{O}_{r-1}(H)| = p$. Thus $|H : \mathcal{O}_{r-1}(H)| \leq p^2$, a contradiction. 

Finally, we mention that we sometimes use Baer’s Theorem 2.5.9 saying that an $M^*$-group $H$ of order $p^n$ is lattice-isomorphic to an abelian group $\bar{H}$ of the same order and therefore of type $(p^{a_1}, \ldots, p^{a_i})$ for integers $a_1 \geq a_2 \geq \cdots \geq a_i$; we also call this the type of $H$.

The case $p = 2$, continued

We want to show that under Hypothesis 5.5.1, $N$ is an $M$-group, $|N'| \leq 2$, $G$ is metabelian and $G$ has derived length at most 3. Recall that $|\mathcal{O}(N)| = 2^m$. So if $m = 1$, $N$ is cyclic since $G$, by (6), does not contain subgroups isomorphic to $Q_8$; then $G$ is metacyclic and 5.2.13 shows that $G$ is metacyclic. Thus all the assertions we want to prove hold in this case and hence we shall assume in the sequel that

(58) $m \geq 2$.

For the proof of our result we have to study three autoproperties of $G$ in some detail: first of all $\sigma = \phi b \psi^{-1}$, as before, but also $\sigma^2 = \phi b^2 \psi^{-1}$ and $aa \sigma^2$. For the convenience of the reader we recall from (11) and (13) the operation of $a$ and $b$ on the bases $\{e_0, \ldots, e_m\}$ and $\{f_0, \ldots, f_m\}$ of $\mathcal{O}(G)$ and $\mathcal{O}(\bar{G})$, respectively. In addition we note that, by Theorem 2.6.7, $\phi$ is induced on $\mathcal{O}(G)$ by an isomorphism $i$. Thus

(59) $e_i = f_i$ for $i = 0, \ldots, m$; $e_0, e_1 \in Z(G)$; $e_i^2 = e_ie_{i-1}$ for $i = 2, \ldots, m$; $f_0 = f_0$, $f_i = f_i f_0$ and $f_i^2 = f_i f_1$.

We shall need the following formulæ (see also (17)).

(60) $\langle e_0 \rangle^\sigma = \langle e_0 \rangle$, $\langle e_1 \rangle^\sigma = \langle e_1 e_0 \rangle$, $\langle e_2 \rangle^\sigma = \langle e_2 e_1 \rangle$, $\langle e_2 e_1 \rangle^\sigma = \langle e_2 e_0 \rangle$.

(61) $\langle e_1 \rangle, \langle e_2 \rangle^\sigma = \langle e_2 e_0 \rangle$, $\langle e_2 e_1 \rangle, \langle e_2 e_0 \rangle^\sigma = \langle e_2 \rangle$.

(62) $\langle e_1 \rangle, \langle e_2 e_1 \rangle^{a \sigma^2} = \langle e_2 e_0 \rangle$, $\langle e_2 e_1 e_0 \rangle^{a \sigma^2} = \langle e_2 \rangle$.

Proof. By (59), $\sigma = \phi b \psi^{-1}$ is induced on $\mathcal{O}(G)$ by the isomorphism $ib^{-1}$, which we shall also call $\sigma$. Then we can compute as follows: $e_0^\sigma = f_0 f_1^\sigma = f_0^\sigma = e_0$, $e_1^\sigma = f_2 f_1^\sigma = e_1 e_0$, $e_2^\sigma = f_2 f_1^\sigma = e_2 e_1 e_0$, $e_2 e_1^\sigma = e_2^\sigma e_1^\sigma = e_2 e_0$. This proves (60); using (60), we obtain: $e_2^\sigma = (e_1 e_0)^\sigma = e_1$, $e_2^\sigma = (e_1 e_0)^\sigma = e_2 e_0$, $e_2 e_1^\sigma = e_2^\sigma e_1^\sigma = e_2$, $e_2 e_0^\sigma = e_2^\sigma e_0^\sigma = e_2$. For the remaining cases, we compute as follows: $e_1^\sigma = (e_1 e_0)^\sigma = e_1$, $e_2^\sigma = (e_2 e_1 e_0)^\sigma = (e_2 e_0)^\sigma = e_2 e_0$, $e_1^\sigma = (e_1 e_0)^\sigma = e_1$, $e_2 e_1 e_0 = (e_2 e_0)^\sigma = e_2$. This proves (62).

Proof. Let $Q = N \cap N^\sigma$ and define $R = N \cap N^{a \sigma^2}$ and $S = N \cap N^{a \sigma a^2}$. Then $Q \cap \langle e_0, e_1, e_2 \rangle = \langle e_2 e_1 \rangle$ and $R \cap \langle e_0, e_1, e_2 \rangle = \langle e_1 \rangle$ and $S \cap \langle e_0, e_1, e_2 \rangle = \langle e_0, e_1, e_2 \rangle$. Then

(63) Again let $Q = N \cap N^\sigma$ and define $R = N \cap N^{a \sigma^2}$ and $S = N \cap N^{a \sigma a^2}$. Then $Q \cap \langle e_0, e_1, e_2 \rangle = \langle e_2 e_1 \rangle$ and since $e_1 e_0 \notin N$, $Q \cap \langle e_0, e_1 \rangle = 1$; it follows that $|Q \cap E| \leq 2$. On the other hand, $\langle e_2 \rangle^\sigma = \langle e_2 e_1 \rangle$.
and hence $\langle e_2 e_1 \rangle \leq N \cap N^\sigma = Q$. Thus $Q \cap E = \langle e_2 e_1 \rangle$. Similarly, since $N \cap \langle e_2, e_0 \rangle = \langle e_2 \rangle$ but $\langle e_2 \rangle = \langle e_2 e_0 \rangle^2 \not\leq N^\sigma$ and $\langle e_2 \rangle = \langle e_2 e_1 e_0 \rangle^{\sigma_{a_o}^{-1}} \not\leq N^{\sigma_{a_o}^{-1}}$, it follows that $R \cap \langle e_0, e_2 \rangle = 1 = S \cap \langle e_0, e_2 \rangle$. Thus $|R \cap E| \leq 2$ and $|S \cap E| \leq 2$; on the other hand, $\langle e_1 \rangle^2 = \langle e_1 \rangle = \langle e_1 \rangle^{\sigma_{a_o}^{-1}}$ implies that $\langle e_1 \rangle \leq N \cap N^\sigma \cap N^{\sigma_{a_o}^{-1}} = R \cap S$ and $R \cap E = \langle e_1 \rangle = S \cap E$. 

(64) $K \leq S$ and $R \cap K = \langle e_1 \rangle$.

Proof. Recall that $K^\sigma = (N^\sigma)_G$. Thus $S^\sigma = (N \cap N^{\sigma_{a_o}^{-1}})^\sigma = N^\sigma \cap (N^\sigma)^\sigma \geq K^\sigma$ and hence $S \geq K$. Suppose, for a contradiction, that $R \cap K > \langle e_1 \rangle$. Then $R \cap K \geq \Omega_2(K) = \langle g \rangle$ since $K$ is cyclic; let $\langle g, a \rangle$ be abelian and hence $\langle g, a \rangle^\sigma = \langle h, b \rangle$ is a 2-group with modular subgroup lattice and $o(h) = 4$. Moreover, by (1), $\langle h \rangle$ is core-free in $\langle h, b \rangle$ and so (54) yields that $\langle [h, b^2] \rangle = \Omega_2(\langle b \rangle) = \langle f_0 \rangle$.

Now $g \in R = N \cap N^\sigma$ implies that $h \in (N \cap N^\sigma)^\sigma = N^\sigma \cap N^{\sigma_{h^2}}$ and hence $f_0 = h^{-1} h^{b^2} \in (N^\sigma)^{b^2}$. Since $f_0 \in Z(G)$, it follows that $f_0 \in N^\sigma$, a contradiction. 

Recall that by (23) there exists $u \in N$ such that $u^{2r-1} = e_1$. For any such $u$,

(65) $N = Q\langle u \rangle$, $Q \cap \langle u \rangle = 1$, $u^{2r-1} = e_1$, $u^a \equiv u$ (mod $\Omega_{r-1}(N)$) and, more generally, $(u^{2k})^a \equiv u^{2k}$ (mod $\Omega_{r-k-1}(N)$) for $k = 0, \ldots, r - 1$.

Proof. The first three assertions have been proved in (23). For $k = 0, \ldots, r - 1$, 

$$(u^{2k})^a \equiv u^{2k} \text{ (mod $\Omega_{r-k-1}(N)$)}.$$ 

and hence by (7), $(u^{2k})^a \equiv u^{2k}$ (mod $\Omega_{r-k-1}(N)$). 

(66) Let $2^s = \text{Exp}Q$. Then there exists $w \in Q$ such that $w^{2s-1} = e_2 e_1$. For any such $w$, $Q = (Q \cap R)\langle w \rangle = (Q \cap S)\langle w \rangle$, $(Q \cap R) \cap \langle w \rangle = 1 = (Q \cap S) \cap \langle w \rangle$ and $N = (Q \cap R)\langle w \rangle\langle u \rangle$; furthermore $w^a \equiv w^{2s-2s}$ (mod $\Omega_{s-1}(N)$).

Proof. To simplify notation, let $\tau$ be one of the two autoprojectivities $\sigma^2$ or $\sigma_{a_o}^{-1}$ of $G$ and let $T = N \cap N^\tau$; thus $T = R$ or $T = S$ and therefore $T \cap \langle e_0, e_1, e_2 \rangle = \langle e_1 \rangle$, by (63). Now (65) and (7) imply that $\Omega_s(N) = Q\Omega_s(\langle u \rangle)$ and $\mathcal{U}_{s-1}(\Omega_s(N)) = \mathcal{U}_{s-1}(Q)\langle e_1 \rangle$. Since $e_1 \not\in Q$ and $\mathcal{U}_{s-1}(Q) \not\equiv 1$, it follows from (11c) that $\langle e_1, e_2 \rangle \leq \mathcal{U}_{s-1}(\Omega_s(N))$ and hence $\langle e_1, e_2 \rangle \cap \mathcal{U}_{s-1}(Q) \not\equiv 1$. Since $Q \cap \langle e_0, e_1, e_2 \rangle = \langle e_1, e_2 \rangle$ and $\mathcal{U}_{s-1}(Q) = \{x^{2s-1} | x \in Q\}$, there exists $w \in Q$ such that $w^{2s-1} = e_2 e_1$. By (8), $T$ is permutable in $N$ and $[N/T]$ is a chain. Thus $T \cap Q$ is also permutable in $Q$ and $[Q/T \cap Q]$ is a chain. Since $T \cap \langle e_0, e_1, e_2 \rangle = \langle e_1 \rangle$, we deduce that $(Q \cap T) \cap \langle w \rangle = 1$ and, by (9), $Q = (Q \cap T)\langle w \rangle$. It follows that $N = Q\langle u \rangle = (Q \cap T)\langle w \rangle\langle u \rangle$. For the last assertion in (66), note that 

$$(w^a)^{2s-1} = (w^{2s-1})^a = (e_2 e_1)^a = e_2 e_1 e_1 = w^{2s-1} u^{2r-1} = (w u^{2r-1})^{2s-1}$$ 

so that $w^a \equiv w^{2s-2s}$ (mod $\Omega_{s-1}(N)$), by (7).
(67) If \( N/\Omega_{-2}(N) \) is not cyclic, we may choose the element \( u \) in (65) from \( R \); similarly, there exists \( u' \in S \) satisfying (65) and (66) in place of \( u \). For these elements,

(67a) \( R = (Q \cap R) \langle u \rangle \) and \( S = (Q \cap S) \langle u' \rangle \),
(67b) \( N = R \langle w \rangle = S \langle w \rangle \) and \( R \cap \langle w \rangle = S \cap \langle w \rangle = 1 \),
(67c) \( N^{a^2} = R \langle w \rangle^{a^2} = R \langle wu^{2^{r-1}} \rangle^{a^2} \), \( R \cap \langle w \rangle^{a^2} = 1 = R \cap \langle wu^{2^{r-1}} \rangle^{a^2} \),
(67d) \( N^{\sigma a} = S \langle w \rangle^{\sigma a} \).

Proof. Again let \( \tau \) be \( a^2 \) or \( \sigma a \) and \( T = N \cap N' \) so that \( T = R \) or \( T = S \). For the present, choose \( u \) as in (65). Then \( N = Q \langle u \rangle = T \langle z \rangle \) for some \( z \in N \), by (8) and (9), and hence by (7), \( \mathcal{U}_{r-1}(N) = \mathcal{U}_{r-1}(Q) \mathcal{U}_{r-1}(\langle u \rangle) = \mathcal{U}_{r-1}(T) \mathcal{U}_{r-1}(\langle z \rangle) \). We are looking for \( t \in T \) such that \( t^{2^{r-1}} = e_1 \). By (11c), \( \mathcal{U}_{r-1}(N) = \langle e_1, \ldots, e_i \rangle \) for some \( i \). If \( i \geq 2 \), then \( |\mathcal{U}_{r-1}(\langle z \rangle)| \leq 2 \) implies that \( \mathcal{U}_{r-1}(T) \cap \langle e_1, e_2 \rangle \neq 1 \). By (63), \( T \cap \langle e_0, e_1, e_2 \rangle = \langle e_1 \rangle \), therefore \( \mathcal{U}_{r-1}(T) \cap \langle e_1, e_2 \rangle = \langle e_1 \rangle \), and hence there exists \( t \in T \) such that \( t^{2^{r-1}} = e_1 \). This, of course, is also the case if \( i = 1 \) and \( \mathcal{U}_{r-1}(T) \neq 1 \). So suppose, for a contradiction, that \( i = 1 \) and \( \mathcal{U}_{r-1}(T) = 1 \). Then \( \text{Exp} \ T \leq 2^{r-1} \) and \( \mathcal{U}_{r-1}(N) = \langle e_1 \rangle = \Omega(\langle z \rangle) = \Omega(\langle u \rangle) \). Since \( Q \cap \langle u \rangle = 1 \), it follows that also \( \text{Exp} Q \leq 2^{r-1} \). If \( Q \leq \Omega_{-2}(N) \), then \( N/\Omega_{-2}(N) \) would be cyclic, contradicting our assumption; thus \( \text{Exp} Q = 2^{r-1} \). Now \( |N: T| = |\langle z \rangle : \langle z \rangle \cap T| \leq 2^{r-1} \) since \( \Omega(\langle z \rangle) = \langle e_1 \rangle \leq T \); on the other hand, \( |T \langle w \rangle : T| = |\langle w \rangle : 2^{r-1} \) since \( \Omega(\langle w \rangle) = \langle e_2 e_1 \rangle \neq T \). Thus \( N = T \langle w \rangle \leq \Omega_{r-1}(N) \), which is a contradiction. Thus in any event there exists \( t \in T \) such that \( t^{2^{r-1}} = e_1 \). By (65), for any such \( t \), \( N = Q \langle t \rangle \) and Dedekind's law yields that \( T = (Q \cap T) \langle t \rangle \). By (66), \( N = \langle t \rangle Q = \langle t \rangle (Q \cap T) \langle w \rangle = T \langle w \rangle \) and \( T \cap \langle w \rangle = T \cap Q \cap \langle w \rangle = 1 \); so (67a) and (67b) are satisfied.

For the proof of (67c), note that \( |N^{a^2} : R| = |N : R| = |\langle w \rangle| \) and that \( \Omega(\langle w \rangle) = \langle e_2 e_1 \rangle \) and \( \Omega(\langle wu^{2^{r-1}} \rangle) = \langle e_2 \rangle \), by (7). Hence by (61) and (63), \( \langle w \rangle^{a^2} \cap R = \langle e_2 e_1 e_0 \rangle \cap R = 1 \) and \( \langle wu^{2^{r-1}} \rangle^{a^2} \cap R = \langle e_2 e_0 \rangle \cap R = 1 \). It follows that \( N^{a^2} = R \langle w \rangle^{a^2} = R \langle wu^{2^{r-1}} \rangle^{a^2} \). Similarly, \( |N^{\sigma a} : S| = |N : S| = |\langle w \rangle| \) and, by (62) and (63), \( \langle w \rangle^{\sigma a} \cap S = \langle e_2 e_0 \rangle \cap S = 1 \); thus \( N^{\sigma a} = S \langle w \rangle^{\sigma a} \) and (67d) holds.

(68) If \( x \in N \) such that \( \Omega_2(\langle x \rangle), a \] = 1, then \( \Omega_{i+2}(\langle x \rangle), a \] \( \leq \Omega_i(N) \) for all \( i \geq 0 \).

Proof. We use induction on \( o(x) \). If \( o(x) \geq 2^a \), then the induction assumption applied to \( x^2 \) yields that \( \Omega_3(\langle x \rangle), a \] \( \leq \Omega(N) \). Therefore, by (3) and (4), \( x \Omega(G) \) satisfies the assumptions of (68) in \( G/\Omega(G) \) and the induction assumption implies that \( \Omega_{i+2}(\langle x \rangle), a \] \( \leq \Omega_i(G) \cap N = \Omega_i(N) \) for all \( i \geq 1 \). Thus we may assume that \( o(x) = 8 \) and have to show that \( \langle x, a \rangle \in \Omega(N) \). Let \( H = \langle x, \Omega_2(N) \rangle \). By (5), \( \Omega_3(N)/\Omega(N) \) is abelian and hence \( H' \leq \Omega(N) \). Let \( K \) be as defined in (19). Since \( \Omega(\langle x \rangle) = \langle x^4 \rangle \) is centralized by \( a \), we obtain \( x^4 = e_1 \in K \), by (11c). Thus \( HK/K \leq \Omega_3(G/K) \) is abelian, by (5) applied to \( G/K \). So \( H' \leq \Omega(N) \cap K = \langle e_1 \rangle \). Since \( (x^e)^4 = (x^w)^4 = e_1 = x^{4^e} \), (7) implies that \( x^e = xz \) for some \( z \in \Omega_2(N) \). By assumption, \( x^2 = (x^2)^e = (x^2)^{a^2} = (xz)^2 = x^2 z \) and hence \( z^2 = [x, z] \) \( \in H' \leq \langle e_1 \rangle = \langle x^4 \rangle \). Thus \( z^2 = x^{4k} \) for some \( k \), hence \( (xz)^{-2k} = 1 \) since \( \Omega_2(N) \) is abelian and therefore \( xz^{-2k} \in \Omega(N) \leq Z(N) \), by Lemma 5.5.6. It follows that \( z \) centralizes \( x \) and hence \( z^2 = [x, z] = 1 \). So \( \langle x, a \rangle = z \in \Omega(N) \), as desired.
We now reduce the proof of our main theorem to a special case which is applicable to the different situations we have to consider.

5.5.7 Lemma. Suppose that Hypothesis 5.5.1 is satisfied and that in addition \( p = 2 \), \( N \) is an \( M \)-group with cyclic commutator subgroup \( N' \) and one of the following holds:

(a) \( N'/N''(N) \) is not cyclic, or
(b) \( \Omega_{r-2}(N) \leq Z(G) \).

Then \( |N'| \leq 2 \).

Proof. We argue by induction on \( |G| \) and first note that the assumptions of the lemma are inherited by \( G/\Omega(G) \). Indeed \( N\Omega(G)/\Omega(G) \simeq N/\Omega(N) \) is clearly an \( M \)-group of exponent \( 2^{r-1} \) with cyclic commutator subgroup. If (a) holds for \( N \), then it also holds for \( N/\Omega(N) \) except possibly when \( r \leq 2 \); but in this case, by (5), \( N \) is abelian and we are done. And if (b) holds, then \( \Omega_{r-2}(N) \leq C_N(a) \) is cyclic by (10). This is equivalent to the type of \( N \) being of the form \((2^r, 2^k, \ldots)\) where \( k \leq r - 2 \) and this is preserved in \( N/\Omega(N) \); hence \( \Omega_{r-3}(N/\Omega(N)) \) is cyclic. Thus \( \Omega_{r-2}(N) = \langle u^{2^{r-2}} \rangle \) for \( u \in N \) with \( o(u) = 2^r \) and \( \Omega_{r-3}(\Omega(G)/\Omega(G)) = \langle u^{2^{r-2}} \Omega(G) \rangle \). Applying (68) with \( x, \alpha \) replaced by \( u, y \) (\( y \in N \)), we obtain \( [u^{2^{r-2}}, y]\alpha \in \Omega(G) \) for all \( y \in N \) and hence, finally, that \( \langle u^{2^{r-3}} \Omega(G) \rangle \leq Z(G/\Omega(G)) \). Thus (b) holds in \( G/\Omega(G) \). The induction assumption implies that \( |N\Omega(G)/\Omega(G)| \leq 2 \) and, since \( N' \) is cyclic, it follows that \( |N'| \leq 4 \). We want to show that \( |N'| \leq 2 \); so we suppose, for a contradiction, that \( |N'| = 4 \). By (11d), \( e_1 \in N' \); so

\[
ed_1 \]

\( N' \) is a cyclic subgroup of order 4 of \( N \) containing \( e_1 \).

Define \( Q \) as in (21) and choose \( u \) and \( w \) as in (65) and (66); then \( N = Q\langle u \rangle \) and \( u^{2^{r-1}} = e_1 \). Since \( e_1 \notin Q \) and \( N' \) is cyclic, \( Q \cap N' = 1 \) and hence \( Q \simeq QN'/N' \) is abelian. Then (55) implies that \( \Omega_{r-2}(N) \leq Q\langle u^4 \rangle \) centralizes \( Q \). Thus

\[
(70) \quad Q \text{ is abelian and } \Omega_{r-2}(N) \leq C_N(Q).
\]

We show next that we may choose \( u \) with the additional property that

\[
(71) \quad [u, a] \in \Omega_{r-2}(N).
\]

This is clear if (b) holds; since then \( \Omega_2(\langle u \rangle) \leq \Omega_{r-2}(N) \leq Z(G) \) and (68) implies (71). So suppose that (a) is satisfied. Then \( N/\Omega_{r-2}(N) \) is not cyclic and \( Q \not\leq \Omega_{r-2}(N) \) since \( N = Q\langle u \rangle \). Thus \( 2^{r-1} \leq o(w) = \text{Exp } Q \). If \( o([u, w]) \leq 2 \), then \( [u, w] \in Z(N) \) and hence \( [u^2, w] = [u, w]^2 = 1 \). It would follow that \( w \in Z(\langle Q, u^2 \rangle) \) and \( o(w) = \text{Exp } Q, u^2 \rangle \). By 2.3.16, \( \langle Q, u^2 \rangle \) would be abelian and (56) would imply that \( N' \) is elementary abelian, contradicting (69). Thus \( o([u, w]) = 4 \) and hence \( N' = \langle z \rangle \)

where \( z = [u, w] \). Since \( N' \leq G \), either \( z^a = z \) or \( z^a = z^{-1} = ze_1 \); in the latter case, \( (ze_2)^a = ze_1e_2e_1 = ze_2 \). Since \( e_1 \in \langle u \rangle \) and \( \langle e_2e_1 \rangle \in \langle w \rangle \), we obtain \( e_2 \in \langle u, w \rangle \) and hence \( H = \langle u, w \rangle \) contains an element \( x \), namely \( x = z \) or \( x = ze_2 \), such that \( x^a = x \) and \( x^2 = e_1 \); the latter follows from \( (ze_2)^2 = z^2e_2^2 = z^2 = e_1 \) where we use 5.5.6 to get \( e_2 \in Z(N) \). Since \( \langle u \rangle \cap \langle w \rangle = 1 \), the subgroup \( H \) is of type \((2^r, 2^r)\) or \((2^r, 2^{r-1})\) and we claim that there exists \( v \in H \) such that \( v^{2^{r-2}} = x \). This is clear if the type of \( H \) is \((2^r, 2^r) \) since then \( \Omega_{r-2}(H) = \Omega_2(H) \). And if \( s = r - 1 \), then \( H/L \) is of type \((2^{r-1}, 2^{r-1})\) where \( L = \Omega_{r-1}(H) = \langle x^2 \rangle \); thus \( xL \in \Omega(H/L) = \Omega_{r-2}(H/L) \) so that there exists \( g \in H \) such
that \( g^{2r-2} \equiv x \pmod{L} \). It follows that \( g^{2r-2} = x \) or \( g^{2r-2} = x^{-1} \), and in both cases there exists \( v \in H \) such that \( v^{2r-1} = e \) and, by (68), \([v,a] \in \Omega_{r-2}(N)\); so if we replace \( u \) by \( v \), (71) is satisfied and we may assume that (71) holds for \( u \).

Now (71) implies that the group \( \langle u, a \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \) is abelian; hence \( \langle u, a \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \) is an M*-group containing \( \langle u \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \), which is a core-free cyclic subgroup of order 4, by (1) applied to \( G/\Omega_{r-2}(G) \). By (54), \( \langle u \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \neq \langle u \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \). Hence if \( \langle u_1 \rangle = \langle u \rangle = \langle u \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \) and \( \langle u_2 \rangle = \langle u \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \) are two different subgroups of order 4 in the abelian group \( \langle u, a \rangle \Omega_{r-2}(G)/\Omega_{r-2}(G) \), and therefore their join contains the socle of this group. Let \( \langle c \rangle = \Omega_{r}(\langle a \rangle) \). Then \( u^2 \) and \( c^2 \) have order 2 modulo \( \Omega_{r-2}(G) \) and it follows that

\[(72) \quad \langle u^2, c^2 \rangle \leq \langle u_1, u_2 \rangle \Omega_{r-2}(G).
\]

By (23), \( N^o = \Omega(\langle a \rangle) = \Omega(\langle u \rangle, \Omega_{r-1}(Q^o)) \cap \langle u_1 \rangle \). Note that \( Q \cap \langle u_1 \rangle = 1 \) and \( Q = N \cap N^o \leq N^o \). As a projective image of \( N \), the subgroup \( N^o \) is an \( M \)-group. By (48) there exists \( k \in N \) such that \( k \equiv 1 \pmod{4} \) and \( x^w = x \). Since \( u_1 \in \langle u, a \rangle \Omega_{r-2}(G) = \langle u, a \rangle \Omega_{r-2}(N) \) and, by (71), this group is abelian modulo \( \Omega_{r-2}(N) \), we obtain \([a^{-1}, u_1^{-1}] \in \Omega_{r-2}(N) \leq C_G(Q) \), by (70). Thus (49) implies that conjugation by \( u_1 \) also raises elements to the power \( k \) in \( Q \). Since \( [N/Q, Q] = 1 \) and \( \langle u_1 \rangle \Omega_{r-1}(Q^o) \) lies in the maximal subgroup \( Q \langle u_2 \rangle \) of \( N \) containing \( Q \), and, since \([u_2, x] = [u, x]^w[u, x] = [u, x]^2 = 1 \) for \( x \in Q \), it follows that \( \langle Q \langle u_2 \rangle \rangle = Q \langle u_2 \rangle \) has order at most 2. By (50), \( x^w = u^k \) for all \( x \in \Omega_{r-1}(Q^o) \). Similarly, if we apply our results to \( \sigma^{-1} \) in place of \( \sigma \), we get that \( u_2 \) induces a power automorphism \( x \to x^k \) in \( Q = N \cap N^o \) and \( \tilde{Q}^o \) and therefore also in \( \Omega_{r-1}(\tilde{Q}) \). We claim that

\[(73) \quad \Omega_{r-1}(Q^o) = \tilde{Q}^o \Omega_{r-1}(\tilde{Q});
\]

then it will follow that, in particular,

\[(74) \quad \langle u_1, u_2 \rangle \text{ induces a group of power automorphisms in } Q.
\]

To prove (73), first note that by (21) and (22), \( Q^o = \Omega(\langle a \rangle) = \Omega_{r}(N) \) where \( p^s = \text{Exp } Q \) and \( s \) is the smallest integer such that \( N/\Omega_{r}(N) \) is cyclic. If \( s = r - 1 \), then \( \Omega_{r-1}(Q^o) = \Omega_{r-1}(N) \) and, similarly, \( \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) = \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) \). So suppose that \( s = r \), that is \( Q = \Omega_{r-1}(Q^o) \). Since \( N^o = \Omega_{r-1}(N) \leq 4 \), by (57); on the other hand, \( u \) and \( w \) are independent elements of order 2 and hence \( [N/\Omega_{r-1}(N) = 4 \) and \( Q = Q_1 \times \langle w \rangle \) where \( \Omega_{r-1}(Q^o) < 2 \). So if \( v: N \to N \) is the homomorphism defined by \( x^v = x^{2^r} \) for \( x \in N \), then by (11c), \( N^v = \langle e_1, e_2 \rangle \). Since \( \Omega_{r-1}(Q^o) = \Omega_{r-1}(N) \) and \([N/Q, Q] = 1 \) a chain of length 2, there exists \( x \in Q^o \) such that \( Q(x) = N \) and \( Q \cap \langle x \rangle = 1 \). As \( \Omega_{r-1}(Q^o) \cap \langle x \rangle = 1 \), we have \( Q \langle x^2 \rangle \leq \Omega_{r-1}(Q^o) \leq v^{-1} \langle e_2 e_1 \rangle < N \). But \( \tilde{Q}^o \langle x^2 \rangle \) is a maximal subgroup of \( N \) and it follows that \( \Omega_{r-1}(Q^o) = v^{-1} \langle e_2 e_1 \rangle \). The same argument with \( Q, Q^o \) replaced by \( \tilde{Q}, \tilde{Q}^o \), \( \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) = \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) \) shows that \( \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) = v^{-1} (Q^o)^v \). Now \( \tilde{Q} \cap \langle e_1, e_2 \rangle = \langle e_2 \rangle \) since, by (60), \( \langle e_2 e_1 \rangle = \langle e_2 \rangle \leq \Omega_{r-1}(Q^o) \cap N = \tilde{Q} \) and \( \langle e_2 e_0 \rangle = \langle e_1 \rangle = \Omega_{r-1}(Q^o) \). Therefore \( \tilde{Q}^o \cap \tilde{Q} = \langle e_2 \rangle \) and, since \( \Omega_{r-1}(Q^o) = \Omega_{r-1}(Q^o) \), we obtain \( \tilde{Q}^o = \langle e_2 \rangle \). Thus \( \tilde{Q}^o = \langle e_2 \rangle \) and so \( \tilde{Q}^o \Omega_{r-1}(\tilde{Q}) = v^{-1} \langle e_2 e_1 \rangle = \Omega_{r-1}(Q^o) \). This proves (73) and (74).

By (74) and (70), every subgroup of \( Q \) is normalized by \( \langle u_1, u_2 \rangle \Omega_{r-2}(N) \). Now \( \Omega_{r-2}(\langle a \rangle) = \langle c^4 \rangle \) and, by (72), \( \langle u_1, u_2 \rangle \Omega_{r-2}(G) = \langle u_1, u_2 \rangle \Omega_{r-2}(N) \langle c^4 \rangle \) contains \( c^2 \);
therefore \( e^4 \in \Phi(\langle c^2 \rangle) \) lies in the Frattini subgroup of this group. Thus \( \langle u_1, u_2 \rangle \Omega_{-2}(G) = \langle u_1, u_2 \rangle \Omega_{-2}(N) \) and now (72) implies that \( u^2 \) normalizes every subgroup of \( Q \). Thus \( u^2 \) induces a universal power automorphism in the abelian group \( Q \); since \([u^2, w] \in N' \cap \langle w \rangle = 1 \) and \( o(w) = \exp Q \), \( u^2 \) centralizes \( Q \) and \( Q \langle u^2 \rangle \) is abelian. Again by (56), \( N' \) is elementary abelian, a final contradiction. \( \square \)

We come now to the main result of this section.

**5.5.8 Theorem** (Busetto and Napolitani [1991]). Suppose that Hypothesis 5.5.1 is satisfied and \( p = 2 \). Then \( N \) is an \( M \)-group and \( |N'| \leq 2 \).

**Proof.** We use induction on \( |N| \) and keep the notation introduced above. By (5) and (6), \( N \) is abelian if \( \exp N = 2^r \leq 4 \) and cyclic if \( m \leq 1 \). Thus we may assume that \( r \geq 3 \) and \( m \geq 2 \). As in the proof of Menegazzo's theorem we apply the induction assumption to various projectivities. First of all, by (3), \( \varphi \) induces a projectivity in \( G/\Omega(G) \) satisfying Hypothesis 5.5.1 and hence \( |N'\Omega(G)/\Omega(G)| \leq 2 \); it follows that \( N' \leq \Omega_2(G) \). Now we apply the induction assumption to the projectivity induced by \( \sigma \) in \( G/K \) and obtain that \( |N'K/K| \leq 2 \). By (11c) applied to \( G/K \), \( N'/K \) contains only one \( a \)-invariant subgroup of order 2 and since, by (19), \( K \) is cyclic and contains \( e_1 \), this subgroup is \( \langle e_2 \rangle K \). Thus \( N' \leq \langle e_2 \rangle K \cap \Omega_2(G) = \langle e_2 \rangle \Omega_2(K) \). By 5.5.6 and (20), both factors are central in \( N \) and hence

\[
(75) \quad N' \leq \langle e_2 \rangle \times \Omega_2(K) \leq Z(N).
\]

Again let \( \Omega_\phi(\langle a \rangle) = \langle c \rangle \). Since \( N' \leq \Omega_2(N) \), it follows that \( N\Omega_2(G)/\Omega_2(G) \) is abelian; therefore by (3) and 5.5.3 there exists \( k \in N \) such that \( c \) induces the power \( k \) in \( N\Omega_2(G)/\Omega_2(G) \). By 5.5.6, \( \Omega(G) \leq Z(\Omega_\phi(\langle a \rangle)) \) and \( \Omega_2(G)/\Omega(G) \leq Z(\Omega_\phi(\langle a \rangle)/\Omega(G)) \) and hence (52) implies that \( c^4 \) induces the power \( k^4 \) in \( N\Omega_2(G) \). In particular,

\[
(76) \quad c^4 \text{ acts as a power automorphism on } N.
\]

We make another remark that will be used later. Suppose that \( z \in N \) such that \( o(z) = 4 \) and \( z^z = z^{-1} \). Then \( (az)^2 = a^2 \) so that \( \langle az \rangle \) and \( \langle a \rangle \) are cyclic subgroups of \( \langle a, z \rangle \) generating this group and intersecting in \( \langle a^2 \rangle \). Their images under \( \varphi \) are cyclic groups generating \( \langle a, z \rangle^\varphi \) and intersecting in \( \langle b^2 \rangle \) and it follows that \( \langle b^2 \rangle \leq Z(\langle a, z \rangle^\varphi) \). In particular, \( b^2 \) centralizes \( \langle z \rangle^\varphi \) and therefore every conjugate of \( \langle z \rangle^\varphi \) in \( N\langle b^2 \rangle \) is contained in \( N \). This shows that the normal closure of \( \langle z \rangle^\varphi \) in \( N\langle b^2 \rangle \) is contained in \( N \) and hence \( \langle z \rangle^\varphi \leq L^\varphi \) if \( L^\varphi = \overline{N\langle b^2 \rangle} \); thus \( z \in L \). Since \( L \leq N \cap N_{(b^2)}^\varphi = R \), (63) shows that \( e_2 e_1 \notin L \). Finally note that if \( N' \) is cyclic and \( N' \leq K \), then by (11d), \( e_1 \in N' \) and hence \( N' = \langle z \rangle \) has order 4; furthermore, by (20), \( C_N(a) = K \) and therefore \( z^z = z^{-1} \). Thus we have shown:

\[
(77) \quad \text{Let } M = N\langle a^2 \rangle \text{ and } L = N_{\varphi^2}. \text{ If } z \in N \text{ such that } o(z) = 4 \text{ and } z^z = z^{-1}, \text{ then } z \in L; \text{ in particular, } N' \leq L \text{ if } N' \text{ is cyclic and not contained in } K. \text{ Furthermore } e_2 e_1 \notin L.
\]

Now let \( Q, R, u, w \) be as in (65) and (66). Then \( Q' \leq N' \cap Q \leq \langle e_2 \rangle \times \Omega_2(K) \cap Q = \langle e_2 e_1 \rangle \), by (63). Since \( w^{2^{2-1}} = e_2 e_1 \), we see that \( Q' \leq \langle w \rangle \) and hence \( \langle w \rangle \leq Q \) and \( Q \cap R \cong Q/\langle w \rangle \) is abelian. Thus
5.5 Normal subgroups of $p$-groups with cyclic factor group

(78) $Q' \leq \langle e_2 e_1 \rangle$, $Q = \langle w \rangle (Q \cap R)$, $\langle w \rangle \cap (Q \cap R) = 1$, $\langle w \rangle \leq Q$ and $Q \cap R$ is abelian.

Since $Q = N \cap N^a$ and $R = N \cap N^{a'}$, it follows that $Q \cap R = N \cap N^a \cap N^{a'} \leq N^a \cap N^{a'} = Q^a$ and $|Q^a|: Q \cap R| = |Q: Q \cap R| = |\langle w \rangle| = 2^l$. Now $\langle w \rangle \leq Q$, so $\langle w \rangle^a$ is permutable in $Q^a$ and since, by (60), $\langle e_2 e_1 \rangle^a = \langle e_2 e_0 \rangle$, we have $\Omega(\langle w \rangle^a) \not\leq N$. Thus $(Q \cap R) \cap \langle w \rangle^a = 1$ and so $Q^a = (Q \cap R)\langle w \rangle^a$. It follows that $N \cap Q^a = (Q \cap R)(N \cap \langle w \rangle^a) = Q \cap R \leq Q^a$ and hence for every $X \leq Q \cap R$, there results $X \langle w \rangle^a \cap (Q \cap R) = X(\langle w \rangle^a \cap (Q \cap R)) = X \leq X \langle w \rangle^a$. So we have shown:

(79) Let $\langle w \rangle^a = \langle w_1 \rangle$. Then $Q^a = (Q \cap R)\langle w_1 \rangle, (Q \cap R) \cap \langle w_1 \rangle = 1$, $Q \cap R \leq Q^a$, $\langle w_1 \rangle$ is permutable in $Q^a$ and induces a group of power automorphisms in $Q \cap R$.

By (7), $(w u^{2r} e^{2r})^2 = w^{2s} u^{2r} e^{2r} = e_2 e_1 e_1 e_0 = e_2 e_0 = w_1^{2s}$ and

(80) $w_1 \equiv w u^{2r} e^{2r} \bmod \Omega_{r+1}(G)$.

Now we distinguish the cases $s = r$, $s = r - 1$, $s \leq r - 2$ and split the first of these into two.

**Case 1:** $s = r$, $\text{Exp}(Q \cap R) = 2^r$.

In this case we show that $N$ is even abelian. Let $x \in Q \cap R$ of order $2^r$. Then by (65) and (66), $\mathcal{U}_{r-1}(N) \geq \Omega(\langle x \rangle) \times \Omega(\langle w \rangle) \times \Omega(\langle u \rangle)$ and hence by (7), $|N/\Omega_{r-1}(N)| \geq 8$. By induction, however, $N/\Omega(N) \simeq N/\Omega(G)/\Omega(G)$ is an $M$-group with cyclic commutator subgroup; it follows from (57) that $N/\Omega(N)$ is abelian. Thus $N' \leq \Omega(N)$ and (75) yields that

(81) $N' \leq \langle e_1, e_2 \rangle$.

If $|N/\Omega_{r-1}(N)| \geq 16$, then $|N/K|/\Omega_{r-1}(N)| \geq 8$; again by induction, $H/K$ is an $M$-group with cyclic commutator subgroup and hence is abelian. Then $N' \leq \langle e_1, e_2 \rangle \cap K = \langle e_1 \rangle$ and, by (25), $N$ is an $M$-group. But then again (57) yields that $N$ is abelian. Thus we are left with the case that $|N/\Omega_{r-1}(N)| = 8$ in which

(82) $N = \langle x, w, u \rangle_{\Omega_{r-1}(N)}$.

Now (65) and (66) show that $a$ normalizes $\langle u \rangle_{\Omega_{r-1}(N)}$ and $\langle w, u \rangle_{\Omega_{r-1}(N)}$. Thus, applying (11c) to $G/\Omega_{r-1}(G)$, we see that $\langle u \rangle_{\Omega_{r-1}(G)}/\Omega_{r-1}(G)$ and $\langle w, u \rangle_{\Omega_{r-1}(G)}/\Omega_{r-1}(G)$ are the only normal subgroups of order 2 and 4, respectively, of $G/\Omega_{r-1}(G)$ contained in the elementary abelian group $N_{\Omega_{r-1}(G)}/\Omega_{r-1}(G)$ of order 8; in particular, $(\langle x \rangle_{\Omega_{r-1}(G)})^G = N_{\Omega_{r-1}(G)}$. Since $N = (Q \cap R)\langle w \rangle\langle u \rangle$, (7) shows that $\langle x \rangle_{\Omega_{r-1}(N)} \leq (Q \cap R)\langle w^2 \rangle\langle u^2 \rangle$ so that $||(Q \cap R)\langle w^2 \rangle\langle u^2 \rangle||^G = N$. Now $N' \leq Z(N) \cap \Omega(N)$ implies that $u^2, w^2 \in Z(N)$. Therefore $(Q \cap R)\langle w^2 \rangle\langle u^2 \rangle$ is abelian and every conjugate of it contains and hence centralizes the normal subgroup $\Omega_{r-1}(N)$. It follows that

(83) $\Omega_{r-1}(N) \leq Z(N)$.

By (65) and (66), $u^a \equiv u$ and $w^a \equiv w u \bmod \Omega_{r-1}(N)$ and by (11c) applied to $G/\Omega(G)$ there exists $z \in N$ such that $x^a \equiv z w \bmod \Omega_{r-1}(N)$. Then $z^{a^2} \equiv (zw)^a \equiv zu$
and \( w^2 \equiv (wu)^2 \equiv w \pmod{\Omega_{r-1}(N)} \); since \( N' \leq \langle e_1, e_2 \rangle \leq C_N(a^2) \) and \( N' \leq \Omega_{r-1}(N) \leq Z(N) \), it follows that \( [z, w] = [z, w]^2 = [z^2, w^2] = [zu, w] = [z, w][u, w] \). Thus \([u, w] = 1 \) and \( \langle w \rangle \leq N \) since \( \langle w \rangle \leq Q \) and \( N = Q \langle u \rangle \). Therefore \( \langle w, z \rangle \) lies in \( \langle w \rangle \cap \langle e_1, e_2 \rangle = \langle w^{2r^2-1} \rangle \) and hence \( w^2 = w^{1+2r^2-1} \) where \( \epsilon \in \{0, 1\} \). Since \( w^2 \equiv w \pmod{\Omega_{r-1}(N)} \), we see that \( H = \langle w, u \rangle \Omega_{r-1}(N) = \langle w, w^2 \rangle \Omega_{r-1}(N) \) is an abelian normal subgroup of \( G \) and has index 2 in \( N \); therefore it contains \( \langle a^{-1}, z^{-1} \rangle \). By (49), \( (w^2)^2 = (w^2)^{1+2r^2}, \) by (83), \( h^2 = h = h^{1+2r^2} \) for all \( h \in \Omega_{r-1}(N) \) and then also for all \( h \in H \). But \( H \langle z \rangle = N \) and Iwasawa’s theorem implies that \( N \) is an \( M \)-group. By (6), \( N \) and its projective image \( N^a \) are \( M^* \)-groups. By (23), \( N^a = \langle u \rangle^a \) and \( Q \cap \langle u \rangle^a = 1 \); furthermore \( Q = N \cap N^a \leq N^a \). So 2.3.14 shows that every subgroup of \( Q \) is normal in \( N^a \); in particular, \( Q \cap R \leq Q \) and by (78), \( Q = (Q \cap R) \times \langle w \rangle \) is abelian. By (21) and (22), \( QQ^a = N \) and hence \( Q \cap Q^a \leq Z(N) \). Since \( \langle N/Q \rangle \) is a chain and \( |N/\Omega_{r-1}(N)| = 2^3 \), there exists an element of order \( 2^r \) in \( Q \cap Q^a \) and, by 2.3.16, \( N \) is abelian. This finishes Case 1.

**Case 2:** \( s = r, \) \( \text{Exp}(Q \cap R) < 2^r \).

By (65), \( N_1 = \Omega_{r-1}(N) \langle u \rangle \) is an \( a \)-invariant subgroup of \( G \) so that, by (2), \( G_1 = N_1 \langle u \rangle, \) \( N_1 \) and the projectivity induced by \( \varphi \) in \( G_1 \) satisfy Hypothesis 5.5.1. By induction, \( N_1 \) is an \( M \)-group and \( |N_1'| \leq 2 \). Since \( N_1' \) is \( a \)-invariant, (11c) yields that \( N_1' \leq \langle e_1 \rangle \leq \langle u \rangle \). By (23) applied to \( N_1 \) and \( Q_1 = N_1 \cap N_1' \), we get that \( N_1 = Q_1 \langle u \rangle, \) \( Q_1 \cap \langle u \rangle = 1 \) and \( N_1^c = Q_1 \langle u^a \rangle, \) \( Q_1 \cap \langle u^a \rangle = 1 \). Since \( |N_1 : \Omega_{r-1}(N_1)| = 2 \), it follows that \( \Omega_{r-1}(N) = \Omega_{r-1}(N_1) = Q_1 \langle u^2 \rangle \). Furthermore \( Q_1 \cap N_1' = 1 \) implies that \( Q_1 \simeq Q_1 N_1'/N_1' \) is abelian, and \( |N_1'| \leq 2 \) yields that \( u^2 \in Z(N_1) \). Thus

(84) \( \Omega_{r-1}(N) = Q_1 \langle u^2 \rangle \) is abelian.

Let \( \langle u^a \rangle = \langle u_1 \rangle \). Then by (48), \( u_1 \) induces a power automorphism in \( Q_1 \leq N_1' \).

From \( \langle e_1 \rangle^a = \langle e_1 e_0 \rangle \), there follows \( u_1^{-1} = (u_1 u)^{2r^2}, \) and hence by (7), \( uc = u_1 y \) for some \( y \in \Omega_{r-1}(G) \). By 5.5.3 applied to \( G^* = \Omega_{r-1}(N) \langle a \rangle = \Omega_{r-1}(G) \langle a \rangle \), elements of \( \Omega_{r-1}(G) \) induce power automorphisms in \( \Omega_{r-1}(N) \), and it follows that \( uc = u_1 y \) induces a power automorphism in \( Q_1 \). By (65), \( [u, a] \in \Omega_{r-1}(N) \) and \( [c, a] = 1 \). Thus \( [a^{-1}, (uc)^{-1}] \in \Omega_{r-1}(N) \leq C_G(Q_1) \) and hence by (49), \( uc \) induces in \( Q_1^a \) the same power as in \( Q_1 \). Since \( s = r \), we see that \( N_1/\Omega_{r-3}(N_1) \) is not cyclic; hence (21) and (22) applied to \( G_1 \) yield that \( Q_1^a \simeq \Omega_{r-1}(N_1) = \Omega_{r-1}(N) \) and this group is abelian. So \( uc \) induces a power automorphism in \( \Omega_{r-1}(N) \). By (79), \( w_1 \) induces a power automorphism in \( Q \cap R \) and, by (80), \( w_1 = wucz \) for some \( z \in \Omega_{r-1}(G) \). Then \( Q \cap R \leq \Omega_{r-1}(N) \) since \( \text{Exp}(Q \cap R) < 2^r \). Thus \( w_1, uc, z \) induce power automorphisms in \( Q \cap R \) and hence so does \( w \). In particular, \( (Q \cap R)^w = Q \cap R \) and (78) shows that

(85) \( Q \) is abelian.

Since \( \Omega(\langle w^a \rangle) = \langle e_2 e_1 \rangle^a = \langle e_2 \rangle \) and \( Q \cap \langle e_2 \rangle = 1 \), it follows that \( N = Q \langle u \rangle = Q \langle w^a \rangle \), by (23). Similarly, by (63), \( Q \cap Q^a \cap \langle e_0, e_1, e_2 \rangle = 1 \) and since \( Q \cap Q^a \) is permutable in \( Q \) with \( [Q/Q \cap Q^a] \) a chain, (9) shows that \( Q = (Q \cap Q^a) \langle w \rangle \); thus \( N = (Q \cap Q^a) \langle w \rangle \langle w^a \rangle \). Now \( Q \) and \( Q^a \) are abelian and \( QQ^a \geq Q \langle w^a \rangle = N \) so that \( Q \cap Q^a \leq Z(N) \). By (75), \( N' \leq Z(N) \) and it follows that

(86) \( N' = \langle [w, w^a] \rangle \) is cyclic of order at most 4.
Since \( r = s \), the group \( N/\Omega_{r-2}(N) \) is not cyclic, and therefore it remains to be shown that \( N \) is an M-group; then the assumptions of 5.5.7(a) will be satisfied and it will follow that \( |N'| \leq 2 \).

For this, suppose first that \( N' \leq K \). Since \( Q \cap K = 1 \), we see that \( N/K \) is abelian of exponent 2\(^r\), and by 5.5.3 there exists \( k \in \mathbb{N} \) such that \( k \equiv 1 \pmod{4} \) and \( x^{2^k} = x^k \pmod{K} \) for all \( x \in N \). Now \( Q \leq N^\sigma = Q\langle u_1 \rangle \) implies that \( x^{-k}x^{2^k} \in Q \cap K = 1 \) for all \( x \in Q \). Thus \( x^{2^k} = x^k \) for all \( x \in Q \) and, by 2.3.4, \( N^\sigma \) is an M-group. Thus \( N \) is an M-group, as desired.

Now suppose that \( N' \not\leq K \). Let \( M = N\langle a^2 \rangle \) and \( L = N_M \). By 5.4.6, \( \varphi \) induces a projectivity from \( M/L \) to \( M/\overline{L} \) for which Hypothesis 5.5.1 is satisfied. By (77), \( N' \leq L \) and \( e_2 e_1 \not\leq L \). Thus \( \langle w \rangle \cap L = 1 \) and hence \( N/L \) is abelian of exponent 2\(^r\). By 5.5.3 applied to \( M/L \), the element \( c \) induces a power \( h \equiv 1 (\mod{4}) \) in \( N/L \) and hence, by (51), also in \( N/L_G \). Since \( u_1 \in \Omega_c(G) = N\langle c \rangle \) and \( N/L_G \) is abelian, \( u_1 \) induces a power \( k \equiv 1 \pmod{4} \) in \( N/L_G \). Now \( e_2 e_1 \not\leq L \) together with (11c) implies that \( \Omega(L_G) \leq \langle e_1 \rangle \) so that \( Q \cap L_G = 1 \). Then again \( Q \leq N^\sigma = Q\langle u_1 \rangle \) implies that \( x^{-k}x^{2^k} \in Q \cap L_G = 1 \) for all \( x \in Q \) and that \( N^\sigma \) is an M-group. Thus also \( N \) is an M-group and this finishes Case 2.

**Case 3: \( s = r - 1 \).**

We observe that \( N/\Omega_{r-2}(N) \) is not cyclic and, by (67), we may assume that

\[
(87) \quad u \in R \text{ so that } R = (Q \cap R)\langle u \rangle \text{ and } N = R\langle w \rangle = (Q \cap R)\langle u \rangle\langle w \rangle.
\]

Since \( N = Q\langle u \rangle \), we have \( \Omega_{r-1}(N) = Q\langle u^2 \rangle \) and the induction assumption yields that

\[
(88) \quad \Omega_{r-1}(N) \text{ is an M-group and } \Omega_{r-1}(N)' \leq \langle e_1 \rangle,
\]

by (11c). Since \( Q \cap \langle e_1 \rangle = 1 \), it follows that

\[
(89) \quad Q \text{ is abelian.}
\]

We want to show next that \( R' \leq \langle e_1 \rangle \). If \( \text{Exp}(Q \cap R) = 2^{r-1} \), then \( \Omega_{r-1}(N) \) has three independent elements of order \( 2^{r-1} \) and cyclic commutator subgroup and therefore, by (57), it is abelian. Then \( N = \Omega_{r-1}(N)\langle u \rangle \) and (75) imply that \( N' \) is elementary abelian and \( N' \leq \langle e_1, e_2 \rangle \). Thus \( R' \leq \langle e_1, e_2 \rangle \cap R = \langle e_1 \rangle \), by (63). Now suppose that \( \text{Exp}(Q \cap R) < 2^{r-1} \) and consider \( S \) as defined in (63). Then (66) implies that \( Q \cap R \leq \Omega_{r-2}(Q) = (Q \cap S)\langle w^2 \rangle \) and by (67) there exists \( u' \in S \) such that \( S = (Q \cap S)\langle u' \rangle \) and \( Q\langle u' \rangle = N \). Now \( R = (Q \cap R)\langle u \rangle \), the commutativity of \( Q \) and \( N' \leq Z(N) \) imply that

\[
R' = [Q \cap R, \langle u \rangle] \leq [(Q \cap S)\langle w^2 \rangle, Q\langle u' \rangle] \leq [Q \cap S, \langle u' \rangle][\langle w^2 \rangle, \langle u' \rangle] \leq S'\langle e_1 \rangle,
\]

since \([w^2, u'] = [w, u']^2 \in \mathfrak{U}(N') = \langle e_1 \rangle\), by (75). By (63) and (64), \( S' \leq \langle e_2 \rangle K \cap S = K \) and so \( R' \leq R \cap K = \langle e_1 \rangle \). Thus in any case,

\[
(90) \quad R' \leq \langle e_1 \rangle.
\]
We wish to apply Lemma 5.5.7(a) and therefore have to show that \( N' \) is cyclic and \( N \) is an \( M \)-group. Now \( N = (Q \cap R) \langle w \rangle \langle u \rangle, u \in R, Q \) abelian and \( N' \leq Z(N) \) imply that

\[
N' = [Q \cap R, \langle w \rangle][Q \cap R, \langle u \rangle][\langle w \rangle, \langle u \rangle] \leq Q'R'[\langle w, u \rangle] \leq \langle e_1 \rangle[\langle w, u \rangle].
\]

Suppose, for a contradiction, that \( N' \) is not cyclic. Then \( e_1 \notin \langle [w, u] \rangle \) and it follows from (75) that \( o([w, u]) = 2 \) and \( [w, u] = e_2e_1 \) or \( [w, u] = e_2 \); in any case, \( N' \leq \Omega(N) \).

Thus \( N\Omega(G)/\Omega(G) \) is abelian and, by 5.5.3, \( c \) acts as a power automorphism on \( N\Omega(G)/\Omega(G) \) and hence also on \( N/\Omega(N) \). By (52) and 5.5.6, \( c^2 \) acts as a power automorphism on \( N \). Since \( N = R \langle w \rangle \) and \( R \cap \langle w \rangle = 1 \), it follows that \( \Omega_{r-2}(N) \leq R \langle w^2 \rangle \). Clearly \( [w^2, u] = [w, u]^2 = 1 \) and \( R' \leq \langle e_1 \rangle \leq \langle u \rangle \) implies \( \langle u \rangle \leq R \); thus \( \langle u \rangle \) is normalized by \( \Omega_{r-2}(N)c^2 = \Omega_{r-2}(G) \).

Now assume first that \( [w, u] = e_2e_1 \); the other case will be similar. Then \( [w, u] \in \langle w \rangle \) and hence \( \langle w \rangle \leq Q\langle u \rangle \) since \( Q \) is abelian. By (67c), \( R = N \cap N^e = N^e \leq N^{e^2} = R\langle w \rangle^{e^2} \) and \( R \cap \langle w \rangle^{e^2} = 1 \); let \( \langle w \rangle^{e^2} = \langle w_2 \rangle \). Since \( \langle w \rangle \leq N \), we obtain that \( \langle w_2 \rangle \) is permutable in \( N^{e^2} \), and hence \( \langle u \rangle\langle w_2 \rangle \cap R = \langle u \rangle\langle w_2 \rangle \cap R = \langle u \rangle \leq \langle w \rangle \langle w_2 \rangle \). Because of \( w_2^{e^2} = e_2e_1e_0 = (w_2c^2)^{e^2} \), we have \( w_2 = w_2c^2x \) for some \( x \in \Omega_{r-2}(G) \), by (7). Now \( w_2, c^2 \) and \( x \) normalize \( \langle u \rangle \), as we have seen, and hence so does \( w \). But this yields \( e_2e_1 = [w, u] \in \langle u \rangle \), a contradiction.

Now assume that \( [w, u] = e_2 \). Then we use \( wu^2 \) instead of \( w \) for our argument. As \( [w^2, u] = [w, u] = e_2 = (w^2)^{e^2} \), the subgroup \( \langle w^2 \rangle \) is normalized by \( u \); furthermore it is centralized by \( Q \) since \( Q \) is abelian and \( u^2 \in Z(N) \). Thus \( \langle w^2 \rangle \leq N \). By (67c), \( N^{e^2} = R\langle w^2 \rangle^{e^2} \) and hence \( \langle v \rangle = \langle w^2 \rangle^{e^2} \) normalizes \( \langle u \rangle \). Finally, \( v^{e^2} = e_2e_1e_0 = (w^2c^2)^{e^2} \) implies that \( v = wu^2c^2y \) for some \( y \in \Omega_{r-2}(G) \). Now \( v, c^2, y \) normalize \( \langle u \rangle \) and hence so does \( w^2 \). But \( [w^2, u] = e_2 \notin \langle u \rangle \), a contradiction. Thus

(91) \( N' \) is cyclic

and it remains to be shown that \( N \) is an \( M \)-group. To prove this, by (47), it will suffice to show that

(92) \( N/\langle e_1 \rangle \) is an \( M \)-group;

note that, by (88), \( \Omega_{r-1}(N) \) is an \( M \)-group and \( \Omega_{r-1}(N) = \langle e_1 \rangle \) is cyclic.

To prove (92), suppose first that \( N' \leq K \) and again let \( \langle w \rangle^{e^2} = \langle w_2 \rangle \). Since \( Q \cap K = 1 \) and \( s = r - 1 \), \( \text{Exp}(N/K) \geq 2^{r-1} \); on the other hand, \( \Omega_{r-1}(N) = \langle e_1 \rangle \leq K \). Thus \( N/K \) is an abelian group of exponent \( 2^{r-1} \) and, by 5.5.3, \( w_2 \in \Omega_{r-1}(G) \) induces a power automorphism \( x \to x^k, k \equiv 1 \pmod{4} \), in \( N/K \). By (67c), \( R = N \cap N^{e^2} \leq N^{e^2} = R\langle w_2 \rangle \) and hence \( x^{-k}x^{w_2} \in R \cap K = \langle e_1 \rangle \), by (64), for every \( x \in R \). Since \( R/R \cap K \simeq RK/K \) is abelian, it follows from 2.3.4 that \( R\langle w_2 \rangle/\langle e_1 \rangle = N^{e^2}/\langle e_1 \rangle \) is an \( M \)-group. By (61), \( \langle e_1 \rangle^{e^2} = \langle e_1 \rangle \) so that \( N/\langle e_1 \rangle \), as a projective image of \( N^{e^2}/\langle e_1 \rangle \), is also an \( M \)-group.

Now suppose that \( N' \nleq K \). Here, as in Case 2, we first study the projectivity induced by \( \varphi \) in \( M = N\langle a^2 \rangle \) and then use \( saa^{-1} \) instead of \( a^2 \); let \( \langle w_3 \rangle = \langle w \rangle^{saa^{-1}} \).

By (77), \( N' \leq L \) and \( e_2e_1 \notin L \) for \( L = N_{a^2} \). Since \( \Omega_{r-1}(N) = \langle e_1 \rangle \leq N' \leq L \), we have \( \text{Exp}(N/L) \leq 2^{r-1} \); on the other hand, \( \langle w \rangle \cap L = 1 \) and hence \( N/L \) is abelian of exponent \( 2^{r-1} \). By 5.5.3 applied to \( M/L \), the element \( c^2 \) induces a power \( h \equiv 1 \)
5.5 Normal subgroups of $p$-groups with cyclic factor group

Consider $S = N \cap N^{a_{aa^{-1}}}$. By (63), $e_2 \notin S$ and $e_2 \notin L$ since $e_1 \in L$ and $e_2 e_1 \notin L$. Therefore by (11c), $\Omega(S_G) = \langle e_1 \rangle = \Omega(L_G)$ so that $S_G$ and $L_G$ are cyclic. Since $N' \leq L$ and, by (64), $K \leq S$, we see that $\Omega_2(L_G) = N'$ and $\Omega_2(S_G) = \Omega_2(K)$. So $N' \leq K$ implies that $N' \not\leq S$ and hence $S \cap L_G = S \cap N' = \langle e_1 \rangle$. By (67d), $S = N \cap N^{a_{aa^{-1}}} \subseteq N^{a_{aa^{-1}}} = S\langle w_3 \rangle$ and hence $x^{-k}w_3 \in S \cap L_G = \langle e_1 \rangle$ for every $x \in S$. Since $S' \leq S \cap N' = \langle e_1 \rangle$, it follows that $S/\langle e_1 \rangle$ is abelian and, by 2.3.4, $S\langle w_3 \rangle/\langle e_1 \rangle = N^{a_{aa^{-1}}}/\langle e_1 \rangle$ is an $M$-group. By (62), $\langle e_1 \rangle^{a_{aa^{-1}}} = \langle e_1 \rangle$, so that $N/\langle e_1 \rangle$, as a projective image of $N^{a_{aa^{-1}}}/\langle e_1 \rangle$, is also an $M$-group. This finishes the proof of (92) and Case 3.

Case 4: $s \leq r - 2$.

Then $N = Q\langle u \rangle$ where $Q \leq \Omega_{r-2}(N)$ and hence $\Omega_{r-2}(N) = \langle u^{2^{r-2}} \rangle$ is cyclic. Let $\Omega_{r-2}(N) = \langle z \rangle$ and suppose first that $z^a = z$. Then $z \in C_N(a) = K$, by (20), and hence $\Omega_{r-2}(N) = \Omega_2(K)$; thus $\text{Exp}(N/K) \leq 2^{-r}$. By (76), $c^4$ induces a power automorphism in $N$ and hence also in $N/K$. Therefore (24) applied to $G/K$ yields that $N/K$ is abelian and (75) implies that $N' \leq \Omega_2(K) = \Omega_{r-2}(N)$. By induction, $\Omega_{r-1}(N)$ is an $M$-group and so (47) shows that $N$ is also an $M$-group. Since $N' \leq K$ is cyclic and, by (20), $\Omega_{r-2}(N) \leq Z(G)$, all the assumptions of Lemma 5.5.7(b) are satisfied and it follows that $|N'| \leq 2$, as desired.

Now suppose that $z^a = z^{-1}$. Then by (77), $\langle z \rangle \leq L$ and $e_2 e_1 \notin L$ if $M = N\langle a^2 \rangle$ and $L = N^{a_{aa^{-1}}}$. Thus $\Omega_{r-2}(N) \leq L$ and hence $\text{Exp}(N/L) \leq 2^{-r}$. Again $c^4$ induces a power automorphism in $N$ and hence also in $N/L$; therefore (24) applied to the projectivity induced by $\phi$ in $M/L$ yields that $N/L$ is abelian. Now $z^2 = e$, and hence $(ze_2)^a = ze_1 e_2 e_1 = ze_2$. As $C_N(a) = K$, it follows that $\langle ze_2 \rangle = \Omega_2(K)$ and so $N' \leq \langle \langle e_2 \rangle \times \langle ze_2 \rangle \rangle \cap L = \langle z \rangle$, since $e_2 e_1 \notin L$. Thus

(93) $N' \leq \langle u^{2^{r-2}} \rangle = \Omega_{r-2}(N)$; furthermore $e_2 \in \langle u \rangle K$ and $\langle u \rangle \cap K = \langle e_1 \rangle$

since $\langle z \rangle = \Omega_2(\langle u \rangle)$ and $\langle ze_2 \rangle = \Omega_2(K)$. Again by induction, $\Omega_{r-1}(N)$ is an $M$-group and since $N/\Omega_{r-2}(N)$ is abelian and $\Omega_{r-2}(N)$ is cyclic, $N$ is an $M$-group. It remains to be shown that $|N'| \leq 2$. Unfortunately, since $\Omega_{r-2}(N) \not\leq Z(G)$, we cannot apply Lemma 5.5.7 in this case. However, we can proceed as follows. Since $N' \leq Z(N)$ and $\langle u^{2^{r-2}} \rangle$ and $Q \cap \langle u \rangle = 1$, the group $Q$ is abelian, and $[u^2, x] = [u, x]^2 \in \Omega(\langle u \rangle)$ for all $x \in N$. Therefore $u^4 \in Z(N)$ and

(94) $\Omega_{r-2}(N) = Q\langle u^4 \rangle$ and $Q\langle u^{2^r} \rangle/\langle e_1 \rangle$ are abelian.

Since $G/\Omega_{r-2}(N) = N\langle a \rangle/\Omega_{r-2}(N)$ and $N/\Omega_{r-2}(N)$ is cyclic of order 4, (55) shows that $a^4$ centralizes $N/\Omega_{r-2}(N)$. By (5), $\Omega_r(\langle a \rangle) \leq \langle a^4 \rangle$ and it follows that $\Omega_r(G)/\Omega_{r-2}(N)$ is abelian. By (23),

$$\Omega_r(G) = \langle u \rangle \langle u^a \rangle \Omega_{r-2}(N) = \langle u \rangle \Omega_r(\langle a \rangle) \Omega_{r-2}(N) = \langle u \rangle^{a_r} \Omega_r(\langle a \rangle) \Omega_{r-2}(N)$$

and hence there exist $v \in \langle u \rangle^{a_r}$ and $c \in \Omega_r(\langle a \rangle)$ such that $u = vc^{-1}$ (mod $\Omega_{r-2}(N)$). Since $\Omega_r(G)/\Omega_r(\langle a \rangle) \Omega_{r-2}(N)$ is cyclic, $\langle v \rangle = \langle u \rangle^{a_r}$ and, similarly, $\langle c \rangle = \Omega_r(\langle a \rangle)$. Finally, since $\Omega_r(G)/\Omega_{r-2}(N)$ is abelian, we have

(95) $v \equiv uc$ and $v^2 \equiv u^2 c^2$ (mod $\Omega_{r-2}(N)$).
Now $N/\Omega_2(N)$ is abelian and hence by 5.5.3 there exists $\lambda \in N$ such that $\lambda \equiv 1 \pmod{4}$ and $c$ induces the power automorphism $x \mapsto x^4$ in $N/\Omega_2(N)$. Since $N$ centralizes $N/\Omega_2(N)$, this automorphism is also induced by $v$ in $N/\Omega_2(N)$. By (52),

\[ v^2 \text{ and } c^2 \text{ induce the power } \lambda^2 \text{ in } N/\Omega(N). \]

Since $Q \leq N^\sigma = Q\langle v \rangle$ and $N^\sigma$ is an $M$-group, $v$ induces a power $\mu$ in $Q$, by (48). Then $v^2$ induces $\mu^2$ in $Q$ and, by (94) and (95), $u^2c^2$ induces the same power in $Q$. Since $|\Omega_{r-1}(N)/\Omega_{r-2}(N)| = 2$, we have $[u^2, a] \in \Omega_{r-2}(N)$ and so $[a^{-1}, (u^2c^2)^{-1}] \in \Omega_{r-2}(N) \leq C_G(1)$ by (49), $u^2c^2$ induces the power $\mu^2$ in $Q^\sigma$ and then also in the abelian group $Q^\sigma = \Omega_4(N)$, by (21) and (22). By (96), $c^2$ induces the power $\lambda^2$ in $N/\Omega(N)$ and then, by (52), also in $Q\langle u \rangle$. Therefore $u^2c^2$ induces in $\Omega_4(Q) = Q\langle u \rangle \cap \Omega_4(N)$ the powers $\lambda^2$ and $\mu^2$ and it follows that $\lambda^2 \equiv \mu^2 \pmod{2^2}$. So $u^2c^2$ induces the power $\lambda^2$ in $Q$ and, since $Q\langle u^2 \rangle/\langle e_1 \rangle$ is abelian, $u^2c^2$ and $c^2$ induce the same automorphism in $Q\langle e_1 \rangle/\langle e_1 \rangle$; thus

\[ c^2 \text{ induces the power } \lambda^2 \text{ in } Q\langle e_1 \rangle/\langle e_1 \rangle. \]

We want to show, finally, that $c^2$ induces a power automorphism in $N/K$. By (96), $u^2 = u^{2r-1}e$ for some $e \in \Omega(N)$. Since the commutator subgroup of $N/\langle e_1, e \rangle$ has order at most 2, $c^2$ induces the power $\lambda^2$ in $Q\langle u \rangle/\langle e_1, e \rangle = N/\langle e_1, e \rangle$, by (50). And by (51), $c^2$ induces this power in $N/\langle e_1, e \rangle_G$. So if $\langle e_1, e \rangle_G = \langle e_1 \rangle$, we are done. And if $\langle e_1, e \rangle_G \neq \langle e_1 \rangle$, then $\langle e_1, e \rangle = \langle e_1, e_2 \rangle$, by (11c), and (93) shows that $\langle u \rangle K \geq \langle e_1, e \rangle$ and $o(uK) = 2r-1$. Therefore $e \equiv u^{2r-2} \pmod{K}$ for some $e \in \mathbb{Z}$ and, since $\exp Q \leq 2r-2$, $c^2$ induces the power $\lambda^2 + \rho 2^{r-2} \equiv 1 \pmod{4}$ and, since $o(uK) \leq 2$, (50) implies that $c^2$ also induces the power $\lambda^2 + \rho 2^{r-2}$ in $Q\langle u \rangle K = N/K$. Thus in any case, $c^2$ induces a power automorphism in $N/K$. Applying (24) to the projectivity $\sigma$ from $G/K$ to $G/K^\sigma$, we conclude that $N/K$ is abelian; finally, (93) shows that $N' \leq \langle u \rangle \cap K = \langle e_1 \rangle$. Thus $|N'| \leq 2$, as desired. This finishes Case 4 and the proof of Theorem 5.5.8.

By 5.5.2 and 5.5.8, the nilpotency class $c(N) \leq 2$ under Hypothesis 5.5.1. A bound for $c(\overline{N})$ is not known; in Example 5.5.5 and in the known examples for $p$ odd, $c(\overline{N}) \leq 2$. The projectivities between metacyclic groups show that neither $c(G)$ nor $c(\overline{G})$ is bounded. Since $N$ is an $M$-group, $N$ and $\overline{N}$ are metabelian. For the derived lengths of $G$ and $\overline{G}$, we obtain the following final result; note that $d(\overline{G}) = 3$ in Example 5.5.5.

5.5.9 Theorem (Busetto and Napolitani [1991]). Suppose that Hypothesis 5.5.1 is satisfied and let $M$ be the maximal subgroup of $G$ containing $N$. Then $G$ is metabelian and $\overline{G}$ has derived length at most 3; more precisely, $M^\sigma$ is metabelian and $\overline{G}^\sigma$ is elementary abelian.

Proof: We first show that $G$ is metabelian. This is clear if $N$ is abelian, so assume that $N' \neq 1$. Then by 5.5.2, $p = 2$; 5.5.8 and (11c) yield that $N$ is an $M$-group and $N' = \langle e_1 \rangle$. Thus $|N/\Omega_{r-1}(N)| \leq 4$, by (57). Again let $N = Q\langle u \rangle$ as in (23). Since $N' \leq \Omega(\Omega(N)) \cap \langle u \rangle$ and $Q \cap \langle u \rangle = 1$, the group $Q$ is abelian and $u^2 \in Z(N)$;
thus $Q\langle u^2 \rangle$ is abelian. From $G = N\langle a \rangle$ follows $G' = [N, \langle a \rangle]N'$; and $[e_2, a] = e_1$
shows that $N' \leq [N, \langle a \rangle]$. So if $|N/\Omega_{r-1}(N)| = 2$, then $G' = [N, \langle a \rangle] \leq \Omega_{r-1}(N)$ and
$\Omega_{r-1}(N) = Q\langle u^2 \rangle$ is abelian; thus $G$ is metabelian. It remains to consider the case
that $|N/\Omega_{r-1}(N)| = 4$. Then by (65), $\Omega_{r-1}(N)\langle u \rangle \leq G$ of index 2 in $N$ so that $G' = [N, \langle a \rangle] \leq \Omega_{r-1}(N)\langle u \rangle$. By (66), $Q\langle u^2 \rangle = \Omega_{r-1}(N)\langle w \rangle$ is not normal in $G$; note
that $\text{Exp} Q = 2'$ since $|N/\Omega_{r-1}(N)| = 4$. Since $Q\langle u^2 \rangle$ is abelian, it follows that
$\Omega_{r-1}(N) = (Q\langle u^2 \rangle)_G \leq Z((Q\langle u^2 \rangle)_G) = Z(N)$. Therefore $\Omega_{r-1}(N)\langle u \rangle$ is abelian and $G$
is metabelian.

The assertions on $\tilde{G}$ both follow from 5.5.3. For, by 5.5.2 and 5.5.8, $N' \leq \langle e_1 \rangle$.
Thus $N\Omega(G)/\Omega(G)$ is abelian and 5.5.3 applied to $G/\Omega(G)$ yields that $\tilde{G}/\Omega(\tilde{G})$ is meta-
belian. So $\tilde{G}' = \Omega(\tilde{G})$, and this group is elementary abelian. By (11), $f_i^{b_i} = f_1$
and since $\tilde{M} = \tilde{N}\langle b^2 \rangle$, it follows that $\langle f_1 \rangle_{\tilde{M}} \leq \tilde{N}$ and so $f_1 \in \tilde{N}_{\tilde{M}}$. This shows
that $\langle e_1 \rangle_{\tilde{M}} \leq \tilde{M}$ and hence $N/\tilde{N}_{\tilde{M}}$ is abelian. Therefore 5.5.3 applied to the projectivity
induced by $\phi$ in $M/\tilde{N}_{\tilde{M}}$ yields that $\tilde{M}/\tilde{N}_{\tilde{M}}$ is metabelian. Thus $\tilde{M}' = \tilde{N}$ and $\tilde{M}' = \tilde{G}$
since $\tilde{M}$ is a maximal subgroup of $\tilde{G}$. So $\tilde{M}' = \tilde{N}_{\tilde{G}} = 1$ and $\tilde{M}$ is metabelian.

Using 5.4.6 and 5.1.6, it is not difficult to extend the results on $N/N_{\tilde{G}}$ and $\tilde{N}/\tilde{N}_{\tilde{G}}$
proved in this section to projectivities between arbitrary finite groups. However, we
leave this and an application to projectivities between finite soluble groups as an
exercise for the reader (Exercises 4–6) since we shall extend these results to arbitrary
groups in § 6.6.

Exercises

1. Let $E = \langle e_0, \ldots, e_m \rangle$ and $F = \langle f_0, \ldots, f_m \rangle$ be elementary abelian $p$-groups of
order $p^{n+1}$ and let $n \in \mathbb{N}$ such that $p^{n-2} \geq m$ and $2^{n-2} > m$ if $p = 2$. Define $G =
E\langle a \rangle$ and $G = F\langle b \rangle$ by $a^{p^{n-1}} = e_0$, $a^{-1}e_0 a = e_0$, $a^{-1}e_1 a = e_1$, $a^{-1}e_i a = e_i e_{i-1}$ for
$i = 2, \ldots, m$ and $b^{p^{n-1}} = f_0$, $b^{-1}f_0 b = f_0$, $b^{-1}f_i b = f_i f_{i-1}$ for $i = 1, \ldots, m$. Construct
a projectivity from $G$ to $G$ mapping the normal subgroup $N = \langle e_1, \ldots, e_m \rangle$ of $G$
to $M = \langle f_1, \ldots, f_m \rangle$ and show that $M_{\tilde{G}} = 1$.

2. (Menegazzo [1978]) Let $p > 2$ and $E = \langle e_0, \ldots, e_p \rangle$ be an elementary abelian $p$-group of
order $p^{n+1}$.

(a) Construct extensions $H^* = E\langle a \rangle$ satisfying $a^{p^i} = e_0$, $a^{-1}e_0 a = e_0$, $a^{-1}e_1 a = e_1$, $a^{-1}e_i a = e_i e_{i-1}$ for $i = 2, \ldots, p$ and $G^* = H^*\langle u \rangle$ where $[H^*, u] = 1$ and
$u^p = e_1^{-1}$.

(b) Show that there exists a projectivity from $G^*$ to the group $G$ of Exercise 5.2.1
mapping the abelian normal subgroup $N = \langle u, e_2, \ldots, e_p \rangle$ of $G^*$ onto the
nonabelian, core-free subgroup $M = \langle y, a_2, \ldots, a_p \rangle$ constructed there.

3. (Busetto and Menegazzo [1985]) If Hypothesis 5.5.1 is satisfied and $p = 2$, show
that $\Omega(\tilde{G}) \leq Z(\Omega_{\tilde{G}}(G))$.

4. Let $N$ be a normal subgroup of an arbitrary finite group $G$ and $\phi$ a projectivity
from $G$ to a group $\tilde{G}$. Show that

(a) $N/N_{\tilde{G}}$ and $\tilde{N}/\tilde{N}_{\tilde{G}}$ are metabelian, and

(b) $N/N_{\tilde{G}}$ is nilpotent of class at most 2 with commutator subgroup of exponent
at most 2; in particular, $N/N_{\tilde{G}}$ is abelian if $|G|$ is odd.
5. Let $N$ be a normal subgroup of the finite group $G$ such that $G/N$ is soluble of derived length $n \in \mathbb{N}$. If $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, show that $\overline{G}^{(3n)} \leq N^\varphi$.

6. If $G$ is a finite soluble group of derived length $d(G) = n$ and $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, show that $d(\overline{G}) \leq 3n - 1$.

### 5.6 Normalizers, centralizers and conjugacy classes

Apart from the index, studied in §4.2, there are other important interrelations between subgroups that may be preserved by a projectivity. We briefly treat three of them and present the classical examples of particularly decent projectivities between nonisomorphic groups.

A projectivity $\varphi$ from a group $G$ to a group $\overline{G}$ is called centralizer preserving if $C_G(H)^\varphi = C_{\overline{G}}(H^\varphi)$ for all $H \leq G$, normalizer preserving if $N_G(H)^\varphi = N_{\overline{G}}(H^\varphi)$ for all $H \leq G$, and conjugacy preserving if for all $X$, $Y \leq W \leq G$, $X$ is conjugate to $Y$ in $W$ if and only if $X^\varphi$ is conjugate to $Y^\varphi$ in $W^\varphi$. These properties are not independent. For example, if $\varphi$ is conjugacy preserving and $X \leq G$, then $X$ is the only subgroup of $W = N_G(X)$ conjugate to $X$ in $W$; therefore the same holds for $X^\varphi$ in $W^\varphi$ and hence $X^\varphi \leq W^\varphi$. Thus $N_G(X)^\varphi \leq N_{\overline{G}}(X^\varphi)$ and, since $\varphi^{-1}$ like $\varphi$ is conjugacy preserving, we obtain the other inclusion. We have shown:

**5.6.1 Theorem.** Every conjugacy preserving projectivity is normalizer preserving.

### Normalizer preserving projectivities

It is less obvious that every normalizer preserving projectivity is centralizer preserving, as we shall see for arbitrary (possibly infinite) groups. For this we give characterizations of both properties via images of commutator subgroups.

**5.6.2 Theorem** (Barnes and Wall [1964]). The following properties of the projectivity $\varphi$ from the group $G$ to the group $\overline{G}$ are equivalent:

(a) $\varphi$ is normalizer preserving,
(b) $(H^\varphi)^0 = (H^0)^\varphi$ for every subgroup $H$ of $G$,
(c) $[H, K]^\varphi = [H^\varphi, K^\varphi]$ for all $H, K \leq G$.

**Proof.** Suppose first that (a) holds and let $H \leq G$. If $H^0 \leq M \leq H$, then $N_G(M) \geq H$ and therefore $N_{\overline{G}}(M^\varphi) = N_G(M)^\varphi \geq H^\varphi$. Thus $(H^\varphi)^0 \leq H^\varphi$ and $H^\varphi/(H^\varphi)^0$ is abelian or hamiltonian. Since every hamiltonian group contains a subgroup isomorphic to $Q_8$ and $\varphi$ induces a projectivity from the abelian group $H/H^0$ to $H^\varphi/(H^\varphi)^0$, it follows that $H^\varphi/(H^\varphi)^0$ is abelian. Thus $(H^\varphi)^0 \leq (H^\varphi)^0$, and this result applied to $H^\varphi$ and the normalizer preserving projectivity $\varphi^{-1}$ yields the other inclusion; so (b) holds.

Now suppose that (b) is satisfied. If $X = \langle x \rangle$ and $Y = \langle y \rangle$ are cyclic subgroups of a group, then $[X, Y] \leq \langle X, Y \rangle$ and the factor group $\langle X, Y \rangle/[X, Y]$ is generated...
by $x[X, Y]$ and $y[X, Y]$. These elements commute modulo $[X, Y]$ and hence $\langle X, Y \rangle / [X, Y]$ is abelian. Thus $\langle X, Y \rangle' \leq [X, Y]$ and, since the other inclusion is trivial, $\langle X, Y \rangle' = [X, Y]$. Therefore if $H$ and $K$ are cyclic subgroups of $G$, then $H^\circ$ and $K^\circ$ also are cyclic and

$$[H, K]^\circ = ((H \cup K)'\circ)^\circ = ((H \cup K)^\circ)' = (H^\circ \cup K^\circ)' = [H^\circ, K^\circ].$$

For arbitrary subgroups $H$, $K$ of $G$, $[H, K] = \bigcup \{[\langle x \rangle, \langle y \rangle] | \langle x \rangle \leq H, \langle y \rangle \leq K \}$ and this is mapped by $\varphi$ to $\bigcup \{[\langle x \rangle^\circ, \langle y \rangle^\circ] | \langle x \rangle^\circ \leq H^\circ, \langle y \rangle^\circ \leq K^\circ \} = [H^\circ, K^\circ]$. Thus (c) holds.

Finally, if (c) is satisfied and $H \leq G$, then $[H^\circ, N_G(H)^\circ] = [H, N_G(H)]^\circ \leq H^\circ$ and hence $N_G(H)^\circ \leq N_G(H^\circ)$. This result applied to $H^\circ$ and $\varphi^{-1}$ yields the other inclusion. Thus (a) holds.

5.6.3 Theorem. The following properties of the projectivity $\varphi$ from the group $G$ to the group $\bar{G}$ are equivalent:

- (a) $\varphi$ is centralizer preserving,
- (b) $Z(H)^\circ = Z(H^\circ)$ for every subgroup $H$ of $G$,
- (c) For all $H \leq G$, $H' = 1$ if and only if $(H^\circ)' = 1$.

Proof. First of all, (a) implies that $Z(H)^\circ = (H \cap C_G(H))^\circ = H^\circ \cap C_G(H^\circ) = Z(H^\circ)$ for all $H \leq G$. Thus (b) follows from (a) and, since $H' = 1$ if and only if $H = Z(H)$, (b) clearly implies (c). Finally, if (c) holds, then for $x \in H$ and $y \in C_G(H)$, the subgroup $\langle x, y \rangle$ is abelian, as is $\langle x, y \rangle^\circ = \langle x \rangle^\circ \cup \langle y \rangle^\circ$. It follows that $\langle y \rangle^\circ \leq C_G(H^\circ)$ and $C_G(H)^\circ \leq C_G(H^\circ)$. This result applied to $H^\circ$ and $\varphi^{-1}$ yields the other inclusion; thus (a) holds.

Now 5.6.3(c) follows from 5.6.2(b) and therefore we obtain the result announced above.

5.6.4 Corollary. Every normalizer preserving projectivity is centralizer preserving.

Of course, our theorems can also be used to prove that a given projectivity is normalizer or centralizer preserving. The commutator subgroup of a group is the join of the commutator subgroups of all its 2-generator subgroups, and a projectivity maps 2-generator groups to 2-generator groups. Therefore 5.6.2(b) yields the following useful criterion.

5.6.5 Remark. A projectivity $\varphi$ from $G$ to $\bar{G}$ is normalizer preserving if $(H')^\circ = (H^\circ)'$ for every 2-generator subgroup $H$ of $G$.

We use this to generalize a result of Spring [1963] to locally finite groups.

5.6.6 Theorem. If $G$ is a nonabelian locally finite $p$-group of exponent $p$, then every projectivity of $G$ is normalizer preserving.
Projectivities and normal structure of finite groups

Proof. Let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). Since \( G \) is nonabelian, 2.2.7 yields that \( \overline{G} \) is a 2-group. Thus if \( H \) is a 2-generator subgroup of \( G \), then \( H \) and \( H^\varphi \) are finite 2-groups of exponent \( p \). It follows that \( (H')^\varphi = \Phi(H)^\varphi = \Phi(H^\varphi) = (H'^\varphi) \). By 5.6.5, \( \varphi \) is normalizer preserving. \( \square \)

We give examples of normalizer preserving projectivities between nonisomorphic finite \( p \)-groups.

5.6.7 Example (Barnes and Wall [1964]). Let \( p \) be a prime, \( 4 \leq n \leq p \) and \( N = \langle s_1 \rangle \times \cdots \times \langle s_{n-2} \rangle \) where \( o(s_i) = p^2 \) and \( o(s_i) = p \) for \( i \geq 2 \); thus \( N \) is an abelian \( p \)-group of type \((p^2, p, \ldots, p)\) and order \( p^{n-1} \). For \( \gamma \in \Lambda = \{1, \ldots, p-1\} \), let \( s = s(\gamma) \) be the automorphism of \( N \) satisfying

\[
s_i^k = s_i s_{i+1} \quad (1 \leq i \leq n-3), \quad s_{n-2}^k = s_{n-2} s_i^k
\]

and let \( G = G_\gamma = N \langle s \rangle \) be the semidirect product of \( N \) and the subgroup of \( \text{Aut} N \) generated by \( s = s(\gamma) \). By (2) of § 1.5, \([s_1^k, s] = [s_1, s]^k = s_k^k = 1\) so that if we define \( s_{n-1}^k = s_i^k \) and \( s_m = 1 \) for \( m \geq n \), an obvious induction yields that \( s_{i+1}^k = \prod_{j=0}^{k} s_{i+j}^j \) for all \( i, k \geq 1 \). Since \( n \leq p \), it follows that \( s^p = 1 \). Thus \( \langle s \rangle = p \) and \( |G| = p^n \). Since \( \langle s_1^k, s_2, \ldots, s_{n-2} \rangle \leq G^' \) has index \( p^2 \) in \( G \),

(2) \( G^' = \langle s_1^k, s_2, \ldots, s_{n-2} \rangle = \Phi(G) \).

Then \( K_i(G) = [K_{i-1}(G), G] = \langle s_1, \ldots, s_{i-1}, s_i^k \rangle \) for \( i = 2, \ldots, n-2 \) and \( K_{n-1}(G) = \langle s_1^k \rangle \), so that \( G \) is a \( p \)-group of maximal class. As \( n \leq p \), the group \( G \) is regular (see Huppert [1967], p. 322) and, since \( G^' \) is elementary abelian, \((xy)^p = x'^py'^p \) for all \( x, y \in G \). In particular, \((ss_1^k)^p = s_i^p\) for all \( \lambda \in \mathbb{Z} \) and since \( G = \langle s, s_1 \rangle \), the maximal subgroups of \( G \) are \( N \) and the groups

(3) \( M_\lambda = \langle ss_1^\lambda, s_2, \ldots, s_{n-2} \rangle \) where \( 0 \leq \lambda < p \).

We show that all the groups \( G_\gamma (\gamma \in \Lambda) \) are lattice-isomorphic but, in general, not isomorphic. More precisely, we claim that for \( G = G_\gamma \) and \( \overline{G} = G_\delta \) \((\gamma, \delta \in \Lambda)\),

(a) \( G \cong \overline{G} \) if and only if there exists \( \xi \in \mathbb{Z} \) such that \( \delta = \xi^n - 2\gamma \) (mod \( p \)),

(b) there exists a bijective map \( \sigma: G \to \overline{G} \) inducing a normalizer preserving projectivity from \( G \) to \( \overline{G} \) such that \( \sigma|_H \) is an isomorphism for every proper subgroup \( H \) of \( G \).

Proof. Let \( \overline{G} = N \langle t \rangle \) satisfy (1) with \( s \) and \( \gamma \) replaced by \( t \) and \( \delta \), respectively.

(a) Suppose first that \( \psi: \overline{G} \to G \) is an isomorphism. Since \( N \) is the only abelian maximal subgroup of \( G \) and \( \overline{G} \), we have \( N^t = N \) and hence \( s_i^t = s_1^t \cdots s_i^t \) where \( n_1 \equiv 0 \) (mod \( p \)); let \( t^i = s_i^t \cdots s_1^t \) where \( j_i \equiv \xi \) (mod \( K_{i+1}(G) \)). Then since \( s_i \in K_i(G) \), a trivial induction yields that for \( 2 \leq i \leq n-2 \),

\[
s_i^t = [s_{i-1}, t] = [s_{i-1}^t, t^i] \equiv [s_{i-1}^t, s_i^t] = s_i^t s_i^t (\text{mod } K_{i+1}(G)).
\]

Thus \( s_{n-2}^t = s_{n-2}^t (\text{mod } K_{n-1}(G)) \) and since \( [s_{n-2}, s] \in K_{n-1}(G) \leq Z(G) \), we get

\[
s_1^t s_1^t = (s_1^t)^t = [s_{n-2}, t]^i = [s_{n-2}^t, t^i] = [s_{n-2}^t, s_i^t] = (s_1^t)^i = s_i^t.
\]

We show that all the groups \( G_\gamma (\gamma \in \Lambda) \) are lattice-isomorphic but, in general, not isomorphic. More precisely, we claim that for \( G = G_\gamma \) and \( \overline{G} = G_\delta \) \((\gamma, \delta \in \Lambda)\),

(a) \( G \cong \overline{G} \) if and only if there exists \( \xi \in \mathbb{Z} \) such that \( \delta = \xi^n - 2\gamma \) (mod \( p \)),

(b) there exists a bijective map \( \sigma: G \to \overline{G} \) inducing a normalizer preserving projectivity from \( G \) to \( \overline{G} \) such that \( \sigma|_H \) is an isomorphism for every proper subgroup \( H \) of \( G \).

Proof. Let \( \overline{G} = N \langle t \rangle \) satisfy (1) with \( s \) and \( \gamma \) replaced by \( t \) and \( \delta \), respectively.

(a) Suppose first that \( \psi: \overline{G} \to G \) is an isomorphism. Since \( N \) is the only abelian maximal subgroup of \( G \) and \( \overline{G} \), we have \( N^t = N \) and hence \( s_i^t = s_1^t \cdots s_i^t \) where \( n_1 \equiv 0 \) (mod \( p \)); let \( t^i = s_i^t \cdots s_1^t \) where \( j_i \equiv \xi \) (mod \( K_{i+1}(G) \)). Then since \( s_i \in K_i(G) \), a trivial induction yields that for \( 2 \leq i \leq n-2 \),

\[
s_i^t = [s_{i-1}, t] = [s_{i-1}^t, t^i] \equiv [s_{i-1}^t, s_i^t] = s_i^t s_i^t (\text{mod } K_{i+1}(G)).
\]

Thus \( s_{n-2}^t = s_{n-2}^t (\text{mod } K_{n-1}(G)) \) and since \( [s_{n-2}, s] \in K_{n-1}(G) \leq Z(G) \), we get

\[
s_1^t s_1^t = (s_1^t)^t = [s_{n-2}, t]^i = [s_{n-2}^t, t^i] = [s_{n-2}^t, s_i^t] = (s_1^t)^i = s_i^t.
\]
Since $o(s_i) = p^2$ and $\eta_1 \neq 0 \pmod{p}$, it follows that $\delta \equiv \xi^{n-2} \gamma \pmod{p}$, as desired. Conversely, suppose that there exists $\zeta \in \mathbb{Z}$ such that $\delta \equiv \xi^{n-2} \gamma \pmod{p}$. Then if we define $s^* = s^\zeta$, $s_1^* = s_1$ and $s_i^* = [s_{i-1}^*, s_i^*]$ for $2 \leq i \leq n-2$, a similar computation as above shows that $s_i^* \equiv s_i^{\zeta-1} \pmod{K_{i+1}(G)}$ and $[s_{n-2}^*, s_i^*] = s_i^{n-2} / p = (s_i^*)^p$. It follows that $G = \langle s^*, s_i^* \rangle \cong G_n(\delta) = \overline{G}$.

(b) Since $\gamma, \delta \in \Lambda = \{1, \ldots, p - 1\}$, there exists $k \in \mathbb{Z}$ such that $\delta \equiv k \gamma \pmod{p}$. For $0 \leq \lambda < p$, let $M_\lambda = \langle ts_1^\lambda, s_2, \ldots, s_{n-2} \rangle$ and define $M_p = N = M_p$. By (3), the $M_\lambda$ and $M_k (0 \leq \lambda \leq p)$ are the maximal subgroups of $G$ and $G$, respectively. For $1 \leq \lambda \leq p - 1$, let $\mu \in \mathbb{Z}$ be such that $\mu \equiv 1 \pmod{p}$, and put $x = ss_1^\lambda$ and $y = ts_1^\lambda$. Then $x_p = s_1^{x_p}$ and $y_p = s_1^{y_p}$ so that $M_\lambda = (\langle s_2 \rangle \times \cdots \times \langle s_{n-2} \rangle \times \langle x_p \rangle) \langle x \rangle$ and $M_k = (\langle s_2 \rangle \times \cdots \times \langle s_{n-2} \rangle \times \langle y_p \rangle) \langle y \rangle$. Since $[s_i, x] = s_{i+1} = [s_i, y]$ for $2 \leq i \leq n-3$,

$[s_{n-2}, x] = s_{i+1} = (x_p)^\mu$ and also $[s_{n-2}, y] = s_{i+1} = (y_p)^\mu$, there exists an isomorphism $v_\lambda: M_\lambda \to M_k$ fixing all the $s_i (2 \leq i \leq n-2)$ and mapping $x$ to $y$. Then $(s_i^p)_\lambda = (x_p)^\mu = (y_p)^\mu = (s_i^p)_\lambda$ and hence all the $v_\lambda$ induce the same automorphism $v$ in $\Phi(G) = \langle s_1^\zeta, s_2, \ldots, s_{n-2} \rangle$. Clearly, we may extend $v$ to an isomorphism $v_p: N \to N$ defining $s_i^p = s_i^\zeta$ and, since $[s_{n-2}, t] = s_1^\zeta = s_1^{y_p} = [s_{n-2}, s]$, there is an extension of $v$ to an isomorphism $v_0: M_0 \to \overline{M}_0$ satisfying $s^0 = t$. Now all the $v_\lambda$ agree on $\Phi(G)$ and therefore the map $\sigma: G \to \overline{G}$ defined by $g^\sigma = g^v$ if $g \in M_\lambda (0 \leq \lambda \leq p)$ is well-defined, induces an isomorphism in every maximal subgroup of $G$ and hence satisfies (5) and (6) of § 1.3. By Theorem 1.3.1, $\sigma$ induces a projectivity $\varphi$ from $G$ to $\overline{G}$. Since $(G')^\varphi = \overline{G}$ and $\sigma$ induces an isomorphism in every maximal subgroup of $G$, 5.6.2 implies that $\varphi$ is normalizer preserving.

The simplest examples of nonisomorphic groups obtained in this way are $G_4(1)$ and $G_4(\gamma)$ of order $p^4$ ($p \geq 5$), where $\gamma$ is a nonquadratic residue (mod $p$). Barnes and Wall give similar examples with $3 \leq p < n$, and also of groups of exponent $p$ (see Exercise 3).

Finally, we remark that the converses of 5.6.1 and 5.6.4 do not hold. For example, the nonabelian group of order $pq$ with $p$ and $q$ primes has only centralizer preserving autoprojectivities and its singular autoprojectivities are not normalizer preserving. Examples of index and centralizer preserving projectivities that are not normalizer preserving are given in Exercise 1. The Rottländer groups, which we shall shortly study, possess normalizer preserving projectivities that are not conjugacy preserving.

**Groups with identical subgroup structures**

There is no general theory of conjugacy preserving projectivities giving results that go beyond those known for arbitrary projectivities. One reason for this is probably the many examples of projectivities between nonisomorphic groups which preserve almost every structural property. We say that two groups $G$ and $\overline{G}$ have *identical subgroup structures* if there exists an index and conjugacy preserving projectivity $\varphi$ from $G$ to $\overline{G}$ such that $H^\varphi \simeq H$ for every proper subgroup $H$ of $G$. The first example of nonisomorphic groups with identical subgroup structures was published by Ada Rottländer in the earliest study of subgroup lattices of groups.
5.6.8 Example (Rottländer [1928]). Let $q \geq 5$ and $p$ be primes such that $q \mid p - 1$ and let $r \in \mathbb{N}$ such that $r \not\equiv 1 \pmod{p}$ and $r^q \equiv 1 \pmod{p}$. For every $\lambda \in \Lambda = \{2, \ldots, q - 1\}$, we define the Rottländer group

$$G_\lambda = \langle x, y, a | x^p = y^p = a^q = [x, y] = 1, a^{-1}xa = x^r, a^{-1}ya = y^{r^\lambda} \rangle$$

and claim that for $\lambda, \mu \in \Lambda$,

(a) $G_\lambda$ and $G_\mu$ have identical subgroup structures, and

(b) $G_\lambda \cong G_\mu$ if and only if $\lambda = \mu$ or $\lambda \mu \equiv 1 \pmod{q}$.

Thus we obtain $(q - 1)/2$ pairwise nonisomorphic groups with identical subgroup structures. The smallest primes occurring are $p = 11$, $q = 5$ with $|G_\lambda| = 605$.

**Proof.** (a) Let $N = \langle x, y \rangle$ so that $G_\lambda = N\langle a \rangle$ and let $G_\mu = N\langle b \rangle$ where $x^b = x^r$ and $y^b = y^{r^\mu}$. Since $\lambda \not\equiv 0, 1 \pmod{q}$, the element $a$ induces different nontrivial power automorphisms in $\langle x \rangle$ and $\langle y \rangle$. Thus $\langle x \rangle$ and $\langle y \rangle$ are the eigenspaces of the automorphism induced by $a$ in $N$ and hence the type of this automorphism is $(0; 1, 1)$. By 4.1.8 there exists a projectivity $\varphi$ from $G_\lambda$ to $G_\mu$ satisfying $N^\varphi = N$ and $\langle a^\varphi \rangle = \langle b \rangle$. Clearly, $\varphi$ is index preserving and, since the maximal subgroups of $G_\lambda$ different from $N$ are all nonabelian of order $pq$, $H^\varphi \cong H$ for every proper subgroup $H$ of $G_\lambda$. The set $\Omega$ of subgroups of order $p$ of $N$ different from $\langle x \rangle$ and $\langle y \rangle$ falls into $(p - 1)/q$ conjugacy classes of length $q$. For every $X \in \Omega$, the subgroup $N$ is the only maximal subgroup of $G_\mu$ containing $X$. Hence there exists an autopjectivity $\rho$ of $G_\mu$ fixing all the $Y \in L(G_\mu) \setminus \Omega$ and permuting the subgroups in $\Omega$ in such a way that $\psi = \varphi \rho$ maps conjugacy classes of subgroups of order $p$ to conjugacy classes. Since any two Sylow $q$-subgroups are conjugate in every subgroup containing them, and since two subgroups of order $pq$ of $G_\lambda$ are conjugate if and only if they intersect in a subgroup of order $p$, it follows that $\psi$ is conjugacy preserving. Thus $G_\lambda$ and $G_\mu$ have identical subgroup structures.

(b) Let $\sigma: G_\lambda \to G_\mu$ be an isomorphism and $a^\sigma = x^iy^jb^k$ where $i, j, k \in \mathbb{N}$. Then $\sigma$ has to map the normal subgroups $\langle x \rangle$, $\langle y \rangle$ of order $p$ of $G_\lambda$ to the normal subgroups $\langle x \rangle$, $\langle y \rangle$ of order $p$ of $G_\mu$. If $\langle z \rangle$ is one of these normal subgroups, $z^a = z^s$ and $(z^b)^j = (z^s)^j$ (s, t $\in \mathbb{N}$), then $(z^a)^s = (z^s)^r = (z^a)^s = (z^s)^{r^\lambda} = (z^s)^{r^\mu} = (z^s)^{r^\lambda \mu}$ and hence $s \equiv r^k \pmod{p}$. Therefore if $\langle x \rangle^\sigma = \langle x \rangle$ and $\langle y \rangle^\sigma = \langle y \rangle$, then $r \equiv r^k \pmod{p}$ and $r^\lambda \equiv r^\mu \pmod{p}$; thus $k \equiv 1 \pmod{q}$ and $\lambda \equiv \mu k \equiv \mu \pmod{q}$. Since $\lambda, \mu \in \{2, \ldots, q - 1\}$, it follows that $\lambda = \mu$. If $\langle x \rangle^\sigma = \langle y \rangle$ and $\langle y \rangle^\sigma = \langle x \rangle$, then $r \equiv r^\mu \pmod{p}$ and $r^\lambda \equiv r^k \pmod{p}$; hence $\mu k \equiv 1 \pmod{q}$ and $\lambda \equiv k \pmod{q}$ so that $\mu \lambda \equiv 1 \pmod{q}$. Conversely, if $\lambda \mu \equiv 1 \pmod{q}$, then $y^{b^\sigma} = y^{r^\sigma} = y^r$ and $x^{b^\sigma} = x^{r^\sigma}$ so that $y, x, b^\sigma$ satisfy the defining relations of $G_\lambda$. It follows that $G_\mu \cong G_\lambda$ and (b) holds.

For any $\lambda \in \Lambda$, there exists a unique $\mu \in \Lambda$ such that $\lambda \mu \equiv 1 \pmod{q}$. If $\lambda \neq q - 1$, then $\lambda^2 \not\equiv 1 \pmod{q}$; thus $\mu \neq \lambda$ and hence these $\lambda$ in pairs yield $(q - 3)/2$ nonisomorphic groups. Together with $G_{q-1}$ we obtain $(q - 1)/2$ pairwise nonisomorphic Rottländer groups of order $p^2q$.

Other examples of nonisomorphic groups with identical subgroup structures were given by Yff and Holmes; those of Yff can also be found in an earlier paper by Honda on subgroup lattices of metacyclic groups.
5.6 Normalizers, centralizers and conjugacy classes

5.6.9 Example. Let $p$ and $q$ be primes such that $q | p - 1$ and let

(a) (Honda [1952], Yff [1967]) $t \in \mathbb{P}$ such that $t \neq p$ and $q | t - 1$, or
(b) (Holmes [1976]) $t = q^2$.

Let $N = P \times T$ with $|P| = p$ and $|T| = t$ be the cyclic group of order $pt$. Then

$\text{Aut } N = A_1 \times A_2$ where $A_1 = C_{\text{Aut } N}(T) \simeq \text{Aut } P$ and $A_2 = C_{\text{Aut } N}(P) \simeq \text{Aut } T$, and therefore $\text{Aut } N$ contains an elementary abelian subgroup $Q = Q_1 \times Q_2$ of order $q^2$ with $Q_i \leq A_i$ and $|Q_i| = q$. For every subgroup $R$ of order $q$ of $Q$ different from $Q_1$ and $Q_2$, let $G_R = NR$ be the semidirect product of $N$ and $R$; thus

$$G_R = \langle x, a|x^p = a^q = 1, a^{-1}xa = x^r \rangle$$

for some $r \in \mathbb{N}$ satisfying $r^q \equiv 1 \pmod{pt}$, $r \neq 1 \pmod{p}$ and $r \neq 1 \pmod{t}$. Then all the $G_R$ have identical subgroup structures. For, if $S$ is another subgroup of order $q$ of $Q$ different from $Q_1$ and $Q_2$, then by 4.1.6 there exists a projectivity $\varphi$ from $G_R$ to $G_S$. This is clear if (a) holds; in case (b), we take $P$ to be a normal Hall subgroup, the nonabelian groups $TR$ and $TS$ of order $q^3$ and exponent $q^2$ as complements and $\tau$ the projectivity induced by an isomorphism $\alpha: TR \to TS$ satisfying $T\alpha = T$ and $R\alpha = S$. It is rather obvious that $\varphi$ preserves indices, conjugacy and satisfies $H^\varphi \simeq H$ for every proper subgroup $H$ of $G$.

An isomorphism $\nu: G_R \to G_S$ maps the cyclic normal subgroup $N$ of order $pt$ of $G_R$ to the cyclic normal subgroup $N$ of order $pt$ of $G_S$ and satisfies

$$(x^r)^{\nu} = (x^a)^{\nu} = (x^r)^{\nu} = (x^r)^{\nu}$$

so that $a^r$ induces the same power as $a$ on $N$; it follows that $S = R$. Thus we obtain $q - 1$ pairwise nonisomorphic groups with identical subgroup structures. The smallest primes occurring are $q = 3$, $p = 7$, $t = 13$ with $|G_R| = 273$ in case (a), and $q = 3$, $p = 7$ with $|G_R| = 189$ in case (b).

The examples constructed in 5.6.8 and 5.6.9 can be generalized to the situation where $q$ does not divide $p - 1$, while those of Rottländer and Honda-Yff extend also to the case where $q$ is not a prime. For this the nonabelian groups of order $pq$ must be replaced by groups of order $p^nq$ in which the cyclic group of order $q$ operates irreducibly on an elementary abelian group of order $p^n$; for $q \in \mathbb{P}$, these groups have been described in 4.1.7(b). In general, however, the projectivities between these groups are not conjugacy preserving (Holmes [1984], Schmidt [1982]).

There are many other examples of nonisomorphic but lattice-isomorphic groups. We mention those due to Niegel [1973a], [1973b] of groups whose orders contain at most three prime divisors or are square-free, Dauks and Heineken [1975] of groups of order $p^6$, Caranti [1979] of $p$-groups of maximal class, Holmes [1971] of direct products of Rottländer groups with certain other groups, Schmidt [1981] of direct products of two isomorphic Rottländer groups, and Schmidt [1982] of groups with elementary abelian normal Hall subgroups.
More important than the investigation of conjugacy preserving projectivities, which are relatively rare, is the question when a single conjugacy class $\Delta$ of $G$ is mapped to a conjugacy class of $\overline{G}$ by a projectivity $\varphi$ from $G$ to $\overline{G}$. For then, not only $G$ but also $\overline{G}$ operates on $\Delta$ via the map $\tau_\Delta : \overline{G} \to \text{Sym} \, \Delta$ defined by

\[(4) \ H(\tau(x)) = H^{\varphi \circ \sigma^{-1}} \text{ for } H \in \Delta; \]

we shall use this fact quite systematically in § 7.7. Of course, we may assume that $|\Delta| \geq 2$ since the operation described above becomes trivial if $|\Delta| = 1$. The first observation one makes is that in many groups there are conjugacy classes of relatively small subgroups which are not mapped to a conjugacy class by some projectivity. For example, the conjugacy classes of subgroups of order $p$ in the Rottländer groups, in the groups of Example 4.1.7(b), or in Exercise 5 have this property. Furthermore, as in the case of projective images of normal subgroups, $P$-groups will cause difficulties. If we exclude these and restrict our attention to maximal subgroups, the situation is better. To show this, we first prove a useful general property of the autoprojectivities induced in $G$ by the elements of $\overline{G}$.

\[5.6.10 \text{ Lemma. Let } \varphi \text{ be a projectivity from the finite group } G \text{ to the group } \overline{G}, \text{ let } x \in G \text{ and } \tau(x) \text{ be the autoprojectivity of } G \text{ defined by } H(\tau(x)) = H^{\varphi \circ \sigma^{-1}} \text{ for all } H \leq G. \text{ If } G \text{ is } P\text{-indecomposable, then } \tau(x) \text{ is index preserving.} \]

**Proof.** Suppose, for a contradiction, that $\tau(x)$ is not index preserving. By 4.2.5, $\tau(x)$ maps Sylow subgroups to Sylow subgroups since $G$ is $P$-indecomposable. Therefore 4.2.1 implies that there exist primes $p \neq q, P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$ such that $P^{\tau(x)} = Q$. Thus $P^{\varphi \circ \sigma^{-1}} = Q^{\varphi}$ and since $|P^{\varphi}| = |P^{\varphi \circ \sigma^{-1}}| = |Q^{\varphi}|$, it follows that $\varphi$ is singular at $p$ or at $q$. If $\varphi$ is singular at $p$, then by 4.2.6 there exists a normal $p$-complement $N$ of $G$ such that $N^\varphi \leq \overline{G}$. But then $N^{\tau(x)} = N^{\varphi \circ \sigma^{-1}} = N$, hence $P^{\tau(x)}N = (PN)^{\tau(x)} = G$ and $P^{\tau(x)} \cap N = (P \cap N)^{\tau(x)} = 1$ so that $|P^{\tau(x)}| = |G : N| = |P|$, a contradiction. If $\varphi$ is singular at $q$, we argue in exactly the same way using $Q$ and $x^{-1}$ instead of $P$ and $x$.

If $G$ is $P$-indecomposable, $\tau(x)$ in general is not index preserving: consider $G = S_3 = \overline{G}$, an autoprojectivity $\varphi$ of $G$ satisfying $A_3^\varphi \neq A_3$ and $x = (123)$. It is also clear that for $P$-indecomposable groups, conjugacy classes $\Delta$ of maximal subgroups in general are not mapped to conjugacy classes by projectivities $\varphi$. However, we show that for finite soluble groups, this is the only situation in which $\Delta^\varphi$ is not a conjugacy class.

\[5.6.11 \text{ Theorem (Schmidt [1977b]). Let } G \text{ be a finite soluble group, } \Delta \text{ a conjugacy class of maximal subgroups of } G \text{ such that } |\Delta| \geq 2, \text{ and } \varphi \text{ a projectivity from } G \text{ to a group } \overline{G}. \text{ If there is an element } g \in \overline{G} \text{ such that } (\Delta^\varphi)^g \neq \Delta^\varphi, \text{ then there are subgroups } S \text{ and } T \text{ of } G \text{ such that } G = S \times T, (|S|, |T|) = 1, S \text{ is a } P\text{-group and } T \leq \bigcap_{H \in \Delta} H. \]

**Proof.** We use induction on $|G|$ and first note that it suffices to show that $G$ is $P$-indecomposable. For then $G = S \times T$ where $(|S|, |T|) = 1$ and $S$ is a $P$-group, so that
5.6 Normalizers, centralizers and conjugacy classes

$L(G) \cong L(S) \times L(T)$ by 1.6.4. Every $X \in \Delta$ is a maximal subgroup of $G$ and hence it follows that either $S \leq X$ or $T \leq X$. If $T \leq X$, then $T \leq X_G = \bigcap_{H \in \Delta} H$ and we are done; so suppose that $S \leq X$. Then $X = S \times (X \cap T)$ and $\Delta_* = \{H \cap T | H \in \Delta\}$ is a conjugacy class of maximal subgroups of $T$ satisfying the assumptions of the theorem. By induction, $T = A \times B$ where $(|A|, |B|) = 1$, $A$ is a $P$-group and $B \leq \bigcap_{H \in \Delta} (H \cap T)$. Then $S_* = A$ and $T_* = S \times B$ satisfy the assertions of the theorem.

Thus suppose, for a contradiction, that $G$ is $P$-indecomposable. Since $|\Delta| \geq 2$, we have $\overline{G} = \langle K^n | K \in \Delta \rangle$, and therefore the assumption $(\Delta^o)^o \neq \Delta^o$ implies that there exist $H, K \in \Delta$ and $x \in K^o$ such that $(H^o)^x \notin \Delta^o$. If $\rho = \tau(x)$ is defined as in 5.6.10, then $H^o = H^{o \circ \rho} \notin \Delta$ and $K^o = K \in \Delta$. Thus $H^o$ and $K^o$ are maximal subgroups of the soluble group $G$ which are not conjugate in $G$. By a theorem of Ore (see Huppert [1967], p. 165), $H^o$ and $K^o$ permute so that $|G : H^o| = |K^o : H^o \cap K^o|$. Since $\rho$ is index preserving, it follows that $|G : H| = |K : H \cap K|$ and hence $G = HK$. This is impossible since $H$ and $K$ are conjugate. Thus $G$ is $P$-decomposable.

5.6.12 Corollary. Let $\Delta$ be a conjugacy class of maximal subgroups of the finite soluble group $G$. If $\varphi$ is an index preserving projectivity from $G$ to a group $\overline{G}$, then $\Delta^o$ is a conjugacy class in $\overline{G}$.

**Proof.** For $|\Delta| = 1$, this follows from 4.3.5; and since an index preserving projectivity of a $P$-group is conjugacy preserving, 5.6.11 yields the result if $|\Delta| \geq 2$.

It is an interesting open problem whether Theorem 5.6.11 and its corollary also hold without the assumption that $G$ is soluble.

**Exercises**

1. Let $G = \langle a, b | a^{p^2} = b^{p^2} = 1, b^{-1}ab = a^{1+p} \rangle$. Show that every autoprojectivity of $G$ is centralizer preserving and find an autoprojectivity which is not normalizer preserving.

2. Find a group $G$ and a projectivity $\varphi$ of $G$ which
   (a) is conjugacy preserving but does not satisfy $H^o \simeq H$ for every $H < G$,
   (b) satisfies $H^o \simeq H$ for every $H < G$ but is not centralizer preserving.

3. (Barnes and Wall [1964]) Let $8 \leq n \leq p$ and $N = \langle s_2 \rangle \times \cdots \times \langle s_{n-1} \rangle$ where $o(s_i) = p$ be an elementary abelian group of order $p^{n-2}$. For $e \in \{+1, -1\}$, let $s_1$ be the automorphism of $N$ satisfying $s_1^i = s_1 s_{i+2}^e (i \geq 2)$, where we put $s_n = s_{n+1} = 1$, and let $M_e = N \langle s_1 \rangle$ be the semidirect product of $N$ and $\langle s_1 \rangle$. Finally, let $G_e = M_e \langle s \rangle$ be the semidirect product of $M_e$ and $\langle s \rangle$ where $s_1^i = s_1 s_{i+1}^e (i \geq 1)$. Show that $G_1$ and $G_{-1}$ are lattice-isomorphic but nonisomorphic groups of order $p^n$, class $n - 1$ and exponent $p$.

4. Draw a Hasse diagram of the subgroup lattice of a Rottländer group of order 605.
5. Let $p > 2$ and $G = C_p \wr C_p$ be the wreath product of two cyclic groups of order $p$ — thus $G = A\langle b \rangle$ where $A = \langle a_1 \rangle \times \cdots \times \langle a_p \rangle$, $o(a_i) = o(b) = p$, $b^{-1}a_ib = a_{i+1}$ $(1 \leq i \leq p-1)$, $b^{-1}a_pb = a_1$ — and let $\Delta = \langle \langle a_1 \rangle, \ldots, \langle a_p \rangle \rangle$ be the conjugacy class of $\langle a_1 \rangle$ in $G$. Let $\sigma$ be the automorphism of $A$ satisfying $a_i^\sigma = a_2$ and $a^\sigma = a$ for all $a \in G'$ and define $\varphi : L(G) \to L(G)$ by $H^\varphi = H^\sigma$ for $H \leq A$ and $H^\varphi = H$ for $H \not\leq A$. Show that $\varphi$ is an autoprojectivity of $G$ such that all the groups in $\Delta^\varphi$ are pairwise nonconjugate.
Chapter 6

Projectivities and normal structure of infinite groups

We have already mentioned that it is possible to generalize most of the results of Chapter 5 to infinite groups. Basic for this is a theorem that was proved independently by Zacher and Rips in 1980. It states that a subgroup of finite index of a group \( G \) is mapped to a subgroup of finite index in \( \overline{G} \) by any projectivity from \( G \) to \( \overline{G} \). This will be proved in § 6.1; in fact, we shall even give a lattice-theoretic characterization of the finiteness of the index of a subgroup in a group. This theorem reduces nearly every lattice-theoretic question on subgroups of finite index to the corresponding question for finite groups.

In the subgroup lattice of a finite group we used modular elements to approximate normal subgroups. The Tarski groups show that this is not reasonable in infinite groups, so we use here the so-called permodular subgroups, introduced by Zacher [1982b]. These are modular subgroups with an additional lattice-theoretic property possessed by projective images of normal subgroups and also by permutable subgroups. So in §§6.2 and 6.3 we study permodular and permutable subgroups of groups as far as necessary for our applications. In contrast to the situation for finite groups, \( M^G/M_e \) in general is not hypercentrally embedded in \( G \) if \( M \) is permutable in \( G \). There is no general structure theorem for permodular subgroups, like the one for modular subgroups of finite groups, which reduces all our problems to the investigation of permutable subgroups. In our applications, however, we may usually assume that \( G \) is finitely generated modulo \( M \). In this situation, it is possible to prove that \( |M^G:M| \) is finite and that the structure theorem holds if \( M \) is permodular in \( G \); and if \( M \) is even permutable in \( G \), then \( M^G/M_e \) is nilpotent of finite exponent.

In §6.4 we use our results on permodular subgroups to generalize the lattice-theoretic characterizations of § 5.3 to infinite groups. In particular, we get characterizations for the classes of simple, perfect, hyperabelian, polycyclic, finitely generated soluble, hypercyclic, and supersoluble groups. However, we do not obtain a characterization of soluble groups; in fact, it is one of the most interesting open problems to find a lattice-theoretic characterization for this class of groups.

In §6.5 we again turn to our main problem. First of all we generalize some of the criteria of § 5.4 to infinite groups. In particular, we prove that, as in the finite case: if \( N \trianglelefteq G, \phi \) is a projectivity from \( G \) to \( \overline{G} \), \( H^\phi \) is the normal closure and \( K^\phi \) is the core of \( N^\phi \) in \( \overline{G} \), then \( H \) and \( K \) are normal subgroups of \( G \). In §6.6 we obtain a structure theorem for \( G/K \) and \( \overline{G}/K^\phi \), mostly due to Zacher [1982a], that is similar to the corresponding result for finite groups. Finally, we prove a number of properties of \( H/K \) and \( H^\phi/K^\phi \), the most important being that \( H/K \) and \( H^\phi/K^\phi \) are soluble of
282  Projectivities and normal structure of infinite groups

derived length at most 4 and 5, respectively. These results emerged from joint efforts
of Busetto, Menegazzo, Napolitani and Zacher in the 1980's. As an important appli-
cation we prove that the projective image of a soluble group (of derived length \( n \)) is
soluble (of derived length at most \( 3n - 1 \)), another result of Busetto, Menegazzo and
Napolitani that improves older bounds of Yakovlev [1970] who was the first to
prove that projective images of soluble groups are soluble.

6.1 Subgroups of finite index

It is easy to prove (see Theorem 1.2.12) that a group is finite if and only if its
subgroup lattice is finite. We wish to show that the finiteness of the index of a
subgroup in a group is also a projective invariant and can be recognized in the
subgroup lattice. For \( K \leq H \leq G \), of course, \( |H : K| \) is finite if and only if there exists
a finite chain of subgroups \( K = H_0 \leq H_1 \leq \cdots \leq H_n = H \) such that \( H_i \) is a maximal
subgroup of \( H_{i+1} \) and \( |H_{i+1} : H_i| \) is finite for all \( i = 0, \ldots, n - 1 \). Therefore we only
have to consider maximal subgroups.

Groups covered by cosets

The main tool in the proofs of our results will be a quite elementary lemma of B. H.
Neumann's on set-theoretic unions of subgroups of a group. To prove this, we have
to study groups that are covered by a set of cosets of subgroups. To simplify nota-
tion, in this section, we shall write \( A_1 \cup \cdots \cup A_n \) for the set-theoretic union of the
cosets \( A_1, \ldots, A_n \) of \( G \).

6.1.1 Lemma. Let \( G \) be a group \( n, m \in \mathbb{N} \), and suppose that \( H_i (i = 1, \ldots, n) \) and \( D \) are
subgroups of \( G \) such that \( D \neq H_i \) for \( i = 1, \ldots, n \). If there exist elements \( x_i, y_j \in G \) such
that

1. \( G = H_1 x_1 \cup \cdots \cup H_n x_n \cup Dy_1 \cup \cdots \cup Dy_m \) and

2. \( G \neq Dy_1 \cup \cdots \cup Dy_m \),

then \( G \) is the union of finitely many right cosets of the subgroups \( H_1, \ldots, H_n \).

Proof. By (2) there exists \( g \in G \) such that \( g \notin Dy_1 \cup \cdots \cup Dy_m \). It follows that
\( Dg \cap (Dy_1 \cup \cdots \cup Dy_m) = \emptyset \) and then (1) shows that \( Dg \subseteq H_1 x_1 \cup \cdots \cup H_n x_n \).
Hence

\[ Dy_j \subseteq (H_1 x_1 \cup \cdots \cup H_n x_n)g^{-1} y_j = H_1 (x_1 g^{-1} y_j) \cup \cdots \cup H_n (x_n g^{-1} y_j) \]

for \( j = 1, \ldots, m \). By (1), \( G \) is the union of finitely many right cosets of the \( H_i \).

6.1.2 Lemma. If the group \( G \) is covered by finitely many right cosets of subgroups, at
least one of these subgroups has finite index in \( G \).
6.1 Subgroups of finite index

\textbf{Proof.} Let $H_i \leq G$ and $x_i \in G$ ($i = 1, \ldots, k$) such that $G = H_1 x_1 \cup \cdots \cup H_k x_k$; we have to show that $|G : H_i|$ is finite for some $i$. We prove this by induction on the number $r$ of different subgroups among the $H_i$. If $r = 1$, then $G$ is the union of $k$ right cosets of one and the same subgroup which then clearly has index at most $k$. So suppose that $|\{H_1, \ldots, H_k\}| = r > 1$, and assume that the assertion is true for $r - 1$. Without loss of generality we may further assume that the cosets are arranged in such a way that $H_i \neq H_k$ for $i = 1, \ldots, n$ and $H_i = H_k$ for $i > n$. Then $H_1, \ldots, H_n$ and $D = H_k$ satisfy (1). Now if $|G : D|$ is finite, we are done. On the other hand, if $|G : D|$ is infinite, then (2) holds and by 6.1.1, $G$ is the union of finitely many cosets of the $r - 1$ subgroups $H_1, \ldots, H_n$. By induction, one of these has finite index in $G$. \hfill \Box

6.1.3 \textbf{Lemma (Neumann [1954]).} Let $H_i$ be subgroups and $x_i$ elements of the group $G$ ($i = 1, \ldots, n$) such that $G = H_1 x_1 \cup \cdots \cup H_n x_n$. If $H_n$ has infinite index in $G$, then $G = H_1 x_1 \cup \cdots \cup H_{n-1} x_{n-1}$.

\textbf{Proof.} By 6.1.2, at least one of the $H_i$ has finite index in $G$. So suppose without loss of generality that $|G : H_i|$ is finite for $i = 1, \ldots, k$ and infinite for $i = k + 1, \ldots, n$; let $D = H_1 \cap \cdots \cap H_k$. Since every subgroup of finite index contains a normal subgroup of finite index, the intersection of a finite number of subgroups of finite index again has finite index. Therefore $|G : D|$ is finite and every $H_i (i = 1, \ldots, k)$ is the union of finitely many cosets of $D$. It follows that $H_1 x_1 \cup \cdots \cup H_k x_k = Dy_1 \cup \cdots \cup Dy_m$ for certain $y_j \in G$. If $G \neq Dy_1 \cup \cdots \cup Dy_m$, then by 6.1.1, $G$ would be the union of finitely many right cosets of the subgroups $H_{k+1}, \ldots, H_n$; however, by 6.1.2, this is impossible since all these $H_i$ have infinite index in $G$. Therefore

$$G = Dy_1 \cup \cdots \cup Dy_m = H_1 x_1 \cup \cdots \cup H_k x_k \subseteq H_1 x_1 \cup \cdots \cup H_{n-1} x_{n-1}. \hfill \Box$$

We are interested in the special case of Neumann's lemma in which all the $x_i = 1$, so that the cosets are subgroups of $G$. The lemma states that all the subgroups of infinite index can be omitted from the covering of $G$. We say that, conversely, $G$ is\textit{ covered irreducibly} by subgroups $H_i (i \in I)$ if $G$ is the set-theoretic union of the $H_i$ and none of these subgroups can be omitted from the covering.

\textbf{Maximal subgroups}

An immediate consequence of Neumann's lemma is the following lattice-theoretic characterization of the finiteness of the index of a nonnormal maximal subgroup.

6.1.4 \textbf{Lemma.} A nonnormal maximal subgroup $M$ of the group $G$ has finite index in $G$ if and only if there are finitely many subgroups $H_i (i = 1, \ldots, n)$ of $G$ such that $G$ is covered irreducibly by the $H_i$ and $\bigcap_{i=1}^n H_i \leq M$.

\textbf{Proof.} If the $H_i$ exist, then by 6.1.3, $|G : H_i|$ is finite for all $i$. Hence the intersection of all the $H_i$ has finite index in $G$ and it follows that $|G : M|$ is finite. Conversely,
suppose that $M$ has finite index in $G$. Then $G/N$ is a finite group if $N = M_0$ is the core of $M$ in $G$. Let $H_i/N$ $(i = 1, \ldots, n)$ be the maximal cyclic subgroups of $G/N$. If $x \in G$, then $\langle x \rangle N/N$ is cyclic and therefore is contained in one of the $H_i/N$; thus $x \in H_i$ and $G$ is covered by the $H_i$. And if $g \in G$ such that $H_i/N = \langle g \rangle N/N$, the maximality of $H_i/N$ implies that $g \notin H_j$ for all $j \neq i$. Thus $H_i$ cannot be omitted from the above covering of $G$. It remains to be shown that the intersection $D$ of all the $H_i$ is contained in $M$. If this is false, then $G = \langle M, D \rangle$ since $M$ is a maximal subgroup of $G$. Since $D/N$ is centralized by all the $H_i/N$, it follows that $D/N \leq Z(G/N)$ and hence that $M \trianglelefteq G$, a contradiction. Thus $D \leq M$, as required.

6.1.5 Remark. (a) Note that the property in Lemma 6.1.4 can be recognized in the subgroup lattice. For, since a subgroup $H$ of $G$ is cyclic if and only if $L(H)$ is distributive and satisfies the maximal condition, $G$ is covered irreducibly by subgroups $H_i$ if and only if

3. for every $H \in L(G)$ for which $[H/1]$ is distributive and satisfies the maximal condition, there exists $H_i$ such that $H \leq H_i$, and

4. for every $H_i$ there exists $H \in L(G)$ for which $[H/1]$ is distributive and satisfies the maximal condition such that $H \leq H_i$ and $H \nsubseteq H_j$ for all $j \neq i$.

In particular, this property is preserved by projectivities.

(b) Therefore if $M$ is a nonnormal maximal subgroup of $G$ of finite index and $\varphi$ a projectivity from $G$ to a group $G$, then $G : M_\varphi$ is finite (and hence a prime). For, $M_\varphi$ inherits the lattice-theoretic property of Lemma 6.1.4 from $M$. Thus if $M_\varphi$ is not normal in $G$, then $G : M_\varphi$ is finite by 6.1.4; and if $M_\varphi \leq G$, then $G : M_\varphi$ is a prime.

We now handle the case of a normal maximal subgroup and first consider projective images.

6.1.6 Lemma. Let $N$ be a normal subgroup of prime index in the group $G$. If $\varphi$ is a projectivity from $G$ to a group $G$, then $G : N_\varphi$ is finite (and hence a prime).

Proof. The assertion of the lemma clearly holds if $N_\varphi \leq G$; so suppose that $N_\varphi$ is not normal in $G$. Let $a \in G \setminus N$ and $\langle b \rangle = \langle a \rangle_\varphi$. Then $|\langle a \rangle : N \cap \langle a \rangle| = |G : N| = p$ and hence $|\langle b \rangle : N_\varphi \cap \langle b \rangle| = q$ for some prime $q$. Consider the autoprojectivity $\sigma$ of $G$ defined by $X_\sigma = ((X_\varphi)^\sigma)^{-1}$ for $X \in G$. Since $b_\sigma \in N_\varphi$, we have $N_\sigma_\varphi = ((N_\varphi)^{\sigma})^{\sigma^{-1}} = N$ and hence

5. $T = N \cap N_\sigma \cap \cdots \cap N_\sigma^{q-1}$ is invariant under $\sigma$.

To simplify notation, we put $N_\sigma^i = N_i (i = 0, \ldots, q)$ and define for $i = 0, \ldots, q - 1$,

6. $R_i = N_0 \cap \cdots \cap N_i$ and $S_i = R_i^q = N_1 \cap \cdots \cap N_{i+1}$.

Finally, let $m$ be the smallest integer such that $R_m = T$. By (5), $m \leq q - 1$ and

7. $S_m = R_m = T$.

Since $N_\sigma^m = N$, we have $N_\sigma^j = N_j$ for all $j$, and it follows that

8. $R_i^\sigma = R_i$ and $S_i^\sigma = S_i$ for $i = 0, \ldots, m.$
We show next that for $i = 0, \ldots, m - 1$,

(9) $R_i \neq S_i, R_{i+1} = N \cap S_i$ is a normal subgroup of index $p$ in $S_i$ and $S_{i+1} = S_i \cap N_{i+2}$ is a maximal subgroup of $S_i$; thus

(10) $S_i = R_{i+1} S_{i+1}$ for $i = 0, \ldots, m - 2$

and the following section of the Hasse diagram of $L(G)$ illustrates the situation.

![Hasse diagram](image)

To prove these assertions, suppose first, for a contradiction, that $R_i = S_i$, that is $R_i = R_i^e$, for some $i \leq m - 1$. Then $R_i = R_i^e \leq N_j$ for all $j = 0, \ldots, q$ and hence $R_i \leq T$, contradicting the choice of $m$. Thus $R_i \neq S_i$ for $i = 0, \ldots, m - 1$ and, by (6), $R_{i+1} = N \cap S_i \leq S_i$ and $S_{i+1} = S_i \cap N_{i+2}$. To complete the proof of (9), it remains to be shown that $R_{i+1} \neq S_i$ and $S_{i+1} \neq S_i$. Then $|S_i : R_{i+1}| = |G : N| = p$ and $S_i \cap N_{i+2}$ is maximal in $S_i$ since $N_{i+2}$, as a projective image of $N$, is modular in $G$ so that $[S_i : S_i \cap N_{i+2}] = [S_i \cap N_{i+2} : N_{i+2}] = [G : N_{i+2}]$. So suppose, for a contradiction, that $R_{i+1} = S_i$ or $S_{i+1} = S_i$. The first assumption yields that $R_i \geq R_{i+1} = S_i = R_i^e$, and the second that $R_{i+1} = R_i$ and hence $R_i^e = S_i \geq R_{i+1} = R_i$. By (8), $R_i^e = R_i$ and so in both cases it would follow that $R_i^e = R_i$, a contradiction, as we have just shown. Thus (9) holds and, since for $i = 0, \ldots, m - 2$, $R_{i+1}$ and $S_{i+1}$ are different maximal subgroups of $S_i$, we clearly get (10).

Our aim is to show that $T$ is a normal subgroup of finite index in $G$. For this we first prove by induction that for $i = 0, \ldots, m - 1$,

(11) $\langle S_i^{e_j} | j = 0, \ldots, q - 1 \rangle = G$.

This is clear if $i = 0$ since $S_0 = N^e \neq N$ is a maximal subgroup of $G$. So suppose that (11) holds for some $i \leq m - 2$ and let $H = \langle S_i^{e_j} | j = 0, \ldots, q - 1 \rangle$. Then (8) and (10) show that $R_{i+1} = R_i^e = S_i^{e_{i+1}} \leq H$ and hence $S_i = R_{i+1} S_{i+1} \leq H$. Again by (8), $H$ is
invariant under \( \sigma \). Therefore all the \( S^*_j \) (\( j = 0, \ldots, q - 1 \)) are contained in \( H \) and, by induction, their join is \( G \). Thus \( H = G \) and (11) holds.

By definition, for any subgroup \( X \) of \( G \), \( (X^\sigma)^\sigma = (X^\sigma)^b \leq \langle X^\sigma, b \rangle \). Thus (11) implies in particular that

\[ \langle S^*_{m-1}, b \rangle = \overline{G}. \]

Again by definition, \( N_{j+1} = N^\sigma_{j+1} = N^\sigma_j \) and hence \( (N^\sigma_j)^b = N^\sigma_{j+1} \) for all \( j = 0, \ldots, q - 1 \). Since \( b^q \in N^\sigma = N^\sigma_0 \), it follows that \( b^q \in N^\sigma_j \) for all \( j \). Thus

\[ b^q \in T^\sigma. \]

By (5), \( T^\sigma \) is normalized by \( b \) and hence \( |\langle b \rangle T^\sigma : T^\sigma| = |\langle b \rangle : \langle b \rangle \cap T^\sigma| = q \). It follows that \( T^\sigma = N^\sigma \cap \langle b \rangle T^\sigma \) and \( T = N \cap \langle a, T \rangle \leq \langle a, T \rangle \). Now (9) implies that \( T = N \cap S_{m-1} \leq S_{m-1} \) and hence \( N_G(T)^\sigma \) contains \( \langle S^*_{m-1}, b \rangle = \overline{G} \). Thus

\[ (14) \quad T \leq G. \]

Again by (9), \( |S_{m-1}/T| = p \). If \( S_{m-i}/T \) is finite for some \( i \in \{1, \ldots, m-1\} \), then also its projective image \( R_{m-i}/T \) is finite and by (10), \( S_{m-i}/T \) is finite. It follows that \( S_0/T \) is finite, as must be \( R_0/T = N/T \); finally,

\[ (15) \quad G/T \text{ is finite.} \]

Let \( H_i/T \) (\( i = 1, \ldots, n \)) be the maximal cyclic subgroups of \( G/T \). Then \( G \) is covered irreducibly by the \( H_i \) and hence, by 6.1.5, \( \overline{G} \) is covered irreducibly by the \( H_i^\sigma \). Suppose, for a contradiction, that the intersection \( D \) of the \( H_i \) is not contained in \( N \). Then \( |D : D \cap N| = |G : N| = p \) and hence \( D/T \) would contain a subgroup \( E/T \) of order \( p \). From \( b^q \in T^\sigma \) and \( \langle a^\sigma \rangle^\sigma = (N \cap \langle a \rangle)^\sigma = N^\sigma \cap \langle b \rangle = \langle b^q \rangle \), it follows that \( a^\sigma \in T \). Therefore \( \langle a \rangle T/T \) and \( S_{m-1}/T \) are two different subgroups of order \( p \) in \( G/T \). One of them is different from \( E/T \) and lies in a maximal cyclic subgroup \( H_j/T \) of \( G/T \). Since \( D \leq H_i \), the cyclic group \( H_j/T \) would contain two different subgroups of order \( p \), a contradiction. Thus \( D \leq N \) and it follows that the intersection of the \( H_i^\sigma \) is contained in \( N^\sigma \). By 6.1.4, \( |\overline{G} : N^\sigma| \) is finite. Then \( \overline{G}/(N^\sigma)\overline{G} \) is a finite group and, by 5.1.2, \( |\overline{G} : N^\sigma| \) is a prime.

\[ \square \]

**The Zacher-Rips theorem**

We come to the main result of this section.

**6.1.7 Theorem** (Zacher [1980], Rips). Let \( \varphi \) be a projectivity from the group \( G \) to the group \( \overline{G} \) and suppose that \( H \) and \( K \) are subgroups of \( G \) such that \( K \leq H \). Then \( K \) has finite index in \( H \) if and only if \( K^\sigma \) has finite index in \( H^\sigma \).

**Proof.** Suppose that \( |H : K| \) is finite and let \( K = H_0 \leq \cdots \leq H_n = H \) such that \( H_i \) is a maximal subgroup of \( H_{i+1} \) for \( i = 0, \ldots, n - 1 \). Then \( |H_{i+1} : H_i| \) is finite and, by 6.1.5 and 6.1.6, also \( |H_i^\sigma : H_i^\sigma| \) is finite for all \( i \). It follows that \( |H^\sigma : K^\sigma| \) is finite.

\[ \square \]
Recall that a group is residually finite if it contains subgroups of finite index intersecting trivially. The above theorem clearly shows that this property is preserved by projectivities.

6.1.8 Corollary. Let \( \varphi \) be a projectivity from the group \( G \) to the group \( \tilde{G} \). If \( G \) is residually finite, then so is \( \tilde{G} \).

### Lattice-theoretic characterizations

The Zacher-Rips Theorem also yields lattice-theoretic characterizations of the finiteness of the index of a subgroup in a group. A first such characterization was given by Zacher [1980]; we present a simpler one and for this we need another consequence of Neumann’s lemma.

6.1.9 Lemma. Suppose that \( M \) is a maximal subgroup of the group \( G \) such that for every \( g \in G \), \( M \cap M^g \) is modular in \( G \) and \([G/M \cap M^g]\) is a finite lattice. Then \( M \) has finite index in \( G \).

**Proof.** This is clear if \( M \subseteq G \); so suppose that \( M \) is not normal in \( G \) and take \( x \in G \) such that \( M \neq M^x \). By assumption, \( D = M \cap M^x \) and \( M \) are modular subgroups of \( G \); furthermore \([G/D]\) is finite. By 2.1.6, \( M^x \) is modular in \( G \) and by 2.1.5, \([<M,M^x>/M^x]\) \(\cong [M/M \cap M^x]\). Since \( M^x \) is a maximal subgroup of \( G \), it follows that \( D \) is a maximal subgroup of \( M \). If \( H \neq M \) is another maximal subgroup of \( G \) containing \( D \), then \( M \cap H \) is maximal in \( H \) and \( D \leq M \cap H < M \). Thus \( D = M \cap H \) and \([G/D]\) is a lattice of length 2. Clearly, \( x \notin M \) and \( x \notin M^x \). Therefore \( M \cap <x> \) is a maximal subgroup of \( <x> \) and is contained in \( M \cap M^x = D \). Since \( D \mod G \), and hence \([<g>/D \cap <g>]\) \(\cong [<D,g>/D]\) for all \( g \in G \), we see that \( D \) is also maximal in \( <D,x> \) and therefore \( <D,x> \) is a maximal subgroup of \( G \) different from \( M \) and \( M^x \). This shows that \([G/D]\) has at least 3 atoms and so is not isomorphic to the subgroup lattice of a cyclic group. But \([<D,g>/D]\) is isomorphic to the subgroup lattice of \( <g>/D \cap <g> \) and it follows that \( <D,g> < G \) for all \( g \in G \). Thus \( G \) is covered by the atoms of \([G/D]\) none of which can be omitted from the covering. By 6.1.4, \(|G:M|\) is finite.

6.1.10 Theorem (Schmidt [1984b]). Let \( H \) and \( K \) be subgroups of the group \( G \) such that \( K \leq H \). Then \( K \) has finite index in \( H \) if and only if there exists a finite chain \( K = H_0 \leq \cdots \leq H_n = H \) of subgroups \( H_i \) such that for every \( i \in \{0, \ldots, n - 1\} \), \( H_i \) is a maximal subgroup of \( H_{i+1} \) and satisfies one of the following two conditions:

(a) \( H_{i+1} \) is covered irreducibly by finitely many subgroups whose intersection is contained in \( H_i \); or

(b) for every automorphism \( \sigma \) of the lattice \([H_{i+1}/1]\), the subgroup \( H_i \cap H_i^\sigma \) is modular in \([H_{i+1}/1]\) and \([H_{i+1}/H_i \cap H_i^\sigma]\) is finite.

**Proof.** If there exists such a chain, then by 6.1.4 and 6.1.9, \(|H_{i+1}:H_i|\) is finite for every \( i \) and hence \(|H:K|\) is finite. Conversely, suppose that \( K \) has finite index in \( H \)
and let \( K = H_0 \leq \cdots \leq H_n = K \) be a maximal chain of subgroups connecting \( K \) and \( H \). If \( i \in \{0, \ldots, n - 1\} \), then \( H_i \) is clearly a maximal subgroup of \( H_{i+1} \). If there exists an autoprojectivity \( \sigma \) of \( H_{i+1} \) such that \( H_i^\sigma \) is not normal in \( H_{i+1} \), then by the Zacher-Rips Theorem, \( H_i^\sigma \) has finite index in \( H_{i+1} \). By 6.1.4, \( H_{i+1} \) is covered irreducibly by finitely many subgroups whose intersection is contained in \( H_i \). Then \( H_{i+1} \) is also covered irreducibly by the images of these subgroups under \( \sigma^{-1} \) and the intersection of these is contained in \( H_i \); thus (a) holds. If there is no such autoprojectivity, then \( H_i^\sigma \) is a normal subgroup of prime index in \( H_{i+1} \) for every automorphism \( \sigma \) of \( [H_{i+1}/1] \). It follows that \( H_i \cap H_i^\sigma \leq H_{i+1} \), and \( H_{i+1}/H_i \cap H_i^\sigma \) is finite for every such \( \sigma \). Thus (b) is satisfied.

As observed in 6.1.5, property (a) can be described in \( L(G) \), so that the above theorem is indeed a lattice-theoretic characterization of the finiteness of \( |H : K| \). Another such characterization is given in Exercise 2.

**Exercises**

1. If a group \( G \) is covered by \( n \) cosets of subgroups \( H_i \), show that \( |G : H_i| < n \) for some \( i \).
2. (Schmidt [1984b]) Show that a maximal subgroup \( M \) of a group \( G \) has finite index in \( G \) if and only if it has one of the following properties:
   (i) \( M \) is not modular in \( G \), but there exists a modular subgroup \( S \) of \( G \) such that \( S \leq M \) and \( [G/S] \) is finite.
   (ii) There exists \( \tau \in P(G) \) such that \( M \cap M^\tau \mod G \) and \( [G/M \cap M^\tau] \) is a lattice of length 2 with at least 3 atoms.
   (iii) If \( \sigma \in P(G) \), then \( M \cap M^\sigma \mod G \) and \( [G/M \cap M^\sigma] = \{G, M, M^\sigma, M \cap M^\sigma\} \).

**6.2 Permodular subgroups**

We call a subgroup \( M \) of the group \( G \) **permodular in** \( G \) if

1. \( M \) is modular in \( G \), and
2. for every \( g \in G \) and \( Y \leq G \) such that \( M \leq Y \leq \langle M, g \rangle \) and \( [\langle M, g \rangle/Y] \) is a finite lattice, the index \( |\langle M, g \rangle : Y| \) if finite.

**6.2.1 Remark.** Since the finiteness of the index of a subgroup can be recognized in the subgroup lattice, and a subgroup \( X \) of \( G \) containing \( M \) has the form \( X = \langle M, g \rangle \) for some \( g \in G \) if and only if there exists \( H \leq G \) such that \( [H/1] \) is a distributive lattice satisfying the maximal condition and \( X = M \cup H \), condition (2) is a lattice-theoretic property. Thus the permodular subgroups can be recognized in the subgroup lattice, and if \( \phi \) is a projectivity from \( G \) to a group \( \bar{G} \) and \( M \) is permodular in \( G \), then \( M^\phi \) is permodular in \( \bar{G} \).
6.2 Permodular subgroups

Permodular subgroups were introduced by Zacher [1982b] who called them "D-embedded" since he used the term "Dedekind subgroup" for a modular subgroup. Our name is intended to express the close connection to modular and permutable subgroups.

6.2.2 Lemma. Every permutable subgroup is permodular.

**Proof.** Let $M$ be permutable in $G$. Then by 2.1.3, $M$ is modular in $G$. If $g \in G$ and $Y \leq G$ such that $M \leq Y \leq \langle M, g \rangle = X$ and $[X/Y]$ is finite, then $X = M\langle g \rangle$ and it follows that $Y = M(\langle g \rangle \cap Y)$. By 2.1.5, $[\langle g \rangle/\langle g \rangle \cap Y] \cong [X/Y]$ is a finite lattice and hence $|\langle g \rangle : \langle g \rangle \cap Y|$ is finite. But then $|X : Y| = |Y\langle g \rangle : Y| = |\langle g \rangle : \langle g \rangle \cap Y|$ is finite and $M$ is permodular in $G$.

Since permodularity is a lattice-theoretic property, the lemma implies that projective images of permutable subgroups, in particular of normal subgroups, are permodular. We want to use these permodular subgroups to approximate normal subgroups in the subgroup lattice. Therefore we have to investigate the structure of $M_G/M_G$ and $G/M_G$ for such a subgroup $M$ of $G$ and, as in the finite case, we want to reduce this problem to the case that $M$ is permutable in $G$. In fact, we shall be able to do this in the two situations which are important for us, namely when $M/M_G$ is periodic and when $G$ is finitely generated modulo $M$.

Basic properties of permodular subgroups

First of all we generalize Lemma 5.2.7 to permodular subgroups.

6.2.3 Lemma. If $M \text{ pmo } G$ and $g \in G$ such that $o(g, M)$ is infinite, then $g \in N_G(M)$.

**Proof.** Let $X = \langle M, g \rangle$ and $T$ be a maximal subgroup of $X$ containing $M$. Since $[X/M] \cong L(\langle g \rangle)$, there exists $Y \leq X$ such that $M \leq Y \leq T$ and $[X/Y]$ is a chain of length 2. By (2), $|X : Y|$ is finite and hence $X/Y_X$ is a finite group. Since $M$ is modular in $X$ and $[X/M]$ is a modular lattice, it follows from (c) of 2.1.6 that $Y$ is modular in $X$. By 5.1.3, $X/Y_X$ is a $p$-group for some prime $p$ and hence $T \leq X$. Now $M$ is the intersection of all the maximal subgroups of $X$ containing $M$. Thus $M \leq X$, as desired.

Our next aim is to replace condition (2) in the definition of a permodular subgroup by properties that are easier to work with. One of them will be that $g \in N_G(M)$ if $o(g, M)$ is infinite. The others are concerned with elements of finite order modulo $M$. First of all note that for a modular subgroup $M$ of $G$ and $g \in G$, by 2.1.5, $[\langle M, g \rangle/M] \cong [\langle g \rangle/\langle g \rangle \cap M]$ and hence

(3) $[\langle M, g \rangle/M]$ is finite if and only if $o(g, M)$ is finite.

We have to compute $M_G$ in a similar way as we did for finite groups in 5.1.6.
6.2.4 Lemma. For $M \leq G$, let $I(M)$ be the set of elements $x \in G$ such that $o(x, M)$ is a prime power or infinite, and let $J(M) = \{ x \in I(M) | o(x, M) < \infty \}$.

(a) If $M \mod G$, then $M_G = \bigcap \{ M^x | x \in I(M) \} = \bigcap \{ M_{M,x} | x \in I(M) \}$.

(b) If $M \permod G$, then $M_G = \bigcap \{ M^x | x \in J(M) \} = \bigcap \{ M_{M,x} | x \in J(M) \}$.

Proof. It is clear that (a) implies (b) since for a permodular subgroup $M$ of $G$, by 6.2.3, $M^x = M = M_{M,x}$ if $o(x, M)$ is infinite. So we have to prove (a). To accomplish this, first note that

$$D(M) = \bigcap \{ M_{M,x} | x \in I(M) \} = \bigcap \{ M^x | x \in I(M) \} =: D(M)$$

since the successive intersections involve fewer conjugates of $M$. We have to show that $D(M) \leq M^g$ for all $g \in G$; then it will follow that $D(M) \leq \bigcap \{ M^g = M_G \}$ and equality will hold in (4). So let $g \in G$. If $g \in I(M)$, then clearly $D(M) \leq M^g$. Thus suppose that $g \notin I(M)$ and let $o(g, M) = n = p_1^{r_1} \ldots p_t^{r_t}$ be the prime factor decomposition of $o(g, M)$. For $i = 1, \ldots, t$, put $n_i = n/p_i^{r_i}$ and take $r_i, s_i \in \mathbb{Z}$ such that $1 = p_i^{r_i}r_i + n_is_i$. Since $(g^{n_i,s_i})^{r_i} = g^{n_i,s_i} \in M$, we have $g^{n_i,s_i} \in I(M)$, and hence by 2.1.5,

$$D(M) \leq \bigcap_{i=1}^{t} M^{g^{n_i,s_i}} \leq \bigcap_{i=1}^{t} (M \cup \langle g^{n_i,s_i} \rangle)^{g^{n_i,s_i}} = \bigcap_{i=1}^{t} ((M \cup \langle g^{n_i,s_i} \rangle)^{g^{n_i,s_i}})^{g^{n_i,s_i}}$$

$$= \bigcap_{i=1}^{t} (M \cup \langle g^{n_i,s_i} \rangle)^{g} = \left( \bigcap_{i=1}^{t} (M \cup \langle g^{n_i,s_i} \rangle) \right)^{g} = \left( M \cup \bigcap_{i=1}^{t} \langle g^{n_i,s_i} \rangle \right)^{g}$$

$$= (M \cup \langle g^{n} \rangle)^{g} = M^g, \quad \text{as desired.}$$

6.2.5 Lemma. Let $M$ be a modular subgroup of the group $G$ normalized by every $g \in G$ with $o(g, M)$ infinite. Then the following properties are equivalent:

(a) $M$ is permodular in $G$;

(b) $|\langle M, g \rangle : M|$ is finite for every $g \in G$ such that $o(g, M)$ is finite;

(c) $|H : M|$ is finite for every $H \leq G$ such that $M \leq H$ and $[H/M]$ is finite;

(d) $|X : M|$ is finite for every $X \leq G$ such that $M \leq X$ and $[X/M]$ is a finite chain.

Proof. If $M \permod G$ and $g \in G$ such that $o(g, M) < \infty$, then by (3), $|\langle M, g \rangle / M|$ is finite and by (2), $|\langle M, g \rangle : M| < \infty$. Thus (a) implies (b). If (b) holds and $M \leq H \leq G$ such that $[H/M]$ is finite, then again by (3), $o(x, M) < \infty$ for all $x \in H$. So if $\mathcal{X} = \{ \langle M, x \rangle | x \in H \}$, it follows from (b) that $|X : M| < \infty$ for every $X \in \mathcal{X}$. Clearly, $H$ is covered irreduicibly by the set $\mathcal{X}^*$ of maximal elements of $\mathcal{X}$ and, by 6.1.3, $|H : X| < \infty$ for every $X \in \mathcal{X}^*$. It follows that $|H : M|$ is finite. Thus (b) implies (c) and we want to show next that (c) implies (a). So suppose that (c) holds and let $g \in G$ and $M \leq Y \leq \langle M, g \rangle$ such that $[\langle M, g \rangle / Y]$ is finite. If $o(g, M)$ is infinite, then by assumption, $M \leq \langle M, g \rangle$ and $\langle M, g \rangle / M$ is cyclic. Thus $|\langle M, g \rangle : Y| < \infty$. And if $o(g, M) < \infty$, then $|\langle M, g \rangle / M|$ is finite and (c) implies that $|\langle M, g \rangle : M| < \infty$. In particular, $|\langle M, g \rangle : Y|$ is finite and $M$ is permodular in $G$.

We have shown that (a), (b), and (c) are equivalent, and it is clear that (c) implies (d). To complete the proof of the lemma, we finally show that (d) implies (b). So
suppose that (d) holds and let \( g \in G \) such that \( o(g, M) < \infty \). Then by (3), \( [\langle M, g \rangle/M] \) is finite and we show by induction on \( |\langle M, g \rangle/M| \) that \( |\langle M, g \rangle : M| < \infty \). For this we may assume that \( \langle M, g \rangle = G \) and that \( [G/M] \) is not a chain. Since \( [G/M] \) is isomorphic to the subgroup lattice of a finite cyclic group, there exist two different maximal subgroups \( R \) and \( S \) of \( G \) containing \( M \) such that \( [G/T] = \{ T, R, S, G \} \) where \( T = R \cap S \). By (c) of 2.1.6, every subgroup of \( G \) containing \( M \) is modular in \( G \). In particular, \( T \mod G \) and, by 6.2.4, \( T_{G} = T_{R} \cap T_{S} \) since for \( x \in I(T) \), \( [\langle T, x \rangle/T] \) is either a chain or infinite and hence \( \langle T, x \rangle \in \{ R, S, T \} \). By 2.1.5, \( R = \langle M, h \rangle \) for some \( h \in \langle g \rangle \) and the induction assumption implies that \( |R : M| < \infty \). In particular, \( |R : T| < \infty \) and hence \( R/T_{R} \) is a finite group. Similarly, \( S/T_{S} \) is finite and therefore \( |T/T_{R} \cap T_{S}| < \infty \). Since \( T_{G} = T_{R} \cap T_{S} \), we see that \( R/T_{G} \) and \( S/T_{G} \) are finite groups. Since \( T/T_{G} \) and an element of prime power order of \( G/T_{G} \) cannot generate \( G/T_{G} \), this element has to lie in \( R/T_{G} \) or \( S/T_{G} \). Therefore \( G/T_{G} \) contains only finitely many such elements and, of course, no element of infinite order. But then every element of \( G/T_{G} \) is the product of its primary components and it follows that \( G/T_{G} \) can only contain a finite number of elements. In particular, \( |G : R| < \infty \) and hence \( |G : M| < \infty \), as desired.

One disadvantage of permodular as compared with modular subgroups is that they do not, at first sight, have the nice inheritance properties of the latter. For example, it is not so easy to see that the join of two permodular subgroups is again permodular. This is proved in 6.2.21 after some detours; however we shall need earlier the special cases of this result given in the following lemma. We do not know a simple, direct proof of 6.2.21.

6.2.6 Lemma. Let \( M \) be a permodular subgroup of the group \( G \).

(a) If \( H \leq G \), then \( M \cap H \) is permodular in \( H \).

(b) If \( N \leq G \), then \( MN \) is permodular in \( G \) and \( MN/N \) is permodular in \( G/N \).

(c) If \( L \) is permodular in \( G \) such that \( [M \cup L/M] \) and \( [M \cup L/L] \) are finite, then \( M \cup L \) is permodular in \( G \).

(d) For every \( g \in G \), \( M \cup M^{g} \) is permodular in \( G \).

Proof. (a) By 2.1.6, \( M \cap H \mod H \). If \( g \in H \), then \( o(g, M \cap H) = o(g, M) \). Therefore if \( o(g, M \cap H) \) is infinite, then \( M^{g} = M \) and hence also \( (M \cap H)^{g} = M \cap H \). If \( o(g, M \cap H) < \infty \) and \( \langle M, g \rangle = T \), then by (2), \( |T : M| < \infty \) and hence \( T/M_{T} \) is a finite group. Thus \( \langle M \cap H, g \rangle/\langle M \cap H, g \rangle \cap M_{T} \) is finite and, since \( \langle M \cap H, g \rangle \cap M_{T} \leq M \cap H \), it follows that \( |\langle M \cap H, g \rangle : M \cap H| < \infty \). By 6.2.5, \( M \cap H \) is permodular in \( H \).

(b) Again by 2.1.6, \( MN \mod G \). For \( g \in G \) such that \( o(g, MN) \) is infinite, \( o(g, M) \) is also infinite and hence \( (MN)^{g} = MN \). Now suppose that \( o(g, MN) < \infty \). If \( o(g, M) \) is infinite, then again \( g \in N_{G}(MN) \) and hence \( |\langle MN, g \rangle : MN| < \infty \). And if \( o(g, M) < \infty \), then by (2), \( |\langle M, g \rangle : M| < \infty \) and therefore \( |\langle MN, g \rangle : MN| = |N \langle M, g \rangle : NM| \) is finite. By 6.2.5, \( MN \) is permodular in \( G \) and hence \( MN/N \) is permodular in \( G/N \).

(c) By 2.1.6, \( H = M \cup L \mod G \). If \( g \in G \) and \( o(g, H) \) is infinite, then \( o(g, M) \) and \( o(g, L) \) are infinite and hence \( H^{g} = M^{g} \cup L^{g} = M \cup L \). We want to verify (d) of 6.2.5 for \( H \) and use induction on the length of the chain \( [X/H] \). So suppose that
Projectivities and normal structure of infinite groups

$H \leq X \leq G$, $[X/H]$ is a finite chain and $|Y : H| < \infty$ for all chains $[Y/H]$ of smaller length. If $H^X \leq X$, then $X/H^X$ is a finite group, $|H^X : H| < \infty$ by induction and hence $|X : H| < \infty$; so assume that $H^X = X$. Then since $[X/H]$ is a chain, there exists $x \in X$ such that $X = H \cup H^X$. As $M = M \cup L$ and $[X/H^X] \simeq [X/H]$ is a chain, it follows that $X = M \cup H^X$ or $X = L \cup H^X$; without loss of generality suppose that $X = M \cup H^X$. Then $[X/M] \simeq (H/H^X \cap M) \simeq [H/H \cap M^{X^{-1}}]$. By 6.2.3 and (b) of 6.2.5, either $M^x = M$ or $\langle M, x \rangle / M_{\langle M, x \rangle}$ is a finite group. In both cases, $|M : M \cap M^{x^{-1}}| < \infty$. By (c) of 6.2.5, $|H : M| < \infty$ and hence $|H : M \cap M^{x^{-1}}| < \infty$. Since $H \cap M^{x^{-1}} \geq M \cap M^{x^{-1}}$, it follows that $|H : H \cap M^{x^{-1}}| < \infty$ and therefore $[H/H \cap M^{x^{-1}}]$ is a finite lattice. Thus $[X/M]$ is finite and, by 6.2.5, $|X : M| < \infty$. In particular, $|X : H| < \infty$ and $H \not\leq G$.

We often have to consider elements or finite subsets of $MG$. We show next that in such a situation we may usually assume that $G$ is finitely generated modulo $M$, and then prove the basic result that in this case $|MG : M|$ is finite for a permodular subgroup $M$ of $G$. Recall that a group $G$ is finitely generated modulo its subgroup $H$ if there exists a finite subset $F$ of $G$ such that $G = \langle H, F \rangle$.

6.2.7 Lemma. If $M \leq G$ and $F$ is a finite subset of $MG$, then there exists a subgroup $L$ of $G$ containing $M$ such that $L$ is finitely generated modulo $M$ and $F \subseteq ML$.

Proof. For any $x \in F \subseteq MG$, there exist $z_i \in G$ and $y_i \in M^{z_i}$ such that $x = y_1 \ldots y_n$. Therefore if $L$ is generated by $M$ and all these $z_i$, then $L$ is finitely generated modulo $M$ and all the $y_i \in M^L$. Thus $x \in M^L$ and it follows that $F \subseteq M^L$.

6.2.8 Lemma. If $M$ is permodular in $G$ and $G$ is finitely generated modulo $M$, then $|MG : M|$ is finite.

Proof. Let $G = \langle M, g_1, \ldots, g_m \rangle$. We prove the assertion by induction on the sum $s$ of all the $o(g_i, M) (i = 1, \ldots, m)$ which are finite. If $M^g = M$ for all $i$, then $M \leq G$ and $|MG : M| = 1$ clearly is finite. So suppose that $M^g \neq M$, say, and consider $H = M \cup M^g$. By 6.2.3 and 6.2.5, $o(g_1, M)$ and $|H : M| \leq |\langle M, g_1 \rangle : M|$ are finite. By (d) of 6.2.6, $H$ is permodular in $G = \langle H, g_1, \ldots, g_m \rangle$ and the sum of all the $o(g_i, H) (i = 1, \ldots, m)$ which are finite is less than $s$. For, since $M < H \leq \langle M, g_1 \rangle$, it follows that $M \cap \langle g_1 \rangle < H \cap \langle g_1 \rangle$ and hence $o(g_1, H) < o(g_1, M)$; furthermore, clearly, $o(g, H) \leq o(g, M)$ for all $g \in G$ and if $o(g, M)$ is infinite, then so is $o(g, H)$ since $|H : M|$ is finite. The induction assumption implies that $|H^G : H| < \infty$. Since $M^G = H^G$ and $|H : M| < \infty$, it follows that $|MG : M| < \infty$.

Permodularity and permutability

In 5.1.1 we proved that a subgroup of a finite group is permutable if and only if it is modular and subnormal. However, it follows from the results of Chapter 2 that a
permutably subgroup of an infinite group need not be subnormal. The following example will also show that some other conceivable statements are not true.

6.2.9 Example. Let \( p \) be a prime, \( T \) an abelian group of type \( p^{\infty} \), and \( \bar{G} = T \langle z \rangle \) the semidirect product of \( T \) and an infinite cyclic group \( \langle z \rangle \) with respect to the automorphism \( t \to t^{1+p} (t \in T) \) of \( T \) (or \( t \to t^5 \) for \( p = 2 \)). By 2.4.11, every subgroup of \( \bar{G} \) is permutable in \( \bar{G} \). Since the automorphism induced by \( z \) in the cyclic subgroup of order \( p^n \) of \( T \) has order \( p^{n-1} \), we have \( \langle z \rangle^{\bar{G}} = 1 \); also a normal subgroup \( H \) of \( \bar{G} \) containing \( \langle z \rangle \) has abelian factor group and therefore contains \( \bar{G}' = T \), thus \( \langle z \rangle^{\bar{G}} = \bar{G} \). In particular, \( \langle z \rangle \) is not subnormal in \( \bar{G} \). For later use, note that if \( N \) is an infinite cyclic group, then by 2.5.14 there exists a projectivity \( \varphi \) from the abelian group \( \bar{G} = T \times N \) to \( \bar{G} \) mapping the normal subgroup \( N \) of \( G \) to the core-free, infinite cyclic subgroup \( \langle z \rangle \) of \( \bar{G} \).

The example shows that in order to generalize Theorem 5.1.1 and to give a criterion for a modular or permodular subgroup \( M \) of an arbitrary group to be permutable, we have to weaken the assumption that \( M \) is subnormal. For the relevant generalizations of subnormality we refer the reader to Robinson [1982], pp. 344 and 364. Note that every subnormal subgroup is ascendant and every ascendant subgroup is serial.

6.2.10 Theorem (Stonehewer [1972], [1976a]; Zacher [1982b]). The following properties of a subgroup \( M \) of the group \( G \) are equivalent:

(a) \( M \) is permutable in \( G \),
(b) \( M \) is permodular and serial in \( G \),
(c) \( M \) is modular and ascendant in \( G \).

Proof. We first show that (b) and (c) follow from (a). So let \( M \) be permutable in \( G \). By 6.2.2, \( M \) is permodular and hence also modular in \( G \). Since every ascendant subgroup is serial, it remains to be shown that \( M \) is ascendant in \( G \). For this we consider the set \( \mathcal{X} \) of ascending series (for ordinals \( \rho \)) of the form

\[
5. M = M_0 \leq M_1 \leq \cdots \leq M_{\rho} \leq M^G
\]

such that \( M_\alpha \) per \( G \) and \( M_{\alpha+1}/M_\alpha \) is a finite cyclic group for every ordinal \( \alpha < \rho \). If we order \( \mathcal{X} \) in the usual way—two series are comparable if one of them is an initial part of the other—Zorn's Lemma yields a maximal element in \( \mathcal{X} \); let (5) be this series and put \( H = M_\rho \). We show that \( H = M^G \); then, clearly, \( M \) is ascendant in \( G \). So suppose, for a contradiction, that \( H \neq M^G \). Then there exists \( g \in G \) such that \( H < HH^g \). Since \( H \) is permutable in \( G \), we can assert \( HH^g \leq H \langle g \rangle \) and by 6.2.3, \( o(g, H) < \infty \). It follows that \( |HH^g : H| \) is finite and hence \( H \leq H \langle g \rangle \) by 5.1.1. Therefore if we put \( L_0 = HH^g \) and form the successive normal closures \( L_\iota+1 = H^{L_\iota} \) \( (i = 0, 1, \ldots) \) of \( H \), this series reaches \( H \). For the last member \( L_\iota \), different from \( H \), of this series, \( H \leq L_\iota \) and \( L_\iota/H \) is cyclic since \( H \leq L_\iota \leq H \langle g \rangle \). Furthermore \( L_\iota \) is permutable in \( G \) since it is a join of conjugates of \( H \). Thus we can extend the series (5) by putting \( M_{\rho+1} = L_\iota \), and this contradicts the maximality of this series.
Now suppose conversely that (b) or (c) is satisfied. Thus $M$ is modular and ascendent, or permodular and serial in $G$, and we have to show that $M$ is permutable in $G$, that is, $\langle M, x \rangle = M \langle x \rangle$ for all $x \in G$. For this we may assume that $M \trianglelefteq \langle M, x \rangle = T$. For, if $M$ is permodular in $G$, then $M \trianglelefteq T$ for $o(x, M)$ infinite; in addition, if $o(x, M) < \infty$, then $[T/M]$ is finite and $M$ serial in $T$ implies that $M \trianglelefteq \trianglelefteq T$. If $M$ is not permodular in $G$, then $M$ is ascendant in $T$ and hence $M \trianglelefteq \trianglelefteq T$ since $[T/M] \simeq [\langle x \rangle/\langle x \rangle \cap M]$ satisfies the maximal condition. So suppose that
\[(6) \quad M = M_0 \trianglelefteq M_{n-1} \leq \cdots \leq M_1 \trianglelefteq M = T = \langle M, x \rangle.\]
Since $M \mod T$, we have $M_1 = M \cup (\langle x \rangle \cap M_1)$ and by induction on the length of the chain (6), $M_1 = M(\langle x \rangle \cap M_1)$. It follows that $T = M_1 \langle x \rangle = M(\langle x \rangle \cap M_1) \langle x \rangle = M \langle x \rangle$.

We want to show next that a permodular subgroup $M$ is permutable if there is an element of infinite order modulo $M$. For this we need a simple lemma.

6.2.11 Lemma. If $M \text{ pmo } G$ and $g \in G$ such that $o(g, M) = \infty$, then $M^x \cap \langle g \rangle = 1$ for all $x \in G$.

Proof. Suppose, for a contradiction, that there exists $x \in G$ such that $M^x \cap \langle g \rangle = \langle g^n \rangle$ for some $n \in \mathbb{N}$. Then $\langle M, g^n \rangle \leq M \cup M^x \leq \langle M, x \rangle$ and, by assumption, $o(g^n, M) = \infty$. Thus by (3), $[\langle M, g^n \rangle/M]$ is infinite, therefore $[\langle M, x \rangle/M]$ and $o(x, M)$ are infinite as well. By 6.2.3, $M^x = M$ and then $M \cap \langle g \rangle = \langle g^n \rangle$. But this contradicts the assumption that $o(g, M)$ is infinite.

6.2.12 Theorem (Zacher [1982b]). Let $M$ be a permodular subgroup of the group $G$ and suppose that there exists $g \in G$ such that $o(g, M)$ is infinite. Then

$$M \trianglelefteq A(M) := \langle x \in G | o(x, M) = \infty \rangle \trianglelefteq G$$

and hence $M$ is permutable in $G$.

Proof. Let $g \in G$ such that $o(g, M)$ is infinite. For $z \in M$,

$$[\langle zg \rangle/\langle zg \rangle \cap M] \simeq [\langle M, zg \rangle/M] = [\langle M, g \rangle/M] \simeq [\langle g \rangle/\langle g \rangle \cap M].$$

It follows that $o(zg, M)$ is infinite and hence $z \in \langle g, zg \rangle \leq A(M)$. Thus $M \leq A(M)$ and $M \trianglelefteq A(M)$ by 6.2.3. Let $x \in G$. Then by 6.2.11, $M^x \cap \langle g \rangle = 1$ and hence $o(g, M^x)$ is infinite. Thus $g \in A(M^x)$ and it follows that $A(M) \leq A(M^x)$. Since $M^x$ is permodular in $G$, we get the other inclusion and hence $A(M) = A(M^x) = A(M)^x$. Thus $A(M) \trianglelefteq G$; in particular, $M \trianglelefteq \trianglelefteq G$ and, by 6.2.10, $M$ is permutable in $G$.

An example of a nonnormal permutable subgroup $M$ with an element of infinite order modulo $M$ is given in Exercise 6.3.2.
6.2 Permodular subgroups

Periodic permodular subgroups

We come to the main subject of this section, the structure of \( G/M_G \) and \( M^G/M_G \) for a permodular subgroup \( M \) of \( G \). We first of all collect the results proved so far on \( M_G \) and \( M/M_G \).

6.2.13 Remark. Let \( M \) be permodular in \( G \) and let \( J(M) \) be the set of elements \( x \in G \) such that \( o(x, M) \) is a prime power. By 6.2.4,

\[
(7) \quad M_G = \bigcap \{ M_{\langle x \rangle} \mid x \in J(M) \}.
\]

Let \( x \in J(M) \) and \( T = \langle M, x \rangle \). Then \( [T/M] \cong [\langle x \rangle/\langle x \rangle \cap M] \) and hence

\[
(8) \quad [T/M] \text{ is a finite chain.}
\]

By 6.2.5, \( |T : M| \) is finite and therefore \( T/M_T \) is a finite group. By 5.1.3,

\[
(9) \quad T/M_T \text{ is nonabelian of order } pq \text{ or a finite } p\text{-group;}
\]

and in the latter case, \( M \) is permutable in \( T \), by 6.2.10. In any case,

\[
(10) \quad M/M_T \text{ is a finite primary group.}
\]

In particular, \( M/M_G \) is a subdirect product of finite nilpotent groups.

We now study permodular subgroups \( M \) for which \( M/M_G \) is periodic.

6.2.14 Theorem. Let \( M \) be a permodular subgroup of the group \( G \) such that \( M/M_G \) is periodic. Then \( M/M_G \) is the direct product of its Sylow subgroups and \( M^G/M_G \) is locally finite. In particular, \( M/M_G \) is locally nilpotent.

Proof. Of course, we may assume that \( M_G = 1 \), and we show first that with this condition \( M \) is \( p \)-closed for every prime \( p \). To do this we let \( x, y \) be \( p \)-elements of \( M \) and suppose that \( z \) is a \( p' \)-element in \( \langle x, y \rangle \). In every finite nilpotent factor group \( M/N \) of \( M \), the elements \( xN \) and \( yN \) generate a \( p \)-group and \( zN \) is a \( p' \)-element in this \( p \)-group; thus \( z \in N \). By 6.2.13, \( M \) is a subdirect product of finite nilpotent groups and it follows that \( z = 1 \). Thus \( \langle x, y \rangle \) is a \( p \)-group and \( M \) is \( p \)-closed. This holds for every prime \( p \) and hence \( M \) is the direct product of its Sylow subgroups. Now let \( g_1, \ldots, g_m \in M \) and \( H = \langle g_1, \ldots, g_m \rangle \). We show that

\[
(11) \quad H \text{ is finite.}
\]

Since \( H \leq M \) is the direct product of its Sylow subgroups, it will follow that \( H \) is a finite nilpotent group and that \( M \) is locally finite and locally nilpotent. As every element is the product of its primary components and \( M \) is the direct product of its Sylow subgroups, we may assume in the proof of (11) that all the \( g_i \) are \( p \)-elements for a fixed prime \( p \). Let \( p' \) be the maximal order of such an element \( g_i \). We show that

\[
(12) \quad H^{(r)} = 1;
\]

then \( H \) is a finitely generated soluble torsion group and hence finite (see Robinson [1982], p. 147). To prove (12), we may assume that \( r \geq 1 \) and, by 6.2.13, we have to
show that $H^{(r)} \leq M_T$ for all the groups $T = \langle M, x \rangle$ with $x \in J(M)$. If $T/M_T$ is non-abelian of order $pq$, then $H^{(r)} \leq M' \leq M_T$; and if $T/M_T$ is a $q$-group for some prime $q \neq p$, then all the $g_i$ are contained in $M_T$ and hence $H \leq M_T$. Finally, suppose that $T/M_T$ is a finite $p$-group. Then $HM_T/M_T \leq \Omega_q(T/M_T)$ and, by (d) of 5.2.8, this group is soluble of derived length at most $r$. Thus again $H^{(r)} \leq M_T$ and (12) holds.

It remains to show that $M^G$ is locally finite. For this let $F$ be a finite subset of $M^G$. By 6.2.7 there exists a subgroup $L$ of $G$ containing $M$ such that $L$ is finitely generated modulo $M$ and $F \subseteq M^L$. By 6.2.8, $|M^L : M|$ is finite. Therefore $\langle F \rangle \cap M$ is a subgroup of finite index in $\langle F \rangle$ and hence is finitely generated (see Robinson [1982], p. 36). Since $M$ is locally finite, $\langle F \rangle \cap M$, and hence $\langle F \rangle$, is finite. Thus $M^G$ is locally finite.

We want to show that if $M$ is permutable in $G$, then the Sylow subgroups of $M/M_G$ appearing in 6.2.14 are permutable in $G/M_G$ and their normal closures are the Sylow subgroups of $M^G/M_G$. In fact, we prove more general assertions.

6.2.15 Lemma. Let $\pi$ be a set of primes and $M$ a $\pi$-subgroup of the group $G$. If

(a) $M \leq \leq G$ or
(b) $M$ per $G$,

then $M^G$ is a $\pi$-group.

Proof. (a) Let $M = M_0 \leq \cdots \leq M_n = G$. We prove the assertion by induction on $n$. Let $H = M_{n-1}$. Then the induction assumption yields that $M^H$ is a $\pi$-group, and since $H \leq G$, we have $M^H \leq M^G \leq H$. It follows that $M^H \leq M^G$ and $M^G = (M^H)^G$ is a product of normal $\pi$-subgroups. Then every element of $M^G$ lies in a product of finitely many normal $\pi$-subgroups and hence is a $\pi$-element. Thus $M^G$ is a $\pi$-group.

(b) Let $x \in M^G$. By 6.2.7 there exists a subgroup $L$ of $G$ containing $M$ that is finitely generated modulo $M$ such that $x \in M^L$ and, by 6.2.8, $|M^L : M| < \infty$. By 6.2.10, $M$ is ascendant in $G$, hence subnormal in $M^L$ and therefore also in $L$. By (a), $M^L$ is a $\pi$-group. Thus $x$ is a $\pi$-element and $M^G$ is a $\pi$-group.

Note that since the product of normal $\pi$-subgroups is a normal $\pi$-subgroup, it follows from 6.2.15 that, quite generally, the join of permutable (or subnormal) $\pi$-subgroups is a $\pi$-group.

6.2.16 Lemma. Let $M = A \times B$ be a periodic permutable subgroup of $G$ and suppose that $(o(a), o(b)) = 1$ for all $a \in A, b \in B$. Then $A$ and $B$ are permutable in $G$.

Proof. We show that $A$ per $G$. Let $\pi = \pi(A)$ be the set of primes dividing the order of an element of $A$ and let $x \in G$. We have to prove that $A \langle x \rangle = \langle x \rangle A$. If $o(x)$ is infinite, then by 6.2.3, $x \in N_G(M)$ and hence $x \in N_G(A)$. So we may assume that $o(x) < \infty$ and then, of course, that $o(x) = p^n$ for some prime $p$. Let $H = M \langle x \rangle$. Then $|H : M| = |\langle x \rangle : \langle x \rangle \cap M|$ and hence $|M : M \cap M^p| = |M^p : M^p|$ is a power of $p$ for every $y \in H$. Therefore if $p \notin \pi$, then $A \leq M_H$ and, as a characteristic subgroup of this group, $A \leq H$. Finally, suppose that $p \in \pi$. By 6.2.10, $M \leq H$, hence $A \leq H$, and
(a) of 6.2.14 shows that $A^H$ is a $\pi$-group. Hence $A^H \langle x \rangle$ is a $\pi$-group and it follows that $A^H \langle x \rangle \cap M = A$. Now (11) of 5.1 yields that $A$ is permutable in $A^H \langle x \rangle$ and this implies that $A \langle x \rangle = \langle x \rangle A$.

\[ \square \]

The above results sufficiently elucidate the structure of $M^G/M_G$ for periodic permutable subgroups $M$ of $G$ (see Theorem 6.3.1). We turn to the more general case of periodic permodular subgroups; we wish to prove a structure theorem similar to 5.1.14 for finite groups. For this purpose it is convenient to introduce a notation for the situation that appears in this theorem. In the literature the term “Schmidt structure” has been used (see Stonehewer [1976b], Zacher [1982a]), but we prefer to speak of $P$-embedded subgroups instead.

**P-embedding**

The subgroup $M$ of the group $G$ is called **$P$-embedded** in $G$ if $G/M_G$ is a periodic group of the form

\[ G/M_G = (S_1/M_G \times S_2/M_G \times \cdots) \times T/M_G, \]

where the number of factors $S_i/M_G$ may be finite (nonzero) or infinite, and for all $i, j$,

\begin{enumerate}
  \item $S_i/M_G$ is a nonabelian (possibly infinite) $P$-group,
  \item $(o(x), o(y)) = 1$ for all $x \in S_i/M_G$ and $y \in S_j/M_G$ with $j \neq i$ or $y \in T/M_G$,
  \item $M/M_G = (Q_1/M_G \times Q_2/M_G \times \cdots) \times (M \cap T)/M_G$ and $Q_i/M_G$ is a nonnormal Sylow subgroup of $S_i/M_G$, and
  \item $M \cap T$ is permutable in $G$.
\end{enumerate}

Every $P$-embedded subgroup is permodular in $G$, as the reader may easily prove. Our aim is to show the converse, at least for nonpermutable subgroups in periodic groups. The situation in arbitrary groups is more complicated; see Exercises 3 and 4.

**6.2.17 Theorem.** Let $M$ be a permodular subgroup of the group $G$ such that $M/M_G$ is periodic. Then $M$ is permutable or $P$-embedded in $G$.

**Proof.** We assume that $M$ is not permutable in $G$ and also, of course, that

\[ M_G = 1. \]

By 6.2.12, $o(g, M)$ is finite for every $g \in G$ and, since $M$ is periodic, it follows that

\[ G \text{ is periodic.} \]

By 6.2.14, $M$ is the direct product of its Sylow subgroups. Since $M$ is not permutable in $G$, there exist Sylow subgroups of $M$ that are not permutable in $G$. Let $Q$ be one of these, $q$ the corresponding prime and $K$ the $q$-complement of $M$, so that

\[ M = Q \times K. \]
We shall show in a number of steps that \(|Q| = q\), \(Q^G\) is a nonabelian \(P\)-group, 
\(G = Q^G \times C_G(Q^G)\) and the groups \(Q^G\) and \(C_G(Q^G)\) are coprime.

Since \(Q\) is not permutable in \(G\), there exists \(x \in G\) of prime power order such that 
\(Q \langle x \rangle \neq \langle x \rangle Q\). Let \(x\) be such an element and \(X = \langle M, x \rangle\). Since \(M\) is permodular in \(G\), \(|X : M|\) is finite. If \(M\) were permutable in \(X\), then by 6.2.16, \(Q\) would also be permutable in \(X\) and hence \(Q \langle x \rangle = \langle x \rangle Q\), a contradiction. Thus \(M\) is not permutable in \(X\), but \(x \in J(M)\); by 6.2.13, \(X/M_X\) is nonabelian of order \(rs\) for primes \(r\) and \(s\). If \(Q \leq M_X\), then \(Q\) would be a characteristic subgroup of \(M_X \leq X\) and therefore \(x \in N_G(Q)\). This is not the case; hence \(QM_X = M\) and it follows that \(|M : M_X| = q\) is the smaller prime dividing \(|X/M_X|\). Thus we have shown:

(21) If \(x \in G\) is of prime power order such that \(Q \langle x \rangle \neq \langle x \rangle Q\), and if \(X = \langle M, x \rangle\),
then \(|M : M_X| = q\) and \(X/M_X\) is nonabelian of order \(rq\) for some prime \(r > q\).

Suppose that \(x\) and \(X\) are as before, let \(y \in G\) and consider \(H = \langle M, x, y \rangle = \langle X, y \rangle\). Since \(M\) is a maximal subgroup of \(X\), we see that \(X = M \cup M^x\) is permodular in \(G\) by (d) of 6.2.6. It follows that \(|H : X|\), and hence also \(|H : M|\), is finite. Then \(H/M_H\) is a finite group containing the core-free modular subgroup \(M/M_H\) with Sylow \(q\)-subgroup \(QM_H/M_H\). By 5.1.14, \(M\) is \(P\)-embedded in \(H\). If \(QM_H\) were permutable in \(H\), it would also be permutable in \(X\), and then \(M = (QM_H)M_X\) would be permutable in \(X\), contradicting (21). Thus \(QM_H/M_H\) is not permutable in \(H/M_H\) and hence it cannot lie in the permutable part of the decomposition (16) of \(M/M_H\). Therefore:

(22) If \(x\) is as in (21), \(y \in G\) and \(H = \langle M, x, y \rangle\), then \(H/M_H\) is a finite group, \(M\) is 
\(P\)-embedded in \(H\), \((QM_H)^H/M_H\) is a nonabelian \(P\)-group, and \(QM_H/M_H\) is a 
Sylow \(q\)-subgroup of order \(q\) of \(H/M_H\).

In particular, \(|Q : Q \cap M_H| = q = |Q : Q \cap M_X|\). But \(X \leq H\) implies \(M_H \leq M_X\) and it follows that \(Q \cap M_X = Q \cap M_H \leq M_H \leq M^q\). Since \(y \in G\) was arbitrary, \(Q \cap M_X \leq M_G = 1\) and hence

(23) \(|Q| = q\).

Now suppose that \(y\) is a \(q\)-element. If \(\langle Q, y \rangle\) is a \(q\)-group and again \(H = \langle M, x, y \rangle\), then by (22), \(QM_H/M_H\) is a Sylow \(q\)-subgroup of \(H/M_H\); on the other hand, \(\langle Q, y \rangle M_H/M_H\) is a \(q\)-group. It follows that \(\langle Q, y \rangle \leq QM_H \leq M\) and then \(y \in Q\) since \(Q\) is the only Sylow \(q\)-subgroup of \(M\). This shows that \(Q\) is a Sylow \(q\)-subgroup of \(G\). If \(\langle Q, y \rangle\) is not a \(q\)-group, then \(\langle Q, y \rangle \neq \langle y \rangle Q\) and we may choose \(y = x\) in (21).

We obtain that \(y\) is contained in a conjugate of \(M\) in \(X = \langle M, x \rangle\) and then, clearly, \(y\) is contained in a conjugate of \(Q\). Thus

(24) \(Q \in \text{Syl}_q(G)\) and every \(q\)-element of \(G\) is contained in \(Q^G\).

Now let \(g \in G \setminus N_G(Q)\), so that \(Q^g \neq Q\). Since \(Q \in \text{Syl}_q(G)\), we have \(Q \langle x \rangle \neq \langle x \rangle Q\) for \(Q^g = \langle x \rangle\). Therefore if \(X = \langle M, x \rangle = \langle M, Q^g \rangle\), then by (21), \(X/M_X\) is a nonabelian group of order \(rq\) for some prime \(r > q\). By (23), \(M_X\) is the \(q\)-complement \(K\) in \(M = Q \times K\). Furthermore, \(Q^gK/K\) is a subgroup of order \(q\) in \(X/K\) and hence is conjugate to \(M/K\). Thus \(Q^gK\) is conjugate to \(M\) and it follows that \(Q^gK = Q^g \times K\). Thus \(K\) is centralized by \(Q^g\) and, since \(g\) was arbitrary,

(25) \(Q^G \leq C_G(K)\).
The nonabelian group \( \langle M, Q^g \rangle /K \) of order \( rq \) has a unique minimal normal subgroup \( S_g/K \), say; clearly, \( \langle M, Q^g \rangle = \langle S_g, M \rangle \). Let \( S = \langle S_g \mid g \in G \rangle \). Then \( Q^g K/K = \langle S_g, M \rangle /K \). For \( g, h \in G \), again write \( X = \langle M, Q^g \rangle \) and \( H = \langle M, Q^g, Q^h \rangle = \langle S_g, S_h, M \rangle \). Then \( K = M_H \) and, by (22), \( H/K \) is a finite group in which \( M/K \) is a modular, nonpermutable subgroup of order \( q \) that together with its conjugates \( Q^g K/K \) and \( Q^h K/K \) generates \( H/K \). By 5.1.9, \( H/K \) is a nonabelian \( P \)-group. Thus \( |S_g/K| = |S_h/K| \), \( [S_g/K, S_h/K] = 1 \) and \( M/K \) induces a universal power automorphism in \( S_g S_h/K \). This shows that \( S/K \) is an elementary abelian \( p \)-group for some prime \( p \), and \( SM/K = Q^g K/K \) is a nonabelian \( P \)-group. By (25), \( Q^g \cap K \leq Z(Q^g) \) and since \( Q^g / Q^g \cap K \approx Q^g K/K \), as a nonabelian \( P \)-group, has trivial centre, it follows that \( Q^g \cap K = Z(Q^g) \leq G \). Now \( M_g = 1 \) implies that \( Q^g \cap K = 1 \) and hence that

(26) \( Q^g \) is a nonabelian \( P \)-group.

Let \( P \) be the normal Sylow \( p \)-subgroup of \( Q^g \). We want to show that \( P \) is the set of \( p \)-elements of \( G \). For this we choose a conjugate \( Q^g = \langle x \rangle \neq Q \) of \( Q \) and put \( X = \langle M, x \rangle \). If \( M \) contained an element of order \( p \), then, since \( n M < M, y > < n M, y > < n M, y > = 1 \), there would exist a subgroup \( H = \langle X, y \rangle \) of \( G \) such that \( M/M_H \) contains an element of order \( p \). By (22), this implies that \( M \) is \( P \)-embedded in \( H \) and \( (QM_H)^R / M_H \) is a nonabelian \( P \)-group. By (26), \( p \) would divide \( |(QM_H)^R / M_H| \) and hence, by (15), could not divide \( |M : M_H| \), a contradiction. Thus \( M \) does not contain an element of order \( p \). Now let \( y \) be an arbitrary \( p \)-element of \( G \) and, this time, \( H = \langle X, y \rangle \). Then again by (22) and (26), \( (QM_H)^R / M_H \) contains the unique Sylow \( p \)-subgroup of \( H/M_H \). It follows that \( y \in Q^g M_H \leq Q^g M \) and, since \( M \) does not contain \( p \)-elements, \( y \in Q^g \). Thus \( y \in P \) and hence

(27) \( P \) is the unique Sylow \( p \)-subgroup of \( G \).

We finally show that

(28) \( G = Q^g \times C_G(Q^g) \).

Every element is the product of its primary components and, by (24) and (27), \( Q^g \) contains every \( p \)-element and every \( q \)-element of \( G \). Therefore to prove (28), we only have to show that for every prime \( t \) such that \( p \neq t \neq q \), every element of order \( t^n \) of \( G \) centralizes \( Q^g \). So let \( x \) be such an element. If \( Q \langle x \rangle \neq \langle x \rangle Q \), we would consider \( X = \langle M, x \rangle \) and obtain from (21) and (26) that \( |X : M_X| = p q \). It would follow that \( x \in M_X \) and hence \( Q^X = Q \), a contradiction. Thus \( Q \langle x \rangle = \langle x \rangle Q \) and hence \( Q \langle x \rangle = \langle x \rangle Q \). By (26), \( Q = Q \langle x \rangle \cap Q^g \leq Q \langle x \rangle \) and so \( x \in N_G(Q) \). If \( g \in G \), then \( x^{g^{-1}} \) also is a \( t \)-element; therefore \( x^{g^{-1}} \in N_G(Q) \), that is, \( x \in N_G(Q^g) \). Thus \( x \) normalizes every \( q \)-subgroup of \( Q^g \) and, since in this \( P \)-group every subgroup is the join of \( q \)-subgroups or is the unique Sylow \( p \)-subgroup of such a join, every subgroup of \( Q^g \) is normalized by \( x \). Hence \( x \) induces a power automorphism in \( Q^g \) which, by 1.4.3, is trivial since \( Z(Q^g) = 1 \). Thus \( x \in C_G(Q^g) \) and (28) holds.

To complete the proof of Theorem 6.2.17, let \( Q_1, Q_2, \ldots \) be those Sylow subgroups of \( M \) which are not permutable in \( G \) and let \( R \) be the join of the other Sylow subgroups of \( M \). Then \( R \) is permutable in \( G \) and \( M = (Q_1 \times Q_2 \times \cdots ) \times R \). Let \( Q_i \)}
be a \( q_i \)-group. By (26), for every \( q_i \), the group \( Q_i^G \) is a nonabelian \( P \)-group in which a prime \( p_i \) involved. By (28), all these \( p_i \) are distinct and also different from the \( q_i \); let \( \pi = \{ p_i, q_i | i \geq 1 \} \). Then \( (Q_1 \times Q_2 \times \cdots)^G = Q_1^G \times Q_2^G \times \cdots \) is the set of \( \pi \)-elements, and \( C_g(Q_1^G \times Q_2^G \times \cdots) = \bigcap_{i \geq 1} C_g(Q_i^G) = T \) is the set of \( \pi' \)-elements of \( G \). In particular,

\[
G = (Q_1^G \times Q_2^G \times \cdots) \times T
\]

and \( R = M \cap T \) is permutable in \( G \). Thus \( M \) is \( P \)-embedded in \( G \).

As an immediate consequence of Theorem 6.2.17 we get the corresponding result in the case that \( G \) is finitely generated modulo \( M \).

6.2.18 Theorem (Zacher [1982b]). Let \( M \) be a permodular subgroup of the group \( G \) and suppose that \( G \) is finitely generated modulo \( M \). Then \( |M^G : M| \) is finite, \( M^G/M_G \) is a locally finite group of finite exponent and, if \( M \) is not permutable in \( G \), then \( M \) is \( P \)-embedded in \( G \).

\textbf{Proof.} We may assume that \( M_G = 1 \); let \( M^G = H \). By 6.2.8, \( |H : M| < \infty \) and hence \( H/M_H \) is a finite group of order \( n \), say. For \( g \in G \), also \( (M_H)^g \leq H \) and \( |H/(M_H)^g| = n \). Therefore if \( x \in H \), then \( x^n \in (M_H)^g \leq M^g \) and it follows that \( x^n \in \bigcap_{g \in G} M^g = M_G = 1 \). Thus \( H \) is periodic of exponent dividing \( n \). The other assertions now follow from 6.2.14 and 6.2.17.

\section*{The join of two permodular subgroups}

We finally want to show that the join of two permodular subgroups is permodular. For this we need a general result on permodular subgroups that is a consequence of Theorem 6.2.18 and is of independent interest.

6.2.19 Theorem. \( M \) is permodular in \( G \), then \( M \) is permutable in \( M^G \).

\textbf{Proof.} Let \( \text{Per}(M) = \{ x \in G | M \text{ per } \langle M, x \rangle \} \). We want to show that \( \text{Per}(M) \) is a subgroup of \( G \) containing \( M^G \), that is

\[
M \leq M^G \leq \text{Per}(M) \leq G.
\]

This will prove the theorem since every \( x \in \text{Per}(M) \) satisfies \( M \langle x \rangle = \langle x \rangle M \) and so (29) implies that \( M \) is permutable in \( M^G \). To prove (29), we take \( x, y \in \text{Per}(M) \), \( a, b, c, d \in G \) and show that

\[
xy^{-1} \in \text{Per}(M) \text{ and } [[[a, b], [c, d]]] \in \text{Per}(M).
\]

This will imply that \( \text{Per}(M) \leq G \) and \( G'' \leq \text{Per}(M) \); since obviously \( M \leq \text{Per}(M) \), (29) will follow. To prove (30), consider \( L = \langle M, a, b, c, d, x, y \rangle \). Then \( L \) is finitely generated modulo \( M \) and, by 6.2.18, either \( M \) is permutable in \( L \) or \( M \) is \( P \)-em-
bedded in \( L \) and \( M^{L}/M_{L} \) has finite exponent. In the first case, \( L \subseteq \text{Per}(M) \) and (30) holds; in the second case, let

\[
L/M_{L} = S_{1}/M_{L} \times \cdots \times S_{r}/M_{L} \times T/M_{L}
\]

and

\[
M/M_{L} = Q_{1}/M_{L} \times \cdots \times Q_{r}/M_{L} \times (M \cap T)/M_{L}
\]

be the decompositions described in (13) and (15). We claim that

\[\text{(31)} \quad \text{Per}(M) \cap L = MT.\]

Indeed \( M \cap T \) is permutable and the \( Q_{i} \) are normal in \( MT \), so \( M = Q_{1} \cdots Q_{r}(M \cap T) \) is permutable in \( MT \) and hence \( MT \subseteq \text{Per}(M) \cap L \). And if \( z \in L \setminus MT \), then \( z = z_{1} \cdots z_{t} \) where \( z_{i} \in S_{i} \), \( t \in T \) and \( z_{j} \notin Q_{j} \) for some \( j \). Since the orders modulo \( M_{L} \) of these elements are coprime, there exists \( m \in \mathbb{N} \) such that \( z^{m}M_{L} = z_{j}M_{L} \). It follows that \( \langle z_{j}M_{L} \rangle \leq \langle zM_{L} \rangle \) and hence \( \langle z_{j}, Q_{j} \rangle \leq \langle z, M \rangle \). Since \( \langle z_{j}, Q_{j} \rangle /M_{L} \) is nonabelian of order \( pq \) for primes \( p, q \) and \( p > q = |Q_{j}/M_{L}| \), the subgroup \( M \cap \langle z_{j}, Q_{j} \rangle = Q_{j} \) is not permutable in \( \langle z_{j}, Q_{j} \rangle \). In particular, \( M \) cannot be permutable in \( \langle M, z \rangle \) and thus \( z \notin \text{Per}(M) \). This proves (31), and (30) is an immediate consequence. For, since \( x, y \in \text{Per}(M) \cap L = MT \), we have \( xy^{-1} \in MT \subseteq \text{Per}(M) \) and since the factor group \( L/T \simeq S_{1}/M_{L} \times \cdots \times S_{r}/M_{L} \) is metabelian, \( [[a, b], [c, d]] \) is contained in \( T \) and hence in \( \text{Per}(M) \).

\[\text{6.2.20 Lemma.} \quad \text{Let} \ G \ \text{be a soluble group. If} \ M \ \text{is a maximal subgroup of} \ G \ \text{that is modular in} \ G, \ \text{then} \ |G : M| \ \text{is a prime.}\]

\[\text{Proof.} \quad \text{We use induction on the derived length of} \ G. \ \text{If} \ G' \leq M, \ \text{then} \ M \leq G \ \text{and} |G : M| \ \text{is a prime; so suppose that} \ G' \nleq M. \ \text{Since} \ M \ \text{is a maximal subgroup of} \ G, \ \text{it follows that} \ G = G'M \ \text{and, since} \ M \ \text{is modular in} \ G, \ M \cap G' \ \text{is maximal and modular in} \ G'. \ \text{By induction,} |G' : M \cap G'| = |G : M| \ \text{is a prime.}\]

\[\text{6.2.21 Theorem (Zacher [1982b]).} \quad \text{If} \ M \ \text{and} \ L \ \text{are permodular subgroups of the group} \ G, \ \text{then} \ M \cup L \ \text{is permodular in} \ G.\]

\[\text{Proof.} \quad \text{By 2.1.6,} H = M \cup L \ \text{is modular in} \ G. \ \text{If} \ g \in G \ \text{and} o(g, H) \ \text{is infinite, then}
\]

\[o(g, M) \ \text{and} o(g, L) \ \text{are infinite and hence} H^{g} = M^{g} \cup L^{g} = M \cup L = H. \ \text{We want to verify (d) of 6.2.5 for} \ H. \ \text{So let} \ H \leq X \leq G \ \text{such that} |X/H| \ \text{is a finite chain. We have to show that} \ |X : H| \ \text{is finite and may assume that} \ X = G. \ \text{Let} \ R = G''H. \ \text{Since}
\]

\[|R/H| \ \text{is a chain, there exists} \ x \in G'' \ \text{such that} \ R = \langle H, x \rangle. \ \text{By 6.2.19,} \ M \ \text{is permutable in} \ G''M \ \text{and hence} M\langle x \rangle = \langle x \rangle M. \ \text{Similarly,} \ L\langle x \rangle = \langle x \rangle L \ \text{and thus} \ R = H\langle x \rangle. \ \text{It follows that}
\]

\[|R : H| = |\langle x \rangle \cdot \langle x \rangle \cap H| \ \text{and} \ |\langle x \rangle /\langle x \rangle \cap H| \simeq |R/H| \ \text{is finite since} \ H \ \text{is modular in} \ G. \ \text{Thus} \ |R : H| \ \text{is finite. By (c) of 2.1.6, every subgroup of}
\]

\( G \) containing \( H \) is modular in \( G; \) in particular, every subgroup of \( G/G'' \) containing \( R/G'' \) is modular in \( G/G''. \) By 6.2.20, any two successive members of the chain \( [G/G'')(R/G'')] \) have prime index in each other and it follows that \( |G : R| \) is finite. Thus \( |G : H| \) is finite and, by 6.2.5, \( H \) is permodular in \( G. \)
We mention without proof three further results of Zacher [1982b]. First of all, Theorem 6.2.21 is the main step needed to prove that the relation \( \rho \) on the subgroup lattice of a group \( G \) defined by

\[ (32) \quad H \rho K \text{ if and only if } H \triangleleft K \text{ and } H \text{ pmo } K \]

is a normality relation on \( L(G) \). This concept was introduced by Zassenhaus [1958], p. 76 who proved a Jordan-Hölder Theorem for lattices with a normality relation. However, since every permutable subgroup is permodular, the remark following 5.2.8 also applies here. Permodular subgroups are the lattice-theoretic approximation to normal subgroups (and their projective images) which we shall use; however, in fact, they approximate permutable subgroups more precisely. It would be preferable to have a better lattice-theoretic approximation of normal subgroups to work with.

The second result is that if \((M_i)_{i \in I}\) is a local system of subgroups of \( M \) such that every \( M_i \) is permodular in \( G \), then \( M \) is permodular in \( G \). Using this, Theorem 6.2.21 implies that the join of an arbitrary family of permodular subgroups is permodular in \( G \).

Thirdly, Theorem 5.1.13 also holds for permodular subgroups of infinite groups: Zacher shows that \( M \text{ pmo } G \) if and only if \( M \text{ pmo } \langle M, g \rangle \) for every \( g \in G \).

We finally remark that quite a few of the results in this section, in particular 6.2.3, 6.2.8, 6.2.14 and Theorem 6.2.17, were inspired by and are more or less due to Stonehewer [1976b], who proved them for modular subgroups in Tarski-free groups.

**Exercises**

All the exercises in this section are due to Zacher [1982b].

1. Let \( M \) be permodular in \( G \) and suppose that there exists \( g \in G \) such that \( o(g, M) \) is infinite. Show that \( M/M_G \) is a subdirect product of finite cyclic groups, hence is abelian, and \( M^G/M_G \) is nilpotent of class at most 2.

2. If \( M \) is \( P \)-embedded in \( G \), show that \( M \) is permodular in \( G \).

3. We say that \( M \) is \textit{locally \( P \)-embedded} in \( G \) if there exists a family \((H_i)_{i \in I}\) of subgroups \( H_i \) of \( G \) containing \( M \) with the following properties.
   (i) \( M \) is \( P \)-embedded in \( H_i \) for every \( i \in I \).
   (ii) For all \( i, j \in I \) there exists \( k \in I \) such that \( H_i \cup H_j \leq H_k \).
   (iii) \( G \) is the set-theoretic union of the \( H_i \).
   Show that a subgroup \( M \) of \( G \) is permodular and not permutable in \( G \) if and only if \( M \) is locally \( P \)-embedded in \( G \).

4. For every \( i \in \mathbb{N} \), let \( p_i \) and \( q_i \) be primes such that \( q_i \mid p_i - 1 \) and \( \{p_i, q_i\} \cap \{p_j, q_j\} = \emptyset \) for \( i \neq j \); let \( S_i = \langle a_i, b_i \rangle \) be a nonabelian group of order \( p_i q_i \), and \( b_i^{-1} a_i b_i = a_i^r \) with \( r_i \in \mathbb{Z} \). Put \( S = \bigcup_{i \in \mathbb{N}} \langle a_i \rangle \) and let \( \tau \) be the automorphism of \( S \) satisfying \( a_i^r = a_i^r \) for all \( i \). Finally, let \( M = \langle \tau \rangle \) and \( G = S M \) be the semidirect product with respect to this automorphism.
   (a) Show that \( M \) is permodular and not permutable in \( G \).
   (b) Show that \( M \) is infinite cyclic and \( M_G = 1 \); hence \( M \) is not \( P \)-embedded in \( G \).
5. Let $M$ be a subgroup of a group $G$ such that $M$ is permodular in $\langle M, g \rangle$ for every $g \in G$ and suppose that $G$ is finitely generated modulo $M$.

(a) Show that $|M^G : M|$ is finite.

(b) If $M$ is not permutable in $G$, show that $M$ is $P$-embedded in $G$.

6. Show that a subgroup $M$ of the group $G$ is permodular in $G$ if and only if $M$ is permodular in $\langle M, g \rangle$ for every $g \in G$. (Hint: Use Exercises 3 and 5.)

6.3 Permutable subgroups of infinite groups

Theorems 6.2.17 and 6.2.18 reduce the problem of determining the structure of $G/M_G$ for a permodular subgroup $M$ to the case where $M$ is permutable in $G$; at least this is so in the two situations that are important for us, namely when $M/M_G$ is periodic and when $G$ is finitely generated modulo $M$. The results of §6.2 also give the structure of $M^G/M_G$ in these situations; the only additional result proved in this section is that $M^G/M_G$ is nilpotent if $G$ is finitely generated modulo $M$. Again no systematic treatment of permutuble subgroups is intended, but a number of special results will be proved in the remainder of this section to prepare the way for the study of the structure of $N^G/N_G$ and $N^G/\widetilde{N}_G$ for a normal subgroup $N$ of $G$ and a projectivity from $G$ to $\tilde{G}$. Basic for this is a theorem of Busetto and Napolitani [1990] stating that if $G$ is generated by a permutuble subgroup $M$ and a subset $F$, then $M^G$ is generated by the $M^{\langle x \rangle}$ for $x \in F$.

Periodic permutuble subgroups

To give the structure of $M^G/M_G$ for a permutuble subgroup $M$ of $G$ with $M/M_G$ periodic, we only have to collect the results proved in 6.2.14–6.2.16.

6.3.1 Theorem. Let $M$ be a permutuble subgroup of the group $G$ such that $M/M_G$ is periodic. Then $M^G/M_G$ is locally finite and the direct product of its Sylow subgroups, the Sylow subgroups of $M/M_G$ are permutuble in $G/M_G$ and their normal closures are the Sylow subgroups of $M^G/M_G$.

Proof. We may assume that $M_G = 1$. By 6.2.14, $M^G$ is locally finite and $M$ is the direct product of its Sylow subgroups $M_p$ ($p \in \mathbb{P}$). Then $M^G$ is the product of the normal closures $M^G_p$. By 6.2.16, $M_p$ is permutable in $G$, and 6.2.15 shows that $M^G_p$ is a $p$-group. It follows that the product of the $M^G_p$ is direct and that $M^G_p$ is the Sylow $p$-subgroup of $M^G$. \qed

The above theorem in particular implies that for a permutuble subgroup $M$ of $G$ with $M/M_G$ periodic, $M^G/M_G$ is locally nilpotent. It need not be nilpotent; in fact, $M/M_G$ need not even be soluble (see Exercise 4). If $G$ is finitely generated modulo $M$, then by 6.2.18, $M/M_G$ is periodic and we want to show that $M^G/M_G$ is nilpotent in this case. For this we need the following lemma.
6.3.2 Lemma. Let $M$ be permutable in $G$, $g_1, \ldots, g_m \in G$ and $H = M^{g_1} \cdots M^{g_m}$. Then $H/(M^{g_i})_H$ is finite and nilpotent for every $i = 1, \ldots, m$.

Proof. If $o(g_j, M)$ is infinite, $M^{g_j} = M$. Thus we may assume that $g_i = 1$, $o(g_j, M) < \infty$ for all $j$ and $G = \langle M, g_1, \ldots, g_m \rangle$. Then by 6.2.8, $|M^G : M| < \infty$; in particular, $H/M_H$ is a finite group. It remains to be shown that this group is nilpotent. For this let $g$ be one of the $g_j$ with $j \neq i$ and $L = H \langle g \rangle$. Since $H$ per $G$ and $o(g, M) < \infty$, the index $|L : H|$ is finite, and hence $L/M_L$ is a finite group. By 5.2.3, $M^L/M_L$ is nilpotent and therefore $H \cap M^L/M_L$ is nilpotent as well. Since $M_L \leq M_H$, finally, $H \cap M^L/M_H$ is a nilpotent normal subgroup of $H/M_H$ containing $MM^g/M_H$. Thus $MM^g/M_H$ is contained in the Fitting subgroup of $H/M_H$ and, since $H$ is generated by these $MM^g$, it follows that $H/M_H$ is nilpotent.

6.3.3 Theorem (Lennox [1981]). If $M$ is a permutable subgroup of the group $G$ such that $G$ is finitely generated modulo $M$, then $M^G/M_G$ is nilpotent.

Proof. Let $H = M^G$. By 6.2.8, $|H : M|$ is finite and hence there exist $g_2, \ldots, g_m \in G$ such that $H = MM^{g_2} \cdots M^{g_m}$. By 6.3.2, $H/M_H$ is nilpotent. Hence some term $K$ of the lower central series of $H$ is contained in $M_H$, and $K \leq G$ since $K$ is a characteristic subgroup of $H = M^G$. It follows that $K \leq M_G$ and hence $M^G/M_G$ is nilpotent.

We remark that although Theorem 5.2.12 and Busetto [1979] contain partial results in this direction, there is no analogue of the Maier-Schmid Theorem for infinite groups. In fact, Exercise 6 shows that $M^G/M_G$ need not be hypercentrally embedded in $G$ even if $M$ is a permutable subgroup of a finitely generated $p$-group $G$. In this example, $M/M_G$ is infinite and it remains an open problem whether a finite core-free permutable subgroup of a group $G$ is contained in the hypercentre of $G$. Furthermore, there are examples of (nonperiodic) core-free permutable subgroups which are not locally soluble (see Gross [1982]).

The normal closure of a permutable subgroup

In the remainder of this section we shall study rather special aspects of permutable subgroups which are necessary for the applications to projective images of normal subgroups. First we want to describe the normal closure of a permutable subgroup $M$ in $G$ and in $M^G$. For this we need a very simple technical lemma.

6.3.4 Lemma. If $M$ per $G$ and $g \in G$, then $M^{\langle g \rangle} = M(M^{\langle g \rangle} \cap \langle g \rangle) = MM^g$.

Proof. Since $M$ is permutable in $G$, we have $M^{\langle g \rangle} \leq M \langle g \rangle$, and Dedekind's law yields that $M^{\langle g \rangle} = M(M^{\langle g \rangle} \cap \langle g \rangle)$. Furthermore, $MM^g \leq M \langle g \rangle = M^g \langle g \rangle$ and again Dedekind's law implies that $MM^g = M(MM^g \cap \langle g \rangle) = M^g(MM^g \cap \langle g \rangle)$. It follows that $MM^g$ is normalized by $g$. Thus $MM^g \leq M \langle g \rangle$ and hence $MM^g = M^{\langle g \rangle}$. □
6.3 Permutable subgroups of infinite groups

6.3.5 Theorem (Busetto and Napolitani [1990]). Let \( M \) be a permutable subgroup and \( F \) a subset of the group \( G \) such that \( G = \langle M, F \rangle \). Then

\[
M^G = \langle M^x | x \in F \rangle = M \langle M^x \cap \langle x \rangle | x \in F \rangle.
\]

Proof. First of all note that we may assume \( |F| = 2 \) and only have to show that

1. \( M^G = M^x M^y \) if \( G = \langle M, x, y \rangle \).

For, if this holds, then for every \( x, y \in F \),

\[
\langle M^x \rangle^\langle y \rangle \leq \langle M^{x,y} \rangle = M^x M^y \leq \langle M^x \rangle^\langle y \rangle
\]

and hence \( \langle M^x \rangle^\langle y \rangle = M^x M^y \). Thus if \( H = \langle M^x | x \in F \rangle \), then

\[
H^\langle y \rangle = \langle M^x | x \in F \rangle^\langle y \rangle = \langle (M^x)^\langle y \rangle | x \in F \rangle = \langle M^x M^y | x \in F \rangle = H
\]

and hence \( y \in N_G(H) \). This holds for arbitrary \( y \in F \) and, since \( G = \langle M, F \rangle \), it follows that \( H \leq G \). Thus \( M^G \leq H \), and the other inclusion is trivial since \( H \) is generated by conjugates of \( M \). Therefore \( M^G = H = \langle M^x | x \in F \rangle = M \langle M^x \cap \langle x \rangle | x \in F \rangle \), by 6.3.4, and the theorem will be proved.

So assume that \( G = \langle M, x, y \rangle \), and consider \( T = M^x = \langle M^g | g \in \langle x \rangle \rangle \). As a join of permutable subgroups, \( T \) is permutable in \( G \) and, if we apply 6.3.4 to \( T \), we obtain that \( T^{\langle x,y \rangle} = TT^{xy} = TT^y = T^{\langle y \rangle} \). Therefore \( T^{\langle y \rangle} = \langle M^x \rangle^{\langle y \rangle} \) is normalized by \( y \) and \( xy \), hence is normal in \( \langle M, xy, y \rangle = G \) and so contains \( M^G \); on the other hand, \( \langle M^x \rangle^{\langle y \rangle} \) is generated by conjugates of \( M \). It follows that

2. \( M^G = \langle M^x \rangle^{\langle y \rangle} \)

and by 6.3.4 applied to the permutable subgroup \( M^x \),

\[
M^G = \langle M^x \rangle^{\langle y \rangle} = M^x (M^x \cap \langle y \rangle) \leq M^x (M^G \cap \langle y \rangle).
\]

The other inclusion is trivial and again by 6.3.4,

3. \( M^G = M(M^x \cap \langle x \rangle)(M^G \cap \langle y \rangle) \).

For the proof of (1) we may assume that \( M_G = 1 \). By (2), we have to show that

4. \( \langle M^x \rangle^{\langle y \rangle} = M^x M^y \).

Since \( G \) is finitely generated modulo \( M \), by 6.2.18 and 6.3.1, \( M^G \) has finite exponent and \( M \) is the direct product of its Sylow subgroups which are permutable in \( G \). Now if \( M = AB \) with \( A \) and \( B \) permutable in \( G \), then \( M^X = A^X B^X \) for every subgroup \( X \) of \( G \); so if (4) holds for \( A \) and \( B \), it follows that

\[
\langle M^x \rangle^{\langle y \rangle} = (A^x)^{\langle y \rangle} (B^x)^{\langle y \rangle} = A^x A^\langle y \rangle B^x B^\langle y \rangle = M^x M^\langle y \rangle,
\]

as desired. Therefore we may assume that \( M \) is a \( p \)-group for some prime \( p \) and that \( G = \langle M, x, y \rangle \) and \( M_G = 1 \). By 6.2.15 and 6.2.8,

5. \( M^G \) is a \( p \)-group and \( |M^G : M| \) is finite;
write \( H = M^G \). Then \( H/M_H \) is a finite \( p \)-group; let \( v \) be the natural epimorphism from \( H \) to \( H/M_H \). If \( H \cap \langle x \rangle = M^{\langle x \rangle} \cap \langle x \rangle \), then (3) and (4) with \( x \) and \( y \) interchanged yields
\[
M^G = M(M^{\langle y \rangle} \cap \langle y \rangle)(M^G \cap \langle x \rangle) = M(M^{\langle y \rangle} \cap \langle y \rangle)(M^{\langle x \rangle} \cap \langle x \rangle) \leq M^{\langle y \rangle}M^{\langle x \rangle}
\]
and hence \( M^G = M^{\langle x \rangle}M^{\langle y \rangle} \), as desired. So suppose that \( H \cap \langle x \rangle \neq M^{\langle x \rangle} \cap \langle x \rangle \). Then \( M^{\langle x \rangle} \cap \langle x \rangle \) is contained in the maximal subgroup of the cyclic \( p \)-group \( H \cap \langle x \rangle \). Since \( M_H \leq M^{\langle x \rangle} \leq H \), this also holds for the images under \( v \) and, since \( H'' \) is a finite \( p \)-group, it follows that \( (M^{\langle x \rangle} \cap \langle x \rangle)^v \) is contained in the Frattini subgroup of \( H'' \). Then (3) and the main property of the Frattini subgroup yield that
\[
H'' = (M^{\langle x \rangle} \cap \langle x \rangle)^v M''(H \cap \langle y \rangle)^v = M''(H \cap \langle y \rangle)^v
\]
and hence \( H = MM_H (H \cap \langle y \rangle) = M(H \cap \langle y \rangle) \). Since \( H \cap \langle y \rangle \) is a cyclic \( p \)-group, it follows that \([H/M]\) is a chain and therefore either \( M^{\langle x \rangle} \leq M^{\langle y \rangle} \) or \( M^{\langle y \rangle} \leq M^{\langle x \rangle} \). In the first case, as \( M^{\langle y \rangle} \leq M^{\langle y \rangle} \), it follows from (2) that \( M^G = (M^{\langle x \rangle})^{\langle y \rangle} \leq M^{\langle y \rangle} \), and hence \( M^G = M^{\langle y \rangle} = M^{\langle x \rangle}M^{\langle y \rangle} \), in the second case, the same argument with \( x \) and \( y \) interchanged yields that \( M^G = M^{\langle x \rangle} \), but this contradicts our assumption that \( H \cap \langle x \rangle \neq M^{\langle x \rangle} \cap \langle x \rangle \). Thus \( M^G = M^{\langle x \rangle}M^{\langle y \rangle} \), as desired.

6.3.6 Corollary. \( M^{M^G} = \langle M^{\langle x \rangle} \cap \langle x \rangle \mid x \in F \rangle \) if \( M \) is permutable in \( G = \langle M, F \rangle \).

**Proof.** By 6.3.5, \( M^G = \langle M^{\langle x \rangle} \cap \langle x \rangle \mid x \in F \rangle \). Now apply Theorem 6.3.5 to \( M^G \) and the set-theoretic union of the \( M^{\langle x \rangle} \cap \langle x \rangle \) (\( x \in F \)) in place of \( G \) and \( F \).

The above result will be used to determine the structure of \( N^G/N \) for a normal subgroup \( N \) of \( G \) and a projectivity from \( G \) to \( \overline{G} \). The structure of \( M^G/M^G \) is rather simple, even for arbitrary permutable subgroups.

6.3.7 Theorem. If \( M \) per \( G \), then \( M^G/M^G \) is nilpotent of class at most 2.

**Proof.** Let \( H = M^G \) and \( S = M^H \). Then \( S \) is generated by conjugates of \( M \) and hence is permutable in \( G \). If \( x \in G \), then \( S^x \leq H^x = H \) and \( SS^x \leq S \langle x \rangle \), so that \( SS^x/S \) is a cyclic normal subgroup of \( H/S \). Since the automorphism group of a cyclic group is abelian, \( SS^x/S \) is centralized by the commutator subgroup \( (H/S)' \) of \( H/S \). But \( H = M^G = S^G \) and therefore \( H/S \) is generated by these \( SS^x/S \). It follows that \( (H/S)' \leq Z(H/S) \). Thus \( H/S \) is nilpotent of class at most 2.

As an application of Corollary 6.3.6 we prove the following rather technical result that will be needed in § 6.6.

6.3.8 Lemma. Let \( p \in P \), \( H \) a core-free permutable \( p \)-subgroup of \( G \) and \( M = \Omega(H) \).
(a) Then \( M^G \) is an elementary abelian \( p \)-group.
(b) If \( M \) is permutable in \( G \) and \( H \) is not normal in \( H^G \), then \( M^G \leq H^G \).
Proof. (a) By 6.2.10, a permutable maximal subgroup of a group is normal. Therefore every element of order $p$ of $G$ normalizes $H^g$ and hence also its characteristic subgroup $\Omega(H^g) = M^g$; it follows that $M^g \leq M^G$ for every $g \in G$.

Let $x \in G \setminus N_G(H)$ and $T = H \langle x \rangle$. By 6.2.3, $\alpha(x, H) = |T : H| < \infty$ and therefore $T/H_T$ is a finite group in which $H/H_T$ is a permutable $p$-subgroup. By 5.1.5, this $p$-subgroup is normalized by the $p'$-component of $xH_T$, and so 5.2.8 shows that $\Omega(H/H_T)$ is elementary abelian. This group contains $MH_T/H_T$ and hence $M/M \cap H_T$ is elementary abelian. Since $H_G = 1$, the intersection of all these $M \cap H_T$ is trivial and so $M$ is elementary abelian.

It follows that $M^g \cap H = M^g \cap M$ and $MM^g/M \cong M^g/M$ for every $g \in G$. Now $M^g/M \cap H$ is elementary abelian and $M^g/H/H$ is cyclic since its subgroup lattice is isomorphic to an interval in $[H^g/H, H] \cong [\langle g \rangle/H, \langle g \rangle \cap H]$. Thus $MM^g/M$ is cyclic of order dividing $p$. Since $MM^g \leq M^G$, the group $M^G/M$ is generated by cyclic normal subgroups of order $p$ and hence is an elementary abelian $p$-group. Since $M_G = 1$, the same holds for $M^G$.

(b) Let $S = H^x$ and $x \in G$. We have to show that $M^x \leq S$. If $x \in N_G(M)$, then clearly $M^x = M \leq S$; so suppose that $x \notin N_G(M)$. Then since $M$ is permutable in $G$, 5.2.7 and 5.1.5 imply that $\alpha(x, H)$ is finite and divisible by $p$. Let $P$ be the subgroup of order $p$ in $\langle x \rangle$. By (a), $M^x \leq M^x$ is elementary abelian and hence $M^x = MP$. Let $X = H^x \cap \langle x \rangle$. If $X \leq N_G(H)$, then $HP \leq H^X \leq S$ since $X \leq H^G$; in particular, $M^X = MP \leq S$, as desired. So we may assume that

\[(6) X = H^x \cap \langle x \rangle \leq N_G(H).\]

By assumption and 6.3.5, $H$ is not normal in $H^G = H\langle H^y \cap \langle y \rangle | y \in G \rangle$ and hence there exists $y \in G$ such that

\[(7) Y = H^y \cap \langle y \rangle \leq N_G(H).\]

Let $L = \langle H, x, y \rangle$ and $Z = H^{xy} \cap \langle xy \rangle$. Now $M \leq H$ and therefore 6.3.5 and 6.3.4 applied to the permutable subgroup $M$ of $L = \langle H, y, xy \rangle$ yield that

\[(8) M^x \leq M^L = M^y M^{xy} = (M^y \cap \langle y \rangle)M(M^{xy} \cap \langle xy \rangle).\]

Of course, $H^L \leq H^G$ and by 6.3.6, $S = H^H \geq H^L = H^X H^Y = H^X H^Z = H^Y = H^Z$ since $X$ normalizes $H$. By (7), $H < H^Y \leq H \langle y \rangle$ and as $H^Y$ is a $p$-group, it contains the subgroup of order $p$ of $\langle y \rangle$. Since $M^y$ is elementary abelian, $M^y \cap \langle y \rangle$ is contained in this subgroup of order $p$ of $\langle y \rangle$ and it follows that $M^{xy} \cap \langle y \rangle \leq H^Y \leq S$. Now $Z \leq N_G(H)$ since $H^Y = H^Z$, and the same argument with $xy$ in place of $y$ shows that $M^{xy} \cap \langle xy \rangle \leq H^Z \leq S$. By (8), $M^x \leq S$, as desired.

We do not know whether the hypothesis that $\Omega(H)$ is permutable in $G$ is redundant in Lemma 6.3.8(b).

Groups generated by cyclic permutable subgroups

If $N \leq G$ and $\varphi$ is a projectivity from $G$ to $\tilde{G}$, then $N\tilde{G}/N$ is generated by subgroups of the form $(N \cup \tilde{N}^x)^{\varphi} \setminus N$ for $x \in \tilde{G}$. These groups are cyclic permodular subgroups
of $G/N$ since $\bar{N} \cup \bar{N}^x \leq \langle \bar{N}, x \rangle$. Therefore we shall need two further technical results on groups containing many cyclic permutable subgroups.

6.3.9 Lemma. Let $G$ be a $p$-group generated by a family $\mathcal{X}$ of cyclic permutable subgroups, and suppose that $S$ is a nonabelian subgroup of $G$ such that every subgroup of $S$ is permutable in $G$ and $S$ does not contain subgroups isomorphic to the quaternion group $Q_8$. If $S$ is not generated by two elements, then $|S \cap \Omega(Z(G))| \geq p^2$.

Proof. Since any two subgroups of $S$ permute, $S$ is a nonabelian locally finite $p$-group with modular subgroup lattice. By 2.4.15, $\text{Exp } S$ is finite. Furthermore, $S$ is not hamiltonian since it does not contain subgroups isomorphic to $Q_8$, and by 2.5.9 there exists an abelian $p$-group lattice-isomorphic to $S$. An abelian group of finite exponent is a direct product of cyclic groups (see Robinson [1982], p. 105) and, since $S$ is not generated by two elements, it follows that

\[(9) \Omega(S) \text{ is elementary abelian of order at least } p^3.\]

Let $1 \neq g \in \Omega(S)$. Since $\langle g \rangle$ per $G$, we have $|\langle x \rangle : \langle g \rangle : \langle x \rangle| \leq p$, and hence $\langle x \rangle^g = \langle x \rangle$ for every $x \in G$. Thus $g$ induces a power automorphism in $G$ that centralizes $\Omega_2(G)$ if $p = 2$; for, an element of order 4 inverted by $g$ would generate, together with $g$, a dihedral group of order 8 in which $\langle g \rangle$ is not permutable. Let $C, D \in \mathcal{X}$. By 5.2.14, $CD$ is a metacyclic $M$-group and 2.3.24 shows that the power automorphism induced by $g$ in $CD$ is universal if $CD$ is an $M^*$-group. If $CD$ is not an $M^*$-group, it is a metacyclic hamiltonian $M$-group and, by 2.3.8, the only such group is $Q_8$; then $CD \leq \Omega_2(G)$ is centralized by $g$. In any case, there exists $r \in \mathbb{Z}$ such that $x^g = x^r$ for all $x \in CD$ and, since $o(g) = p$ and $g$ centralizes $\Omega_2(G)$ if $p = 2$,

\[(10) r \equiv 1 \pmod{p}, r \equiv 1 \pmod{4} \text{ if } p = 2, \text{ and } r^p \equiv 1 \pmod{|D|}.\]

We have to consider two cases. If $\{|C| : C \in \mathcal{X}\}$ is not bounded, we claim that $g \in Z(G)$. If this is false, there is a $C \in \mathcal{X}$ such that $C = \langle c \rangle$ and $c^g \neq c$. Then there exists $D = \langle d \rangle \in \mathcal{X}$ such that $o(d) > o(c) = p^n$ and for the universal power automorphism $x \rightarrow x'$ induced by $g$ in $CD$, we have $r^p \equiv 1 \pmod{p^{n+1}}$. It follows that $r \equiv 1 \pmod{p^n}$ and hence $c^g = c$, a contradiction. This shows that $g$ centralizes every $C \in \mathcal{X}$ and thus $g \in Z(G)$ since $G = \langle C | C \in \mathcal{X} \rangle$. Thus $\Omega(S) \leq Z(G)$ and $|S \cap \Omega(Z(G))| \geq p^3$.

Now assume that $\{|C| : C \in \mathcal{X}\}$ is bounded and take $C \in \mathcal{X}$ such that $|C|$ is maximal. This time, at least $C_{\text{tris}}(C) \leq Z(G)$. For, if $g \in C_{\text{tris}}(C)$ and $D \in \mathcal{X}$, then the power automorphism $x \rightarrow x'$ induced by $g$ in $CD$ satisfies $r \equiv 1 \pmod{|C|}$ and, since $|C| \geq |D|$, it follows that $g$ centralizes $D$; again $G = \langle D | D \in \mathcal{X} \rangle$ implies $g \in Z(G)$. Now for $p > 2$, $\text{Aut } C$ is cyclic and for $p = 2$, (10) shows that the automorphisms induced by $\Omega(S)$ in $C$ lie in the cyclic subgroup of $\text{Aut } C$ generated by $x \rightarrow x^5$. Thus $\Omega(S)/C_{\text{tris}}(C)$ is cyclic and, by (9), $|S \cap \Omega(Z(G))| \geq p^2$. \qed

6.3.10 Lemma. Let $M$ be a permutable subgroup and $F$ a subset of the group $G$ such that $H = \langle M, F \rangle$ is a $p$-group for some prime $p$ and $|H : M|$ is finite. Assume further that for all $x, y \in F$, $\langle M, x \rangle$ is permutable in $G$ and the interval $[\langle M, x, y \rangle : M]$ is isomorphic to the subgroup lattice of some $p$-group. Then every subgroup $T$ such that $M \leq T \leq M^H$ is permutable in $G$.\qed
6.3 Permutable subgroups of infinite groups

Proof. Our first aim is to show that we may assume that $G$ is a finite $p$-group. We have to show that

$$T\langle c \rangle = \langle c \rangle T$$

and for this we clearly may assume that $G = \langle H, c \rangle$ and $M_0 = 1$. As a join of the permutable subgroups $\langle M, x \rangle$, $x \in F$, $H$ is permutable in $G$. So $G = H\langle c \rangle$ and we first consider the case that $o(c, H)$ is infinite. Then $[G/H] \cong [\langle c \rangle / (c) \cap H]$ is isomorphic to the subgroup lattice of an infinite cyclic group and therefore $o(g, H)$ is infinite for every $g \in G \setminus H$. In particular, $o(g, M)$ is infinite and by 6.2.3, $g \in N_G(M)$ for all $g \in G \setminus H$. Since these elements generate $G$, it follows that $M \trianglelefteq G$. But then $M^H = M$ and the assertion is trivial.

So suppose that $o(c, H) = |G : H| < \infty$. Then our hypothesis yields that $|G : M| < \infty$ and $G$ is a finite group since $M_0 = 1$. To prove (11), we now may assume that $o(c)$ is a power of some prime $q$. By 5.2.4, $G/C_0(M^G)$ is a $p$-group. So if $q \neq p$, it follows that $c \in C_0(M^G)$ and hence $T\langle c \rangle = \langle c \rangle T$. Therefore it remains to consider the case $q = p$ and, since $H$ is a $p$-group, we are finally reduced to the situation that

$$G$$

is a finite $p$-group.

Now we argue by induction on $|M^H : M|$. If $x, y \in F$, then $M^{(x)} \leq M^{(x)}$ and hence $[M^{(x)} / M]$ is a chain. Furthermore, by assumption, $[\langle M, x, y \rangle / M] \cong L(W)$ for some $p$-group $W$. Since $\langle M, x \rangle$ and $\langle M, y \rangle$ are modular in $[\langle M, x, y \rangle / M]$, the group $W$ is the product of two cyclic permutable subgroups and hence is an $M$-group by 5.2.14. Then 2.5.9 shows that $W$ is lattice-isomorphic to an abelian $p$-group or is hamiltonian, and in the latter case, $W \cong Q_8$ since it is generated by two elements. Thus for all $x, y \in F$,

$$[\langle M, x, y \rangle / M]$$

is isomorphic to $L(Q_8)$ or to the subgroup lattice of an abelian $p$-group generated by two elements.

Let $x \in F$ such that $|M^{(x)} : M|$ is maximal. If $M^{(y)} \leq M^{(x)}$ for every $y \in F$, then by 6.3.5, $M^H = \langle M^{(y)} \rangle y \in F \leq M^{(x)}$, and hence $[M^H / M]$ is a chain. $M^H$ is permutable in $G$ being a join of conjugates of $M$ and, by 5.2.10, $T$ is permutable in $G$. So suppose that there exists $y \in F$ such that $M^{(y)} \not\leq M^{(x)}$ and let $L = \langle M, x, y \rangle$. We claim that there exists $N \leq G$ such that

$$N \triangleleft M \leq N \leq M^H, \quad N / M$$

is elementary abelian of order $p^2$ and every $R \leq G$ satisfying $M < R < N$ is permutable in $G$.

To see this, first note that by 6.3.5, $M^{L} = M^{(x)}M^{(y)}$, so that $[M^L / M]$ is not a chain. Therefore, if $[M^L / M]$ had only one atom, it could not be isomorphic to the subgroup lattice of an abelian group and, by (13), it would follow that $L / M \cong L(Q_8)$. Since $L$ is a $p$-group, $M^L < L$ and hence $[M^L / M]$ would be a chain, a contradiction. Thus $[M^L / M]$ has more than one atom and, if $N$ is the join of two of these, $M \leq N$ and $N / M$ is elementary abelian of order $p^2$, again by (13). Let $M < R < N$. Any element $w$ in an abelian $p$-group $W = \langle a \rangle \times \langle b \rangle$ has the form $w = a^n b^m$ with integers $n = ip^r$, $m = jq^s$, $i \neq 0 \neq j \pmod{p}$ and $r \leq s$, say. So if $\tilde{a} = a^nb^{ps-r}$, then $w = \tilde{a}^r \in \langle \tilde{a} \rangle$ and $W = \langle \tilde{a}, b \rangle$. If we apply this via (13) to $L / M \cong L(W)$, we see that there exist $u, v \in L$ such that $L = \langle M, u, v \rangle$ and $R \leq \langle M, u \rangle$. Since $[M^L / M]$ is
not a chain, \( M^L = M^{\langle u \rangle} M^{\langle v \rangle} \not\leq M^{\langle v \rangle} \) and hence \( M < M^{\langle u \rangle} \). Now \([M^{\langle u \rangle}/M]\) is a chain containing \( R \) and \( M^{\langle u \rangle} \) and, since \( |R : M| = p \), it follows that \( R \leq M^{\langle u \rangle} \). Again by 5.2.10, \( R \) is permutable in \( G \) and (14) holds.

It is easy to see that now every \( R \) such that \( M < R < N \) satisfies the hypotheses of the lemma. Clearly, \( \langle R, F \rangle = H \) is a finite \( p \)-group, and \( \langle R, x \rangle = \langle M, x \rangle R \) is permutable in \( G \) where \( x \in F \); if \( R \leq \langle M, x, y \rangle \) with \( y \in F \), then by (13), \([\langle R, x, y \rangle/R] = [\langle M, x, y \rangle/R]\) is isomorphic to the subgroup lattice of an abelian \( p \)-group and, if \( R \not\leq \langle M, x, y \rangle \), then \([\langle R, x, y \rangle/R] \cong [\langle M, x, y \rangle/M]\). Furthermore \( R^H = M^H \) so that \( |R^H : R| < |M^H : M| \). By induction, we get that \( TR \) is permutable in \( G \); in particular, \( TR^c = <c>TR \) is a subgroup of \( G \). If there exists such an \( R \) satisfying \( \langle c, T \rangle \cap R = M \), then Dedekind’s law implies that \( \langle c, T \rangle = \langle c, T \rangle \cap \langle c \rangle TR = \langle c \rangle T(\langle c, T \rangle \cap R) = \langle c \rangle TM = \langle c \rangle T \) and therefore \( \langle c \rangle T = T \langle c \rangle \). So assume that \( R \leq \langle c, T \rangle \) and hence

\[
\langle c, T \rangle = TR^c \quad \text{for all } R \text{ such that } M < R < N.
\]

Then \( N \leq TR^c = T\langle c \rangle R \) and, again by Dedekind’s law, \( N = (N \cap T\langle c \rangle)R \). It follows that \( N \cap T\langle c \rangle \not\leq R \); let \( z \in (N \cap T\langle c \rangle) \setminus R \). Then \( z = td \) with \( t \in T \) and \( d \in \langle c \rangle \), and since \( N/M \) is elementary abelian, \( S = \langle M, z \rangle \) satisfies \( M < S < N \). By (14), \( S \) is permutable in \( G \) and, since \( M \leq S \cap T \) has index \( p \) in \( S \), we have \( |ST : T| \leq p \). Thus \( z \in N_0(T) \) and hence \( T = T^z = T^{td} = T^d \). It follows that \( S = \langle M, td \rangle \leq T \langle d \rangle \leq T \langle c \rangle \) and (15) yields that \( \langle c, T \rangle = TS \langle c \rangle \leq TT \langle c \rangle \langle c \rangle = T\langle c \rangle \). Thus \( \langle c, T \rangle = T\langle c \rangle \) and so, finally, \( T\langle c \rangle = \langle c \rangle T \), as desired.

Using similar methods, Napolitani and Zacher [1983] and Cardin [1984] determined the structure of groups \( G \) generated by a family \( \mathbb{X} \) of (cyclic) permutable subgroups such that for all \( C, D \in \mathbb{X} \), every subgroup of \( CD \) is permutable in \( G \). Such a group \( G \) is locally nilpotent (see Robinson [1982], p. 344, and recall that every permutable subgroup is ascendant), so the problem divides into the nonperiodic case and the investigation of \( p \)-groups. We give their results without proof.

6.3.11 Theorem. Let \( G \) be a group generated by a family \( \mathbb{X} \) of cyclic permutable subgroups such that for all \( C, D \in \mathbb{X} \), every subgroup of \( CD \) is permutable in \( G \).

(a) (Napolitani and Zacher [1983]) If \( G \) is periodic, then \( G \) is metabelian.
(b) (Cardin [1984]) If \( G \) is not periodic, then \( L(G) \) is modular.

The exact structure of \( p \)-groups with this property is given in Exercise 7. Napolitani and Zacher used their theorem to show that if \( N \not\leq G \), then \( N\overline{G}/N \) is metabelian for \( N \leq G \) and a projectivity from \( G \) to \( G \). Following Busetto and Napolitani [1990], we shall similarly use 6.3.9 and 6.3.10 to prove the stronger result that \( N\overline{G}/N \) is metabelian.

Exercises

1. (Gross [1971]) Let \( M \) be a core-free permutable subgroup of the group \( G \).
   (a) If \( n \in \mathbb{N} \) and \( x, y \in M \) such that \( x^n = 1 = y^n \), show that \( (xy)^n = 1 \).
   (b) Show that \( T(M) = \{ x \in M \mid \alpha(x) < \infty \} \) is a locally nilpotent and locally finite subgroup of \( G \). (Hint: Use 5.2.8 and Exercise 5.2.4.)
2. (Gross [1975a]) Let $M$ be a permutable subgroup of the group $G$ and $n \in \mathbb{N}$.
(a) If $M$ is subnormal in $G$ of defect at most $n$, that is, there exist $M_i \leq G$ such that $M = M_0 \unlhd \cdots \unlhd M_n = G$, show that $M/M_G$ is soluble with derived length at most $n - 1$.
(b) Deduce from 6.2.12 that $M/M_G$ is abelian if there exists $g \in G$ such that $o(g, M)$ is infinite; compare with Exercise 6.2.1.
(c) Let $G = \langle a, b, c | a^2 = b^8 = [a, c] = 1, [a, b] = b^4, b^{-1}cb = c^{-1} \rangle$ and $H = \langle a \rangle$.
Show that $H$ is permutable in $G$, $o(c, H)$ is infinite and $|H : H_G| = 2$.
3. Let $(G_i)_{i \in I}$ be a collection of coprime (periodic) groups and suppose that for every $i \in I$, $M_i$ is a permutable subgroup of $G_i$. Show that $M = \bigoplus_{i \in I} M_i$ is permutable in $G = \bigoplus_{i \in I} G_i$.
4. Let $\mathcal{P} = \{p_1, p_2, \ldots\}$ be the set of primes and for every $n \in \mathbb{N}$, let $G_n$ be a finite $p_n$-group containing a core-free permutable subgroup $M_n$ with derived length $n$ (by Stonehewer [1974], such $G_n$ exist). Show that $G = \bigoplus_{n \in \mathbb{N}} G_n$ contains a non-soluble core-free permutable subgroup.
5. (Busetto [1980b]) Let $n \geq 3$ and $G = \langle x, y | y^{2^n} = 1, y^{-1}xy = x^{-1} \rangle$. Show that $M = \langle xy^2 \rangle$ is permutable in $G$, infinite cyclic and $|M/M_G| = 2^{n-2}$.
6. (Busetto and Napolitani [1992]) Let $p$ be a prime such that there exists an extended Tarski group $T$ of exponent $p^3$ (see Olshanskii [1991], p. 344 for the existence of such a prime). Let $A$ be the group algebra of the Tarski group $T/Z(T)$ over the field with $p$ elements, $N$ the augmentation ideal of $A$ and let $G$ be the semidirect product of $N$ by $T$ where the action of $T$ on $N$ is induced by $T/Z(T)$ via right multiplication in $A$.
(a) Show that $G$ is a finitely generated $p$-group (note that since $T/Z(T)$ is finitely generated, $N$ is a finitely generated right ideal of $A$) with $\Omega(G) = N\Omega(T)$ elementary abelian.
(b) Show that $[\Omega(G), G] = [N, G] = N$ (note that since $T/Z(T)$ is perfect, $N^2 = N$ as an ideal of $A$) and hence $G$ is perfect.
(c) If $g \in G \setminus N\Omega(T)$, show that $\langle g^{p^x} \rangle = \Omega(T)$ (note that $g = xy$ with $x \in T \setminus Z(T)$, $y \in N$ and hence $g^{p} = x^{p}w$ with $w \in N$).
(d) If $M$ is a maximal subgroup of $\Omega(G)$ such that $\Omega(T) \not\leq M \neq N$, show that $M$ is permutable in $G$, $M/M_G$ is infinite and $M^G/M_G$ is not hypercentrally embedded in $G$.
7. (Cardin [1984]) Show that the $p$-group $G$ is generated by a family $\mathcal{X}$ of cyclic permutable subgroups such that for all $C, D \in \mathcal{X}$, every subgroup of $CD$ is permutable in $G$, if and only if $L(G)$ is modular or $p = 2$ and $G = H \times A$ where $A$ is an elementary abelian 2-group and $H$ is a central product of the form $Q_{8^n}D_{8^n}, Q_{8^n}D_{8^n}C_{2}, Q_{8^n}^+D_{8^n}$ for some $n \in \mathbb{N}$ in which the central subgroups of order 2 of the $2n$ or $2n + 1$ factors are identified.

6.4 Lattice-theoretic characterizations of classes of infinite groups

In this section we want to extend the lattice-theoretic characterizations of §5.3 to arbitrary groups.
Simple groups

6.4.1 Theorem (Zacher [1982b]). The group $G$ is simple if and only if 1 and $G$ are the only permodular subgroups of $G$.

Proof. If 1 and $G$ are the only permodular subgroups of $G$, then $G$ in particular has no proper nontrivial normal subgroups, that is, $G$ is simple. Conversely, let $G$ be simple and suppose, for a contradiction, that there exists a permodular subgroup $M$ of $G$ different from 1 and $G$. Then $MG'' = G$ and, by 6.2.19, $M$ is permutable in $G$; furthermore, of course, $M_G = 1$ and $M^G = G$. We now follow an argument due to Stonehewer [1972] and show that every finitely generated subgroup of $G$ is residually nilpotent and therefore has a normal series with abelian factors; such groups are called SI-groups (see Robinson [1982], p. 365). A theorem of Malcev (see Kurosh [1956], p. 183) will then imply that $G$ is an SI-group, contradicting the simplicity of $G$. So let $X = G = M^G$. Then there exist finitely many elements $g_1, \ldots, g_m \in G$ such that $X < M_1 \cdots M_m$. Let $g \in G$ and $H = M^g M_1 \cdots M_m$. By 6.3.2, $H/(M^g)_H$ is nilpotent and hence so is $X/X \cap (M^g)_H$. Since $X \cap (M^g)_H \leq M^g$, the intersection of all these normal subgroups of $X$ is contained in $M_g = 1$ and it follows that $X$ is residually nilpotent.

Since projectivities map permodular subgroups onto permodular subgroups, we get the following corollary.

6.4.2 Corollary (Zacher [1982a]). If $G$ is a simple group and $\varphi$ is a projectivity from $G$ to a group $\tilde{G}$, then $\tilde{G}$ is also simple.

Perfect groups

A group is perfect if it equals its commutator subgroup, that is, if it has only trivial abelian factor groups. To express this property in the language of lattice theory, we have to find a good translation for “abelian group”. The Tarski groups show that “modular lattice” is inadequate for infinite groups; on the other hand, our results on groups with modular subgroup lattice show that we only have to avoid the Tarski groups. So the following definition should work:

We call a lattice $L$ permodular if it is modular and for all $a, b \in L$ such that $b \leq a$, $[a/b]$ is a finite lattice whenever it has finite length.

6.4.3 Theorem. The following properties of the group $G$ are equivalent.

(a) $L(G)$ is permodular.
(b) $L(G)$ is modular and $G$ is soluble (or metabelian).
(c) Every subgroup of $G$ is permodular in $G$.

Proof. If $L(G)$ is permodular, then no Tarski group can be involved in $G$ and, by 2.4.21, $G$ is metabelian.
Now let $L(G)$ be modular and $G$ soluble. Then every subgroup $M$ of $G$ clearly is modular in $G$. Let $g \in G$ and $M \leq Y \leq \langle M, g \rangle$ such that $\langle M, g \rangle / Y$ is a finite lattice. Then there exist subgroups $X_i$ such that $Y = X_0 < \cdots < X_n = \langle M, g \rangle$ and $X_i$ is maximal in $X_{i+1}$ for all $i$. By 6.2.20, $|X_{i+1} : X_i|$ is a prime and it follows that $|\langle M, g \rangle : Y| < \infty$. Thus $M$ is permodular in $G$.

Finally, suppose that every subgroup of $G$ is permodular in $G$. Then $L(G)$ is clearly modular. If $B \leq A \leq G$ are such that $[A/B]$ is of finite length, then there exists a chain of subgroups $B = A_0 < \cdots < A_m = A$ with $A_i$ maximal in $A_{i+1}$ for all $i$. Since $A_i$ is permodular in $G$, the index $|A_{i+1} : A_i|$ is finite. It follows that $|A : B| < \infty$ and hence $[A/B]$ is a finite lattice. Thus $L(G)$ is permodular.

Theorem 6.4.3 in particular implies that the subgroup lattice of an abelian group is permodular. We can now characterize the class of perfect groups; however, it is somewhat easier to state this in terms of nonperfect groups.

**6.4.4 Theorem** (Zacher [1982b]). The group $G$ is not perfect if and only if there exists a proper permodular subgroup $M$ of $G$ having one of the following three properties.

1. $[G/M]$ is a finite chain.
2. $[G/M]$ is permodular and contains an element $X$ such that $[X/M]$ is isomorphic to the subgroup lattice of an infinite cyclic group.
3. $[G/M]$ is isomorphic to the partially ordered set $(\mathbb{N}, <)$ of positive integers and every subgroup of $M$ that is invariant under $P(M)$ is permodular in $G$.

**Proof.** First suppose that $G$ is not perfect. Then $G/G'$ is a nontrivial abelian group. If there exists an element of infinite order in $G/G'$, then $M = G'$ satisfies (2). So suppose that $G/G'$ is a torsion group. It is well-known (see Robinson [1982], p. 107) that an abelian group which is not torsion-free has a nontrivial direct factor which is either cyclic of prime power order or quasicyclic; let $M/G'$ be a complement to such a direct factor in $G/G'$. Then $M$ is permodular in $G$ and $[G/M]$ is a finite chain, that is (1) holds, or $G/M \cong C_p$ for some prime $p$ and hence $[G/M] \cong (\mathbb{N}, <)$ in this case. Every subgroup of $M$ that is invariant under $P(M)$ is characteristic in $M$, hence normal in $G$, in particular permodular in $G$. Thus (3) holds.

Conversely, suppose that $M$ is a proper permodular subgroup of $G$ having one of the properties (1)--(3). If (1) is satisfied, then $|G : M| < \infty$ and hence $G/M_0$ is a finite group. By 5.1.3, it is a $p$-group or a $P$-group; in any case, $G$ is not perfect. If (2) holds and $x \in X \setminus M$, then $[\langle x \rangle / \langle x \rangle \cap M] \cong [\langle M, x \rangle / M]$ and hence $o(x, M)$ is infinite. By 6.2.12, $M \leq A(M) \leq G$ and by 6.4.3, $G/A(M)$ and $A(M)/M$ are metabelian. Thus $G^{(4)} \leq M < G$ and $G$ is not perfect. Finally, suppose that (3) holds and, for a contradiction, that $G$ is perfect. Then $G'' = G$ and by 6.2.19,

(4) $M$ is permutable in $G$.

Since $[G/M] \cong (\mathbb{N}, <)$, it follows that

(5) $G$ is not finitely generated modulo $M$.

Furthermore, there exists a subgroup $M_1$ of $G$ such that $M$ is maximal in $M_1$. Since $M$ is permutable in $G$, the index $|M_1 : M| = p$ is a prime. For every proper subgroup
Projectivities and normal structure of infinite groups

Let $H$ be a finite normal subgroup of $G$ containing $M$, $[H/M]$ is a finite chain and hence

(6) $H = M \langle x \rangle$ for some $x \in G$.

Therefore $|H : M|$ is finite and by 5.1.3,

(7) $H/M_H$ is a finite $p$-group.

If $M/M_H$ were cyclic for every $M \leq H < G$, it would follow that $G'' \leq M$. For, (5) and (6) show that any four elements $a, b, c, d$ of $G$ together with $M$ generate a proper subgroup $H = M \langle x \rangle$ of $G$. It follows by 5.2.13, that $H/M_H = (M/M_H) \langle xM_H \rangle$ is metacyclic, and hence $[[a,b],[c,d]] \in H'' \leq M_H \leq M$. Thus $G'' \leq M$, a contradiction. Hence there exists a noncyclic factor group $M/M_H$ and therefore a normal subgroup $K$ of $M$ such that

(8) $M/K$ is elementary abelian of order $p^2$.

Let $D = \bigcap_{\sigma \in P(M)} K^\sigma$. If $\sigma \in P(M)$, then $K^\sigma$ is permodular in $M$ and hence $|M : K^\sigma| < \infty$.

Suppose first that $K^\sigma$ is not normal in $M$ and let $N_1, \ldots, N_{p+1}$ be the maximal subgroups of $M$ containing $K^\sigma$. Then none of the $N_i$ is normal in $M$; for, $N_i \leq M$ would imply that $K^\sigma = N_i \cap N_j \leq N_i$ for all $j \neq i$ and hence $K^\sigma \leq M$. Therefore $(K^\sigma)^M = M$. Since the lattice $[M/K^\sigma]$ is directly indecomposable, 5.1.14 shows that $M/(K^\sigma)_M$ is a $P$-group or $K^\sigma$ is permutated in $M$. In the latter case, 6.2.10 would imply that $K^\sigma \leq N_i$ for all $i$ and hence again $K^\sigma \leq M$, a contradiction. Thus $M/(K^\sigma)_M$ is a $P$-group and, since $K^\sigma$ is contained in exactly $p + 1$ maximal subgroups of $M$, it follows that $M/(K^\sigma)_M \in P(n, p)$ for some $n \in \mathbb{N}$. If $K^\sigma \leq M$, then, as a projective image of $M/K$, $M/K^\sigma \in P(2, p)$. In both cases, $M'' \leq K^\sigma$ and $x^{p(p-1)} \in K^\sigma$ for every $x \in M$. This holds for all $\sigma \in P(M)$ and hence $M'' \leq D$ and $x^{p(p-1)} \in D$ for all $x \in M$. Thus

(9) $M/D$ is metabelian of exponent dividing $p(p-1)$;

we remark that by Exercise 6.5.8, $M/D$ is an elementary abelian $p$-group. Now suppose, for a contradiction, that $M \leq D^G$. Since $|M/K| = p^2$, there exist $x, y \in M$ such that $M = \langle K, x, y \rangle$ and by 6.2.7 there exists a subgroup $L \geq D$ of $G$, finitely generated modulo $D$, such that $x, y \in D^L$. Write $L = \langle D, z_1, \ldots, z_n \rangle$ and $H = \langle M, z_1, \ldots, z_n \rangle$. By (5) and (6), $H = M \langle g \rangle < G$ for some $g \in G$ and it follows that

$\langle D, x, y \rangle \leq D^L \leq D^H = D^M \langle g \rangle = D^g \leq \langle D, g \rangle$.

Since $D$ is invariant under $P(M)$, our assumption (3) implies that $D$ is permodular in $G$ and hence $[[\langle D, g \rangle/D] \cong [\langle g \rangle/\langle g \rangle \cap D]$ is a distributive lattice. It follows that $\langle D, x, y \rangle/D$ is cyclic and hence $\langle K, x, y \rangle/K = M/K$ is cyclic, a contradiction. Thus

(10) $M \nleq D^G$;

let $D^G = N$. Then $N \neq G$ and by (9), $MN/N \simeq M/M \cap N$ is metabelian of exponent dividing $p(p-1)$. Since $G$ is perfect, $MN \neq G$. It follows that $[G/MN] \simeq (\mathbb{N}, <)$ and $MN/N$ is a permutated subgroup of $G/N$ of exponent dividing $p(p-1)$. For every element $uN$ in some conjugate of $MN/N$, the index $|(MN/N)\langle uN \rangle : MN/N|$ divides
6.4 Lattice-theoretic characterizations of classes of infinite groups

o(uN) and hence p(p − 1); on the other hand, by (7), |MN ⟨u⟩ : MN| is a power of p. Thus u is contained in the atom of the infinite chain [G/MN] and, since uN was arbitrary, it follows that (MN)^6 < G. But then again [G/(MN]^6] ≅ (N, <) and, by 1.2.3, G/(MN)^6 is abelian, a final contradiction. Thus G is not perfect.

As in the finite case, we can use Theorem 6.4.4 to characterize the final term \( G_{\infty} \) of the (transfinitely extended) derived series of G. For, this subgroup is clearly perfect, it contains every perfect subgroup of G, and hence it is the maximum perfect subgroup of G. We only note the usual corollary; recall that a group G for which \( G_{\infty} = 1 \) is called hypoabelian.

6.4.5 Corollary (Napolitani [1982]). If ϕ is a projectivity from the group G to a group \( \overline{G} \), then \( (G_{\infty})^\phi = \overline{G}_{\infty} \). In particular, the classes of perfect and of hypoabelian groups are invariant under projectivities.

Generalized soluble groups

We want to generalize our characterizations 5.3.5 and 5.3.7 of finite soluble and supersoluble groups. There are several classes of infinite groups that are candidates for such a generalization. We remind the reader that a group G is called hyperabelian (hypercyclic) if every nontrivial epimorphic image of G contains a nontrivial abelian (cyclic) normal subgroup. Equivalent is (see Robinson [1972a], p. 14) that there exists an ascending series \( (N_\alpha)_{\alpha \leq \gamma} \) of normal subgroups \( N_\alpha \) of G, \( \gamma \) an ordinal number, such that \( N_0 = 1 \), \( N_\gamma = G \), \( N_{\alpha+1}/N_\alpha \) is abelian (cyclic) for every ordinal \( \alpha < \gamma \) and \( N_\beta = \bigcup_{\alpha < \beta} N_\alpha \) for limit ordinals \( \beta \). If \( \gamma \) can be chosen finite, G is called soluble (supersoluble). We first characterize the class of hyperabelian groups and for this we have to study permodular subgroups with permodular subgroup lattice.

6.4.6 Lemma. If M is a nontrivial permodular subgroup of G with permodular subgroup lattice, then \( M^G \) contains a nontrivial abelian normal subgroup of G.

Proof. First consider the case that \( M^G \) is torsion-free. Let \( g \in G \) and \( L = \langle M, g \rangle \). By 6.2.8, \( |M^L : M| \) and \( |M^L : M^g| \) are finite and hence so is \( |M^L : M \cap M^g| \). By 2.4.9, \( M \) and \( M^g \) are abelian and therefore \( M \cap M^g \leq Z(M \cup M^g) \). It follows that \( M \cap M^g/Z(M \cup M^g) \) is finite. A well-known theorem of Schur’s (see Robinson [1982], p. 278) states that then \( (M \cup M^g) \) is finite and hence trivial since \( M^G \) is torsion-free. Thus \( M \cap M^g \) is abelian for every \( g \in G \). This shows that \( M \leq Z(M^G) \), and that \( Z(M^G) \) is a nontrivial abelian normal subgroup of G.

Now suppose that \( M^G \) is not torsion-free. Then there exist elements of prime order \( p \), say, in \( M^G \). If any two of these commute, then \( A = \langle u \in M^G | o(u) = p \rangle \) is an elementary abelian characteristic subgroup of \( M^G \), and hence a nontrivial abelian normal subgroup of G contained in \( M^G \). So suppose that \( u, v \) are elements of order \( p \) of \( M^G \) such that \([u, v] \neq 1\). Then \( u = a_1 \ldots a_r \) and \( v = a_{r+1} \ldots a_n \) where \( a_i \in M^{g_i} \),
Let \( g_i \in G \); let \( L = \langle M, g_1, \ldots, g_n \rangle \) and \( H = M \cup M^{g_1} \cup \cdots \cup M^{g_n} \). By 6.2.21, \( H \) is permodular in \( G \). Clearly,

(11) \( u, v \in H \leq M^L \)

and we want to show that \([u, v] \in H_G\). For this let \( x \in G \) such that \( o(x, H) \) is a prime power and let \( T = \langle H, x \rangle \). By 6.2.13, \( T/H_T \) is nonabelian of order \( rs \) or a finite \( r \)-group for primes \( r, s \). In the first case, \( H/H_T \) is abelian and hence \([u, v] \in H_T\); in the second, \( H/H_T \) is a core-free permutable subgroup of the \( r \)-group \( T/H_T \) with cyclic supplement \( \langle xH_T \rangle \), and then (c) of 5.2.8 shows that \([u, v] \in H_T\). Thus in both cases, \([u, v] \in H_T\) and, since \( H_G \) is the intersection of these \( H_T \), it follows that

(12) \( 1 \neq [u, v] \in H_G\).

By 6.2.8, \( |M^L : M| < \infty \). Since \( H \leq M^L \), it follows that \( |H : M| \), and hence \( H/M_H \), is finite. By 5.2.5, \( M^H/M_H \) is soluble. If \( H_0 = M^H \) and \( H_i = M^H(M^H \cup \cdots \cup M^{g_i}) \) for \( i = 1, \ldots, n \), then \( M^H = H_0 \leq \cdots \leq H_n = H, H_i \equiv \mod H \) and \([H_{i+1}/H_i]\) is isomorphic to an interval in \([H_i \cup \langle g_{i+1} \rangle/H_i]\) \( \simeq \langle g_{i+1} \rangle/\langle g_{i+1} \rangle \cap H_i\). Hence every \([H_{i+1}/H_i]\) is distributive and, by 5.3.7, \( H/M^H \) is supersoluble. By 6.4.3, \( M \) is soluble. Since \( H/M^H, M^H/M_H \) and \( M_H \) are soluble, we finally conclude that \( H \) is soluble. By (12), \( H_G \neq 1 \), so it contains a nontrivial abelian characteristic subgroup \( A \). Since \( H_G \leq M^G \), we see that \( A \) is an abelian normal subgroup of \( G \) contained in \( M^G \).

6.4.7 Theorem (Busetto [1980a], Zacher [1982b]). The group \( G \) is hyperabelian if and only if it has an ascending series \((M_a)_{a \leq \gamma}\) of permodular subgroups \( M_a \) of \( G \), \( \gamma \) an ordinal number, such that \( M_0 = 1, M_\gamma = G, [M_{a+1}/M_a] \) is permodular for every ordinal \( a < \gamma \) and \( M_\beta = \bigcup_{a < \beta} M_a \) for limit ordinals \( \beta \).

Proof. If \( G \) is hyperabelian, there exists an ascending series \((M_a)_{a \leq \gamma}\) of normal subgroups \( M_a \) of \( G \) such that \( M_{a+1}/M_a \) is abelian for every \( a \), and this series clearly has the desired properties. Conversely, suppose that \((M_a)_{a \leq \gamma}\) is a series with the properties stated in the theorem and let \( N \) be a proper normal subgroup of \( G \). Define \( \delta = \min \{a \leq \gamma \mid M_a \not\leq N\} \). Then \( M_\varepsilon \leq N \) for every \( \varepsilon < \delta \) and hence \( \delta \) is not a limit ordinal. It follows that \( M_{\delta-1} \leq N < M_\delta N \) and thus \( M_\delta N/N \) is a nontrivial permodular subgroup of \( G/N \) with subgroup lattice isomorphic to \([M_\delta/M_\delta \cap N]\), that is, with permodular subgroup lattice. By 6.4.6 there exists a nontrivial abelian normal subgroup in \( G/N \). Thus \( G \) is hyperabelian.

It is interesting to note that the property of Theorem 6.4.7 with finite \( \gamma \), which seems to be the most natural lattice-theoretic approximation of solubility, in fact does not characterize the class of soluble groups. Indeed, Stonehewer [1973] has constructed a nonsoluble group \( G \) that is the product of two metabelian subgroups \( H \) and \( K \) which are permutable in \( G \) and have modular subgroup lattice. By 6.4.3, \( L(H) \) and \( L(K) \) are permodular and so \( 1 < H < G, H \) is permodular in \( G, [H/1] \) and \([G/H] \simeq [K/H \cap K] \) are permodular. If we restrict ourselves to finitely generated groups, the situation is better.
6.4 Lattice-theoretic characterizations of classes of infinite groups

6.4.8 Theorem (Previtiato [1978]). Let $G$ be a finitely generated group. Then $G$ is soluble if and only if there exist subgroups $M_i$ of $G$ such that $1 = M_0 \leq \cdots \leq M_n = G$, $M_i$ is permodular in $G$ and $[M_{i+1}/M_i]$ is permodular $(i = 0, \ldots, n - 1)$.

Proof. The members of the derived series of a soluble group of course have the given property. So suppose, conversely, that $G$ has a chain of subgroups $M_i$ as described in the theorem. We show by induction on the length $n$ of this chain that $G$ is soluble. For this let $M_1 = M$; by 6.4.3, $M$ is soluble. Since $G$ is finitely generated, 6.2.8 yields that $|G^G : M| < \infty$ and hence $G^G/M^G$ is a finite group. The existence of a chain $1 = M_0 \leq \cdots \leq M_n = G$ of modular subgroups $M_i$ with modular intervals $[M_{i+1}/M_i]$ is inherited by subgroups and factor groups. Therefore $G^G/M^G$ has such a chain and hence, by 5.3.5, is soluble. Thus $G^G$ is soluble and, since the chain of the $M_i M^G/M^G$ $(i = 1, \ldots, n)$ in $G/M^G$ has length $n - 1$ and $G/M^G$ is finitely generated, the induction assumption implies that $G/M^G$ is soluble. Thus $G$ is soluble.

Since the cyclic groups are characterized lattice-theoretically, it is possible to decide in the subgroup lattice whether a group is finitely generated. Therefore Theorem 6.4.8 yields a lattice-theoretic characterization of the class of finitely generated soluble groups. A lattice-theoretic characterization of the class of all soluble groups is not known. However, we shall prove in 6.6.4 that this class at least is invariant under projectivities.

Recall that a group $G$ is polycyclic if there exists a finite chain $1 = G_0 \leq \cdots \leq G_n = G$ of subgroups $G_i$ such that $G_i \leq G_{i+1}$ and $G_{i+1}/G_i$ is cyclic $(i = 0, \ldots, n - 1)$. It is well-known (see Robinson [1982], p. 147) that the polycyclic groups are precisely the hyperabelian or (finitely generated) soluble groups satisfying the maximal condition for subgroups. Therefore 6.4.7 and 6.4.8 both yield lattice-theoretic characterizations of the class of polycyclic groups. We give another characterization which is closer to the above definition.

6.4.9 Theorem. The group $G$ is polycyclic if and only if there exist subgroups $M_i$ of $G$ such that $1 = M_0 \leq \cdots \leq M_n = G$, $M_i$ is permodular in $M_{i+1}$, $[M_{i+1}/M_i]$ is distributive and satisfies the maximal condition $(i = 0, \ldots, n - 1)$.

Proof. A polycyclic group clearly has this property. So suppose, conversely, that $G$ is a group with such a chain of subgroups $M_i$. We use induction on the length $n$ of this chain to prove that $G$ is polycyclic. The induction assumption implies that $M_{n-1}$ is polycyclic; furthermore, $M_{n-1}$ is permodular in $G$. Since $[G/M_{n-1}]$ satisfies the maximal condition, there exists a subgroup $M$ of $G$ containing $M_{n-1}$ and maximal with respect to these two properties. Suppose, for a contradiction, that $M$ is not normal in $G$. Then by 6.2.13 there exists $x \in J(M)$ such that $M \neq M^x$ and, if $T = \langle M, x \rangle$, $T/M_T$ is nonabelian of order $pq$ or a finite $p$-group, $p$ and $q$ primes. In both cases, $T/M_T$ and $M_T$ are polycyclic and hence so is $T$. In particular, $M \cup M^x$ is polycyclic and, by 6.2.6, permodular in $G$. This contradicts the maximality of $M$. Thus $M \leq G$ and, since $[G/M]$ is distributive and satisfies the maximal condition, $G/M$ is cyclic. It follows that $G = M$ is polycyclic.
We remark that we did not use the deeper results of §6.2 to prove Theorems 6.4.7–6.4.9; note that we can use 6.2.6(d) instead of 6.2.21 in the proof of 6.4.6.

Supersoluble groups

In the following characterization of supersoluble groups, however, we have to study cyclic permodular subgroups and for this we need Theorem 6.2.17.

6.4.10 Lemma. If $M$ is a finite cyclic permodular subgroup of the group $G$, then $M^G/M_G$ is hypercyclically embedded in $G$.

Proof. We may assume that $M_G = 1$. By 6.2.17, $M$ is permutable or $P$-embedded in $G$. In the first case, 5.2.12 yields that $M^G$ is hypercentrally embedded in $G$. In the second case, $G = S \times T$ where $S$ is a direct product of $P$-groups, $M^G = S \times (M \cap T)^G$ and $M \cap T$ is permutable in $G$. Clearly, $S$ is hypercyclically embedded in $G$ and so is $(M \cap T)^G$, again by 5.2.12. Finally (c) of 5.2.1 shows that $M^G$ is hypercyclically embedded in $G$.

6.4.11 Theorem (Busetto [1980b], Zacher [1982b]). The group $G$ is supersoluble if and only if there exist subgroups $M_i$ of $G$ such that

\[ I = M_0 \leq \cdots \leq M_n = G, \quad M_i \text{ is permodular in } G, \quad [M_{i+1}/M_i] \text{ is distributive and satisfies the maximal condition (} i = 0, \ldots, n - 1 \).\]

Proof. In the first place, every supersoluble group has this property. Suppose, conversely, that $G$ is a group with such a chain of subgroups $M_i$. We use induction on the length $n$ of this chain to prove that $G$ is supersoluble. Let $M = M_1$; then $M$ is cyclic. By 2.1.7, $L(G)$ satisfies the maximal condition. In particular, $G$ is finitely generated and 6.2.18 shows that $M^G/M_G$ is periodic. Therefore $M/M_G$ is a finite cyclic permodular subgroup of $G/M_G$ and, by 6.4.10, $M^G/M_G$ is hypercyclically embedded in $G$. Since $G$ satisfies the maximal condition, this implies that there exists a finite chain $M_G = N_0 \leq \cdots \leq N_m = M^G$ of normal subgroups $N_i$ of $G$ such that $N_{i+1}/N_i$ is cyclic ($i = 0, \ldots, m - 1$). Since $M_G$ is cyclic and $G/M^G$, by induction, is supersoluble, it follows that $G$ is supersoluble.

To characterize the class of hypercyclic groups, one also has to study infinite cyclic permodular subgroups.

6.4.12 Lemma. Let $M$ be an infinite cyclic subgroup of $G$ and let $T(M^G)$ be the torsion subgroup of $M^G$.

(a) If $M$ is permutable in $G$, then $T(M^G) \leq Z_x(G)$.

(b) If $M$ is permodular in $G$, then $T(M^G)$ is hypercyclically embedded in $G$.

The proof of 6.4.12 is complicated. We refer the reader to Busetto [1980b] where he proves (a) and instead of (b) the corresponding result for modular subgroups in Tarski-free groups; this proof can be carried over literally to permodular subgroups.
6.4 Lattice-theoretic characterizations of classes of infinite groups

6.4.13 Theorem (Busetto [1980b], Zacher [1982b]). The group $G$ is hypercyclic if and only if it has an ascending series $(M_\gamma)_{\gamma \leq \gamma}$ of permodular subgroups $M_\gamma$ of $G$, $\gamma$ an ordinal number, such that $M_0 = 1$, $M_\gamma = G$, $[M_{\gamma+1}/M_\gamma]$ is distributive and satisfies the maximal condition for every ordinal $\alpha < \gamma$ and $M_\beta = \bigcup_{\alpha < \beta} M_\alpha$ for limit ordinals $\beta$.

Further topics

There are a number of interesting open problems. First of all, we do not know a lattice-theoretic characterization of the class of soluble groups; this is perhaps the most exciting problem altogether on subgroup lattices of groups. Furthermore, we would like to know which classes of groups are described by properties (b) and (c) of Theorem 5.3.5 if the word "modular" throughout is replaced by "permodular". Finally, there are many classes of generalized soluble groups of which it is not known whether they are invariant under projectivities; naturally, no lattice-theoretic characterizations of these classes are known. An important exception is the class of SN-groups, that is, of groups possessing a series with abelian factors (see Robinson [1982], p. 365). As a special case of a general theorem on varieties of groups, Hickin and Phillips [1973] prove that $G$ is an SN-group if and only if for every finitely generated subgroup $K$ of $G$, $K' \leq K$. Using Theorem 6.4.4, it is now easy to give a lattice-theoretic characterization of this class of groups.

We conclude this section with a lattice-theoretic characterization of a somewhat different type of class of groups; for similar results see Exercises 3–5.

6.4.14 Theorem (de Giovanni and Franciosi [1983]). The group $G$ is residually supersoluble if and only if for every nontrivial element $x$ in $G$ there exist subgroups $M_i$ of $G$ such that $x \not\in M_0 \leq \cdots \leq M_n = G$, $M_i$ is permodular in $G$, $[M_{i+1}/M_i]$ is distributive and satisfies the maximal condition ($i = 0, \ldots, n - 1$).

Proof. A residually supersoluble group of course has the given property. For the proof of the converse, we need some preliminaries. Let us call a chain $M = M_0 < \cdots < M_n = G$ of permodular subgroups $M_i$ of $G$ such that $[M_{i+1}/M_i]$ is distributive and satisfies the maximal condition ($i = 0, \ldots, n - 1$) a supersoluble chain connecting $M$ and $G$. Then for $N \leq G$,

\begin{equation}
(13) \frac{MN}{N} = \frac{M_0N}{N} \leq \cdots \leq \frac{M_nN}{N} = \frac{G}{N}
\end{equation}

is a supersoluble chain connecting $MN/N$ and $G/N$. In particular, for $N = M^G$, the chain (13) connects $M^G/M^G$ with $G/M^G$ and 6.4.11 shows that

\begin{equation}
(14) \frac{G}{M^G} \text{ is supersoluble.}
\end{equation}

By 2.1.7, $[G/M]$ satisfies the maximal condition and hence $G$ is finitely generated modulo $M$. Thus 6.2.8 yields that $|M^G : M| < \infty$. Therefore if $G/M^G$ is finite, then
Projectivities and normal structure of infinite groups

$|G : M| < \infty$ and $G/M_G$ is a finite group. By 5.2.5, $M^G/M_G$ is hypercyclically embedded in $G$ and, considering (14), we conclude that

(15) $G/M_G$ is supersoluble if $G/M^G$ is finite.

If $G/M^G$ is not finite, then $G/M^G$ has a torsion-free normal subgroup $R/M^G$ of finite index (see Robinson [1982], p. 148). Every $x \in R \setminus M^G$ has infinite order modulo $M$ and, by 6.2.12, $M$ is permutable in $G$, $M \leq A(M) \leq G$ and $R \leq M^G A(M) \leq A(M)$. Thus $|G : A(M)| < \infty$ and hence $M$ has only finitely many conjugates $M^{g_1}, \ldots, M^{g_n}$. Then $M^G = M^{g_1} \cdots M^{g_n}$ and, by 6.3.2, $M^G/(M^{g_i})_{M^{g_i}}$ is finite and nilpotent for all $i = 1, \ldots, n$. Since $M_G = \bigcap_{i=1}^n (M^{g_i})_{M^{g_i}}$, it follows that $M^G/M_G$ is a finite nilpotent group. Considering (14), we obtain in this case, and hence in general,

(16) $G/M_G$ is polycyclic.

Now suppose that $G$ is a group with the property given in the theorem and let $1 \neq x \in G$. We have to find a normal subgroup $N$ of $G$ such that $x \not\in N$ and $G/N$ is supersoluble. By assumption there exist a permutable subgroup $M$ of $G$ and a supersoluble chain $M = M_0 \leq \cdots \leq M_n = G$ connecting $M$ and $G$ such that $x \not\in M$. Then by (16), $G/M_G$ is polycyclic and a well-known theorem of Malcev's (see Robinson [1982], p. 148) says that $M$ is the intersection of subgroups of finite index in $G$. Since $x \not\in M$, there exists such a subgroup $H$ of finite index such that $x \not\in H$; let $N = H_G$. Then $G/N$ is finite, $x \not\in N$ and (13) is a supersoluble chain connecting $MN/N$ and $G/N$. Since $MN \leq H$, we have $(MN)_G = N$, and therefore (15) applied to $MN/N$ shows that $G/N$ is supersoluble. Thus $G$ is residually supersoluble.

Finally we remark that most of the results of this section differ slightly from the theorems proved in the cited papers. For example, the classes of hyperabelian, hypercyclic, and hence also of supersoluble (that is hypercyclic with maximal condition) groups were characterized by Busetto [1980a], [1980b] using properties of modular subgroups in certain Tarski-free groups. Zacher [1982b] realized that the main tools in these papers can be proved literally the same way for permodular subgroups of arbitrary groups using the corresponding properties of permodular subgroups; this yielded Lemmas 6.4.6, 6.4.10 and 6.4.12. He then stated the characterizations of hyperabelian and of hypercyclic groups that are more or less Theorems 6.4.7 and 6.4.13.

Exercises

1. Let $p > 2$ be a prime, $G = \langle a, b, x | a^p = b^p = [a, b] = 1, a^x = ab, b^x = b \rangle$ and $M = \langle a, bx^p \rangle$. Show that $M$ per $G$ and $\langle a \rangle$ is invariant under $P(M)$ but not permodular in $G$.

2. Use 6.4.10 and 6.4.12 to prove 6.4.13.

3. (de Giovanni and Franciosi [1983]) Show that the group $G$ is residually polycyclic if and only if for every nontrivial element $x \in G$ there exist subgroups $M_i$ of $G$ such that $x \not\in M_0 \leq \cdots \leq M_n = G$, $M_i$ is permodular in $G$, $[M_{i+1}/M_i]$ is permodular and satisfies the maximal condition ($i = 0, \ldots, n - 1$).
4. Show that the group $G$ is residually polycyclic if and only if for every nontrivial element $x \in G$ there exist a permodular subgroup $M$ and subgroups $M_i$ of $G$ such that $x \not\in M = M_0 \leq \cdots \leq M_n = G$, $M_i$ is permodular in $M_{i+1}$, $[M_{i+1}/M_i]$ is distributive and satisfies the maximal condition ($i = 0, \ldots, n - 1$).

5. Find a lattice-theoretic characterization for the class of residually finitely generated soluble groups (de Giovanni and Franciosi [1983]).

6.5 Projective images of normal subgroups of infinite groups
and index preserving projectivities

The main result of this section will be that $N^G$ and $N_G$ are normal subgroups of $G$ if $N \trianglelefteq G$ and $\varphi$ is a projectivity from $G$ to $G$; therefore $\varphi$ induces a projectivity from $G/N_G$ to $G/N_G$. This, in particular, will reduce all problems about projective images of subgroups of finite index to the corresponding problems for finite groups. We use this fact to give some applications to index preserving projectivities. We show that a projectivity is index preserving if it preserves all the indices in cyclic subgroups. This enables us to generalize the results of §4.2 on singular projectivities of finite groups to locally finite groups; for example, we prove that every projectivity of such a group induces an index preserving projectivity in the second commutator subgroup. We prove some results on singular projectivities of groups with elements of infinite order and show that index preserving projectivities of arbitrary groups map ascending subgroups to ascending subgroups and therefore preserve the Gruenberg radical. Finally we give a lattice-theoretic characterization of the locally finite radical of a group.

Criteria for normality

First of all we give a number of useful criteria for a projective image of a normal subgroup to be normal. All these are immediate consequences of our results on permodular subgroups in §6.2.

6.5.1 Theorem (Zacher [1980]). If $N \trianglelefteq G$ and $G/N$ is infinite cyclic, then $N^o \trianglelefteq \tilde{G}$ for every projectivity $\varphi$ from $G$ to a group $\tilde{G}$.

Proof. By 6.2.1, $N^o$ is permodular in $\tilde{G}$. Let $x \in G$ such that $G = \langle N, x \rangle$. Then $\tilde{G} = N^o \cup \langle x \rangle^o$ and $\langle x \rangle^o = \langle y \rangle$ is cyclic. Since $[\langle y \rangle/\langle y \rangle \cap N^o] \simeq [\langle x \rangle/\langle x \rangle \cap N] \simeq L(G/N)$, it follows that $o(y, N^o)$ is infinite. By 6.2.3, $y$ normalizes $N^o$ and hence $N^o \trianglelefteq \tilde{G}$. □

In the sequel we frequently have to study nonnormal projective images of normal subgroups. We collect the basic features of this situation.
6.5.2 Remark. Let \( \varphi \) be a projectivity from \( G \) to \( \bar{G} \), let \( N \trianglelefteq G \) and suppose that \( N^\varphi = \bar{N} \) is not normal in \( \bar{G} \). Since \( \bar{N} \) is permodular in \( \bar{G} \), 6.2.13 shows that

\[
N_{\bar{G}} = \bigcap \{ \bar{N}_{<N,y>} | y \in J(\bar{N}) \}.
\]

In particular, there exists \( y \in J(\bar{N}) \) such that \( \bar{N}^y \neq \bar{N} \); let \( T, D, M \leq G \) such that \( T = \langle \bar{N}, y \rangle \), \( \bar{D} = \bar{N}_T \) and \( \bar{M} = \bar{N}^y \). As a projective image of \( N \),

\[
M = N^{\varphi y} \quad \text{is permodular in } G.
\]

Furthermore, \( [\bar{T}/\bar{N}^y] \simeq [\bar{T}/\bar{N}] \simeq [\langle y \rangle/\langle y \rangle \cap \bar{N}] \) is a finite chain and hence \( \bar{N} \cap \bar{N}^y < \bar{N} < \bar{N} \cup \bar{N}^y \). Thus

\[
D \leq N \cap M < N < NM \leq T \text{ and } [T/N] \simeq [T/M] \text{ is a finite chain;}
\]

it follows that

\[
T/N \text{ is cyclic of prime power order.}
\]

Finally, (9) in 6.2.13 shows that

\[
(5) \quad \bar{T}/\bar{D} \text{ is a finite } p\text{-group}
\]

or nonabelian of order \( pq \) for primes \( p, q \). In the second case let \( p > q \) and \( \bar{L}/\bar{D} \) be a minimal subgroup of \( \bar{T}/\bar{D} \) different from \( \bar{N}/\bar{D} \) and \( \bar{M}/\bar{D} \). Then \( D = N \cap M \leq M \) and \( D = N \cap L \leq L \) and hence \( D \leq M \cup L = T \). Being a projective image of \( \bar{T}/\bar{D} \), the group \( T/D \) belongs to \( P(2, p) \); since \( N \trianglelefteq T \) but \( \bar{N} \) is not normal in \( \bar{T} \), there exists a prime \( r \) such that

\[
(6) \quad |T/D| = pr, |N/D| = p \geq r, |\bar{T}/\bar{D}| = pq, |\bar{N}/\bar{D}| = q < p.
\]

We shall show in 6.5.6 that \( D \leq T \). Therefore if (5) holds, then \( \varphi^{-1} \) induces a projectivity from the nonabelian \( p \)-group \( \bar{T}/\bar{D} \) onto \( T/D \) and 2.2.6 implies that

\[
(7) \quad \bar{T}/\bar{D} \text{ and } T/D \text{ are finite } p\text{-groups.}
\]

Note that for the moment only (5) or (6) holds in the situation we consider; as soon as 6.5.6 is proved, we shall know that (6) or (7) is satisfied.

The above discussion in particular yields (where again 6.5.6 is used for the last assertion in (b)):

6.5.3 Theorem. Let \( \varphi \) be a projectivity from the group \( G \) to the group \( \bar{G} \), let \( N \trianglelefteq G \) and \( K \trianglelefteq G \) such that \( K^\varphi = (N^\varphi)_\bar{G} \).

(a) If \( |G:N| = r \) is a prime, then either \( N^\varphi \trianglelefteq \bar{G} \) or there exist primes \( p \) and \( q \) such that \( \bar{G}/K^\varphi \) and \( G/K \) are contained in \( P(2, p) \) and, more precisely,

\[
|G/K| = pr, |N/K| = p \geq r, |\bar{G}/K^\varphi| = pq, |N^\varphi/K^\varphi| = q < p.
\]

(b) Let \( G/N \) be cyclic of prime power order \( p^n, n \geq 2 \). Then \( \bar{G}/K^\varphi \) is a finite primary group; if \( N^\varphi \) is not normal in \( \bar{G} \), then \( G/K \) and \( \bar{G}/K^\varphi \) are finite \( p \)-groups.
Proof. By assumption, $G/N$ is cyclic of prime power order; let $x \in G$ such that $G = \langle N, x \rangle$ and let $\langle x \rangle^* = \langle y \rangle$. If $N^\circ$ is not normal in $\widetilde{G}$, then $(N^\circ)^* \neq N^\circ$ and $T = G$ satisfies the assumptions of 6.5.2. If $|G : N| = r$ is a prime, then (5) cannot hold since maximal subgroups of finite $p$-groups are normal. Therefore (6) is satisfied and that is the assertion in (a). Now suppose that $|G/N| = p^n$ and $n \geq 2$. Then (6) cannot hold and hence $\widetilde{G}/K^\circ$ is a finite primary group. Clearly this is also true if $N^\circ \leq \widetilde{G}$. Since $G/N$ is a $p$-group, the last assertion in (b) follows from (7); for this we need 6.5.6. \hfill \Box

In the following criterion we extend 5.4.9 (a) to infinite groups. Exercise 2, however, shows that (b) and (c) of 5.4.9 do not hold for arbitrary groups. Since the group $G$ in this example is perfect, it shows in addition that normal subgroups of perfect groups in general are not mapped to normal subgroups under projectivities (compare with Theorem 5.3.4 for finite groups).

6.5.4 Theorem. Let $N$ be a normal subgroup of the group $G$ and suppose that one of the following is satisfied:

(a) $G/N$ has no nontrivial cyclic normal subgroup.

(b) $N$ is perfect.

(c) $N$ has no proper subgroup of finite index.

Then $N^\circ \leq \widetilde{G}$ for every projectivity $\varphi$ from $G$ to a group $\widetilde{G}$.

Proof. Suppose, for a contradiction, that $N^\circ$ is not normal in $\widetilde{G}$ and let $y, T, M$ be as in 6.5.2. Then $N \cap M < N < NM$ and $[N/N \cap M] \cong [NM/M]$ is a finite chain. By 6.2.6, $N \cap M$ is permular in $N$ and 6.2.5 yields that $|N : N \cap M|$ is finite. This contradicts (c) and also (b) because of 5.1.3. Furthermore, $NM/N$ is a finite cyclic permular subgroup in $G/N$. By 6.4.10 there exists a nontrivial cyclic normal subgroup in $G/N$ and this contradicts (a). Thus we get a contradiction if any of our three assumptions hold. It follows that $N^\circ \leq \widetilde{G}$ in all cases. \hfill \Box

The normality of $N\widetilde{G}$ and $N_{\widetilde{G}}$

We come to the main result of this section. We want to show that the preimages of the core and the normal closure of a projective image of a normal subgroup are normal subgroups. The main step in the proof of this theorem is the following partial result.

6.5.5 Lemma. Let $N \leq G$ and $G/N$ be finitely generated. If $\varphi$ is a projectivity from $G$ to a group $\widetilde{G}$ and $H^\circ = (N^\circ)^\widetilde{G}$, then $H \leq G$.

Proof. Let $N^\circ = \widetilde{N}$ and $\overline{K} = N_{\widetilde{G}}$. Then $\widetilde{N}$ is permular in $\widetilde{G}$ and $\widetilde{G}$ is finitely generated modulo $\overline{N}$. By 6.2.8, $|\overline{N}^\widetilde{G} : \overline{N}| < \infty$, hence $[H/N]$ and therefore also

(8) $|H : N|$ is finite.

We suppose, for a contradiction, that the lemma is false and choose a counterexample in which $|H : N|$ is as small as possible. For every normal subgroup $L$ of $G$
such that $N \leq L \leq H$, we have $(L^\circ)^G = H^\circ$ and the minimality of $|H : N|$ implies that $L = N$. Thus $N$ is the maximal normal subgroup of $G$ contained in $H$ and since $H$ is not normal in $G$,

$(9) \ N = H_G < H.$

If $N$ is not permutable in $G$, then by 6.2.18, $N$ is $P$-embedded in $G$. Thus $G/K$ is periodic, $G/K = \bar{S}/K \times \bar{U}/K$ with coprime groups $\bar{S}/K$ and $\bar{U}/K$ and $\bar{S}/K$ is a $P$-group whose nonnormal Sylow subgroup is $\bar{N} \cap \bar{S}/K$. By 1.6.4, $L(G/K) \simeq L(\bar{S}/K) \times L(\bar{U}/K)$ and $[G/\bar{N}] \simeq [\bar{S} \cup \bar{N}/\bar{N}] \times [\bar{U} \cup \bar{N}/\bar{N}]$. Now $\varphi$ induces an isomorphism from $L(G/N)$ onto this lattice and it follows from 1.6.5 that $G/N = S/N \times U/N$. In particular, $SN \leq G$; but $SN \leq H$ since $\bar{S} \leq \bar{N}G = \bar{H}$, and (9) implies that $SN = N$, a contradiction. Thus

$(10) \ N$ is permutable in $G.$

Since $N$ is not normal in $G$, there exists $y \in J(N)$ such that $N^y \neq N$; let $\bar{T} = \langle \bar{N}, y \rangle$ and $\bar{M} = \bar{N}^y$ as in 6.5.2 and let $x \in G$ such that $\langle x \rangle^\circ = \langle y \rangle$. Then $T = \langle N, x \rangle$ and $T/N$ is cyclic of order $p^n$ for some prime $p$ and $n \in \mathbb{N}$. By 6.2.6, $MN/N$ is permutable in $G/N$; furthermore, $\bar{N} \leq \bar{N} \cap \bar{N}^y \leq \bar{H}$ and (9) imply that $(MN)_G = N$. If $MN$ is not permutable in $G$, then by 6.2.18, $MN$ is $P$-embedded in $G$; hence $G/N$ is periodic and there exist coprime groups $S/N$ and $U/N$ such that $G/N = S/N \times U/N$ and $S/N$ is a $P$-group containing the $p$-group $MN/N$. Since $\bar{N}$ is subnormal but not normal in $\bar{T}$, we see that $[\bar{T}/\bar{N}]$ is a chain of length at least 2. Thus $T/N$ is cyclic of order at least $p^2$ and must be contained in the $P$-group $S/N$, a contradiction. We conclude that $MN/N$ is a cyclic permutable subgroup of $G/N$. By 5.2.11, every subgroup of $MN/N$ is permutable in $G/N$. In particular,

$(11) \ \Omega(T/N) = R/N$ is a permutable subgroup of order $p$ of $G/N$ contained in $H/N$.

By (9), $R$ is not normal in $G$ and (b) of 5.2.9 shows that we may choose $z \in G$ such that $R^z \neq R$ and $o(zN) = p^m$ for some $m \in \mathbb{N}$. Let $W = \langle N, x, z \rangle$, $\rho$ be the projectivity induced by $\varphi$ in $W$ and $H^\rho_0 = (N^\rho)^W$. By 5.2.9, $R^\rho/C = R/N \times (R^G/N \cap Z(G/N))$ and (9) implies that $H \cap R^G = R$. Since $x \in W$ and $R \leq MN$, we have $R \leq \bar{N}W = H^\rho_0 \leq \bar{H}$ and hence also $R = H_0 \cap R^G$. So if $H_0 \leq W$, then $R = H_0 \cap R^G \leq W$, contradicting $R^z \neq R$. Thus $H_0$ is not normal in $W$, that is, the lemma is false for the normal subgroup $N$ of $W$ and the projectivity $\rho$. Therefore we may assume without loss of generality that $G = W$, that is

$(12) \ G = \langle N, x, z \rangle.$

Now let $A/N$ be a cyclic $q$-subgroup of $G/N$ for some prime $q \neq p$. Let $A = \langle N, a \rangle$ and $\langle a \rangle^\circ = \langle b \rangle$; then $b \in J(N)$. Therefore if $\bar{N}^b \neq \bar{N}$, then, applying (11) to $\langle N, a \rangle = A$ in place of $\langle N, x \rangle = T$, we obtain that $\Omega(A/N) = R_1/N$ is a permutable subgroup of order $q$ of $G/N$ contained in $H/N$. By 5.2.9, $R_1/N$ is centralized by the $p$-elements $xN$ and $zN$, and thus $R_1 \leq G$, contradicting (9). Thus $\bar{N}^b = \bar{N}$ and hence

$(13) \ N^\circ \leq A^\circ.$
Write $C/N = C_{G/N}(R/N)$ and suppose next that $A/N$ is a cyclic $p$-subgroup of $G/N$ such that $A \not\subseteq C$. Then by (e) of 5.2.9, $\Omega(A/N) \leq Z(G/N)$ and (9) implies that $A \cap H = N$. Since $H^o \subseteq \bar{G}$, it follows that $N^o = A^o \cap H^o \subseteq A^o$ in this case also. Finally, let $B/N$ be any cyclic subgroup of $G/N$ such that $B \not\subseteq C$. Then by 5.2.9, $B/N$ is finite and its $p'$-part is contained in $C/N$. It follows that its $p'$-part is not contained in $C/N$ and therefore (13) holds for every Sylow subgroup $A/N$ of $B/N$; thus $N^o \subseteq B^o$. Now $C/N \neq G/N$ since $RZ \neq R$, and hence $G/N$ is generated by the cyclic subgroups $B/N$ not contained in $C/N$. It follows that $N^o \subseteq \bar{G}$ and $H = N \leq G$, a contradiction.

6.5.6 Theorem (Busetto [1982]). Let $N$ be a normal subgroup of the group $G$, $\varphi$ a projectivity from $G$ to a group $\bar{G}$, $H = N_{\bar{G}}$ and $K = N_{\bar{G}}$, that is $H^o$ the normal closure and $K^o$ the core of $N^o$ in $\bar{G}$. Then $H^o$ and $K^o$ are normal subgroups of $G$.

Proof. We first show that $H \leq G$. So take $g \in G$ and let $\mathcal{X}$ be the set of all subgroups $F$ of $G$ such that $\langle N, g \rangle \leq F$ and $F/N$ is finitely generated. For $F \in \mathcal{X}$, let $H(F)$ be the subgroup of $F$ such that $H(F)^o = NF$. By 6.5.5, $H(F) \leq F$; in particular, $H(F)^o = H(F)$. Since $NF \leq N_{\bar{G}}$, we have $H(F) \leq H$; on the other hand, to every $y \in \bar{G}$ there exists $x \in G$ such that $\langle x \rangle^o = \langle y \rangle$ and hence $\bar{N}^o \leq \bar{N}^\mathcal{F}$ for $F = \langle N, g, x \rangle \in \mathcal{X}$. Thus $H = \langle H(F) | F \in \mathcal{X} \rangle$. It follows that $H^o = H$ and since $g$ was arbitrary, $H \leq G$.

We have proved the assertion of the theorem about the normal closure for arbitrary normal subgroups and projectivities, of course. This result immediately implies the assertion for the core. For, if we apply it to the normal subgroup $K^o = N_{\bar{G}}$ of $\bar{G}$ and the projectivity $\varphi^{-1}$, it yields that $(K^G)^o \leq \bar{G}$. Since $K \leq N \leq G$, we obtain $K \leq K^G \leq N$, and hence $N_{\bar{G}} = K^o \leq (K^G)^o \leq N$. But $N_{\bar{G}}$ is the largest normal subgroup of $\bar{G}$ contained in $N$. It follows that $(K^G)^o = N_{\bar{G}} = K^o$ and hence $K = K^G \leq G$.

Subgroups of finite index

An immediate consequence of Busetto's theorem and the Zacher-Rips Theorem is the following result that was first proved by Rips in an unpublished manuscript.

6.5.7 Theorem (Rips). Let $H$ be a subgroup of finite index of the group $G$ and let $\varphi$ be a projectivity from $G$ to a group $\bar{G}$. Then there exists a normal subgroup $K$ of $G$ such that $K \leq H$, $K^o \leq \bar{G}$ and $G/K$ and $\bar{G}/K^o$ are finite groups.

Proof. Let $N = H_{\bar{G}}$ and $K \leq G$ such that $K^o = (N^o)_{\bar{G}}$. Then $K \leq H$, $K^o \leq \bar{G}$ and, by 6.5.6, $K \leq G$. Furthermore $|G : N| < \infty$ and therefore by 6.1.7 $|\bar{G} : N^o| < \infty$. It follows that $\bar{G}/K^o$ is finite and, as a projective image of this group, $G/K$ is finite, too.

Index preserving projectivities

We give an application of Rips's theorem to a problem on index preserving projectivities. It is easy to see that a projectivity $\varphi$ between finite groups is index preserving
if it preserves indices in the cyclic subgroups. For, if this is the case, \( \varphi \) has to map Sylow \( p \)-subgroups to \( p \)-groups of the same order and 4.2.1 yields the assertion. It was unknown for some time whether this was also true for infinite groups.

6.5.8 Theorem (Zacher [1980]). A projectivity is index preserving if and only if it induces in every cyclic subgroup an index preserving projectivity.

Proof. One implication is trivial. To prove the other, let \( \varphi \) be a projectivity from \( G \) to \( \overline{G} \) inducing in every cyclic subgroup an index preserving projectivity, and let \( K \leq H \leq G \). If \(|H : K|\) is infinite, then so is \(|H^\varphi : K^\varphi|\), by 6.1.7; so suppose that \(|H : K|\) is finite. Then by 6.5.7 there exists a normal subgroup \( N \) of \( H \) such that \( N \leq K \), \( N^\varphi \leq H^\varphi \) and \( H/N \) and \( H^\varphi/N^\varphi \) are finite. If \( A/N \) is a cyclic subgroup of \( H/N \) and \( B/N \leq A/N \), then there exists \( a \in H \) such that \( A/N = \langle aN \rangle = \langle a \rangle N/N \) and hence \( B/N = (B \cap \langle a \rangle)N/N \). It follows that \( A^\varphi/N^\varphi = \langle a \rangle^\varphi N^\varphi/N^\varphi \), \( B^\varphi/N^\varphi = \langle B \cap \langle a \rangle \rangle^\varphi N^\varphi/N^\varphi \) and hence

\[
|A^\varphi/N^\varphi : B^\varphi/N^\varphi| = |\langle a \rangle^\varphi : (B \cap \langle a \rangle)^\varphi| = |\langle a \rangle : B \cap \langle a \rangle| = |A/N : B/N|.
\]

Thus the projectivity induced by \( \varphi \) in \( H/N \) induces index preserving projectivities in the cyclic subgroups of \( H/N \) and hence is index preserving since \( H/N \) is finite. As \( N \leq K \leq H \), it follows that \(|H^\varphi : K^\varphi| = |H : K|\), as desired.

Not much is known about singular projectivities between infinite torsion groups. For example, any two Tarski groups have isomorphic subgroup lattices and therefore these groups possess singular projectivities. On the other hand, using Theorem 6.5.8, it is not difficult to generalize the main results of §4.2 to locally finite groups; we do this for Corollary 4.2.9.

6.5.9 Theorem. Every projectivity of a locally finite group \( G \) induces an index preserving projectivity in the second commutator subgroup \( G'' \).

Proof. By 6.5.8, we have to show that for every \( x \in G'' \), \(|\langle x \rangle^\varphi| = |\langle x \rangle|\). Now \( x \) is a product of commutators of elements of \( G \) which in turn are products of commutators of elements of \( G \). Hence there exists a finitely generated subgroup \( F \) of \( G \) such that \( x \in F'' \). Since \( G \) is locally finite, \( F \) is finite and, by 4.2.9, \( \varphi \) induces an index preserving projectivity in \( F'' \). It follows that \(|\langle x \rangle^\varphi| = |\langle x \rangle|\), as desired.

Some results on singular projectivities of groups with elements of infinite order can be found in Zacher [1982a]. We prove one of these which will be used in the next section. For this we need two simple lemmas.

6.5.10 Lemma. Let \( \varphi \) be a projectivity from the cyclic group \( X \) to the group \( Y \), let \( K \leq H \leq X \) such that \(|H : K| = p\) is a prime and suppose that \(|H^\varphi : K^\varphi| = q\). If \( U \leq V \leq X \) such that \(|V : U| = p^n (n \in \mathbb{N})\), then \(|V^\varphi : U^\varphi| = q^n\). (We say that \( \varphi \) maps \( p \)-indices in \( X \) to \( q \)-indices in \( Y \).)
Proof. There exists \( N \leq X \) such that \( |X : N| = p \); let \( |Y : N^p| = r \). If \( S \leq X \) such that \( |X : S| = p^m \) (\( m \in \mathbb{N} \)), then \( X/S \) is cyclic of order \( p^m \), and hence \( Y/S^p \) is cyclic of order \( s^m \) for some prime \( s \). Since \( S \leq N \), we have that \( r \) divides the order of \( Y/S^p \) and hence \( |Y : S^p| = r^m \). Now suppose that \( U \leq V \leq X \) such that \( |V : U| = p^k \) and let \( |X : V| = p^k t \) where \((p, t) = 1\), \( k \geq 0 \). Then if \( R \) is the subgroup of index \( p^k \) and \( T \) that of index \( p^{k+n} \) in \( X \), it follows that \( T \cap V = U \) and \( TV = R \). Therefore \( |V^p : U^p| = |V^p : T^p \cap V^p| = |R^p : T^p| = r^p \). If we apply this to \( V = H \) and \( U = K \), we get that \( r = q \), as desired.

6.5.11 Lemma. Let \( G = XP \) where \( X \) is infinite cyclic and \( |P| = p \). If \( \varphi \) is a projectivity from \( G \) to a group \( \overline{G} \), then \( |P^p| = p \) and \( \varphi \) maps \( p \)-indices in \( X \) to \( p \)-indices in \( X^p \).

Proof. \( G/XG \) is finite since \( |G : X| = p \). Thus \( XG \) is infinite cyclic; let \( N \) be the subgroup of index \( p^2 \) in \( XG \) and \( H = XG P \). We want to show that \( N^p \leq H^p \). If \( XG \) is centralized by \( P \), then \( H = XG \times P \) has exactly \( p \) infinite cyclic subgroups intersecting in the subgroup of index \( p \) in \( XG \). The image of this subgroup is centralized by the images of these infinite cyclic groups and hence by \( H^p \); in particular, \( N^p \leq Z(H^p) \). If \( XG \) is not centralized by \( P \), then \( p = 2 \), \( X = XG \) and \( G \) is an infinite dihedral group. In this case, \( X \) is the only infinite cyclic subgroup of \( G \) and hence \( X^p \leq G \). In both cases, \( N^p \leq H^p \) and \( \varphi \) induces a projectivity from \( H/N \) to \( H^p/N^p \). Since \( H/N \) is neither cyclic nor elementary abelian, 2.2.6 shows that \( H^p/N^p \) is a \( p \)-group. It follows that \( |P^p| = |P^pN^p/N^p| = p \) and, by 6.5.10, \( \varphi \) maps \( p \)-indices in \( X \) to \( p \)-indices in \( X^p \).

6.5.12 Theorem. Suppose that the group \( G \) has an abelian normal subgroup \( A \) containing elements of infinite order and let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \).

(a) Then \( |H^p| = |H| \) for every subgroup \( H \) of \( G \).

(b) If there exists a subgroup of order \( p \) in \( G \), \( p \) a prime, then \( |V^p : U^p| = p \) for all \( U \leq V \leq A \) such that \( |V : U| = p \) (that is, \( \varphi \) maps \( p \)-indices in \( A \) to \( p \)-indices in \( A^p \)).

Proof. If \( |H| \) is infinite, then so is \( |H^p| \); thus in the proof of (a), we may assume that \( |H| \) is finite. If (a) holds for all subgroups of prime order in \( G \), then \( \varphi \) induces index preserving projectivities in the Sylow subgroups of \( H \), and 4.2.1 shows that \( |H^p| = |H| \). Therefore to prove (a), we may assume that

(14) \( |H| = p \) is a prime.

This is also the assumption in (b) and we now prove both assertions simultaneously. More precisely, we show that \( |H^p| = p \), that is (a) holds, and that

(15) \( |V^p : U^p| = p \) if \( U \leq V \leq A \), \( |V : U| = p \) and \( V \) is infinite cyclic.

For this we clearly may assume that \( G = AH \). Let \( V \) be an infinite cyclic subgroup of \( A \) and write \( B = \langle V^p \rangle \) \( h \in H \). Then \( B \) is invariant under \( H \) and hence \( B \leq G \). As a finitely generated abelian group,

(16) \( B = B_1 \times \cdots \times B_r \) with cyclic groups \( B_r \) \( r \in \mathbb{N} \).
Since $B$ is infinite, at least one of the $B_i$ is also infinite, say $B_1$. If all the other $B_i$ are finite, then $|B : B_i|$ is finite, hence so is $|B : B_i|$ for all $h \in H$ and, since $|H| = p$, $|B : X|$ is finite where $X = \bigcap_{h \in H} B_i$. It follows that $X$ is an infinite cyclic group invariant under $H$ and 6.5.11, applied to $XH$, yields that $|H^\sigma| = p$ and that $\phi$ maps $p$-indices in $X$ to $p$-indices in $X^\sigma$. Since $|B : X|$ is finite, $X \cap V \neq 1$ and then 6.5.10 implies that $|V^\sigma : U^\sigma| = p$. Thus (15) holds in this case.

Now suppose that $B_i$ is infinite for some $i \geq 2$, let $N = \langle b^p \rangle | b \in B \rangle$ and $L = BH$. Then $N \leq L$ and $L/N$ is a finite $p$-group that is neither cyclic nor elementary abelian. By 2.6.10, $\phi$ is induced by an isomorphism on $B$. In particular, $|V^\sigma : U^\sigma| = p$, $N^\sigma \leq B^\sigma$ and $|N : K| = |N^\sigma : K^\sigma|$ for every subgroup $K$ of $N$. By (a) of 6.5.3, $N^\sigma \leq (NH)^\sigma$.

By (a) of 6.5.3, $N^\sigma \leq L^\sigma$ and $\phi$ induces a projectivity from $L/N$ to $L^\sigma/N^\sigma$. By 2.2.6, $L^\sigma/N^\sigma$ is a $p$-group and hence $|H^\sigma| = |H^\sigma N^\sigma/N^\sigma| = p$. This completes the proof of (a) and of (15).

We finally prove (b) for arbitrary $V \leq A$. Since $|V : U| = p$, we have $V = U \langle g \rangle$ for some $g \in A$ and $|\langle g \rangle : \langle g \rangle \cap U| = |V : U| = p$. Then $V^\sigma = U^\sigma \cup \langle g \rangle^\sigma$ and, by (a) or (15), $|\langle g \rangle^\sigma : \langle g \rangle^\sigma \cap U^\sigma| = p$. So if $U^\sigma \leq V^\sigma$, it follows that $|V^\sigma : U^\sigma| = |\langle g \rangle^\sigma : \langle g \rangle^\sigma \cap U^\sigma| = p$. If $U^\sigma$ is not normal in $V^\sigma$ and $K^\sigma = (U^\sigma)_\nu$, then 6.5.3(a) yields that $V/K$ and $V^\sigma/K^\sigma$ are in $P(2, s)$ where $s = |V^\sigma : U^\sigma|$. Since $V$ is abelian, $V/K$ is elementary abelian of order $s^2$ and it follows that $s = |V : U| = p$, as desired.

We mention without proof a much deeper result.

**6.5.13 Theorem** (Stonehewer and Zacher [1991b]). Let $\phi$ be a projectivity from $G$ to $\overline{G}$ and suppose that $M$ is a permodular subgroup of $G$ having an ascending series with factors locally finite or abelian. Let $h(M)$ be the sum of the torsion free ranks of the abelian factors of this series and assume that $h(M) \geq 3$ or $h(M) = 2$ and either $L(M)$ is modular or there exists $g \in G$ such that $o(g, M)$ is infinite. Then $\phi$ is index preserving.

**Ascendant subgroups and the Gruenberg radical**

We finally generalize 5.4.11 to infinite groups and apply the result to the image of the Gruenberg radical under a projectivity.

**6.5.14 Lemma.** Let $\phi$ be an index preserving projectivity from $G$ to $\overline{G}$.

(a) If $N \leq G$, then $N^\sigma$ is permutable in $\overline{G}$.

(b) If $N$ is ascendant in $G$, then $N^\sigma$ is ascendant in $\overline{G}$.

**Proof.** (a) We have to show that $N^\sigma \langle y \rangle = \langle y \rangle N^\sigma$ for all $y \in \overline{G}$. For this purpose let $x$ be an element of $G$ such that $\langle x \rangle^\sigma = \langle y \rangle$ and put $T = \langle N, x \rangle$. If $T/N$ is infinite, then even $N^\sigma \leq T^\sigma = \langle N^\sigma, y \rangle$, by 6.5.1. If $T/N$ is finite, then by 6.5.7 there exists a normal subgroup $K$ of $T$ such that $K \leq N$, $K^\sigma \leq T^\sigma$ and $T/K$ and $T^\sigma/K^\sigma$ are finite. Since $\phi$ induces an index preserving projectivity in $T/K$, 5.4.11 implies that $N^\sigma/K^\sigma$ is permutable in $T^\sigma/K^\sigma$ and hence $N^\sigma \langle y \rangle = N^\sigma K^\sigma \langle y \rangle = N^\sigma \langle y \rangle K^\sigma = \langle y \rangle K^\sigma N^\sigma = \langle y \rangle N^\sigma$. 


(b) Let \((N_x)_{x\leq \gamma}\) be an ascending series such that \(N_0 = N\) and \(N_\gamma = G\). Then (a) and 6.2.10 imply that \((N^\varphi_x)_{x\leq \gamma}\) is an ascending chain such that \(N^\varphi_0 = N^\varphi\), \(N^\varphi_x\) is ascendant in \(N^\varphi_{x+1}\) for all \(x < \gamma\) and \(N^\varphi_\gamma = \bar{G}\). By transfinite induction, we obtain that \(N^\varphi_x\) is ascendant in \(N^\varphi_x\) for all \(x \leq \gamma\). Thus \(N^\varphi\) is ascendant in \(\bar{G}\).

Recall that the Gruenberg radical of a group \(G\) is the join of all the cyclic ascendant subgroups of \(G\). Now if \(\varphi\) is an index preserving projectivity from \(G\) to \(\bar{G}\), then \(\varphi^{-1}\) is also index preserving and 6.5.14 shows that \(\varphi\) and \(\varphi^{-1}\) map cyclic ascendant subgroups to cyclic ascendant subgroups. It follows that the joins of all these subgroups in \(G\) and \(\bar{G}\) are mapped onto each other. Thus we have the following result.

6.5.15 Theorem (Zacher [1982a]). Every index preserving projectivity from \(G\) to \(\bar{G}\) maps the Gruenberg radical of \(G\) to the Gruenberg radical of \(\bar{G}\).

The locally finite radical

We finally give a lattice-theoretic characterization of the locally finite radical \(G^{L\bar{\Lambda}}\), the join of all locally finite normal subgroups, of a group \(G\). We also show that \(G^{L\bar{\Lambda}}\) is locally finite, a classical result in the theory of radicals (see Robinson [1972a], p. 35). We need the following simple lemma.

6.5.16 Lemma. Let \(H\) and \(K\) be locally finite subgroups of a group \(G\). If \(H\) is permodular in \(G\), then \(H \cup K\) is locally finite.

Proof. Let \(F\) be a finitely generated subgroup of \(H \cup K\). Since every generator of \(F\) is a product of finitely many elements of \(H\) and \(K\), there exist finitely generated subgroups \(A\) of \(H\) and \(B\) of \(K\) such that \(F \leq A \cup B\). Since \(H\) and \(K\) are locally finite, \(A\) and \(B\) are finite. By 6.2.6, \(M = H \cap (A \cup B)\) is permodular in \(A \cup B\). Clearly \(A \leq M \leq A \cup B\), so \(A \cup B = M \cup B\) and, since \(M\) is modular in \(A \cup B\), we see that \([A \cup B/M] \cong [B/B \cap M]\) is a finite lattice. By 6.2.5, \(|A \cup B : M|\) is finite. It follows that \(M\) is finitely generated (see Robinson [1982], p. 36); therefore, as a subgroup of \(H\), it is finite. Thus \(A \cup B\) is finite and hence so is \(F\).

6.5.17 Theorem (Stonehewer and Zacher [1994]). If \(G\) is a group, then \(G^{L\bar{\Lambda}}\) is locally finite and is the join of all locally finite permodular subgroups of \(G\). In particular, \((G^{L\bar{\Lambda}})^\varphi = \bar{G}^{L\bar{\Lambda}}\) for every projectivity \(\varphi\) from \(G\) to a group \(\bar{G}\).

Proof. Since every normal subgroup is permodular, \(G^{L\bar{\Lambda}}\) is contained in the join \(J\) of all locally finite permodular subgroups of \(G\). If \(F\) is a finitely generated subgroup of \(J\), then \(F\) is contained in a join \(K\) of finitely many locally finite permodular subgroups of \(G\). By 6.2.21 and 6.5.16, the join of any two of these is permodular and locally finite, and hence so is \(K\). Thus \(F\) is finite and \(J\) is locally finite. It follows that \(J \leq G^{L\bar{\Lambda}}\) and so \(G^{L\bar{\Lambda}} = J\) is locally finite. By 1.2.12 and 6.2.1, every projectivity maps locally finite permodular subgroups to locally finite permodular subgroups. It follows that \((G^{L\bar{\Lambda}})^\varphi = \bar{G}^{L\bar{\Lambda}}\) if \(\varphi\) is a projectivity from \(G\) to \(\bar{G}\).
Exercises

In Exercises 1, 3, 4, and 7 assume that \( \varphi \) is a projectivity from \( G \) to \( \overline{G} \).

1. (Zacher [1982a]) If \( N \leq G \) and \( G/N \) is a finite perfect group, show that \( N^\varphi \leq \overline{G} \).

2. (Busetto and Napolitani [1992]) Let \( G \) be the group constructed in Exercise 6.3.6, let \( \Omega(T) = \langle e_0 \rangle \) and \( N = \langle e_1 \rangle \times N_1 \) where \( \langle e_1 \rangle \) is cyclic of order \( p \). Let \( \sigma \) be the automorphism of \( \Omega(G) \) satisfying \( e_0^\sigma = e_0 \), \( e_1^\sigma = e_0 e_1 \) and \( x^\sigma = x \) for all \( x \in N_1 \). Show that there exists an autoprojectivity \( \varphi \) of \( G \) induced by \( \sigma \) on \( \Omega(G) \) and by the identity on \([G/\Omega(T)]\). Note that \( N^\varphi \) is not normal in \( G \) although \( G \) is perfect and there exists no normal subgroup \( L \) of \( G \) such that \( L < N \) and \( N/L \) is cyclic.

3. Show that \( \varphi \) is index preserving if and only if for all \( U \leq V \leq G \) such that \( U \) is a normal subgroup of prime index in \( V \), \( U^\varphi \trianglelefteq V^\varphi \) and \( |V^\varphi : U^\varphi| = |V : U| \).

4. If \( \varphi \) is index preserving and \( N \leq G \), show that \( N^\varphi \) is \( \omega \)-ascendant in \( \overline{G} \), that is, there exist subgroups \( H_i \) of \( \overline{G} \) \((i \in \mathbb{N}_0)\) such that \( H_0 = N^\varphi \), \( H_i \leq H_{i+1} \) for all \( i \) and \( \bigcup_{i \in \mathbb{N}} H_i = \overline{G} \). (Hint: Define \( H_1 = \langle g \in \overline{G} | \sigma(g, N^\varphi) \in \mathcal{P} \cup \{ \infty \} \rangle \) and \( H_{i+1} = \langle g \in \overline{G} | \sigma(g, H_i) \in \mathcal{P} \rangle \).)

5. Generalize Theorem 4.2.7 to locally finite groups.

6. Let \( B \) be a normal subgroup of prime index in the group \( A \) and let \( (C_i)_{i \in I} \) be a family of normal subgroups of \( A \) such that \( C_i \leq B \) and \( A/C_i \) is a \( P \)-group for all \( i \in I \). If \( \langle C_i | i \in I \rangle \) is a proper subgroup of \( B \), show that \( A/\bigcap_{i \in I} C_i \) is a \( P \)-group.

7. (Zacher [1980]) Let \( N \leq G \) such that \( G/N \in P(n, p) \), \( p \) a prime, \( 2 \leq n \leq \infty \) and let \( K = (N^\varphi)_{\overline{G}} \). Show that either \( N^\varphi \leq \overline{G} \) or \( |N : K| = p \) and \( G/K \in P(n+1, p) \).

8. (Zacher [1982a]) Let \( N \leq G \) such that \( G/N \) is elementary abelian of order \( p^n \), \( 2 \leq n \leq \infty \). Show that \( G/\bigcap_{\sigma \in \mathcal{P}(G)} N^\sigma \) is an elementary abelian \( p \)-group.

9. (Zacher [1980]) Let \( N \leq G \) such that \( |G/N| \) is a prime. Show that \( G/\bigcap_{\sigma \in \mathcal{P}(G)} N^\sigma \) is abelian or a \( P \)-group.

10. (Stonehewer and Zacher [1991b]) Let \( G \) be the semidirect product of a subgroup \( A \) of \( (\mathbb{Q}, +) \) containing \( \mathbb{Z} \) by an infinite cyclic group \( \langle g \rangle \), and suppose that the action of \( g \) on \( A \) is multiplication by \( m/n , (m, n) = 1 \). If \( p \) and \( q \) are primes dividing \( mn \), show that there exists an autoprojectivity \( \varphi \) of \( G \) and an element \( x \in A \) such that \( \varphi \) maps \( p \)-indices in \( \langle x \rangle \) to \( q \)-indices in \( \langle x \rangle^\varphi \).

6.6 The structure of \( N^G/N_G \) and \( \overline{N}^G/\overline{N}_G \) and projective images of soluble groups

We come now to the deeper results on the structure of \( N^G/N_G \) and \( \overline{N}^G/\overline{N}_G \) for a normal subgroup \( N \) of \( G \) and a projectivity from \( G \) to \( \overline{G} \). The main theorem will be that \( N^G/N_G \) and \( \overline{N}^G/\overline{N}_G \) are soluble of derived length 4 and 5, respectively. As for finite groups, we first prove that \( \overline{N} \) is permutable or \( P \)-embedded in \( \overline{G} \). This will reduce our problem, and also many others, to the case that \( \overline{N} \) is permutable in \( \overline{G} \). After further reductions we may assume that \( G \) and \( \overline{G} \) are \( p \)-groups and \( |N^G : N| \) is
finite so that we can apply the results of §§ 5.5 and 6.3. As an important application of our methods we get that projective images of soluble groups are soluble and obtain a bound for the derived length of the image group.

The structure of $N/N_0$ and $\bar{N}/\bar{N}_0$

We first study the structure of $N/N_0$ and $\bar{N}/\bar{N}_0$. Here we reap the reward of our efforts in § 5.5.

6.6.1 Theorem (Busetto and Napolitani [1991]). Let $N$ be a normal subgroup of the group $G$ and $\varphi$ a projectivity from $G$ to a group $\bar{G}$. Then $N/N_0$ and $\bar{N}/\bar{N}_0$ are subdirect products of finite primary groups with modular subgroup lattices; in particular, they are metabelian. Furthermore, $N/N_0$ is nilpotent of class at most 2 with commutator subgroup of exponent at most 2.

Proof. We shall prove all the assertions simultaneously. Since, by 6.5.6, $\varphi$ induces a projectivity from $G/N_0$ to $\bar{G}/\bar{N}_0$, we may assume that $\bar{N}_0 = 1$ and, of course, $N \neq 1$. Then by 6.5.2, $N_0$ is the intersection of the $\bar{N}_{\langle y \rangle}$ where $y \in J(\bar{N})$. If the statements of the theorem hold for all these $\langle \bar{N}, y \rangle$ in place of $G$, then they also hold for $G$; therefore we may finally assume that $G = \langle \bar{N}, y \rangle$ for some $y \in J(\bar{N})$, and hence that $G/N$ is cyclic of prime power order. By 6.5.3, $G$ and $\bar{G}$ then lie in $P(2, p)$ or are finite $p$-groups for some prime $p$. In the first case, $N$ and $\bar{N}$ are cyclic and, clearly, all the assertions of the theorem hold. In the second case, Hypothesis 5.5.1 is satisfied. By 5.5.2 and 5.5.8, $N$ and $\bar{N}$ are $p$-groups with modular subgroup lattices and $|N'| \leq 2$. In particular, $N$ and $\bar{N}$ are metabelian.

It is not known whether $\bar{N}/\bar{N}_0$ is nilpotent (of class at most 2). In Example 5.5.5 and Exercise 5.5.2, $\bar{N}_0 = 1$, $\bar{c}(\bar{N}) = 2$ and $\bar{N}'$ is cyclic of order 4 and $p$, respectively. It is another interesting open problem whether $N/N_0$ is an $M$-group and $|N'| \leq 2$ for arbitrary groups $G$.

Projective images of soluble groups

Another immediate consequence of the results in §§ 5.5 and 6.5 is the theorem on projective images of soluble groups which we are now going to present. More generally, we study projective images of normal subgroups with soluble factor group. Recall that for $n \in \mathbb{N}$, $G^{(n)}$ is the $n$-th term of the derived series of $G$ and $G^* = \langle g^n | g \in G \rangle$; thus $G^2$ is the smallest normal subgroup of $G$ whose factor group is an elementary abelian 2-group. The basic result is the following lemma.

6.6.2 Lemma. Let $N$ be a normal subgroup with abelian factor group of the group $G$. If $\varphi$ is a projectivity from $G$ to a group $\bar{G}$, then $(\bar{G}^*)^2$ and $(N^*G^2)^{-}$ are contained in $N^*$; in particular, $G^{(3)} \leq N^*$. 

Proof. We have to show that all the natural generators of \((G')^2\) and \((\overline{N}G')^2\) are contained in \(\overline{N}\). Since these generators are squares of products of iterated commutators, or iterated commutators of products of elements of \(\overline{N}\) with squares of elements of \(G\), we may assume that \(G\) is finitely generated modulo \(\overline{N}\). Then \(G/N\) is a finitely generated abelian group and hence a direct product of cyclic groups. It follows that \(N\) is the intersection of normal subgroups of \(G\) with cyclic factor groups of infinite or prime power order. Let \(M\) be one of these. If \(M \subseteq G\), then \(G/M\) is cyclic and hence \(G' = M\). If \(M\) is not normal in \(G\), then by 6.5.1, \(G/M\) is finite and 6.5.3 shows that \(G/MG\) and \(\overline{G}/\overline{MG}\) are either \(P\)-groups or finite \(P\)-groups for some prime \(p\). In the first case, \(\overline{G}' \leq \overline{M}\); in the second, Hypothesis 5.5.1 is satisfied for \(G/MG\) and \(M/MG\). By 5.5.9, \((G')^2\) and \((\overline{N}G')^2 \leq (\overline{M}G')^2\) are contained in \(\overline{M}\). In any case, \((G')^2\) and \((\overline{N}G')^2\) are contained in the intersection of all the \(\overline{M}\), that is, in \(\overline{N}\). Since \(G' < (G')^2 < N\).

6.6.3 Theorem (Busetto and Napolitani [1991]). Let \(N\) be a normal subgroup of the group \(G\) such that \(G/N\) is soluble of derived length \(n \in \mathbb{N}\). If \(\varphi\) is a projectivity from \(G\) to some group \(\overline{G}\), then \(\overline{G}^{(3n)} \leq N^\varphi\).

Proof. We use induction on \(n\), the case \(n = 1\) being settled by Lemma 6.6.2. If \(n \geq 2\), there exists a normal subgroup \(M\) of \(G\) such that \(N \leq M \leq G\), \(G/M\) is abelian and \(M/N\) is soluble of derived length \(n - 1\). By 6.6.2, \(\overline{G}^{(3)} \leq \overline{M}\) and, by induction, \(\overline{M}^{(3n-3)} \leq \overline{N}\); thus \(\overline{G}^{(3n)} \leq \overline{N}\), as desired.

6.6.4 Corollary. If \(G\) is a soluble group of derived length \(d(G) = n\) and \(\varphi\) is a projectivity from \(G\) to a group \(\overline{G}\), then \(\overline{G}\) is soluble of derived length \(d(\overline{G}) \leq 3n - 1\).

Proof. We apply Theorem 6.6.3 to \(N = G^{(n-1)}\) and get that \(\overline{G}^{(3n-3)} \leq \overline{N}\). As a projective image of an abelian group, \(\overline{N}\) is metabelian by 2.4.21. It follows that \(\overline{G}^{(3n-1)} = 1\).

The above corollary improves an older result due to Yakovlev [1970]. Using different methods, he had proved that \(d(\overline{G}) \leq 4n^3 + 14n^2 - 8n\) and thereby was the first to show that \(\overline{G}\) is soluble. Even the new bound may not be best possible. For, since projective images of abelian groups are metabelian, an obvious conjecture is that \(d(\overline{G}) \leq 2d(G)\). Furthermore, the only examples known for which \(d(\overline{G}) \neq d(G)\) are the projectivities between abelian and nonabelian groups, and Example 5.5.5 in which \(d(G) = 2\) and \(d(\overline{G}) = 3\). Therefore it is even possible that we have the same phenomenon as for the Fitting length of finite groups (see 4.3.3), namely, that only for small derived length can it happen that \(d(\overline{G}) \neq d(G)\), and \(d(\overline{G}) = d(G)\) for \(d(G) \geq 4\).

P-embedding

Our next aim is to show that \(\overline{N}\) is either permutable or P-embedded in \(\overline{G}\). For this we first of all have to show that \(\overline{N}/\overline{NG}\) is periodic if \(\overline{N}\) is not permutable in \(\overline{G}\). We
prove a slightly more general result. Note that if \( \overline{N} \) is permutable in \( \overline{G} \), \( \overline{N}/\overline{N}_G \) need not be periodic: in Example 6.2.9, \( \overline{N} = \langle z \rangle \) is infinite cyclic and core-free.

### 6.6.5 Lemma

Let \( N \leq G \) and let \( \varphi \) be a projectivity from \( G \) to \( \overline{G} \). If \( N \) is soluble and \( N^\varphi \) is not permutable in \( \overline{G} \), then \( N \) is periodic.

**Proof.** Assume, for a contradiction, that \( N \) is not periodic. Since \( N \) is soluble, there exists \( m \in \mathbb{N} \) such that \( N^{(m)} = 1 \). Now \( N/N^{(m)} \) is periodic and \( N/N^{(m)} \) is not; hence there exists \( i \in \mathbb{N} \) such that \( N/N^{(i-1)} \) is periodic and \( N/N^{(i)} \) is not. We put \( A = N^{(i-1)} \) and \( B = N^{(i)} = A' \). Then since \( N \leq G \),

1. \( B \leq A \leq N \), \( B \leq G \), \( A \leq G \), \( A/B \) is abelian, \( N/A \) is periodic and \( NB \) is not periodic.

Thus there exists an element of infinite order in \( N/B \) and, by 6.2.12,

2. \( B \) is permutable in \( \overline{G} \).

Since \( N/A \) is periodic, \( A/B \) contains an element of infinite order and, as an abelian group, is then generated by elements of infinite order. By 6.5.1,

3. \( \overline{B} \leq \overline{A} \).

Since \( \overline{N} \) is not permutable in \( \overline{G} \), there exists \( y \in \overline{G} \) such that \( o(y, \overline{N}) \) is a prime power and \( \overline{N} \langle y \rangle \neq \langle y \rangle \overline{N} \). We may assume that \( \overline{G} = \langle \overline{N}, y \rangle \); let \( \overline{K} = \overline{N}_G \). By 6.2.10, \( \overline{N} \) is not subnormal in \( \overline{G} \) and then 6.5.3 shows that there exist primes \( p, q, r \) such that \( G/K \) and \( \overline{G}/\overline{K} \) lie in \( P(2, p) \) and, more precisely,

4. \( |\overline{G} : \overline{N}| = p > q = |\overline{N} : \overline{K}|, |G : N| = r \leq p = |N : K| \).

Let \( S/K \) be one of the \( p + 1 \) minimal subgroups of \( G/K \), and write \( |S : K| = s \) and \( \overline{|S/\overline{K}|} = t \), so that \( s = p \) or \( s = r \) and \( t = p \) or \( t = q \). Then there exists \( g \in G \) such that \( S = K \langle g \rangle \), and it follows that \( |\langle g \rangle : \langle g \rangle \cap K| = |S : K| = s \) and \( |\langle g \rangle^\varphi : \langle g \rangle^\varphi \cap \overline{K}| = |S : \overline{K}| = t \). By 6.5.10,

5. \( \varphi \) maps \( s \)-indices in \( \langle g \rangle \) to \( t \)-indices in \( \langle g \rangle^\varphi \).

Now suppose that \( o(g, B) \) is finite. Then since \( B = N^{(i)} \leq N' \leq K \), we see that \( s = |\langle g \rangle : \langle g \rangle \cap K| \) divides \( |\langle g \rangle : \langle g \rangle \cap B| = o(g, B) \), and therefore \( \langle g \rangle/\langle g \rangle \cap B \) contains a subgroup \( X/\langle g \rangle \cap B \) of order \( s \). Then \( |BX/B| = |X : X \cap B| = s \) and hence \( B \leq \langle BX \rangle^\varphi \) since \( B \) is maximal and ascendant, by (2) and 6.2.10, in \( \langle BX \rangle^\varphi \). Since \( B \leq A \), \( \varphi \) induces a projectivity \( \rho \) from \( AX/B \) to \( (AX)^\varphi/B \) and \( A/B \) is a nonperiodic abelian normal subgroup of \( AX/B \). By 6.5.12, \(|(BX/B)^\rho| = s \) and \( \rho \) maps \( s \)-indices in \( A/B \) to \( s \)-indices in \( \overline{A}/\overline{B} \). On the other hand, \( X \leq \langle g \rangle \) and (5) imply that \(|(BX/B)^\rho| = |BX/B| = |X/B| \cap X| = |X : \langle g \rangle \cap B|^\rho| = t \) and hence \( s = t \). We have shown:

6. If \( o(g, B) \) is finite, then \( s = t \) and the projectivity \( \varphi \) induced by \( \varphi \) in \( A/B \) maps \( s \)-indices in \( A/B \) to \( s \)-indices in \( \overline{A}/\overline{B} \).

We now apply (5) and (6) to various subgroups of \( G/K \). For \( S = N \), (4) shows that \( s = p \) and \( t = q \neq p \). Therefore (6) implies that if \( N = K \langle u \rangle \), then \( o(u, B) \) is infinite and (5) yields that \( \varphi \) maps \( p \)-indices in \( \langle u \rangle \) to \( q \)-indices in \( \langle u \rangle^\varphi \). Since \( G/A \) is periodic
and \( o(u) \) is infinite, \( \langle u \rangle \cap A = \langle a \rangle \neq 1 \) and

\[
(7) \quad \langle aB \rangle \text{ is an infinite cyclic subgroup of } A/B \text{ in which } \psi \text{ maps } p\text{-indices to } q\text{-indices.}
\]

Now let \( S/K \) be such that \( |S/K| = p \) and let \( S = K \langle v \rangle \). If \( |S/K| = p \), then \( o(v, B) \) is infinite since otherwise (6) and (7) would contradict each other. Again \( \langle v \rangle \cap A = \langle b \rangle \neq 1 \) and \( \langle bB \rangle \) is an infinite cyclic subgroup of \( A/B \). By (5), \( \phi \) maps \( p\)-indices to \( q\)-indices.

Then (7) implies that \( \langle aB \rangle \cap \langle bB \rangle = 1 \) and, by 2.6.10, \( \psi \) is induced by an isomorphism. But this contradicts (7). Thus \( |S/K| \neq p \), in particular

\[
(8) \quad r < p.
\]

Finally, let \( T/K \) be a subgroup of order \( r \) of \( G/K \) that is different from \( S/K \) and let \( T = K \langle w \rangle \). Then \( |T/K| = q \) and by (5), \( \phi \) maps \( r\)-indices in \( \langle w \rangle \) to \( q\)-indices in \( \langle w \rangle^o \). If \( o(w, B) \) is finite, (6) implies that \( r = q \) and that \( \psi \) maps \( q\)-indices to \( q\)-indices. But then by (7), \( \psi \) maps \( p\)-indices and \( q\)-indices in \( \langle aB \rangle \) to \( q\)-indices, and this is impossible. Therefore \( o(w, B) \) is infinite, again \( \langle w \rangle \cap A = \langle c \rangle \neq 1 \) and \( \langle cB \rangle \) is an infinite cyclic subgroup of \( A/B \) in which \( \psi \) maps \( r\)-indices to \( q\)-indices. In \( \langle aB \rangle \), \( \psi \) maps \( p\)-indices to \( q\)-indices and since \( r \neq p \), it follows that \( \langle aB \rangle \cap \langle cB \rangle = 1 \). Again Baer’s theorem yields that \( \psi \) is induced by an isomorphism and this contradicts (7).

6.6.6 Theorem (Zacher [1982a], Napolitani and Zacher [1983]). Let \( N \) be a normal subgroup of the group \( G \), \( \varphi \) a projectivity from \( G \) to a group \( \overline{G} \), \( H = N^G \) and \( K = N_G \), that is, \( H^o \) is the normal closure and \( K^o \) the core of \( N^o \) in \( G \). Then \( H \) and \( K \) are normal subgroups of \( G \). If \( N^o \) is not permutable in \( \overline{G} \), then \( G/K \) is periodic and there are primes \( p_1, q_1 \) and \( n_1 \in \mathbb{N} \cup \{\infty\} \) such that

\[
G/K = (S_1/K \times S_2/K \times \cdots) \times T/K \text{ and } \overline{G}/K^o = (S_1^o/K^o \times S_2^o/K^o \times \cdots) \times T^o/K^o
\]

where the number of factors \( S_j/K \) may be finite (nonzero) or infinite and for all \( i \in \mathbb{N} \),

(a) \( S_i^o/K^o \) is a \( P \)-group of order \( p_i^n, q_i, \) \( p_i > q_i \) and all the direct factors \( S_j^o/K^o \) (\( j \in \mathbb{N} \)), \( T^o/K^o \) are coprime,

(b) \( S_i/K \in P(n_i + 1, p_i) \) and all the direct factors \( S_j/K \) (\( j \in \mathbb{N} \)), \( T/K \) are coprime,

(c) \( N/K = ((N \cap S_1)/K \times (N \cap S_2)/K \times \cdots) \times (N \cap T)/K, \) \( |(N \cap S_j)/K| = p_i,\)

(d) \( H/K = (S_1/K \times S_2/K \times \cdots) \times (H \cap T)/K \text{ and } (H \cap T)^o \text{ is the normal closure of } (N \cap T)^o \text{ in } T^o.\)

Proof. That \( H \) and \( K \) are normal subgroups of \( G \) has been shown in 6.5.6. In the remainder of the proof we may therefore assume that \( K = 1 \) and that \( \overline{N} \) is not permutable in \( \overline{G} \). Then by 6.6.1, \( N \) is soluble and hence periodic, by 6.6.5; by 6.2.17, \( \overline{N} \) is \( P \)-embedded in \( \overline{G} \). This means that \( \overline{G} \) is periodic and a direct product \( \overline{G} = (S_1 \times S_2 \times \cdots) \times \overline{T} \) of coprime groups \( S_i \) and \( \overline{T} \), where \( S_i \) is a \( P \)-group of order \( p_i^n, q_i, \)

\( p_i > q_i, n_i \in \mathbb{N} \cup \{\infty\} \), \( \overline{N} = ((\overline{N} \cap S_1) \times (\overline{N} \cap S_2) \times \cdots) \times (\overline{N} \cap \overline{T}), \) \( |\overline{N} \cap S_i| = q_i \text{ and } \overline{N} \cap \overline{T} \text{ is permutable in } \overline{G}. \)

By 1.6.6, \( G = (S_1 \times S_2 \times \cdots) \times T \) with coprime groups \( S_i \) and \( T \). By 2.2.5, \( S_j \in P(n_j + 1, p_j) \) and \( |N \cap S_j| = p_i \) for all \( i \) since \( N \leq G \). Thus (a)–(c) are satisfied and (d) follows from 2.2.2. \( \square \)
6.6 The structure of $N^G/G$ and $\bar{N}^G/\bar{G}$ and projective images of soluble groups

Like Theorem 5.4.7 for finite groups, the above result reduces questions about projective images $\bar{N}$ of normal subgroups to the case where $\bar{N}$ is permutable in $\bar{G}$. The difference from the situation for finite groups, however, is that there is no Maier-Schmid Theorem for permutable subgroups of infinite groups.

The structure of $N^G/G$ and $\bar{N}^G/\bar{G}$

We shall prove a number of deep structural restrictions for the groups $N^G/G$ and $\bar{N}^G/\bar{G}$. One reason for this is that $N^G/N$ is generated by finite cyclic permutable subgroups of the form $(\bar{N}^{(xy)^\phi})^x/N$ ($x \in G$) and is therefore hypercyclically embedded in $G$ (see Exercise 4). The main reason, however, is that the results of §§6.2 and 6.3 reduce most of these problems to the case that $N^G/N$ is a finite $p$-group. We make this more precise.

6.6.7 Remark. Let $N \leq G$, $\phi$ a projectivity from $G$ to $\bar{G}$, $H = N^G$, $K = N_{\bar{G}}$, and $S = N^H$ where $H = H^\phi$. If we want to prove that

(a) $S \leq G$, or
(b) $H/N$ is metabelian, or
(c) $H^\phi/K^\phi$ is soluble of derived length at most 5,

we may assume without loss of generality that

(9) $K = 1$,
(10) $N^\phi$ is permutable in $\bar{G}$,
(11) $|H : N|$ and $|H^\phi : N^\phi|$ are finite,
(12) $H$ and $H^\phi$ are $p$-groups of finite exponent for some prime $p$, and
(13) $H^\phi$ is nilpotent.

Proof: First of all, all three statements deal with the structure of $G/K$ or $\bar{G}/\bar{K}$ and, since $\phi$ induces a projectivity from $G/K$ to $\bar{G}/\bar{K}$, clearly we may assume that $K = 1$.

Suppose next that $N$ is not permutable in $\bar{G}$. Then $G = (S_1 \times S_2 \times \cdots) \rtimes T$ has all the properties given in Theorem 6.6.6. In particular,

$S = (S_1 \times S_2 \times \cdots) \times (N \cap T)^{\bar{H} \cap \bar{T}}$

and, if (a) holds for the normal subgroup $N \cap T$ of $T$ with permutable image $(N \cap T)^\phi$, then it also holds for $N$ in $G$. Similarly, since the $S_i$ and $S_i^\phi$ are metabelian, also (b) and (c) hold in general if they are true for $N \cap T$ in $T$. Thus we may assume that $N$ is permutable in $\bar{G}$.

We show next that in all three cases we may assume that

(14) $G/N$ is finitely generated.

In the proof of (a), we suppose, for a contradiction, that $S$ is not normal in $G$. Then there exists $g \in S$ such that $S^g \not\leq S$ and, since $\bar{S} = \langle \bar{N}^y | y \in \bar{H} \rangle$, there exists $y \in \bar{H}$
such that $((\overline{N^n})^{\varphi^{-1}})^n \not\subseteq S$. Since $\overline{H} = \langle \overline{N^n} | z \in \overline{G} \rangle$, there exist $z_1, \ldots, z_n \in \overline{G}$ such that $y \in \overline{N^{z_1}} \cdots \overline{N^{z_n}}$. So if $W = \langle N, g, (\overline{N^n})^{\varphi^{-1}} | i = 1, \ldots, r \rangle$ and $S_0 = \overline{N^nW}$, then $(\overline{N^n})^{\varphi^{-1}} \subseteq S_0$ and $((\overline{N^n})^{\varphi^{-1}})^n \not\subseteq S_0$ since $y \in \overline{N^nW}$ and $S_0 \subseteq S$. Thus $S_0$ is not normal in $W$ and we may assume that $G = W$ is finitely generated modulo $N$. In the proof of (b), we have to show that $H'' \leq N$, hence that for all $x_i \in H$, $[[x_1, x_2], [x_3, x_4]] \in N$. Since $\langle x_i \rangle^{\varphi} = \langle y_i \rangle$ with $y_i \in \overline{H} = \langle \overline{N^n} | z \in \overline{G} \rangle$, there exist $z_1, \ldots, z_n \in G$ such that $y_i \in \overline{N^{z_1}} \cdots \overline{N^{z_n}}$ for $i = 1, \ldots, 4$. So if $W = \langle N, \langle z_i \rangle^{\varphi^{-1}} | i = 1, \ldots, s \rangle$ and (b) holds for normal subgroups with finitely generated factor groups, then $[[x_1, x_2], [x_3, x_4]] \in (\overline{N^nW})^{\varphi} \leq N$ and thus $H'' \leq N$. For assertion (c), the situation is similar; we just have to consider longer commutators of elements in $\overline{H}$. Thus in all three cases we may assume that (14) holds and then, of course, again that $K = 1$ for this smaller group $G$.

It follows that $\overline{G}$ is finitely generated modulo $\overline{N}$. By 6.2.18 and 6.3.3, $|\overline{H} : \overline{N}| < \infty$ and $\overline{H}$ is nilpotent of finite exponent. Thus $\overline{H} = \overline{P_1} \times \cdots \times \overline{P_r}$ is a direct product of finitely many Sylow subgroups $\overline{P}_i$. By 1.6.6, $H = P_1 \times \cdots \times P_r$ with coprime groups $P_i$, and so $N = (N \cap P_1) \times \cdots \times (N \cap P_r)$ where the $N \cap P_i$ are characteristic subgroups of $N$ and hence normal subgroups of $G$. Now clearly $H = H_1 \times \cdots \times H_r$ and $S = S_1 \times \cdots \times S_r$ where $H_i = (N \cap P_i)^G$ and $S_i = (N \cap P_i)^H$. Thus if one of our statements holds for every $N \cap P_i$, it holds for $N$. Thus we may assume that $N$ is one of the $N \cap P_i$, that is, $\overline{H}$ is a nilpotent $p$-group of finite exponent for some prime $p$ and $|\overline{H} : \overline{N}| < \infty$. Then $[\overline{H} : \overline{N}]$ and hence $H/N$ is finite so that (11) and (13) hold. Furthermore $\overline{H}$ is locally finite and if $H$ is not a $p$-group, 2.2.7 shows that $\overline{H}$ is abelian; thus $S = N \leq G$, $H$ is metabelian and therefore (a)–(c) hold. Therefore we may assume that $H$ is a $p$-group; as a projective image of $\overline{H}$, it clearly has finite exponent.

6.6.8 Lemma. Let $N \leq G$, $\varphi$ a projectivity from $G$ to $\overline{G}$, $H = N^\varphi$ and $S = N^H$ where $\overline{H} = H^\varphi$. Then $S \leq G$ and $H/S$ is abelian.

**Proof.** By the above remark, we may assume in the proof of the first assertion that (9)–(13) are satisfied. Thus $N$ is a $p$-group of finite exponent $p^n$ and we use induction on $n$ to show that $S \leq G$. Let $M = \Omega(N)$. Then $M \leq G$ and hence $\overline{M}$ is modular in $\overline{G}$. Since $\overline{H}$ is nilpotent, $\overline{M}$ is ascendant in $\overline{G}$ (see Robinson [1982], p. 350) and so by 6.2.10, $\overline{M}$ is permutable in $\overline{G}$. By 6.3.8 applied to the core-free permutable $p$-subgroup $\overline{N}$ of $\overline{G}$, $\overline{M^G}$ is elementary abelian and either $\overline{N} \leq \overline{N^G} = \overline{H}$ or $\overline{M^G} \leq \overline{N^H} = S$. In the first case, $S = N \leq G$, as desired. So suppose that $\overline{M^G} \leq \overline{S}$ and let $L \leq G$ such that $L = M^G$. By 6.5.6, $L \leq G$ and $\varphi$ induces a projectivity $\psi$ from $G/L$ to $\overline{G/L}$. Since $L$ is elementary abelian, $NL/L$ is a normal $p$-subgroup of exponent $p^{n-1}$ of $G/L$ and $H/L$ is the normal closure of its image $\overline{NL/L}$ under $\psi$ in $\overline{G/L}$. Since $\overline{L} \leq \overline{S} \leq \overline{H}$, we have $\overline{(NL/L)^{H/L}} = \overline{S} \overline{L}$ and the induction assumption yields that $S/L \leq G/L$. Thus $S \leq G$, as desired.

To prove that $H/S$ is abelian, no reduction is necessary. We need only note that $\overline{S} \leq \overline{H} \leq \overline{G}$ and $\overline{S}$ is modular in $\overline{G}$ since $\overline{S} \leq \overline{G}$; thus by 6.2.10,

(15) $\overline{S}$ is permutable in $\overline{G}$. 


6.6 The structure of $N^G/N_G$ and $\overline{N^G/N_G}$ and projective images of soluble groups

Now let $x \in H$, $g \in G$ and write $\langle x \rangle^g = \langle x \rangle$, $\langle g \rangle^x = \langle g \rangle$ and $\langle xg \rangle^g = \langle \bar{z} \rangle$. By 6.3.5 applied to the permutable subgroup $\bar{S}$ of $W = \langle \bar{S}, x, \bar{g} \rangle = \langle \bar{S}, \bar{x}, \bar{z} \rangle$, we have $\bar{S}^w = S^{(x)}(\bar{S})^g = S^{(x)}(\bar{S})^z$. Since $\bar{S} \leq H$ and $\bar{x} \in \bar{H}$, it follows that $S^{(x)} = \bar{S}$ and hence

$$\bar{S}^w = \bar{S}^{(g)^{x^{-1}}}/S = (g)S/S \cap (xg)S/S \text{ is centralized by } gS \text{ and } xgS,$n

and hence by $xS$. Now $\bar{S}^w = H$ implies that $H/S$ is generated by these subgroups $(\bar{S}^{(g)^{x^{-1}}}/S$ and hence it follows that $xS \in Z(H/S)$. Since $x \in H$ was arbitrary, $H/S$ is abelian.

Remark 6.6.7 implies that in the proofs of the next two theorems we may also assume that (9)-(13) are satisfied. We want to describe the basic structure of $S/N$ in this situation. Clearly, $H = \langle NNx | x \in G \rangle$ and, since $N < NNx < N(x)$, there exists $y \in \langle x \rangle$ such that $NNx = R(y)$. By (11), $H : NNx < \infty$ and hence there are finitely many $y_i \in H$ such that

$$(16) \quad \bar{H} = \langle \bar{N}, y_1, \ldots, y_n \rangle \quad \text{and} \quad \bar{N} \langle y_i \rangle \text{ is permutable in } \bar{G}$$

since $\bar{N} \langle y_i \rangle$ is the product of two permutable subgroups. Then 6.3.5 implies that

$$(17) \quad \bar{S} = \langle \bar{N} \langle y_i \rangle | i = 1, \ldots, n \rangle.$$

Now $H/N$ and $\bar{H}/\bar{N}_G$ are finite $p$-groups and hence all subgroups between $N$ and $H$ and between $\bar{N}$ and $\bar{H}$ are subnormal in $G$ and $\bar{G}$, respectively. Since $\varphi$ and $\varphi^{-1}$ map modular subgroups to modular subgroups, it follows from 6.2.10 that for all $L \in [H/N]$, $L$ is permutable in $G$ (in $H$) if and only if $\bar{L}$ is permutable in $\bar{G}$ (in $\bar{H}$).

As a join of permutable subgroups, $\bar{N} \langle y_i \rangle$ is clearly permutable in $\bar{G}$ and since $\bar{N} \langle y_i \rangle \leq \bar{N} \langle y_i \rangle$,

$$\left( \bar{N}^{\langle y_i \rangle} \right)^{g^{-1}}/N \text{ is a cyclic permutable subgroup of } G/N (i = 1, \ldots, n).$$

Of course, (17) and (19) show that $S/N$ is generated by cyclic permutable subgroups. Since $\bar{N} \langle y_i \rangle$ is permutable in $\bar{G}$ and $[\langle \bar{N}, y_i, y_j \rangle/\bar{N}]$ is isomorphic to the subgroup lattice of the $p$-group $\langle \bar{N}, y_i, y_j \rangle^{g^{-1}}/N$, it is clear that $M = \bar{N}$ and $F = \{y_1, \ldots, y_n\}$ satisfy the assumptions of Lemma 6.3.10. It follows that every subgroup $T$ of $G$ such that $\bar{N} \leq T \leq \bar{N}^H = \bar{S}$ is permutable in $\bar{G}$ and, by (18), this yields that

$$(20) \quad \text{every subgroup of } S \text{ containing } N \text{ is permutable in } G.$$

In particular, $S/N$ is an $M$-group and we finally want to show that it is an $M^*$-group. So suppose, for a contradiction, that there is a quaternion group $Q_8$ involved in $S/N$. Then by 2.3.8, $S/N = S_1/N \times S_2/N$ where $S_i/N \simeq Q_8$ and $S_2/N$ is an elementary abelian 2-group. By (17) and (19), $S/N$ is generated by the cyclic subgroups $(\bar{N}^{\langle y_i \rangle})^g/N (i = 1, \ldots, n)$ and it follows that two of these, for $i = 1, 2$, say, have order 4 and generate a quaternion group. However, by (16) and (18), the $(\bar{N} \langle y_i \rangle)^{g^{-1}}/N$, $i = 1, 2$, are cyclic permutable subgroups of the 2-group $H/N$. By 5.2.14, they generate a metacyclic $M$-group containing this $Q_8$ and therefore equal to this $Q_8$. It
follows that $\overline{N}\langle y_1 \rangle = \overline{N} \langle y_1 \rangle$, a contradiction since all the conjugates of $\overline{N}$ in $\overline{N} \langle y_1 \rangle$ must lie in the maximal subgroup of $\overline{N} \langle y_1 \rangle$ containing $\overline{N}$. Thus

(21) $S/N$ is an $M^*$-group.

We can now prove the announced result on the structure of $H/N$.

6.6.9 Theorem (Busetto and Napolitani [1990]). If $N \trianglelefteq G$ and $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, then $N^\varphi/N$ is metabelian.

Proof. Again let $H = N^\overline{G}$ and $S = N^H$. By 6.6.7, we may assume that (9)–(13) hold, so that (16)–(21) are also satisfied; let $y_i (i = 1, \ldots, n)$ be as defined in (16). In particular, $H$ is a $p$-group and $H/N$ is finite. Therefore it is possible to use induction on $|H : L|$ to prove the following result:

(22) If $N \leq L \leq S$ and $L \leq H$, then $H/L$ is metabelian.

The theorem follows on setting $L = N$. To prove (22), we first handle the case that $S/L$ is metacyclic. Since $H/S$ is abelian, (22) clearly holds if $S/L$ is abelian. Thus we assume that

(23) $S/L$ is metacyclic but not cyclic.

By (17) and (19), $S/L$ is generated by the cyclic permutable subgroups $(\overline{N} \langle y_i \rangle)^{\varphi^{-1}} L/L (i = 1, \ldots, n)$ and, since $S/L$ is metacyclic, there exist $a, b \in H$ such that $\langle a \rangle^{\varphi} = \langle y_1 \rangle$, $\langle b \rangle^{\varphi} = \langle y_j \rangle$ and $S/L = ((\overline{N} \langle y_i \rangle)^{\varphi^{-1}} L/L)((\overline{N} \langle y_j \rangle)^{\varphi^{-1}} L/L)$. Since $(N \langle a \rangle)^{\varphi} = \overline{N} \langle y_1 \rangle$ per $G$, we obtain $N \langle a \rangle$ per $G$, and hence $\langle L, a \rangle/L$ is permutable in $H/L$; similarly for $\langle L, b \rangle/L$. Since $S \trianglelefteq G$, finally,

(24) $\langle L, a \rangle/L$ and $\langle L, b \rangle/L$ are permutable subgroups of $H/L$ and $\overline{L}^{\langle a \rangle^{\varphi}} \overline{L}^{\langle b \rangle^{\varphi}} = \overline{S}$.

We choose elements $a, b \in H$ satisfying (24) such that

(25) $\langle L, a, b \rangle/L$ has maximal order

and put $R = \langle L, a, b \rangle$. Then $R/L$ is the product of two cyclic permutable subgroups and hence, by 5.2.14, is a metacyclic $M$-group. If $R/L \simeq Q_8$, then $\langle L, a \rangle/L$ and $\langle L, b \rangle/L$ have order 4 and by (24), $S/L$ is contained in the subgroup of order 2 in this $Q_8$. But we assume that $S/L$ is not cyclic, a contradiction. Thus

(26) $R/L$ is a metacyclic $M^*$-group.

We denote the natural epimorphism from $H$ to $H/L$ by $v$ and want to show that for $z \in H$,

(27) $[S^v, z^v] = 1$ if $\langle z^v \rangle \cap R^v = 1$.

To see this, we study $\overline{L}^{\langle a, z \rangle^{\varphi}}$. Since $\overline{S} \leq \overline{H}$ and $\langle L, z \rangle \cap S \leq \langle L, z \rangle \cap R = L$, we see that $L^{\varphi} = \langle L, z \rangle^{\varphi} \cap S^{\varphi} \leq \langle L, z \rangle^{\varphi}$, and hence that $\overline{L}^{\langle z \rangle^{\varphi}} = \overline{L}$. By (18), $\overline{L}$ per $\overline{H}$ and 6.3.5 implies that

$$\overline{L}^{\langle a, z \rangle^{\varphi}} = \overline{L}^{\langle a \rangle^{\varphi}} \overline{L}^{\langle z \rangle^{\varphi}} = \overline{L}^{\langle az \rangle^{\varphi}} \overline{L}^{\langle z \rangle^{\varphi}} = \overline{L}^{\langle a \rangle^{\varphi}} = \overline{L}^{\langle az \rangle^{\varphi}}.$$
Thus \((\overline{L}^{(a)*}_{e_1}) = (\overline{L}^{(a)*}_{e_1})_{e_1} \leq L^{(a)} \cap L^{(a)}\) and this shows that \((\overline{L}^{(a)*}_{e_1})_{e_1} / L\) is centralized by \(aL\) and \(azL\) and hence by \(zL\). The same holds for \((\overline{L}^{(b)*}_{e})_{e} / L\) and, since \(S/L\) is generated by these two groups, it is centralized by \(zL\). This proves (27).

Since \(R^e\) is metacyclic, there exists a cyclic normal subgroup \(T^e\) of \(R^e\) with cyclic factor group \(R^e/T^e\) and we claim that

\[(28) T^e \cap S^e \subseteq H^e.\]

For this we show that every cyclic permutable subgroup \(<z^e>\) of \(H^e\) normalizes \(T^e \cap S^e\); since, by (16), \(H^e\) is generated by cyclic permutable subgroups, this will suffice to prove (28). Now for \(<z^e>\) there are three possibilities. If \(<z^e> \leq R^e\), it clearly normalizes \(T^e \cap S^e\) since \(T^e \cap S^e \leq R^e\). If \(<z^e> \cap R^e = 1\), then by (27), \(z^e\) centralizes \(S^e\) and hence also \(T^e \cap S^e\). Thus it remains to consider the case that

\[(29) 1 \neq <z^e> \cap R^e \neq <z^e>.\]

By 2.5.9, the \(M^*-\) group \(R^e\) is lattice-isomorphic to an abelian group in which the Frattini subgroup does not contain a maximal cyclic subgroup. It follows that there exists \(c^e \in R^e\) such that \(<z^e> \cap R^e \leq <c^e>\) and \(c^e \notin \Phi(R^e)\). If \(<a^e, c^e>\) and \(<b^e, c^e>\) were both proper subgroups of \(R^e\), then \(c^e\) would be contained in the maximal subgroup of \(R^e\) containing \(<a^e>\) and \(<b^e>\), respectively, and, since the intersection of these is \(\Phi(R^e)\), it would not follow that \(c^e \in \Phi(R^e)\). This is not the case and hence

\[(30) R^e = <a^e, c^e>,\]

say. From \(<z^e> \cap R^e \leq <c^e>\) we obtain that

\[(31) <c^e, z^e> \cap R^e = <c^e> <z^e> \cap R^e = <c^e> (<z^e> \cap R^e) = <c^e>.\]

Since \(H/S\) is abelian and \(S \leq R \leq H\), we have \(R \leq H\) and hence \(<c^e> \leq <c^e, z^e>\). Thus \(<c^e, z^e>\) is the product of two cyclic permutable subgroups and hence is a metacyclic \(M^*-\) group by 5.2.14. If this were a quaternion group, then \(o(c^e) = |<L, c> : L| = 4\) and hence \(L^o \leq <L, c>^o\), by (53) of § 5.5. Then by (24), 6.3.5 and (30),

\[
\overline{S} = \overline{L}^{(a)*}_{e_1} \overline{L}^{(b)*}_{e_1} = \overline{L}^{R} = \overline{L}^{(a)*} \overline{L}^{(c)*} = \overline{L}^{(a)*}.\]

Therefore \(S/L\) would be cyclic, contradicting our assumption (23). Thus

\[(32) <c^e, z^e>\] is a metacyclic \(M^*-\) group.

Suppose, for a contradiction, that \(o(z^e) > o(c^e)\). Then \(z^e\) has maximal order in the \(M^*-\) group \(<c^e, z^e>\) and by 2.3.11 there exists \(t^e \in <c^e, z^e>\) such that \(<c^e, z^e> = <t^e, z^e>\) and \(<t^e> \cap <z^e> = 1\). Since \(1 \neq <z^e> \cap R^e \leq <c^e>\), we have \(<c^e> \cap <z^e> \neq 1\) and hence \(<t^e> \cap <c^e> = 1\). By (31), \(<t^e> \cap R^e = <t^e> \cap <c^e, z^e> \cap R^e = <t^e> \cap <c^e> = 1\). It follows that \(<L, t> \cap S = L\), hence \(L^o = <L, t>^o \leq S^o \leq <L, t>^o\) and so \(\overline{L}^{(t)*} = \overline{L}\). Then \(<a^e, c^e, z^e> = <R^e, z^e> = <a^e, t^e, z^e>\) and \(\overline{S} \leq H\) together with 6.3.5 imply that

\[
\overline{S} = \overline{L}^{(R, z)*} = \overline{L}^{(a)*} \overline{L}^{(z)*} \overline{L}^{(t)*} = \overline{L}^{(a)*} \overline{L}^{(z)*}.\]
and thus \(a, z\) satisfy (24). Now \(\langle a^\ast \rangle \cap \langle z^\ast \rangle \leq \langle a^\ast \rangle \cap R^\ast \cap \langle z^\ast \rangle \leq \langle a^\ast \rangle \cap \langle c^\ast \rangle\) and \(\langle z^\ast \rangle \rangle \langle c^\ast \rangle\); thus \(\langle a^\ast, z^\ast \rangle = |R^\ast| = |\langle L, a, b \rangle / L|\), which contradicts the choice of \(a, b\). Thus

\[(33) \; o(z^\ast) \geq o(c^\ast) .\]

Now \(c^\ast\) has maximal order in the \(M^*\)-group \(\langle c^\ast, z^\ast \rangle\) and there exists \(t^\ast\) such that \(\langle c^\ast, z^\ast \rangle = \langle c^\ast, t^\ast \rangle\) and \(\langle c^\ast \rangle \cap \langle t^\ast \rangle = 1\). By (31), \(\langle t^\ast \rangle \cap R^\ast \leq \langle t^\ast \rangle \cap \langle c^\ast \rangle = 1\) and (27) shows that \(t^\ast\) centralizes \(S^\ast\). Since \(S^\ast \cap T^\ast\) is normalized by \(c^\ast \in R^\ast\), it follows that \(\langle c^\ast, t^\ast \rangle \leq N_{M}(S^\ast \cap T^\ast)\). In particular, \(z^\ast\) normalizes \(S^\ast \cap T^\ast\) and this proves (28).

By (28), \(S^\ast \cap T^\ast\) is a cyclic normal subgroup of \(H^\ast\). Since the automorphism group of a cyclic group is abelian, \(H^\ast/C_{H^\ast}(S^\ast \cap T^\ast)\) is abelian and hence \((H^\ast)^\prime\) centralizes \(S^\ast \cap T^\ast\). By 6.6.8, \(H/S\) is abelian and therefore \((H^\ast)^\prime \leq S^\ast\). So, finally, \(T^\ast \cap S^\ast \cap (H^\ast)^\prime = T^\ast \cap (H^\ast)^\prime\) is a central subgroup of \((H^\ast)^\prime\) with cyclic factor group \((H^\ast)^\prime / T^\ast \cap (H^\ast)^\prime \cong T^\ast \cap H^\ast / T^\ast\). It follows that \((H^\ast)^\prime\) is abelian and thus \(H^\ast\) is metabelian. This proves (28) in the case that \(S/L\) is metacyclic.

For the general case, we use induction on \(|H : L|\) and assume that \(S/L\) is not metacyclic. If \(S/L\) is abelian, then \(H/L\) is metabelian by 6.6.8. Thus we also assume that \(S/L\) is not abelian. Then (16), (20) and (21) show that \(H/L\) and \(S/L\) satisfy the hypotheses of Lemma 6.3.9. Since \(S/L\) is not metacyclic but an \(M^*\)-group, it is not generated by two elements and 6.3.9 yields that it contains two different minimal normal subgroups \(L_1/L\) and \(L_2/L\) of \(H/L\). By induction, \(H/L_i\) is metabelian for \(i = 1, 2\) and, since \(L_1 \cap L_2 = L\), it follows that \(H/L\) is metabelian. This completes the proof of (22) and of the theorem.

The main theorem

We come to our final result on the structure of \(N^G/N_G\) and \(\overline{N^G}/\overline{N}_G\). By 6.6.1 and 6.6.9, \(N/N_G\) and \(\overline{N^G}/N\) are metabelian so that \(N^G/N_G\) is soluble of derived length at most 4. Furthermore, since \(\overline{N^G}/N\) is metabelian, Theorem 6.6.3 yields that \((\overline{N^G})^{(6)} \leq \overline{N}\) and hence \(\overline{N^G}/\overline{N}_G\) is soluble of derived length at most 6. However this can be improved.

6.6.10 Theorem (Busetto and Napolitani [1990]). Let \(N\) be a normal subgroup of the group \(G\) and \(\varphi\) a projectivity from \(G\) to a group \(\overline{G}\). Then \(N^G/N_G\) and \(\overline{N^G}/\overline{N}_G\) are soluble of derived length at most 4 and 5, respectively.

Proof. Again let \(\overline{H} = \overline{N^G}\) and \(\overline{S} = \overline{N^H}\). We have to show that \(\overline{H}^{(4)}\) is contained in \(\overline{N}\); as a normal subgroup of \(\overline{G}\) it will then be contained in \(\overline{N}_G\), and \(\overline{N^G}/\overline{N}_G\) will be soluble of derived length at most 5. By 6.6.7, we may assume that (9)–(13), and hence also (16)–(21), are satisfied. By (11), (12) and 6.6.9, \(H/N\) is a finite metabelian \(p\)-group; let \(N \leq M \leq H\) such that \(H/M\) and \(M/N\) are abelian. Then if \(p > 2\), Lemma 6.6.2 shows that \(\overline{H}^{(4)} \leq \overline{M}\) and \(\overline{M}^{(4)} \leq \overline{N}\), so that \(\overline{H}^{(4)} \leq \overline{N}\).

Thus we can suppose that \(p = 2\). Since \(H/S\) is abelian, we may assume that \(M \leq S\). Let \(L/M = \Omega(S/M)\) and \(T/N = \Phi(M/N)\) so that \(L/M\) and \(M/T\) are elementary abe-
6.6 The structure of $N^G/N_\overline{G}$ and $\overline{N}^G/\overline{N}_\overline{G}$ and projective images of soluble groups

lian 2-groups. By 6.3.7, $\overline{H}/\overline{S}$ is nilpotent of class at most 2; in particular, $\overline{H}'' \leq \overline{S}$. Since $H/M$ is abelian, $(\overline{H}'')^2 \leq \overline{M}$ by 6.6.2. Therefore $[\overline{H}''/\overline{M}] \simeq [\overline{H}''/\overline{H}' \cap \overline{M}]$ is an interval in $[\overline{H}'/\overline{H}'')^2]$, and hence $(\overline{H}')^2/M$ is an elementary abelian subgroup of $S/M$. Thus $(\overline{H}')^2/M \leq \Omega(S/M) = L/M$ and $\overline{H}'' \leq \overline{L}$.

Now $M/N$ is abelian and therefore by 6.6.2, $(N\overline{M})^2 = \overline{T}'' \leq \overline{N}$. Finally, since $L/T$ is a 2-group of exponent at most 4, (53) of § 5.5 shows that $\overline{T} \leq \overline{L}$. By (21), $S/N$ is an $M^*$-group. Hence $L/T$ and its projective image $\overline{L}/\overline{T}$ are $M^*$-groups of exponent at most 4; by 2.3.7, $\overline{L}/\overline{T}$ is abelian. It follows that $\overline{H}(3) \leq \overline{N}$.

Theorem 6.6.10 is the culmination of the work of four mathematicians from Padua: Busetto, Menegazzo, Napolitani and Zacher. The first step, however, was taken by Yakovlev [1970], who proved that under Hypothesis 5.5.1, $d(\overline{G}) \leq 24d(N) - 20$. He used this to show that a projective image of an arbitrary soluble group $G$ is soluble and its derived length is at most $4n^3 + 14n^2 - 8n$ if $d(G) = n$. Then Menegazzo [1978] realized that, in fact, $N$ is abelian if Hypothesis 5.5.1 is satisfied and $p > 2$; he deduced that for an arbitrary finite group of odd order, $N/NG$ is abelian and therefore $\overline{N}/\overline{NG}$ is metabelian. The Zacher-Rips Theorem prepared the ground for an investigation of projective images of normal subgroups in infinite groups, and Zacher [1982a] showed that if it were possible to prove a similar, but perhaps somewhat weaker, result for $p = 2$—for example, that under Hypothesis 5.5.1, $d(N)$ is bounded by a constant $c$—then for arbitrary groups, $N/NG$ would be soluble of derived length at most $c$. This was carried out by Busetto [1984] with $c = 3$, and he proved that $N/NG$ and $\overline{N}/\overline{NG}$ are soluble of derived length at most 3 and 4, respectively. At the same time Busetto and Stonehewer [1985] produced Example 5.5.5 showing that $N/NG$ in general need not be abelian. Meanwhile, Napolitani and Zacher [1983] had shown that $N^G/N_\overline{G}$ and $\overline{N}^G/\overline{N}_\overline{G}$ are soluble and that $d(N^G/N) \leq 32$. Busetto and Menegazzo [1985] proved Theorem 6.6.3 with $6n$ instead of $3n$, and improved Busetto’s bound to $d(\overline{N}/\overline{NG}) \leq 3$; their result also yielded better bounds for the derived length of $N^G/N_\overline{G}$ and $\overline{N}^G/\overline{N}_\overline{G}$. Finally Busetto and Napolitani [1990], [1991] obtained the results of §§ 5.5 and 6.6 in the form presented here.

Elements of infinite order

We conclude this chapter with a remark that is perhaps somewhat surprising. Whereas for the proof of Theorem 6.6.10 we needed nearly all of our deep results of Chapters 5 and 6, the situation is much simpler if $G/N$ contains an element of infinite order. In fact, $N^G/N_\overline{G}$ and $\overline{N}^G/\overline{N}_\overline{G}$ are abelian in this case and the proof of this is quite elementary, using only 6.2.3, 6.2.11 and 6.3.5.

6.6.11 Theorem (Busetto and Napolitani [1990]). Let $N$ be a normal subgroup of the group $G$ and $\varphi$ a projectivity from $G$ to a group $\overline{G}$. If $G/N$ contains an element of infinite order, then $N^G/N_\overline{G}$ and $\overline{N}^G/\overline{N}_\overline{G}$ are abelian.

Proof. Write $H = N^G$, $K = N_\overline{G}$ and let $g \in G$ be such that $o(gN)$ is infinite; by 6.2.12, $N$ is permutable in $\overline{G}$. By 6.5.1, $N^{(g)^*} = N$ and therefore 6.3.5 implies that for
x \in G, \quad \overline{N}^\langle x \rangle^\sigma = \overline{N}^\langle x \rangle^\sigma \overline{N}^\langle g \rangle^\sigma = \overline{N}^\langle x \rangle^\sigma \overline{N}^\langle g \rangle^\sigma = \overline{N}^\langle x \rangle^\sigma = \overline{N}^\langle xg \rangle^\sigma.

It follows that \((\overline{N}^\langle x \rangle^\sigma)^{-1} \leq N^\langle x \rangle \cap N^\langle xg \rangle\) and \((\overline{N}^\langle x \rangle^\sigma)^{-1}/N\) is centralized by \(xN\) and \(xgN\) and hence also by \(gN\). Since \(H/N\) is generated by these \((\overline{N}^\langle x \rangle^\sigma)^{-1}/N\), \(x \in G\), the group \(H/N\) is centralized by \(gN\). It follows that the group \(\langle H, g \rangle/N = \langle H/N, gN \rangle\) is generated by elements of infinite order and that these elements centralize \(H/N\). Thus \(H/N \leq Z(\langle H, g \rangle/N)\) and, as a cyclic extension of a central subgroup, \(\langle H, g \rangle/N\) is abelian.

By 6.5.1, \(\overline{N} \leq \langle H, g \rangle^\sigma\) and \(\varphi\) induces a projectivity from \(\langle H, g \rangle/N\) to \(\langle H, g \rangle^\sigma/\overline{N}\). The first group is abelian and hence the second is an \(M\)-group with elements of infinite order. By 6.2.3, \(H/\overline{N}\) is generated by finite cyclic subgroups of the form \(\overline{N}^\langle y \rangle/\overline{N}, y \in G\); therefore it is contained in the torsion subgroup of \(\langle H, g \rangle^\sigma/\overline{N}\), and hence is abelian by 2.4.8. Thus \(\overline{H} \leq \overline{N}\) and since \(\overline{H} \leq \overline{G}, \overline{H} \leq \overline{N_G} = \overline{K}\), that is, \(\overline{H}/\overline{K}\) is abelian.

If \(z \in \overline{G}\), then \(\varphi = \varphi z \varphi^{-1}\) is an autoprojectivity of \(G\). Since \(\langle H, g \rangle/N\) is generated by elements of infinite order, \(N^\sigma \leq \langle H, g \rangle^\sigma\) and \(\varphi\) induces a projectivity from \(\langle H, g \rangle/N\) to \(\langle H, g \rangle^\sigma/N^\sigma\). Thus \(\langle H, g \rangle^\sigma/N^\sigma\) is an \(M\)-group with abelian torsion subgroup and therefore \(H^\sigma/N^\sigma\) is abelian. But \(H^\sigma = H\) since \(\overline{H} \leq \overline{G}\) and it follows that \(\overline{H}/\bigcap_{z \in \overline{G}} N^\varphi z \varphi^{-1} = H/K\) is abelian.

There exist examples in which \(G/N\) is not periodic and \(\overline{N}\) is not normal in \(\overline{G}\); see Exercise 6.

**Exercises**

In Exercises 1–5 let \(N \trianglelefteq G\), \(\varphi\) a projectivity from \(G\) to \(\overline{G}\), \(H = N\overline{G}\), \(K = N\overline{G}\) and \(S = N\overline{H}\). Exercises 3–6 are due to Busetto and Napolitani [1990].

1. If \(G/N\) is a torsion group without nontrivial 2-elements and \(G^{(m)} \leq N\), show that \(\overline{G}^{(2m)} \leq \overline{N}\).

2. If \(G\) is a finite group of odd order, show that \(H/K\) and \(\overline{H}/\overline{K}\) are soluble of derived length at most 3 and 4, respectively.

3. Let \(S_1 = S\) and \(S_{i+1} = N\overline{S}_i\) (\(i \in \mathbb{N}\)). Show that \(S_i \trianglelefteq G\) and \(S_i/S_{i+1} \leq Z(H/S_{i+1})\) for all \(i \in \mathbb{N}\).

4. Show that \(H/N\) is hypercyclically embedded in \(G\), and hypercentrally embedded in \(G\) if \(\overline{N}\) is permutable in \(\overline{G}\). (Hint: Use 6.4.10 and 5.2.12.)

5. For every \(n \in \mathbb{N}\), construct \(N, G, \varphi\) such that \(H/N\) is nilpotent of class \(n\). (Hint: By 2.5.9, \(G = \langle a, b, c | a^p = b^{p^{-1}} = c^{p-1} = [a, b] = 1, a^c = a^{1+p}, b^c = b^{1+p} \rangle\) has an autoprojectivity mapping \(\langle a \rangle\) to \(\langle c \rangle\).)

6. Let \(G = \langle a, b, c | a^2 = b^8 = [a, b] = [a, c] = 1, c^b = c^{-1} \rangle\) and \(\overline{G} = \langle \overline{a}, \overline{b}, \overline{c} \rangle\) with the same defining relations except that \([a, b] = 1\) is replaced by \([\overline{a}, \overline{b}] = \overline{b^4}\). Show that there exists a projectivity from \(G\) to \(\overline{G}\) mapping \(\langle a \rangle\) to \(\langle \overline{a} \rangle\); note that \(\langle a \rangle \trianglelefteq G\), \(G/\langle a \rangle\) contains elements of infinite order and \(\langle \overline{a} \rangle\) is not normal in \(\overline{G}\) (see Exercise 6.3.2).
Chapter 7

Classes of groups and their projectivities

In this final chapter on projectivities of groups we study certain interesting classes of groups and try to find out whether they are invariant under projectivities and, especially, which groups in these classes are determined by their subgroup lattices. Recall that a group $G$ is said to be determined by its subgroup lattice if it is isomorphic to every group $\bar{G}$ such that $L(\bar{G}) \simeq L(G)$; it is strongly determined by its subgroup lattice if every projectivity of $G$ is induced by a group-isomorphism. Groups with this property we have met are the noncyclic elementary abelian 2-groups (see 2.2.5 and 2.6.7), the hamiltonian 2-groups (see 2.5.1), and the abelian groups with two independent elements of infinite order (see 2.6.10). Not strongly determined but at least determined by their subgroup lattices are the following: the infinite cyclic groups (see 1.2.6), the additive group of rational numbers (see 2.6.14), the generalized quaternion groups, certain dihedral groups, and the alternating group $A_4$ (see § 1.4). We shall show that many other groups have these properties.

In 1941 Sadovskii proved that every free group $F$ of rank $r \geq 2$ is strongly determined by its subgroup lattice. We prove this, and, in fact, a more general result on 2-free groups, in § 7.1 using a lattice-theoretic description, due to Yakovlev [1974], of the subgroup lattice, the elements and the multiplication of $F$. This will, in addition, yield a characterization of those lattices which are isomorphic to the subgroup lattice of an arbitrary group, a result interesting in itself. We mention, but do not prove, generalizations of Sadovskii's theorem to free products and free products with amalgamation.

Another theorem of Sadovskii’s is that every nonabelian torsion-free nilpotent group is strongly determined by its subgroup lattice. We use an unpublished manuscript of G.E. Wall’s to prove this in § 7.2. In addition, we give a lattice-theoretic characterization, due to Kontorovič and Plotkin [1954], of the class of torsion-free nilpotent groups.

For mixed and periodic nilpotent groups the situation is not so good since there are obvious examples of nilpotent and nonnilpotent groups with isomorphic subgroup lattices and of projectivities between nonisomorphic nilpotent groups. However, in § 7.3 we give a lattice-theoretic characterization of the class of finitely generated nonperiodic nilpotent groups. There are also generalizations of Sadovskii's theorem to mixed nilpotent groups. The main result in this direction, which is due to Yakovlev [1988], is that a nilpotent group $G$ of class $n$ containing a free nilpotent group of class $n$ as a subgroup is strongly determined by its subgroup lattice. However, we shall not prove this but only note that the assumption cannot be weakened to the hypothesis that $G$ contains a torsion-free subgroup of class $n$ or contains two...
independent elements of infinite order; this last assumption does not even imply that $G$ is determined by its subgroup lattice. On the other hand, we shall prove a theorem due to Barnes and Wall [1964] stating that every normalizer preserving projectivity maps a nonabelian almost free group of a nilpotent variety to an isomorphic group. This will yield as a corollary that every nilpotent group of class 2 and exponent $p$ is determined by its subgroup lattice.

A nilpotent torsion group is the direct product of its primary components, and its subgroup lattice then is the direct product of the subgroup lattices of these components. Therefore in our study of subgroup lattices of periodic nilpotent groups in § 7.4, we restrict our attention to nilpotent $p$-groups. We first use the ideas of Kontorovič and Plotkin to characterize the nilpotent groups among the $p$-groups. This yields that every projectivity maps nonabelian nilpotent $p$-groups to nilpotent $p$-groups, a result due to Yakovlev [1965]. Furthermore we obtain a lattice-theoretic characterization of the class of nilpotent primary groups and $P$-groups. Finally, we study finite $p$-groups and prove that $p$-groups of maximal class are nearly always mapped to $p$-groups of maximal class under projectivities, a result due to Caranti [1979].

The lattice-theoretic characterizations of §§ 5.3 and 6.4 show that certain classes of soluble and generalized soluble groups are invariant under projectivities. In § 7.5 we prove in addition that the rank of a finite soluble group is preserved under projectivities, and present some further results of Schmidt [1974], [1987] on formations of finite soluble groups. Roughly speaking, we show that if $\mathfrak{F}$ is defined locally by classes $\mathfrak{F}(p)$ which are invariant under projectivities, then $\mathfrak{F}$ is also invariant under projectivities and $\mathfrak{F}$-residual and $\mathfrak{F}$-projectors are mapped onto $\mathfrak{F}$-residual and $\mathfrak{F}$-projectors, respectively, by every projectivity between finite soluble groups. At the other end of the spectrum of solubility, we prove that the class of radical groups is invariant under projectivities, a result due to Pekelis [1972b].

In the final three sections of this chapter we return to the question of whether the members of a given class of groups are determined or even strongly determined by their subgroup lattices. In § 7.6 we study direct products of groups and prove a generalization of Suzuki’s theorem that the direct product of two isomorphic copies of a finite nonabelian simple group is determined by its subgroup lattice; we show that this still holds for arbitrary perfect groups with trivial centre. We deal briefly with the more general question whether the direct product of $n$ isomorphic groups ($n > 2$) is (strongly) determined by its subgroup lattice. There are results in this direction for certain classes of groups due to Schmidt [1982] and Schenke [1987a], [1987b]. Similarly, we only sketch the results on projectivities of wreath products due to Menegazzo [1973] and to Arshinov and Sadovskii [1973]. Finally we show that a finite perfect group with trivial centre has the property that the direct product of all its pairwise nonisomorphic projective images is determined by its subgroup lattice.

In § 7.7 we present a fruitful general method to prove that a given group generated by involutions is determined by its subgroup lattice. This method is applied to permutation groups and we are able to show in this way that every triply transitive permutation group of degree at least 4 which is generated by involutions is determined by its subgroup lattice. The same holds for large classes of doubly transitive
and even certain primitive groups. All these results are due to Schmidt [1975b], [1977b], [1980a].

Finally, in §7.8 we note that the classification of finite simple groups yields that every finite nonabelian simple group is determined by its subgroup lattice. Unfortunately, a direct proof for this important result is not known; but the methods of §7.7 at least yield proofs for certain classes of finite simple groups. In contrast to this, it is not difficult to see that these groups in general are not strongly determined by their subgroup lattices. Here the alternating groups and also the 3-dimensional projective special linear groups yield examples; we study the groups of autoproperties of the alternating groups and also of the finite symmetric groups in some detail. We finish this chapter by determining the finite lattice-simple groups, that is, the finite groups \( G \) having no nontrivial proper \( P(G) \)-invariant subgroup. These are precisely the cyclic groups of square-free order, the \( P \)-groups, and the direct products of isomorphic nonabelian simple groups.

### 7.1 Free groups

We give necessary and sufficient conditions for a lattice \( L \) to be isomorphic to the subgroup lattice of a free group \( F \) of rank \( r \geq 2 \). For this purpose we describe the elements of \( F \) and their multiplication in the lattice. And since we are able to identify the normal subgroups of \( F \), we also get a characterization of those lattices which are isomorphic to the subgroup lattice of an arbitrary group. Another immediate consequence will be that \( F \) and, more generally, every 2-free group, is strongly determined by its subgroup lattice. First of all we need some definitions.

#### Cyclic elements and complexes

**7.1.1 Definition.** Let \( L = (L, \leq) = (L, \cap, \cup) \) be a complete lattice and \( O \) its least element. An element \( a \in L \) is called cyclic if \( [a/O] \) is a distributive lattice with maximal condition; the set of cyclic elements of \( L \) is denoted by \( C(L) \) or \( C \), for short. For \( a, b \in C \) and \( A, B \subseteq C \), we define \( a \circ b = \{ x \in C | x \cup a = x \cup b = a \cup b \} \) and \( A \circ B = \{ x \in C | x \in a \circ b, a \in A, b \in B \} \). We also write \( a \circ B \) for \( A \circ B \) if \( A = \{ a \} \) consists of only one element.

All the \( a \circ b \) and \( A \circ B \) are subsets of \( C \) and we clearly have

1. \( a \circ a = [a/O] \) and \( a \circ O = \{ a \} \);

Indeed, every \( b \in [a/O] \) is contained in \( C \) and satisfies \( b \cup a = a = a \cup a \). and the only element \( x \in L \) such that \( x \cup a = x \cup O = a \), is \( x = a \). By 1.2.5, the cyclic elements of the subgroup lattice \( L(G) \) of a group \( G \) are the cyclic subgroups of \( G \) and, if \( x, y \in G \),

2. \( \langle x^v y^\mu \rangle \in \langle x \rangle \circ \langle y \rangle \) for all \( v, \mu \in I = \{ +1, -1 \} \),
since \( \langle x'y'' \rangle \cup \langle x \rangle = \langle x'y'' \rangle \cup \langle y \rangle = \langle x \rangle \cup \langle y \rangle = \langle x, y \rangle \). It will be one of the fundamental properties of a free group \( F \) that for \( x, y \in F \) with \( x \neq 1 \neq y \) and \( \langle x \rangle \cap \langle y \rangle = 1 \), the set \( \langle x \rangle \circ \langle y \rangle \) precisely consists of the four elements \( \langle xy \rangle, \langle x'y^{-1} \rangle, \langle xy^{-1} \rangle \) and \( \langle x^{-1}y^{-1} \rangle \) (see 7.1.7). In general, however, \( \langle x \rangle \circ \langle y \rangle \) contains other cyclic subgroups; for example, if \( G = \langle x \rangle \times \langle y \rangle \) is the elementary abelian group of order \( p^2 \) for some prime \( p \), every subgroup of order \( p \) of \( G \) different from \( \langle x \rangle \) and \( \langle y \rangle \) lies in \( \langle x \rangle \circ \langle y \rangle \).

7.1.2 Definition. Let \( L \) and \( C = \mathcal{C}(L) \) be as in 7.1.1, let \( n \in \mathbb{N} \), \( e_i \in C \) (\( i = 1, \ldots, n \)) and put \( E = (e_1, \ldots, e_n) \). For \( O \neq a \in C \), the \( n \)-tuple \( \alpha = (A_1, \ldots, A_n) \) is called an \( a \)-complex with respect to \( E \) if for all \( i, j \in \{1, \ldots, n\} \) with \( i \neq j \),

\begin{enumerate}
\item \( A_i \) is a 2-element subset of \( e_i \circ a \) and
\item \( a_i \circ a_j \cap e_i \circ e_j \neq \emptyset \) for all \( a_i \in A_i, a_j \in A_j \).
\end{enumerate}

Let \( K(a, E) \) be the set of all \( a \)-complexes with respect to \( E \). We call \( \varepsilon = (\{e_1\}, \ldots, \{e_n\}) \) the \( O \)-complex with respect to \( E \) and put \( K(O, E) = \{\varepsilon\} \). Finally, a complex is an \( a \)-complex for some \( a \in C \) and \( \mathcal{K}(E) \) is the set of all complexes with respect to \( E \), where two such complexes \( \alpha = (A_1, \ldots, A_n) \) and \( \beta = (B_1, \ldots, B_n) \) are considered equal if and only if \( A_i = B_i \) for all \( i = 1, \ldots, n \).

If there is no ambiguity, we omit the phrase "with respect to \( E \)" and speak of complexes and \( a \)-complexes. Of course, \( K(a, E) \) may be empty for some \( a \in C \); for example, this will certainly be so if \( a \neq O \) and \( |e_i \circ a| \leq 1 \) for some \( i \). In subgroup lattices it is often possible to construct examples in the following way.

7.1.3 Example. Let \( G \) be a group and \( L = L(G) \) so that \( C \) is the set of cyclic subgroups of \( G \); take nontrivial elements \( g_i \) (\( i = 1, \ldots, n \)) of \( G \), define \( e_i = \langle g_i \rangle \) and put \( E = (e_1, \ldots, e_n) = (\langle g_1 \rangle, \ldots, \langle g_n \rangle) \).

(a) Let \( 1 \neq a \in G \). By (2), \( e_i \circ \langle a \rangle = \langle g_i \rangle \circ \langle a \rangle \) contains the (not necessarily distinct) elements \( \langle g_ia \rangle, \langle g_i^{-1}a \rangle, \langle gia^{-1} \rangle \), and \( \langle g_i^{-1}a^{-1} \rangle \) of \( C \). Therefore if \( \langle g_ia \rangle \neq \langle g_i^{-1}a \rangle \) for all \( i \in \{1, \ldots, n\} \), then \( A_i = \{\langle g_i, \langle g_i^{-1}a \rangle \} \) is a 2-element subset of \( e_i \circ \langle a \rangle \); and for \( v, \mu \in \{+1, -1\} \), both \( \langle g_i^va \rangle \circ \langle g_i^{-1}a \rangle \) and \( \langle g_i \rangle \circ \langle g_i^\mu \rangle \) contain the element \( \langle g_i^v g_j^{-\mu} \rangle \) of \( C \), again by (2). It follows that \( \langle g_i^va \rangle \circ \langle g_i^\mu a \rangle \cap \langle g_i \rangle \circ \langle g_i \rangle \neq \emptyset \) if \( i \neq j \), and hence \( \alpha = (A_1, \ldots, A_n) \) is an \( \langle a \rangle \)-complex with respect to \( E \).

(b) Suppose that \( G \) is torsion-free and \( g^{-1}ag \neq a^{-1} \) for all \( a, g \in G \) with \( a \neq 1 \). (Note that in a free group, \( g^{-1}ag = a^{-1} \) implies \( a = 1 \), see (18), so that the condition is satisfied.) Then for \( g \neq 1 \), the element \( g^{-1}a \) is different from the two generators \( ga \) and \( (ga)^{-1} \) of the group \( \langle ga \rangle \) and it follows that \( g^{-1}a \neq \langle ga \rangle \). Thus the assumption \( \langle g_ia \rangle \neq \langle g_i^{-1}a \rangle \) of (a) is satisfied, and \( \alpha = (A_1, \ldots, A_n) \) with \( A_i = \{\langle g_i, \langle g_i^{-1}a \rangle \} \) is an \( \langle a \rangle \)-complex with respect to \( E \). We denote it by \( \alpha(a, E) \) and put \( \alpha(1, E) = \varepsilon = (\{\langle g_1 \rangle\}, \ldots, \{\langle g_n \rangle\}) \).

Finally, we define a multiplication of complexes.

7.1.4 Definition. Let \( L, C, n, E, \mathcal{K}(E) \) be as in 7.1.2 and let \( \alpha = (A_1, \ldots, A_n) \) and \( \beta = (B_1, \ldots, B_n) \) be complexes in \( \mathcal{K}(E) \). We define the product \( \alpha \beta \) of \( \alpha \) and \( \beta \) to be the
set of all complexes \( \delta = (D_1, \ldots, D_n) \in \mathcal{K}(E) \) for which there exist \( a, b, d \in C \) such that

1. \( d \in a \circ b \),
2. \( x \in K(a, E), \beta \in K(b, E), \delta \in K(d, E) \), and
3. \( D_i \circ B_j \cap A_i \circ e_j \neq \emptyset \) for all \( i, j \in \{1, \ldots, n\} \).

For subsets \( A, B \) of \( \mathcal{K}(E) \), we define \( AB = \bigcup \{ x\beta | x \in A, \beta \in B \} \) and also write \( A\beta \) for \( AB \) if \( B = \{ \beta \} \) consists of only one element.

Clearly, \( AB \) and \( AB \) are (possibly empty) subsets of \( \mathcal{K}(E) \). We continue to study Example 7.1.3 and show the following.

**7.1.5 Lemma.** Let \( G \) be a torsion-free group and \( g^{-1}xg \neq x^{-1} \) for all \( x, g \in G \) with \( x \neq 1 \). If \( a, b, d \in G \) are such that \( ab = d \) and \( x = x(a, E), \beta = x(b, E), \delta = x(d, E) \) are the complexes constructed in 7.1.3, then \( \delta \in x{\beta} \).

**Proof.** Let \( x = (A_1, \ldots, A_n), \beta = (B_1, \ldots, B_n) \) and \( \delta = (D_1, \ldots, D_n) \). By 7.1.3, \( x \in K(\langle a \rangle, E), \beta \in K(\langle b \rangle, E), \delta \in K(\langle d \rangle, E) \) and by (2), \( \langle d \rangle = \langle ab \rangle \in \langle a \rangle \circ \langle b \rangle \). It remains to be shown that (7) holds. For \( a \neq 1 \), \( A_i = \{ \langle g_i a \rangle, \langle g_i^{-1}a \rangle \} \) and if \( a = 1 \), \( x = e \) so that \( A_i = \{ \langle g_i \rangle \} = \{ \langle g_i a \rangle \} \). In both cases, (2) implies that \( \langle g_i a g_j^{-1} \rangle = \langle g_i d b^{-1} g_j^{-1} \rangle \) is contained in \( \langle g_i a \rangle \circ \langle g_j \rangle \subseteq A_i \circ e_j \) and in \( \langle g_i d \rangle \circ \langle g_j b \rangle \subseteq D_i \circ B_j \). Thus \( D_i \circ B_j \cap A_i \circ e_j \neq \emptyset \) and (7) holds.

We can now give a sufficient condition for a lattice to be isomorphic to the subgroup lattice of a group.

**7.1.6 Theorem (Yakovlev [1974]).** Let \( L \) be a complete lattice in which every element is the join of cyclic elements, and suppose that there exists a system \( E = (e_1, \ldots, e_n) \) of elements \( e_i \in C = C(L) \) with the following properties.

1. For every \( a \in C \) such that \( a \neq 0, |K(a, E)| = 2 \).
2. If \( a \in C, x = (A_1, \ldots, A_n) \in K(a, E), x' = (A_1', \ldots, A_n') \in K(a, E) \) and \( x \neq x' \), then \( e_i \circ A'_i \cap A_i \circ e_j \neq \emptyset \) for all \( i, j \in \{1, \ldots, n\} \).
3. If \( a, b \in C, x \in K(a, E), \beta \in K(b, E) \) such that \( x = \beta \), then \( a = b \).
4. For all \( x, \beta \in \mathcal{K}(E) \), the product \( x\beta \) consists of a unique complex \( x \ast \beta \).
5. For all \( x, \beta, \gamma \in \mathcal{K}(E), (x\beta)\gamma = x(\beta \gamma) \).
6. Let \( a \in C \) and \( X \subseteq C \) such that \( a \leq \bigcup X \) and let \( x \in K(a, E) \). Then there exist finitely many elements \( b_i \in X \) and \( \beta_i \in K(b_i, E) \) such that \( x \in ((\ldots (\beta_1 \beta_2) \beta_3 \ldots) \beta_{m-1}) \beta_m \).

Then \( G = \mathcal{K}(E) \) with the operation \( \ast : G \times G \to G \) given by (11), \( (x, \beta) \mapsto x \ast \beta \) for \( x, \beta \in G \), is a group whose subgroup lattice is isomorphic to \( L \).
Proof. By (11) and (12), \( \ast \) is an associative binary operation on \( G \) and we show first that \((G, \ast)\) is a group with identity element \( e = (\{e_1\}, \ldots, \{e_n\}) \). For this let \( x \in G \), that is, \( x = (A_1, \ldots, A_n) \in K(a, E) \) for some \( a \in C \). We show that \( x \in xe \); it will follow from (11) that

\[ (14) \quad x \ast e = x. \]

If \( a = O \), then \( x = e \) and, since \( O \circ O = \{O\} \), (5) and (6) show that \( ee \) can only contain the \( O \)-complex \( e \); by (11), \( e \circ e = e \). So suppose that \( a \neq O \). Then by (1), \( a \in a \circ O \) so that (5) and (6) hold for \( \beta = e \) and \( \delta = x \). To prove (7), let \( i, j \in \{1, \ldots, n\} \). By (3), \( A_i \) is a 2-element subset of \( e_j \circ a \subseteq C \) and therefore contains an element \( e \neq O \) of \( C \). By (8) there exists a \( c \)-complex and hence \( e_j \circ c \neq \emptyset \). Since \( e_j \circ c = c \circ e_j \subseteq A_i \circ e_j \), it follows that \( A_i \circ e_j \neq \emptyset \) and that (7) holds. Thus \( x \in xe \) and this proves (14).

Again let \( a \neq O \) and \( x = (A_1, \ldots, A_n) \in K(a, E) \). By (8) there exists a unique further complex \( x' = (A'_1, \ldots, A'_n) \) in \( K(a, E) \). By (1) and (9), \( O \in a \circ a \) and \( e_i \circ A'_j \cap A_i \circ e_j \neq \emptyset \) so that (5)–(7) hold for \( \beta = x' \) and \( \delta = e \). Thus \( x \in xx' \) and (11) yields that

\[ (15) \quad x \ast x' = e. \]

This shows that \((G, \ast)\) is a group. By (10), for every \( x \in G \) there exists a unique \( a \in C \) such that \( x \in K(a, E) \) and by (8), the map \( i: G \rightarrow C \) defined by \( x' = a \) if \( x \in K(a, E) \) is surjective. Since \( L \) is a complete lattice, we may form arbitrary joins in \( L \) and hence there exists the map \( \varphi: L(G) \rightarrow L \) defined by \( H^\varphi = \bigcup_{x \in H} x' \) for \( H \in L(G) \). We show that \( \varphi \) is an isomorphism, which will prove the theorem. First, to see that \( \varphi \) is surjective, let \( x \in L \) and consider \( H = \{x \in G \mid x' \leq x\} \). For \( x, \beta \in H \) and \( \delta = x \ast \beta \), (5) and (6) show that \( \delta' \leq x' \cup \beta' \); then Definition 7.1.1 implies that \( \delta' \leq x' \cup \beta' \leq x \) and so \( \delta \in H \). By (15), \( (x^{-1})' = x' \leq x \) and hence \( x^{-1} \in H \). Thus \( H \) is a subgroup of \( G \). By assumption, \( x \) is the join of the cyclic elements contained in \( x \) and, since \( i \) is surjective, any such element is of the form \( x' \) where \( x \in H \). It follows that \( x = \bigcup_{x' \in H} x' = H^\varphi \). Thus \( \varphi \) is surjective.

Now suppose that \( A, B \leq G \) such that \( A^\varphi \leq B^\varphi \). If \( x \in A \), then \( x' \leq A^\varphi \leq B^\varphi = \bigcup \beta' \) and by (13) applied to \( a = x' \) and \( X = \{\beta' \mid \beta \in B\} \) there exist \( b_1, \ldots, b_m \in X \) and \( \beta_i \in K(b_i, E) \) such that \( x = \beta_1 \ast \cdots \ast \beta_m \). Since \( b_i \in X \), there exists \( \beta \in B \) such that \( \beta' = b_i \) and (15) implies that \( \beta_i = \beta \) or \( \beta_i = \beta^{-1} \). In any case, \( \beta_i \in B \) for all \( i \) and hence \( x \in B \). Thus \( A \leq B \). It follows that if \( A^\varphi = B^\varphi \), then \( A \leq B \) and \( B \leq A \) and therefore \( A = B \). This shows that \( \varphi \) is injective and hence bijective. Furthermore \( A^\varphi \leq B^\varphi \) implies \( A \leq B \), as we have just shown, and the reverse implication follows trivially from the definition of \( \varphi \). By 1.1.2, \( \varphi \) is an isomorphism.

Conversely we want to show that the subgroup lattice of a free group of rank at least 2 satisfies the assumptions of Theorem 7.1.6. We handle a slightly larger class of groups since our method works in the more general situation as well.

2-free groups

A group is called 2-free if it is nonabelian and any two of its elements generate a free group. If \( G \) is a free group of rank \( r \geq 2 \), the Nielsen-Schreier Theorem says that
every subgroup of $G$ is free; in particular, $G$ is 2-free. However, a 2-free group need not even be locally free; an example can be found in Baumslag [1962].

We note some simple properties of the subgroup $F = \langle a, b \rangle$ generated by two elements $a, b$ of a 2-free group. By definition, $F$ is free and has some rank $r \leq 2$, of course. If $r \leq 1$, $F$ is cyclic and, in particular, $ab = ba$. Since any two nontrivial subgroups of an infinite cyclic group intersect nontrivially, it follows that $r = 2$ if $a \neq 1 \neq b$ and $\langle a \rangle \cap \langle b \rangle = 1$. Now suppose that $r = 2$. Then $F$ is free on $\{a, b\}$ (see Robinson [1982], p. 160) and therefore every element in $F$ can be written uniquely in normal form with respect to the generators $a, b$. Therefore if $a^i b^j = b^j a^i$ for some $i, j \in \mathbb{Z}$, it follows that $i = 0$ or $j = 0$. In particular, $\langle a \rangle \cap \langle b \rangle = 1$. We have proved the following three assertions.

Let $G$ be a 2-free group and let $a, b \in G$.

(16) If $\langle a \rangle \cap \langle b \rangle \neq 1$, then $\langle a, b \rangle$ is cyclic and $ab = ba$.

(17) If $\langle a \rangle \cap \langle b \rangle = 1$ and $a \neq 1 \neq b$, then $F = \langle a, b \rangle$ is free on $\{a, b\}$.

(18) If there exist $i, j \in \mathbb{Z} \setminus \{0\}$ such that $a^i b^j = b^j a^i$, then $ab = ba$.

Furthermore, let $c \in G$ and suppose that $\langle a^c c \rangle \cap \langle b \rangle \neq 1 \neq \langle a^c c \rangle \cap \langle b \rangle$ for some $r, s \in \mathbb{Z}$ such that $r \neq s$. Then by (16), $C_G(b)$ contains $a^r c$ and $a^s c$ and hence also $a^r c (a^s c)^{-1} = a^{r-s}$. By (18), $ab = ba$ and, using (17), we get the following.

(19) Let $a \neq 1 \neq b$ and $\langle a \rangle \cap \langle b \rangle = 1$. If $c \in G$ and $r \in \mathbb{Z}$ such that $\langle a^r c \rangle \cap \langle b \rangle \neq 1$, then $\langle a^r c \rangle \cap \langle b \rangle = 1$ for every integer $s \neq r$.

Now we can prove the following simple, but basic fact.

7.1.7 Lemma. If $G$ is a 2-free group and $a, b \in G$ such that $a \neq 1 \neq b$ and $\langle a \rangle \cap \langle b \rangle = 1$, then

$$\langle a \rangle \circ \langle b \rangle = \{\langle ab \rangle, \langle a^{-1} b \rangle, \langle ab^{-1} \rangle, \langle a^{-1} b^{-1} \rangle\}$$

and these four groups are distinct.

Proof. By (17), $F = \langle a, b \rangle$ is free on $\{a, b\}$ and by (2), the four assigned groups lie in $\langle a \rangle \circ \langle b \rangle$. If $x \in \langle a \rangle \circ \langle b \rangle$, then $F = \langle a, b \rangle = \langle a, x \rangle = \langle b, x \rangle$ contains $x$ and therefore $x$ can be written in normal form with respect to $\{a, b\}$, that is, $x = a_{x_1} b_{x_2} \ldots a_{x_n} b_{x_n}$ where $n \geq 1, x_i, \beta_n \in \mathbb{Z}$ and $x_i, \beta_j \in \mathbb{Z} \setminus \{0\}$ for $i > 1$ and $j < n$. Since $F = \langle a, x \rangle$, there exist $x, x' \in \mathbb{Z}$ such that the normal form of $y = a^x x a^{x'}$ starts and ends with nontrivial powers of $b$. If we write $y = c w c^{-1}$ where $w \in F$ is cyclically reduced and $c \in F$ is reduced, then $y' = c w' c^{-1}$ is reduced for every $r \in \mathbb{Z} \setminus \{0\}$, and we see that the normal form of $y'$ starts and ends with nontrivial powers of $b$. It follows that an equation of the form $b = a^{r_1} y^{r_2} \ldots a^{r_m} y^{r_m}$ with $r_1, \delta_m \in \mathbb{Z}$ and $r_i, \delta_j \in \mathbb{Z} \setminus \{0\}$ for $i > 1$ and $j < m$ can only hold for $m = 1, r_1 = 0$ and $y^{r_1} = b$; on the other hand, $b \in F = \langle a, x \rangle = \langle a, a^x x a^{x'} \rangle = \langle a, y \rangle$ and hence $b$ satisfies an equation of this form. Thus $y = b^v$ and hence $x = a^{-2} b^v a^{-x}$ where $v \in I = \{+1, -1\}$ and $x, x' \in \mathbb{Z}$. In exactly the same way we see that $x = b^\beta a^\beta b^\beta$ where $\mu \in I$ and $\beta, \beta' \in \mathbb{Z}$. It follows that $x = a^\mu b^v$ or $x = b^v a^\beta$ where $\mu, v \in I$. These 8 elements are clearly distinct and generate the 4 assigned subgroups. □
We need a technical lemma.

7.1.8 Lemma. Let $G$ be a 2-free group, $k$, $l$, $r$, $s$, $t \in \mathbb{Z}$ and $a$, $b$, $c \in G$ such that $a \neq 1 \neq b$ and $\langle a \rangle \cap \langle b \rangle = 1$.

(a) If $k \neq 0 \neq l$ and $\langle a^k b^r \rangle \cap \langle a^l b^s \rangle \cap \langle a^t \rangle \neq \emptyset$, then $r = s$.

(b) If $\langle ab^t \rangle \cap \langle b^s \rangle \cap \langle a^t \rangle \neq \emptyset$, then $\langle b^s \rangle = \langle b^{r+t} \rangle$ or $\langle b^s \rangle = \langle b^{-r+t} \rangle$.

Proof. By (17), $F = \langle a, b \rangle$ is free on $\{a, b\}$.

(a) If $\langle a^k b^r \rangle \cap \langle a^l b^s \rangle \neq 1$, then (16) implies that $a^k b^r a^l b^s = a^l b^s a^k b^r$ and, since $k \neq 0 \neq l$, this equation can only hold if $r = s$. Suppose that $\langle a^k b^r \rangle \cap \langle a^l b^s \rangle = 1$. Then by 7.1.7, $\langle a^k b^r \rangle \cap \langle a^l b^s \rangle$ consists of the four groups $\langle a^k b^r a^l b^s \rangle$, $\langle b^{-r+a^{-1}} \rangle$ and $\langle b^{-r+a^{-1}} \rangle$. By assumption, one of these groups lies in $\langle a^k \rangle \cap \langle a^l \rangle$ and hence its generators are contained in $\langle a^k, a^l \rangle \leq \langle a \rangle$. In all cases, this implies that $r = s$.

(b) Let $X \in \langle ab^t \rangle \cap \langle b^s \rangle \cap \langle a^t \rangle \cap \langle b^s \rangle$. Since $F$ is free on $\{a, b\}$, $\langle a \rangle \cap \langle b^s \rangle = 1$ and $\langle ab^t \rangle \cap \langle b^s \rangle \neq 1$, then by (16), $b^s$ would centralize $ab^t$ and hence also $a$; therefore (18) would imply that $ab = ba$, a contradiction. Thus $\langle ab^t \rangle \cap \langle b^s \rangle = 1$.

If $r = 0 = s$, then by (1), $X = \langle ab^t \rangle = \langle a \rangle$ and hence $t = 0$ and $\langle b^s \rangle = \langle b^{r+t} \rangle$. Suppose next that $r \neq 0$ and $s \neq 0$. Then $X = \langle a \rangle$ and by 7.1.7 there exist signs $\mu, \nu \in I = \{+1, -1\}$ such that $\langle a \rangle = X = \langle (ab^t)^s(b^s)^s \rangle$. It follows that $\nu = 1$ and $t = -\mu s$ so that $\langle b^s \rangle = \langle b^t \rangle = \langle b^{r+t} \rangle$. Now suppose that $r \neq 0$ and $s = 0$. Then there exist $\mu, \nu \in I$ such that $\langle ab^t \rangle = X = \langle a^r b^s \rangle$. This implies $\nu = 1$ and $t = r \mu$, that is, $\langle b^s \rangle = \langle b^{r+t} \rangle = \langle b^{-r-t} \rangle$. Finally, if $r \neq 0 \neq s$, there exist signs $\nu, \mu, \lambda, \omega \in I$ such that $\langle (ab^t)^s(b^s)^s \rangle = \langle a^r b^{s+\omega} \rangle$. If $\nu = -1$, we get that $t = 0$ and $s = \mu r = r \omega$ so that $\langle b^s \rangle = \langle b^t \rangle = \langle b^{r+t} \rangle$; if $\nu = 1$, it follows that $t + \mu s = r \omega$ and hence $\langle b^s \rangle = \langle b^{-s+r} \rangle = \langle b^{-r+t} \rangle$. In all cases, $\langle b^s \rangle = \langle b^{r+t} \rangle$ or $\langle b^s \rangle = \langle b^{-r+t} \rangle$, as desired.

We are now going to describe the product of two elements of a 2-free group in the subgroup lattice.

7.1.9 Lemma. Let $G$ be a 2-free group and let $u, v \in G$ be such that $u \neq 1 \neq v$ and $\langle u \rangle \cap \langle v \rangle = 1$. Let $259 \leq m \in \mathbb{N}$ and for $i = 1, \ldots, m$, let $k_i, l_i \in \mathbb{Z} \setminus \{0\}$ be such that $u_i = u^{k_i}$ and $v_i = v^{l_i}$ satisfy

(20) $\langle u_i \rangle \neq \langle u_j \rangle$ and $\langle v_i \rangle \neq \langle v_j \rangle$ for all $i \neq j$.

If $a, b, c \in G$ are such that

(21) $\langle u \rangle \cap \langle a \rangle = \langle u \rangle \cap \langle b \rangle = \langle u \rangle \cap \langle c \rangle = \langle v \rangle \cap \langle b \rangle = 1$

and if for every pair $(i, j)$ with $i, j \in \{1, \ldots, m\}$ there exist signs $\mu, \nu, \omega \in I = \{+1, -1\}$ satisfying

(22) $\langle u_i \rangle a \cap \langle v_j \rangle b \cap \langle u_i \rangle a \cap \langle v_j \rangle \neq \emptyset$, then $c = ab$.

Proof. By (20), there can be at most one $i$ for which $u_i a = 1$ with $\lambda \in I$ is satisfied; for this equation implies $\langle u_i \rangle = \langle a \rangle$. The same holds for the equation $u_i c = 1$ and
for the relations $\langle u_i^\mu a \rangle \cap \langle v \rangle \neq 1$ and $\langle u_i^\mu c \rangle \cap \langle v \rangle \neq 1$; the latter follows from (19) applied to $u$ and $v$ in place of $a$ and $b$. Therefore we may assume without loss of generality that if one of these equations or relations holds for some $\lambda \in I$ and $i \in \{1, \ldots, m\}$, then $i \in \{1, \ldots, 4\}$; that is,

\[(23) \ u_i^\mu a \neq u_i^\mu c \text{ and } \langle u_i^\mu a \rangle \cap \langle v \rangle = 1 \neq \langle u_i^\mu c \rangle \cap \langle v \rangle \text{ for all } i \geq 5 \text{ and } \lambda \in I.\]

In the sequel, we shall always assume that $5 \leq i \leq m$. Then we may apply (19) with $v, u_i^\mu c$ instead of $a, b$, and deduce that there is at most one $l \in \mathbb{Z}$ such that $\langle v^l b \rangle \cap \langle u_i^\mu c \rangle \neq 1$. By (20), there is at most one $k = k_1(i) \in \{1, \ldots, m\}$ such that $v^l = v_k^\mu$ for some $\mu \in I$, that is, satisfying $\langle v_k^\mu b \rangle \cap \langle u_i^\mu c \rangle \neq 1$. Similarly, there is at most one $k = k_2(i) \in \{1, \ldots, m\}$ such that $\langle v_k^\mu b \rangle \cap \langle u_i^{-1} c \rangle \neq 1$ for some $\mu \in I$. Thus if $j$ is different from $k_1(i)$ and $k_2(i)$, then $\langle u_i^\mu c \rangle \cap \langle v_k^\mu b \rangle = 1$ and, by (23), also $\langle u_i^\mu a \rangle \cap \langle v_j \rangle = 1$ for all $\lambda, \mu, v \in I$. This, in particular, holds for the triple $(\lambda, \mu, v)$ that satisfies (22) for the pair $(i, j)$. By (23), furthermore, $u_i^\mu c \neq 1 \neq u_i^\mu a$ and, since $v \neq 1$ and $\langle v \rangle \cap \langle b \rangle = 1$, also $v_j \neq 1 \neq v_j^\mu b$. Therefore by 7.1.7,

$\langle u_i^\mu c \rangle \circ \langle v_j^\mu b \rangle = \{ \langle (u_i^\mu c)^\varphi (v_j^\mu b)^\varphi \rangle | \alpha, \beta \in I \}$

and

$\langle u_i^\mu a \rangle \circ \langle v_j \rangle = \{ \langle (u_i^\mu a)^\gamma v_j^\delta \rangle | \gamma, \delta \in I \},$

and (22) implies that there exist signs $\alpha, \beta, \gamma, \delta, \omega \in I$ such that

\[(24) \ (u_i^\mu c)^\varphi (v_j^\mu b)^\varphi = ((u_i^\mu a)^\gamma v_j^\delta)^\omega.\]

Thus if $i \in \{5, \ldots, m\}$ is fixed, then for every one of the at least 257 indices $j \in \{1, \ldots, m\} \setminus \{k_1(i), k_2(i)\}$ there exists an 8-tuple $(\lambda, \mu, v, x, \beta, \gamma, \delta, \omega)$ of signs such that (24) holds. Since there are only $2^8 = 256$ different such 8-tuples, there exist two different indices $j$ for which the 8-tuples in (24) coincide. That is, for the given $i$, there exist an 8-tuple $(\lambda, \mu, v, x, \beta, \gamma, \delta, \omega)$ of signs and two indices $j, k \in \{1, \ldots, m\}$ such that $j \neq k$,

\[(25) \ (u_i^\mu c)^\varphi (v_j^\mu b)^\varphi = ((u_i^\mu a)^\gamma v_j^\delta)^\omega \text{ and } (26) \ (u_i^\mu c)^\varphi (v_k^\mu b)^\varphi = ((u_i^\mu a)^\gamma v_k^\delta)^\omega.\]

We want to simplify these equations and first show that they can only hold if

\[(27) \ \omega = 1.\]

So suppose, for a contradiction, that $\omega = -1$ and consider first the case that $\beta = 1$. Then (25) yields $(u_i^\mu c)^\varphi v_j^\mu b = v_j^{-\delta}(u_i^\mu a)^{-\gamma}$ and hence $v_j^\delta(u_i^\mu c)^\varphi v_j^\mu = (u_i^\mu a)^{-\gamma} b^{-1}$. From (26) we get the same equation with $v_j$ replaced by $v_k$ and it follows that

$\nu_j^\delta(u_i^\mu c)^\varphi v_j^\mu = u_k^\delta(u_i^\mu c)^\varphi v_k^\mu$;

but this is impossible since by (23) and (17), $F = \langle u_i^\mu c, v \rangle$ is free on $\{u_i^\mu c, v\}$ and
$v_j^\delta \neq v_k^\delta$. Similarly for $\beta = -1$, we get the equation

$$v_j^{-\delta}(u_i^\gamma a)^{-\gamma}v_j^\mu = v_k^{-\delta}(u_i^\gamma a)^{-\gamma}v_k^\mu$$

and therefore the same contradiction. Thus (27) holds. Since $\omega = 1$, (25) implies

$$(28) (v_j^\mu b)^{\beta}v_j^{-\delta} = (u_i^\gamma c)^{-\gamma}(u_i^\gamma a)^\gamma$$

and (26) yields the same equation with $v_j$ replaced by $v_k$. It follows that

$$(29) (v_j^\mu b)^{\beta}v_j^{-\delta} = (v_k^\mu b)^{\beta}v_k^{-\delta}.$$ 

If $b \neq 1$, then by (21) and (17), $\langle b, v \rangle$ is free on $\{b, v\}$ and, since $\langle v_j \rangle$ and $\langle v_k \rangle$ are different subgroups of $\langle v \rangle$, we obtain $v_j^\rho \neq v_k^\rho$ for all $\rho \in \mathbb{Z} \setminus \{0\}$. It follows that (29) can only hold for $\beta = -1$ and $v_j^{-\mu-\delta} = v_k^{-\mu-\delta} = 1$; thus (28) implies

$$(30) b^{-1} = (u_i^\gamma c)^{-\gamma}(u_i^\gamma a)^\gamma.$$ 

If $b = 1$, (29) yields $v_j^{\mu-\delta} = v_k^{\mu-\delta}$ and it follows that $\mu \beta - \delta = 0$; therefore once again (28) implies (30).

Thus we have shown that for every $i \in \{5, \ldots, m\}$ there exists a quadruple $(\lambda, \nu, \alpha, \gamma)$ of signs such that (30) holds. Since there are only 16 such quadruples but $m \geq 259$, there exist two different indices $i, h \in \{5, \ldots, m\}$ for which these quadruples coincide; that is,

$$(31) (u_i^\lambda c)^{\mu}b^{-1} = (u_i^\nu a)^\gamma \quad \text{and} \quad (32) (u_h^\lambda c)^{\mu}b^{-1} = (u_h^\nu a)^\gamma.$$ 

We study the four possibilities for the signs $\alpha$ and $\gamma$. If $\alpha = \gamma = 1$, then (31) and (32) yield that $u_i^{\lambda-\nu} = abc^{-1} = u_h^{\lambda-\nu}$. It follows from (20) that $\lambda - \nu = 0$ and hence $ab = c$, as desired. In the other three cases, (31) and (32) yield equations of the form

$$(33) u_\rho^\rho xu_\rho^\eta = yz = u_\rho^\rho xu_\rho^\eta$$

where $\rho, \eta \in I$ and $x, y, z \in \{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$; indeed, in the case $\alpha = 1 = -\gamma$, we get $u_i^{\lambda-\alpha}a^{-1}u_i^{\gamma-\nu} = cb^{-1} = u_h^{\lambda-\alpha}a^{-1}u_h^{\gamma-\nu}$; if $\gamma = 1 = -\alpha$, we have $u_i^{\lambda-\gamma}c^{-1}u_i^{\nu-\gamma} = ab = u_h^{\lambda-\gamma}c^{-1}u_h^{\nu-\gamma}$; and for $\alpha = \gamma = -1$, finally, $u_i^{\lambda-\alpha}b^{-1}u_i^{\nu} = ca^{-1} = u_h^{\lambda-\alpha}b^{-1}u_h^{\nu}$. If $x \neq 1$ in (33), then by (21) and (17), $\langle u, x \rangle$ would be free on $\{u, x\}$; it would follow that $u_\rho^\rho = u_\rho^\rho$, contradicting (20). Thus $x = 1$ and hence $u_\rho^\rho x^n = u_\rho^\rho x^n$, which again is only possible if $\rho + \eta = 0$. So (33) implies that $yz = x = 1$ and this in all three cases yields the desired equation $c = ab$.

We can now prove, as stated above, that the subgroup lattice of a 2-free group satisfies the assumptions of Theorem 7.1.6. Of course, it is complete and any of its elements is the join of cyclic elements; so we have to find a system $E$ with the properties (8)–(13). For this we just have to take enough cyclic subgroups $\langle u \rangle, \langle v \rangle, \langle u_i \rangle, \langle v_i \rangle$ as in Lemma 7.1.9. But first of all we give such a system a name.

**7.1.10 Definition.** A basic system of a complete lattice $L$ is a family

$$E = \{e_{11}, \ldots, e_{1m}, e_{21}, \ldots, e_{2m}, \ldots, e_{n1}, \ldots, e_{nm}\}$$
of elements \( e_{ij} \in C(L) \setminus \{O\} \) satisfying

(34) \( e_{ij} \neq e_{kl} \) for all \( i, k \in \{1, \ldots, n\} \) and \( j, l \in \{1, \ldots, m\} \) such that \((i, j) \neq (k, l)\),

(35) there exist \( e_1, \ldots, e_n \in C(L) \) such that \( e_i \cap e_k = O \) for \( i \neq k \) and \( e_{ij} \leq e_i \) for all \( i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\} \), and

(36) \( n \geq 5, m \geq 259 \).

7.1.11 Theorem. Let \( G \) be a 2-free group.

(a) Then \( L(G) \) possesses basic systems.

(b) Every basic system \( E \) of \( L(G) \) satisfies (8)–(13). The map \( \sigma : G \to \mathcal{X}(E) \) mapping every \( a \in G \) to the complex \( \chi(a, E) \) defined in 7.1.3 is an isomorphism from \( G \) onto the group \( \langle \mathcal{X}(E), * \rangle \) defined in 7.1.6. Furthermore, \( K(\langle a \rangle, E) = \{ \chi(a, E), \chi(a^{-1}, E) \} = \{ a^\sigma, (a^{-1})^\sigma \} \) for \( 1 \neq a \in G \).

Proof. (a) Let \( n, m \in \mathbb{N} \) such that \( n \geq 5 \) and \( m \geq 259 \). Since \( G \) is not abelian, there exist \( x, y \in G \) such that \( xy \neq yx \) and then \( F = \langle x, y \rangle \) is a free group of rank 2. It is well-known (see Robinson [1982], p. 157) that such a group contains a free subgroup \( H \) of infinite rank. So if \( H = \langle X \rangle \) is free on \( X \), we may choose \( n \) distinct elements \( g_1, \ldots, g_n \in X \), and then clearly \( \langle g_i \rangle \cap \langle g_k \rangle = 1 \) for \( i \neq k \). Every \( \langle g_i \rangle \) contains \( m \) distinct subgroups \( \langle g_{i1} \rangle \) and the system of these \( \langle g_{i1} \rangle \) is a basic system of \( L(G) \).

(b) Now let \( E = (\langle g_{11} \rangle, \ldots, \langle g_{1m} \rangle, \ldots, \langle g_{n1} \rangle, \ldots, \langle g_{nm} \rangle) \) be a basic system of \( L(G) \) and let \( g_i \in G \) such that

(37) \( \langle g_{ij} \rangle \leq \langle g_i \rangle \) and \( \langle g_{ij} \rangle \cap \langle g_{jk} \rangle = 1 \) for all \( j \in \{1, \ldots, m\} \) and \( i, k \in \{1, \ldots, n\}, i \neq k \);

let \( C \) be the set of cyclic elements of \( L(G) \). We have to prove that \( E \) satisfies (8)–(13) and we show first that (8) holds, that is, \( |K(\langle a \rangle, E)| = 2 \) for every \( 1 \neq \langle a \rangle \in C \). Since \( G \) is torsion-free and, by (18), \( g^{-1}ag \neq a^{-1} \) for all \( g \in G \), 7.1.3 shows that \( K(\langle a \rangle, E) \) contains the two complexes

(38) \( \chi = \chi(a, E) = (A_{11}, \ldots, A_{nn}) \) and \( \chi' = \chi(a^{-1}, E) = (A'_{11}, \ldots, A'_{nn}) \)

where \( A_{ij} = \{ \langle g_{ij}a \rangle, \langle g_{ij}^{-1}a \rangle \} \) and \( A'_{ij} = \{ \langle g_{ij}a^{-1} \rangle, \langle g_{ij}^{-1}a^{-1} \rangle \} \). These are different. Indeed, by (37) there exists \( i \in \{1, \ldots, n\} \) such that \( \langle a \rangle \cap \langle g_i \rangle = 1 \) and, by (17), \( \langle a, g_i \rangle \) is free on \( \{a, g_i\} \) so that \( \langle g_{i1}a \rangle \neq \langle g_{i1}^{-1}a^{-1} \rangle \) for both \( \lambda \in I = \{ \pm 1, -1 \} \); thus \( A_{i1} \neq A'_{i1} \) and hence \( \chi \neq \chi' \). To prove (8), we therefore have to show that there are no further \( \langle a \rangle \)-complexes with respect to \( E \).

So suppose that \( \gamma = (C_{11}, \ldots, C_{nm}) \in K(\langle a \rangle, E) \). By (37) there exists \( i \in \{1, \ldots, n\} \) such that \( \langle g_{ij} \rangle \cap \langle a \rangle = 1 \); let \( j, l \in \{1, \ldots, m\} \) such that \( j \neq l \). By (3) and 7.1.7, \( C_{ij} \) is a 2-element subset of \( \langle g_{ij} \rangle \circ \langle a \rangle = \{ \langle g_{ij}a^\mu \rangle | \lambda, \mu \in I \} \). For \( \langle g_{ij}a^\mu \rangle \in C_{ij} \) and \( \langle g_{ij}^{-1}a^\mu \rangle \in C_{ij} \), (4) yields that \( \langle g_{ij}a^\mu \rangle \circ \langle g_{ij}^{-1}a^\mu \rangle \neq \emptyset \) and (a) of 7.1.8 implies that \( \mu = \omega \). This shows that there exists \( \mu = \mu(i) \in I \) such that \( C_{ij} = \{ \langle g_{ij}^\mu a^\mu \rangle, \langle g_{ij}^{-1}a^\mu \rangle \} \) for every \( j \in \{1, \ldots, m\} \). We now fix an \( i \in \{1, \ldots, n\} \) such that \( \langle g_i \rangle \cap \langle a \rangle = 1 \), put \( \mu = \mu(i) \) and show that for all \( k \in \{1, \ldots, n\} \) and \( l \in \{1, \ldots, m\} \),

(39) \( C_{kl} = \{ \langle g_{kl}a^\mu \rangle, \langle g_{kl}^{-1}a^\mu \rangle \} \).
This is clear if \( k = i \). So let \( k \neq i \) and suppose first that \( \langle g_k \rangle \cap \langle a \rangle = 1 \). Then \( \mu(k) \) exists and (4) implies that \( \langle g_{ij}a_{u(i)} \rangle \circ \langle g_{kl}a_{u(k)} \rangle \cap \langle g_{ij} \rangle = \emptyset \) for all \( j, l \in \{1, \ldots, m\} \). It follows from 7.1.9 with \( u = g_i, v = g_k \) and \( a, b, c \) replaced by \( 1, a_{u(k)}, a_{u(i)} \), that \( \mu(k) = \mu(i) = \mu \) and hence (39) holds for \( k \). Now suppose that \( \langle g_k \rangle \cap \langle a \rangle \neq 1 \). By (16), \( \langle g_k, a \rangle = \langle h \rangle \) is cyclic. Let \( \langle c \rangle \in C_{kl} \). Then \( \langle c \rangle \in \langle g_{kl} \rangle \circ \langle a \rangle \) and hence \( \langle c \rangle \leq \langle g_k, a \rangle \leq \langle g_k, a \rangle = \langle h \rangle \). Thus there exist \( r, s, t \in \mathbb{Z} \) such that \( g_k = h^r, c = h^s \) and \( a^u = h^t \). By (4), again

\[
\langle g_{ij}a^u \rangle \cap \langle c \rangle \cap \langle g_{ii} \rangle \circ \langle g_{kl} \rangle = \langle g_{ij}h^r \rangle \cap \langle h^s \rangle \cap \langle g_{ii} \rangle \circ \langle h^t \rangle \neq \emptyset
\]

and \( \langle g_{ij} \rangle \cap \langle h \rangle = 1 \) since \( \langle g_i \rangle \cap \langle g_k \rangle = 1 \). Therefore the assumptions of 7.1.8(b) are satisfied with \( a, b \) replaced by \( g_{ii}, h \) and hence \( h^s = \langle h^{s+t} \rangle \) or \( h^s = \langle h^{-s+t} \rangle \), that is, \( \langle c \rangle = \langle g_{kl}a^u \rangle \) or \( \langle c \rangle = \langle g_{kl}^{-1}a^u \rangle \). Since \( |C_{kl}| = 2 \), it follows that \( C_{kl} \) consists of these two groups and (39) is also proved in this case. So (39) holds for all \( k, l \). Now if \( \mu = 1 \), then \( \gamma = x \), and if \( \mu = -1 \), we get \( \gamma = x' \). Thus

(40) \( K(\langle a \rangle, E) = \{x, x'\} \)

and (8) holds. Moreover, (2) shows that if \( i, k \in \{1, \ldots, n\} \) and \( j, l \in \{1, \ldots, m\} \), then \( \langle g_{ij}a_{g_{ij}^{-1}} \rangle \) is contained in \( \langle g_{ij} \rangle \circ \langle g_{ij}^{-1} \rangle \subseteq \langle g_{ij} \rangle \circ g_{ij}^l \) and in \( \langle g_{ij}a \rangle \circ \langle g_{kl} \rangle \subseteq g_{ij}^l \circ \langle g_{ij} \rangle \). Thus \( \langle g_{ij} \rangle \circ g_{ij}^l \cap g_{ij}^l \circ \langle g_{kl} \rangle \neq \emptyset \) and this proves (9).

Let \( \beta = x(b, E) = (B_{11}, \ldots, B_{nn}) \). Suppose that \( \beta = x \), that is, \( B_{ij} = A_{ij} \) for all \( i, j \). Since \( n \geq 5 \) and \( \langle a \rangle \) and \( \langle b \rangle \), by (37), can intersect at most two of the \( \langle g_k \rangle \) nontrivially, there exist two indices, 1 and 2, say, such that \( \langle g_1 \rangle \cap \langle b \rangle = \langle g_2 \rangle \cap \langle b \rangle = \langle g_1 \rangle \cap \langle h \rangle = 1 \). If \( i, j \in \{1, \ldots, m\} \), then \( \langle g_{ij}a \rangle \in A_{11} \) and \( \langle g_{ij}b \rangle \in B_{2j} = A_{2j} \), and hence by (4), \( \langle g_{ij}a \rangle \circ \langle g_{ij}b \rangle \cap \langle g_{ij} \rangle \neq \emptyset \). Now 7.1.9 applied with \( u = g_1, v = g_2, u_i = g_{1i} \) and \( v_j = g_{2j} \) yields that \( a = b \). Thus we have shown:

(41) If \( a, b \in G \) such that \( \kappa(a, E) = \kappa(b, E) \), then \( a = b \).

So if \( \langle a \rangle, \langle b \rangle \in C, \kappa \in K(\langle a \rangle, E) \) and \( \beta \in K(\langle b \rangle, E) \) such that \( \kappa = \beta \), then, by (40), \( \kappa = \kappa(a^u, E) \) and \( \beta = \kappa(b^u, E) \) for some \( \kappa, \mu \in I \) and, by (41), \( a^u = b^u \) and hence \( \kappa = \beta \). This proves (10).

By (40), \( \kappa(\langle a \rangle) = \{a(a, E)|a \in G\} \) where we denote the trivial complex \( e \) by \( \kappa(1, E) \). Thus if \( \kappa, \beta \in \kappa(\langle a \rangle) \), there exist \( a, b \in G \) such that \( \kappa = \kappa(a, E) \) and \( \beta = \kappa(b, E) \). We show that

(42) \( \kappa \beta = \{\kappa(ab, E)\}; \)

this will prove (11). By 7.1.5, \( \kappa(ab, E) \in \kappa \beta \). So suppose that \( \delta = (D_{11}, \ldots, D_{nm}) \in \kappa \beta \) and let \( d \in G \) such that \( \kappa = \kappa(d, E) \). Since \( n \geq 5 \) and any of the groups \( \langle a \rangle, \langle b \rangle, \langle d \rangle \) can intersect at most one of the \( \langle g_k \rangle \) nontrivially, there exist two indices, again 1 and 2, say, such that \( \langle g_1 \rangle \cap \langle a \rangle = \langle g_1 \rangle \cap \langle b \rangle = \langle g_1 \rangle \cap \langle d \rangle = \langle g_2 \rangle \cap \langle b \rangle = 1 \). If we write \( \kappa = (A_{11}, \ldots, A_{nm}) \) and \( \beta = (B_{11}, \ldots, B_{nm}) \), then by Definition 7.1.4, \( \delta \in \kappa \beta \) implies that \( D_{ij} \circ B_{2j} \cap A_{1i} \circ \langle g_{2j} \rangle \neq \emptyset \) for all \( i, j \in \{1, \ldots, m\} \), and this means that for any such pair \( i, j \) there exist signs \( \lambda, \mu, \nu \in I \) such that \( \langle g_{ij}^\lambda d \rangle \circ \langle g_{2j}^\nu b \rangle \cap \langle g_{1j}^\mu a \rangle \circ \langle g_{2j} \rangle \neq \emptyset \). Thus the assumptions of Lemma 7.1.9 are satisfied with \( u_i = g_{1i} \) and \( v_j = g_{2j} \) and it follows that \( d = ab \). This proves (42) and hence also (11).
7.1 Free groups

If we write $x \ast \beta$ for the unique complex in $x\beta$, the map $\ast : \mathcal{H}(E) \times \mathcal{H}(E) \to \mathcal{H}(E)$ sending $(x, \beta)$ to $x \ast \beta$ for $x, \beta \in \mathcal{H}(E)$ is a binary operation on $\mathcal{H}(E)$. By (40), (41), and (42), the map $\sigma : G \to \mathcal{H}(E)$ defined by $a^\sigma = \kappa(a, E)$ for $a \in G$ is bijective and multiplicative. It follows that $(\mathcal{H}(E), \ast)$ is a group and $\sigma$ is an isomorphism from $G$ onto this group. In particular, $\ast$ is associative, that is, (12) holds. Furthermore, by (40) and (38),

$$K(\langle a \rangle, E) = \{\kappa(a, E), \kappa(a^{-1}, E)\} = \{a^\sigma, (a^{-1})^\sigma\}$$

for $1 \neq a \in G$. Finally, to prove (13), let $\langle a \rangle \in C$ and $X \subseteq C$ such that $\langle a \rangle \subseteq \bigcup X$ and let $a \in K(\langle a \rangle, E)$. Then $a = \kappa(a^\lambda, E)$ for some $\lambda \in I$ and, since $\bigcup X = \langle x \rangle \langle x \rangle \in X \rangle$, there exist finitely many $\langle b_i \rangle \in X$ such that $a^\lambda = b_1 \ldots b_s$. So if we write $\beta_i = \kappa(b_i, E)$, then $\beta_i \in K(\langle b_i \rangle, E)$ and

$$a = \kappa(a^\lambda, E) = (a^\sigma)^\sigma = b_1^\sigma \ast \cdots \ast b_s^\sigma = \beta_1 \ast \cdots \ast \beta_s.$$

Thus (13) holds and this finishes the proof of the theorem.

Subgroup lattices of free groups

We can now characterize the subgroup lattices of free groups.

7.1.12 Theorem. Let $r \geq 2$ be a cardinal number. A group $G$ is free of rank $r$ if and only if its subgroup lattice $L$ has the following properties.

(43) For every $c \in C(L) \setminus \{O\}$, $[c/O]$ is infinite.

(44) If $a, b \in C(L)$ such that $a \cup b \notin C(L)$ and if $d \in a \circ b$, then $d \cap a = d \cap b = O$.

(45) There exists a basic system $E$ of $L$ and a subset $S$ of $C(L)$ such that $\bigcup S = \bigcup L$ and that for every finite sequence $b_1, \ldots, b_s$ of elements $b_i \in S$ with $b_i \neq b_{i+1}$ ($i = 1, \ldots, s - 1$) and $a_i \in L$ with $O \neq a_i \subseteq b_i$ and $a_i \in K(a_i, E)$, the trivial complex $e$ is not contained in $((\ldots(\ldots x_1 x_2 x_3\ldots)y_s\ldots)\ldots)\ldots$. $x_s$.

Proof. Suppose first that $G$ is free on $X$ and $|X| = r$. For $c \in C(L) \setminus \{O\}$ there exists $1 \neq g \in G$ such that $c = \langle g \rangle$ and, since $\langle g \rangle$ is infinite cyclic, $[c/O] \simeq H(\langle g \rangle)$ is infinite. Thus (43) holds. Let $\langle a \rangle, \langle b \rangle \in C(L)$ such that $\langle a \rangle \cup \langle b \rangle \notin C(L)$ and suppose that $\langle d \rangle \in \langle a \rangle \circ \langle b \rangle$. Then, by (16) and 7.1.7, $\langle a \rangle \cap \langle b \rangle = 1$ and $d = a^\lambda b^\mu$ where $\lambda, \mu \in \{+1, -1\}$. If $\langle d \rangle \cap \langle a \rangle \neq 1$, then, again by (16), a would centralize $d$ and hence also $b$; but this would contradict (17). Thus $\langle d \rangle \cap \langle a \rangle = 1$, similarly $\langle d \rangle \cap \langle b \rangle = 1$ and so (44) holds. Finally, by 7.1.11 there exists a basic system $E$ of $L$; let $\sigma : G \to \mathcal{H}(E)$ be the isomorphism given in 7.1.11(b) and let $S = \{\langle x \rangle \mid x \in X \}$. Then $|S| = r$ and $\bigcup S = \bigcup x \in X = G = \bigcup L$. Suppose that $b_1, a_i, x_i$ are as in (45). Then $b_1 = \langle x_i \rangle$ for some $x_i \in X$, $a_i = \langle y_i \rangle$ where $1 \neq y_i \in \langle x_i \rangle$, and $x_i \in K(a_i, E) = \{y_i^\sigma, (y_i^{-1})^\sigma\}$, by 7.1.11; thus there exists $k_i \in \mathbb{Z} \setminus \{0\}$ such that $x_i = x_i^{k_i^\sigma}$. As $E$ satisfies (11), the only complex contained in $((\ldots(\ldots x_1 x_2 x_3\ldots)y_s\ldots)\ldots)\ldots x_s$ is $x_1 \ast \cdots \ast x_s$, and
Classes of groups and their projectivities

\[(x_1 \cdots x_s)^{g^{-1}} = x_1^{g^{-1}} \cdots x_s^{g^{-1}} = x_1^{k_1} \cdots x_s^{k_s} \neq 1\] since \(G\) is free on \(X\) and \(x_i \neq x_{i+1}\) for all \(i\). Thus \(x_1 \cdots x_s \neq 1^g = e\) and (45) holds.

Conversely, suppose that \(G\) is a group whose subgroup lattice \(L\) satisfies (43)–(45) and let \(E\) and \(S\) be as in (45). By (43), \(G\) is torsion-free and (44) implies that \(g^{-1}xg = x^{-1}\) for all \(g, x \in G\) such that \(x \neq 1\). Indeed, if \(x, g \in G\) such that \(g^{-1}xg = x^{-1}\), then \((x, g)\) would be nonabelian and hence, in particular, \(\langle x \rangle \cup \langle g \rangle \notin C(L)\) and \(g \neq 1\); by (2), \(\langle xg \rangle \in \langle x \rangle \circ \langle g \rangle\) but \(g^{-1}xg = x^{-1}\) would imply \(1 \neq g^2 \in \langle xg \rangle \cap \langle g \rangle\), contradicting (44). Thus \(G\) satisfies the assumptions of 7.1.3(b) and 7.1.5. It follows that there exists the complex \(\alpha(a, E)\) defined in 7.1.3 and that \(\alpha(ab, E) = \alpha(a, E) \alpha(b, E)\) for all \(a, b \in G\). A trivial induction yields that for \(a_1, \ldots, a_r \in G\),

\[(46) \quad \alpha(a_1 \cdots a_r, E) \in (\ldots ((\alpha(a_1, E) \alpha(a_2, E)) \alpha(a_3, E)) \ldots) \alpha(a_r, E).
\]

We want to prove that \(G\) is free on \(X\) where we obtain \(X\) by choosing from every subgroup \(\langle x \rangle \in S\) one of its generators. For this we have to show (see Robinson [1982], p. 47) that every element of \(G\) can be written uniquely as a product of powers of the \(x_i \in X\). Since \(\bigcup S = \bigcup L = G\), the set \(X\) generates \(G\). If there were an element that could be written in two different ways, there would exist \(s \in \mathbb{N}, x_i \in X\) \((i = 1, \ldots, s)\) with \(x_i \neq x_{i+1}\) for all \(i\) and \(k_i \in \mathbb{Z} \setminus \{0\}\) such that \(1 = x_1^{k_1} \cdots x_s^{k_s}\). If \(b_i = \langle x_i \rangle \in S, a_i = \langle x_i^{k_i} \rangle \leq \langle b_i \rangle\) and \(x_i = \alpha(x_i^{k_i}, E) \in K(a_i, E)\), then (46) implies that \(e = \alpha(1, E) = \alpha(x_1^{k_1} \cdots x_s^{k_s}, E) \in (\ldots ((\alpha(x_1, E) \alpha(x_2, E)) \alpha(x_3, E)) \ldots) \alpha(x_r, E)\) and this contradicts (45). Thus \(G\) is free on \(X\) and \(|X| = r\).

7.1.13 Theorem (Yakovlev [1974]). Let \(r \geq 2\) be a cardinal number. The lattice \(L\) is isomorphic to the subgroup lattice of a free group of rank \(r\) if and only if \(L\) is complete, any of its elements is the join of cyclic elements and \(L\) has the properties (43)–(45) where the basic system \(E\) in addition satisfies (8)–(13).

Proof. If \(L\) has these properties, then by 7.1.6 there exists a group \(G\) such that \(L \approx L(G)\); and, since \(L(G)\) satisfies (43)–(45), \(G\) is free of rank \(r\), by 7.1.12.

Conversely, if \(L \approx L(G)\) and \(G\) is free of rank \(r\), then \(L\) is complete, any element of \(L\) is the join of cyclic elements and, by 7.1.12, \(L\) has the properties (43)–(45). By (b) of 7.1.11, the basic system \(E\) in (45) satisfies (8)–(13).

**Characterization of subgroup lattices**

To characterize those lattices which are isomorphic to the subgroup lattice of an arbitrary group, we have to identify the normal subgroups in the subgroup lattice of a free group. To do this, we describe conjugation by elements.

7.1.14 Definition. If \(L\) is a lattice and \(x, y \in C(L)\), we define

\[y \uparrow x = \{z \in C(L) | z \in (x \circ y) \circ x, z \notin (x \circ x) \circ y, z \circ z \leq (x \circ (y \circ y)) \circ x\}.
\]

7.1.15 Lemma. If \(G\) is a 2-free group and \(a, b \in G\) such that \(a \neq 1 \neq b\) and \(\langle a \rangle \cap \langle b \rangle = 1\), then \(\langle b \rangle \uparrow \langle a \rangle = \{\langle b^a \rangle, \langle b^{a^{-1}} \rangle\}\).
Proof. By 7.1.7, \( \langle a \rangle \circ \langle b \rangle = \{ \langle a^\mu b^\nu \rangle | \mu, \nu \in I \} \) where \( I = \{+1, -1\} \) and, since \( \langle a, b \rangle \) is free on \( \{a, b\} \), we have \( \langle a^\mu b^\nu \rangle \cap \langle a \rangle = 1 \) for all \( \mu, \nu \in I \). Thus, again by 7.1.7,

\[
(47) \quad \langle a \rangle \circ \langle b \rangle \circ \langle a \rangle = \{ \langle (a^\mu b^\nu) a^\lambda \rangle | \mu, \nu, \lambda, \omega \in I \}.
\]

By (1), \( \langle a \rangle \circ \langle a \rangle = \{ \langle a^k \rangle | k \in \mathbb{Z} \} \) and therefore 7.1.7 and (1), in the case \( k = 0 \), yield that

\[
(48) \quad \langle a \rangle \circ \langle a \rangle \circ \langle b \rangle = \{ \langle a^k b^i \rangle | k \in \mathbb{Z}, i \in I \}.
\]

Now \( \langle (a^\mu b^\nu)^{-1} a^\lambda \rangle = \langle b^{-\gamma} a^{-\mu+\lambda} \rangle = \langle a^{-\mu} b^\nu \rangle \) and hence (47) and (48) show that an element \( \langle c \rangle \in C(L(G)) \) is contained in \( \langle a \rangle \circ \langle b \rangle \circ \langle a \rangle \) and not contained in \( \langle a \rangle \circ \langle a \rangle \circ \langle b \rangle \) if and only if

\[
(49) \quad \langle c \rangle = \langle a^\mu b^\nu a^\lambda \rangle \text{ where } \mu, \lambda, \nu \in I.
\]

By (48), \( \langle a \rangle \circ \langle (b \circ \langle b \rangle) \rangle = \{ \langle a^\mu b^\nu \rangle | \mu, \nu \in I, k \in \mathbb{Z} \} \) and hence every element of \( \langle (a \circ (b \circ \langle b \rangle)) \rangle \circ \langle a \rangle \) is of the form \( \langle (a^\mu b^\nu) a^\delta \rangle \) where \( i, \gamma, \delta \in I, k \in \mathbb{Z} \). So if \( \mu = \lambda \) in (49), then \( \langle c^2 \rangle = \langle a^\mu b^\nu a^\gamma b^\nu a^\delta \rangle \neq \langle (a \circ \langle b \circ \langle b \rangle) \rangle \circ \langle a \rangle \); since, however, \( \langle c^2 \rangle \in \langle c \rangle \circ \langle c \rangle \), it follows that \( \langle c \rangle \circ \langle c \rangle \notin \langle (a \circ \langle b \circ \langle b \rangle) \rangle \circ \langle a \rangle \). On the other hand, if \( \mu = -\lambda \), then \( \langle c \rangle = \langle a^\mu b^\nu a^{-\lambda} \rangle = \langle b^\nu \rangle \) and, by (1),

\[
\langle c \rangle \circ \langle c \rangle = \{ \langle c \rangle \} \subseteq \{ \langle a^\mu b^\nu a^{-\lambda} \rangle | i \in I, n \in \mathbb{Z} \} \subseteq \langle (a \circ (b \circ \langle b \rangle)) \circ \langle a \rangle \).
\]

This shows that \( \langle c \rangle \in \langle b \rangle \uparrow \langle a \rangle \) if and only if \( \mu = -\lambda \), that is, if and only if \( \langle c \rangle = \langle b^\nu \rangle \) or \( \langle c \rangle = \langle b^{-\nu} \rangle \).

An immediate consequence of 7.1.15 is the following description of normal subgroups in a 2-free group.

7.1.16 Lemma. Let \( G \) be a 2-free group and let \( N \leq G \). Then \( N \unlhd G \) if and only if \( \langle b \rangle \uparrow \langle a \rangle \subseteq [N/1] \) for all \( a \in G, b \in N \) such that \( a \neq 1 \neq b \) and \( \langle a \rangle \cap \langle b \rangle = 1 \).

Proof. If \( N \unlhd G \) and \( a \in G, b \in N \) such that \( a \neq 1 \neq b \) and \( \langle a \rangle \cap \langle b \rangle = 1 \), then by 7.1.15, \( \langle b \rangle \uparrow \langle a \rangle = \{ \langle b^a \rangle, \langle b^{a^{-1}} \rangle \} \subseteq [N/1] \). Conversely, suppose that this condition holds and let \( a \in G, b \in N \). If \( \langle a, b \rangle \) is abelian, then clearly \( b^a = b \in N \). And if \( \langle a, b \rangle \) is not abelian, then \( a \neq 1 \neq b \) and, by (16), \( \langle a \rangle \cap \langle b \rangle = 1 \); the assumption and 7.1.15 yield that \( \langle b^a \rangle \in \langle b \rangle \uparrow \langle a \rangle \subseteq [N/1] \) and hence \( b^a \in N \). Thus \( N \unlhd G \).

We can now give the desired characterization of subgroup lattices.

7.1.17 Theorem (Yakovlev [1974]). The lattice \( L \) is isomorphic to the subgroup lattice of some group if and only if there exist a lattice \( L^* \) and an element \( d \in L^* \) with the following properties.

\[
(50) \quad L^* \text{ is a complete lattice in which every element is the join of cyclic elements; furthermore, } L^* \text{ satisfies (43)–(45) for some cardinal number } r \geq 2 \text{ where for the basic system } E \text{ in addition (8)–(13) hold.}
\]
If \( a, b \in C(L^*) \setminus \{O\} \) such that \( a \cap b = O \) and \( b \leq d \), then \( b \uparrow a \subseteq [d/O] \).

(52) \( L \cong [I^*/d] \) where \( I^* \) is the greatest element of \( L^* \).

**Proof.** If \( L \cong L(G) \) for some group \( G \), then there exist a cardinal number \( r \geq 2 \), a free group \( F \) of rank \( r \), and a normal subgroup \( N \) of \( F \) such that \( G \cong F/N \). Thus, if \( L^* = L(F) \) and \( d = N \), then \( L \cong [I^*/d] \) and (50) and (51) hold by 7.1.13 and 7.1.16.

Conversely, suppose that \( L^* \) and \( d \in L^* \) satisfy (50)-(52). Then by 7.1.13 there exists a free group \( F \) of rank \( r \) such that \( L(F) \cong L^* \); let \( N \) be the image of \( d \) under this isomorphism. By (51) and 7.1.16, \( N \subseteq F \) and (52) implies that \( L \cong L(F/N) \).

Using similar ideas, Scoppola [1981], [1985] characterizes the subgroup lattices of torsion-free abelian groups of rank at least 2 and of abelian groups containing two independent elements of infinite order.

### Projectivities of free groups

The results proved so far show at once that a free group is determined by its subgroup lattice. Indeed, if \( G \) is free of rank \( r \geq 2 \) and \( \phi \) is a projectivity from \( G \) to a group \( G' \), then \( L(G) \) inherits the properties (43)-(45) from \( L(G') \); by 7.1.12, \( G \) is free of rank \( r \) and hence \( \overline{G} \cong G \). It is also not difficult to show that \( \phi \) is induced by an isomorphism from \( G \) onto \( G' \). We prove this, more generally, for 2-free groups.

**7.1.18 Theorem (Yakovlev [1974]).** Every projectivity of a 2-free group is induced by a unique isomorphism.

**Proof.** Let \( G \) be a 2-free group and let \( \phi \) be a projectivity from \( G \) to a group \( G' \). For \( u, v \in \overline{G} \), there exist \( x, y \in G \) such that \( \langle x \rangle^\phi = \langle u \rangle \) and \( \langle y \rangle^\phi = \langle v \rangle \) and then \( \langle x, y \rangle^\phi = \langle x \rangle^\phi \cup \langle y \rangle^\phi = \langle u, v \rangle \). Since \( G \) is 2-free, \( \langle x, y \rangle \) is free and, by 7.1.12 or 1.2.5, \( \langle u, v \rangle \) is free. Thus \( \overline{G} \) is 2-free.

By 7.1.11 there exists a basic system \( E = (e_1, \ldots, e_m) \) of \( L(G) \), and the map \( \sigma: G \to \mathcal{X}(E) \) defined by \( x^\sigma = \mathcal{X}(x, E) \) for \( x \in G \) is an isomorphism from \( G \) onto \((\mathcal{X}(E), \ast)\). Then Definition 7.1.10 shows \( \overline{E} = (e_1^\overline{E}, \ldots, e_m^\overline{E}) \) is a basic system of \( L(\overline{G}) \) and (b) of 7.1.11 implies that the map \( \tau: \overline{G} \to \mathcal{X}(\overline{E}) \), defined by \( u^\tau = \mathcal{X}(u, \overline{E}) \), is an isomorphism from \( \overline{G} \) onto \((\mathcal{X}(\overline{E}), \ast)\).

We extend \( \phi \) in the usual way to subsets \( \mathcal{X} \) of \( L(G) \), that is, define \( \mathcal{X}^\phi = \{X^\phi : X \in \mathcal{X}\} \). Since \( \phi \) is an isomorphism from \( L(G) \) onto \( L(\overline{G}) \),

\[
(53) \quad (a \circ b)^\phi = a^\phi \circ b^\phi \quad \text{for all } a, b \in C = C(L(G)).
\]

For an \( a \)-complex \( \alpha = (A_1, \ldots, A_m) \in \mathcal{X}(E) \), we define \( \alpha^\phi = (A_1^\phi, \ldots, A_m^\phi) \). Then 7.1.2 shows that \( A_i^\phi \) is a 2-element subset of \( (e_{i1}, e_{in}) \); \( (e_{i1}, a)^\phi = e_{i1}^\phi \circ a^\phi \) and that (4) holds for the \( A_i^\phi \) and \( e_{in}^\phi \). Thus \( \alpha^\phi \) is an \( a^\phi \)-complex with respect to \( \overline{E} \), that is,

\[
(54) \quad \alpha^\phi \in K(a^\phi, \overline{E}) \text{ if } \alpha \in K(a, E), a \in C.
\]

Thus \( \rho \) defines a map from \( \mathcal{X}(E) \) into \( \mathcal{X}(\overline{E}) \). The inverse map is defined in exactly the same way, using \( \phi^{-1} \) instead of \( \phi \), so that \( \rho \) is bijective. If \( \alpha, \beta \in \mathcal{X}(E), \alpha \in C \).
7.1 Free groups

\[ \delta = x \ast \beta \] is the unique complex for which there exist \( a, b, d \in C \) satisfying (5)–(7). By (53) and (54), the images \( x^p, \beta^p, \delta^p \) and \( a^p, b^p, d^p \) also satisfy (5)–(7), that is, \((x \ast \beta)^p = \delta^p \in x^p \beta^p = \{x^p \ast \beta^p\}\). Thus \((x \ast \beta)^p = x^p \ast \beta^p\) and \( \rho \) is an isomorphism. It follows that \( \mu = \sigma \rho \tau^{-1} \) is an isomorphism from \( G \) onto \( \hat{G} \). Now 7.1.11 and (54) show that for \( x \in G \) and \( \langle x \rangle^\circ = \langle u \rangle \),

\[
\{x, x^{-1}\}^\circ = \{x^\sigma, (x^{-1})^\sigma\}^{\rho \tau^{-1}} = K(\langle x \rangle, E)^{\rho \tau^{-1}} = K(\langle u \rangle, \bar{E})^{\tau^{-1}} = \{u, u^{-1}\}.
\]

This implies that \( \langle x \rangle^\circ = \langle u \rangle = \langle x \rangle^\circ \), that is, \( \varphi \) and \( \mu \) coincide on the cyclic and hence on all subgroups of \( G \). Thus \( \varphi \) is induced by \( \mu \). By 1.5.8 and 1.4.2, \( \text{Pot } G = 1 \) and so \( \mu \) is the unique isomorphism inducing \( \varphi \).

As a corollary to Yakovlev’s theorem we get a classical result of Sadovskii’s.

7.1.19 Theorem (Sadovskii [1941]). Every nonabelian locally free group is strongly determined by its subgroup lattice.

Proof. Let \( G \) be a nonabelian locally free group and \( \varphi \) be a projectivity from \( G \) to a group \( \hat{G} \). Let \( \mathcal{S} \) be the set of all nonabelian finitely generated subgroups of \( G \). Clearly, every element of \( G \) is contained in some \( X \in \mathcal{S} \); and if \( X, Y \in \mathcal{S} \), then \( Z = \langle X, Y \rangle \) is finitely generated and hence lies in \( \mathcal{S} \). Thus \( \mathcal{S} \) is a local system of subgroups of \( G \). Every \( X \in \mathcal{S} \) is a nonabelian free group and so, by 7.1.18, the projectivity induced by \( \varphi \) in \( X \) is induced by a unique group-isomorphism. By 1.3.6, \( \varphi \) is induced by an isomorphism from \( G \) onto \( \hat{G} \).

Free products

It was shown by Sadovskii [1947] that every group decomposable into a nontrivial free product is determined by its subgroup lattice; but he left open the question whether, in this case, every projectivity is induced by an isomorphism. This problem was solved independently by Arshinov [1970a] and Holmes [1969] who proved that every nontrivial free product is strongly determined by its subgroup lattice. Holmes, in addition, studied free products with amalgamation. We give his main result without proof.

7.1.20 Theorem (Holmes [1969]). Let \( G \) be the free product of the groups \( A \) and \( B \) with amalgamated subgroup \( C = A \cap B \) where \( A \neq C \neq B \) and suppose that \( |A : C| > 2 \) or \( |B : C| > 2 \). Let \( \varphi \) be a projectivity from \( G \) to a group \( \hat{G} \).

(a) If \( C \leq G \), then \( \hat{G} \simeq G \).

(b) If \( C \leq Z(G) \), then \( \varphi \) is induced by a unique group-isomorphism.

Another generalization of Sadovskii’s theorem was given by Yakovlev. He studied groups with a set \( X \) of generators such that every projectivity of a subgroup of the form \( \langle x_1, x_2, x_3 \rangle \) \((x_i \in X, x_1 \neq x_2 \neq x_3 \neq x_1)\) is induced by a unique isomorphism. He was able to show that, under slight additional assumptions, such a group is determined by its subgroup lattice. As a corollary, he obtained the following result.
Classes of groups and their projectivities

7.1.21 Theorem (Yakovlev [1986]). Assume that the group $G$ has a presentation with generators $x_1, \ldots, x_n$ and a single defining relation $w = 1$. If $w$ is cyclically reduced and contains at least three distinct generating elements, then $G$ is determined by its subgroup lattice.

7.2 Torsion-free nilpotent groups

Another important class of groups which are strongly determined by their subgroup lattices is the class of nonabelian torsion-free locally nilpotent groups. We prove this result, due to Sadovskii, using an unpublished manuscript of G.E. Wall's. First we give a simple lattice-theoretic characterization for this class of groups.

Lattice-theoretic characterization

A group $G$ is nilpotent if and only if it has a central series. And since a subgroup $H$ of $G$ is central if and only if $H \cup \langle x \rangle$ is abelian for every $x \in G$, we can try to use the obvious description of cyclic and abelian groups to identify central subgroups and central series in $L(G)$.

7.2.1 Definition. Let $L$ be a complete lattice, $O$ its least and $I$ its greatest element, and let $C(L)$ be the set of cyclic elements of $L$ as defined in 7.1.1.

(a) The element $a \in L$ is modularly embedded in $L$ if and only if $[a \vee c/0]$ is a modular lattice for all $c \in C(L)$.

(b) A modular chain (of length $t$) in $L$ is a finite chain $0 = a_0 < a_1 < \cdots < a_t = I$ such that $a_{i+1}$ is modularly embedded in $[I/a_i]$ for all $i = 0, \ldots, t - 1$.

7.2.2 Lemma. Let $G$ be a torsion-free group and $H \leq G$. Then $H$ is modularly embedded in $L(G)$ if and only if $H \leq Z(G)$.

Proof: First suppose that $H$ is modularly embedded in $L(G)$ and let $x \in G$. Then $L(H \cup \langle x \rangle) \cong [H \cup \langle x \rangle/1]$ is modular and, since $G$ is torsion-free, 2.4.9 shows that $H \cup \langle x \rangle$ is abelian. Thus $H \leq Z(G)$. Conversely, if $H \leq Z(G)$ and $X$ is a cyclic element in $L(G)$, then $X$ is a cyclic group and hence $H \cup X$ is abelian. Thus $[H \cup X/1]$ is modular and $H$ is modularly embedded in $G$. □

Of course, a group $G$ is torsion-free if and only if $[X/1]$ is infinite for every $X \in L(G)$ such that $X \neq 1$. Therefore to characterize the class of torsion-free nilpotent groups, we only have to tell when a torsion-free group is nilpotent. For this, let us call an element $a$ of a complete lattice $L$ isolated if $a \cap c = O$ or $a \cap c = c$ whenever $c \in C(L)$. Then a subgroup $H$ of a torsion-free group $G$ is isolated in $L(G)$ if and only if $o(x, H)$ is infinite for every $x \in G \setminus H$, and a normal subgroup $N$ of $G$ is isolated in $L(G)$ if and only if $G/N$ is torsion-free. It is well-known (see Robinson
[1982], p. 133) that for a torsion-free nilpotent group $G$ and every $n \in \mathbb{N}$,

(1) $G/Z_n(G)$ is torsion-free;

thus these iterated centres are isolated elements of $L(G)$.

7.2.3 Theorem (Kontorovič and Plotkin [1954]). Let $G$ be a torsion-free group. Then $G$ is nilpotent (of class at most $c$) if and only if $L(G)$ possesses a modular chain (of length $c$) consisting of isolated elements.

Proof. If $G$ is nilpotent, then the ascending central series of $G$ is a modular chain in $L(G)$ and, by (1), every $Z_n(G)$ is isolated in $L(G)$. Conversely, suppose that $1 = H_0 \leq \cdots \leq H_c = G$ is a modular chain in $L(G)$ consisting of isolated elements $H_i$. We use induction on $c$ to show that $G$ is nilpotent of class at most $c$. By 7.2.2, $H = H_1 \leq Z(G)$. Thus if $c = 1$, $G = H$ is abelian and we are done. So let $c \geq 2$ and assume that the assertion is true for $c - 1$. Since $H$ is isolated in $L(G)$, the group $G/H$ is torsion-free and $1 = H_1/H \leq \cdots \leq H_c/H = G/H$ is a modular chain of length $c - 1$ in $L(G/H)$ consisting of isolated elements. By induction, $G/H$ is nilpotent of class at most $c - 1$ and hence $G$ is nilpotent of class at most $c$.

$\varphi$-mappings

In the remainder of this section we show that every projectivity $\varphi$ of a nonabelian torsion-free nilpotent group $G$ is induced by a group-isomorphism. Basic for the proof of this result is the notion of a $\varphi$-mapping, that is, an element map $x : G \to \bar{G}$ such that

(2) $H^\varphi = H^x = \{x^h | x \in H \}$ for all $H \leq G$, and

(3) $x|_A$ is an isomorphism for every abelian subgroup $A$ of $G$.

By (2), $G^\varphi = G^x = \bar{G}$ so that $x$ is surjective. And for $x, y \in G$, (2) and (3) imply that $x^y$ generates $\langle x \rangle^\varphi$; so if $x^y = x^y$, then $\langle x \rangle^\varphi = \langle y \rangle^\varphi$ and (3) yields that $x = y$. Thus

(4) every $\varphi$-mapping is bijective.

We use Theorem 2.6.10 to show that $\varphi$-mappings exist. First of all we note that $\varphi$ is normalizer preserving.

7.2.4 Lemma. Every projectivity of a torsion-free locally nilpotent group is normalizer preserving.

Proof. Let $G$ be a torsion-free locally nilpotent group and let $\varphi$ be a projectivity from $G$ to a group $\bar{G}$. By 5.6.5, we have to show that $(H^\varphi)^\varphi = (H^\varphi)^\varphi$ for every 2-generator subgroup $H$ of $G$. Since $G$ is locally nilpotent, $H$ is nilpotent of class $c$, say. By 7.2.2, $Z(H)^\varphi = Z(H^\varphi)$ and, since $H/Z(H)$ is torsion-free, a trivial induction yields that $Z_i(H)^\varphi = Z_i(H^\varphi)$ for $i = 1, \ldots, c$. In particular, $H^\varphi$ is nilpotent of class $c$ (see also Theorem 7.2.3).
Now if \( H \) is abelian, then \( H^\phi \) is also abelian and \((H')^\phi = 1 = (H^\phi)'\). If \( H \) is non-abelian, then \( H/Z_{c_2}(H) \) is also nonabelian and so \( H/Z_{c_1}(H) \) is not cyclic. On the other hand, \( H/Z_{c_1}(H) \) is a homomorphic image of the abelian 2-generator group \( H/H' \). By the structure of finitely generated abelian groups there exist generators \( x, y \) of \( H/H' \) such that \( Z_{c_1}(H)/H' = \langle x^i, y^j \rangle \) where \( i, j \in \mathbb{Z} \). Since \( H/Z_{c_1}(H) \) is torsion-free and not cyclic, it follows that \( H' = Z_{c_1}(H) \). Similarly, \((H^\phi)' = Z_{c_1}(H^\phi)\) and hence \((H')^\phi = (H^\phi)',\) as required.

7.2.5 Lemma. Let \( G \) be a torsion-free nilpotent group which is not locally cyclic and let \( \phi \) be a projectivity from \( G \) to a group \( \overline{G} \).

(a) There exist exactly two \( \phi \)-mappings \( \alpha_1 \) and \( \alpha_2 \); for all \( x \in G \), \( x^{\alpha_2} = (x^{\alpha_1})^{-1} \).

(b) If \( 1 \neq H \leq G \) and \( \psi \) is the projectivity induced by \( \phi \) in \( H \), there exist exactly two \( \psi \)-mappings and these are \( \alpha_1|_H \) and \( \alpha_2|_H \).

**Proof.** (a) By Zorn’s Lemma, every abelian subgroup \( A \neq 1 \) of \( G \) is contained in a maximal abelian subgroup \( M \) of \( G \). We claim that \( M \) contains two independent elements of infinite order. This is clear if \( M = G \); for, in this case, by assumption, \( M \) has a finitely generated noncyclic subgroup. And if \( M \neq G \), then \( Z(G) \triangleleft M \) and \( M/Z(G) \) is torsion-free; hence if \( 1 \neq z \in Z(G) \) and \( x \in M \setminus Z(G) \), then \( \langle x \rangle \cap \langle z \rangle = 1 \).

By 2.6.10, \( \phi \) is induced by an isomorphism on \( M \) and therefore also on \( A \). Then 1.5.7 shows that

\[
\phi \text{ is induced on } A \text{ by exactly two isomorphisms } \epsilon \text{ and } \delta \text{ and } a^\epsilon = (a^\delta)^{-1} \text{ for all } a \in A.
\]

Let \( \beta: Z(G) \to Z(G)^\phi \) be one of these two isomorphisms for \( A = Z(G) \). For every \( x \in G \), the subgroup \( A_x = \langle x, Z(G) \rangle \) is abelian and hence there is a unique isomorphism \( \alpha_x: A_x \to A_x^\phi \) inducing \( \phi \) on \( A_x \) whose restriction to \( Z(G) \) is \( \beta \). Let \( x: G \to \overline{G} \) be defined by \( x^a = x^{\alpha_x} \) for \( x \in G \). We want to show that \( x \) is a \( \phi \)-mapping. For this suppose that \( A \) and \( M \) are as before. Then \( Z(G) \leq M \) and by (5) there exists a unique isomorphism \( \gamma: M \to M^\phi \) inducing \( \phi \) on \( M \) such that \( \gamma|_{Z(G)} = \beta \). If \( a \in A \), then \( \alpha_x = \gamma|_{A_x} \) and hence \( a^\gamma = a^\beta \). Thus \( \alpha|_A = \gamma|_A \) is an isomorphism and (3) holds. The same argument applied to \( A = A_x \) shows that \( \langle x \rangle^x = \langle x \rangle^\gamma = \langle x \rangle^\phi \) for \( x \in G \). It follows that (2) is satisfied and \( x \) is a \( \phi \)-mapping.

So if \( \beta_1 \) and \( \beta_2 \) are the isomorphisms inducing \( \phi \) on \( Z(G) \), we obtain two \( \phi \)-mappings \( \alpha_1 \) and \( \alpha_2 \) such that \( \alpha_i|_{Z(G)} = \beta_i \). If \( x \) is any \( \phi \)-mapping, then \( \phi \) is induced on \( Z(G) \) by the isomorphism \( \alpha|_{Z(G)} \) and it follows from (5) that \( \alpha|_{Z(G)} = \beta_i \) for some \( i \).

Since \( \phi \) is induced on \( A_x \) by the isomorphisms \( \alpha|_{A_x} \) and \( \alpha|_{A_x} \) whose restrictions to \( Z(G) \) both are \( \beta_i \), it follows that \( \alpha|_{A_x} = \alpha|_{A_x} \) and hence \( x^{\alpha} = x^{\beta_i} \). This holds for all \( x \in G \) and so \( \alpha = \alpha_i \). Thus \( \alpha_1 \) and \( \alpha_2 \) are the only \( \phi \)-mappings and, since \( \alpha_1|_{A_x} \) and \( \alpha_2|_{A_x} \) are different isomorphisms inducing \( \phi \) on \( A_x \), again (5) yields that \( x^{\alpha_2} = (x^{\alpha_1})^{-1} \).

(b) It is clear that the restriction of a \( \phi \)-mapping to \( H \) is a \( \psi \)-mapping and, by (a), \( \alpha_1|_H \neq \alpha_2|_H \). If \( H \) is abelian, then (3) implies that the \( \psi \)-mappings are just the isomorphisms inducing \( \psi \) and, by 1.5.7, \( H \) has at most two such isomorphisms. If \( H \) is nonabelian, then by (a), there are exactly two \( \psi \)-mappings. In both cases, it follows that \( \alpha_1|_H \) and \( \alpha_2|_H \) are all the \( \psi \)-mappings. \( \square \)
Our aim is to show that one of the two \( \varphi \)-mappings constructed in the above lemma is an isomorphism; the other will then be an anti-isomorphism, that is, will satisfy \((xy)^a = y^a x^a\) for all \( x, y \in G \). We use induction on the class of \( G \) to prove this and first settle the basis for this induction.

### Nilpotent groups of class 2

We remind the reader that a torsion-free nilpotent group \( G \) is an \( R \)-group (see Kurosh [1956], p. 247) so that for all \( x, y \in G \):

1. If \( x^m = y^m \) for some \( m \in \mathbb{Z} \setminus \{0\} \), then \( x = y \).
2. If there exist \( m, n \in \mathbb{Z} \setminus \{0\} \) such that \( x^m y^n = y^n x^m \), then \( xy = yx \).

Furthermore, if \( H = \langle x, y \rangle \) has class 2, then \( \langle [x, y] \rangle \leq H' \leq Z(H) \); and if \( x^j y^j [x, y] k \in Z(H) \), then \( y^j \in C_H(x) \) and (7) implies that \( j = 0 \). Similarly \( i = 0 \) and it follows that

\[
(8) \ H' = \langle [x, y] \rangle = Z(H).
\]

#### 7.2.6 Theorem (Pekelis and Sadovskii [1963]).

Let \( G \) be a torsion-free nilpotent group of class 2 and let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). Then one of the two \( \varphi \)-mappings (see 7.2.5) is an isomorphism, the other is an anti-isomorphism.

**Proof.** Let \( \alpha \) be one of the two \( \varphi \)-mappings and let \( a, b \in G \). Then by (3),

\[
(9) \ (ab)^a = a^a b^a \text{ if } ab = ba;
\]

in particular,

\[
(10) \ (a^n)^a = (a^n)^a \text{ for all } n \in \mathbb{Z}.
\]

Now suppose that \( ab \neq ba \) and let \( H = \langle a, b \rangle \). By (8), \( H' = \langle [b, a] \rangle = Z(H) \) and, since \( \varphi \) is normalizer preserving and induced by \( \alpha \),

\[
(11) \ \langle [b, a] \rangle^a = Z(H^o) = Z(H^o) = (H^o)' = \langle [b^a, a^a] \rangle.
\]

Since \( H/Z(H) \) is not cyclic, 2.6.10 yields that the projectivity induced by \( \varphi \) in \( H/Z(H) \) is induced by an isomorphism. On the other hand, \( \varphi \) is induced by \( \alpha \) and it follows that there exist \( e, \delta \in \{+1, -1\} \) and \( z_1 \in Z(H^o) \) such that \( (ab)^a = (a^e)^o (b^\delta)^o z_1 \). We put \( x = (a^e)^o \) and \( y = (b^\delta)^o \) so that \( H^o = \langle x, y \rangle \) and \( Z(H^o) = (H^o)' = \langle [y, x] \rangle \). If we further put \( c = [b, a] \) and \( z = [y, x] \), then by (11), \( \langle c^a \rangle = Z(H^o) = \langle z \rangle \) and so

\[
(12) \ c^e = z^e \text{ where } e \in \{+1, -1\}, \ c = [b, a], \ z = [y, x];
\]

in addition there exists \( r \in Z \) such that \( z_1 = z^r \) and hence

\[
(13) \ (ab)^a = xyz^r \text{ where } r \in Z, \ x = (a^e)^o, \ y = (b^\delta)^o \text{ and } e, \delta \in \{+1, -1\}.
\]

By (3), \( (abc)^a = (ab)^a c^a \) and therefore

\[
(14) \ (ba)^a = (abc)^a = xyz^{r+v} = yxz^{r+v-1}.
\]
For $n \in \mathbb{N}$, we put $H_n = \langle a^n, b^n \rangle$ and compute $(a^n b^n)^\epsilon$ in two different ways. By (10), $H_n^\epsilon = \langle (a^n)^\epsilon, (b^n)^\epsilon \rangle = \langle x^n, y^n \rangle$. By (10) and (13), $((ab)^\epsilon)^\rho = ((ab)^\epsilon)^\rho = (xy)^\rho z^n = x^n y^n z_2$ where $z_2 \in Z(H^\epsilon)$. Since $a^n b^n = (ab)^\epsilon c_1$ with $c_1 \in Z(H)$, (9) implies that

$$(a^n b^n)^\epsilon = (ab)^\epsilon c_1 = x^n y^n z_2 c_1 = x^n y^n z_3$$

where $z_3 = z_2 c_1 \in Z(H^\epsilon)$. Now $z_3 = y^{-n} x^{-n} (a^n b^n)^\epsilon \in H_n^\epsilon$ and hence $z_3 \in Z(H^\epsilon) \cap H_n^\epsilon \leq Z(H_n^\epsilon)$. By (7), $H_n$ is not abelian and therefore $Z(H_n^\epsilon) = (H_n^\epsilon)' = \langle \{x^n, y^n\} \rangle$, by (11). It follows that there exists $k_n \in \mathbb{Z}$ such that $z_3 = [y^n, x^n]^k_n = [y, x]^n z_4 = z_4 z_2 k_n$. Thus, finally,

$$(15) \quad (a^n b^n)^\epsilon = x^n y^n z_4 z_2^k_n.$$
Since every element of $H^\sigma$ can be written uniquely in the form $(a^s)^{(b^t)^\xi}$ with $s, t \in \mathbb{Z}$ and $w \in Z(H^\sigma)$, the first equation implies that $\sigma = \lambda = 1$ and the second that $\sigma = \lambda$, $\delta = \mu$ and $z = c^\xi = [b^\mu]_E(a_\lambda^\lambda)^E = [y, x]z^{\xi} = z^{1+\xi}$, a contradiction. Thus $\sigma = 1$ in this case. And if $\nu = -1$, (20) yields that $(abc)^\sigma = xy = (a^s)^{(b^t)^\xi}$ and hence

$$(a^s)^{(b^t)^\xi} = (a^s)^{(b^t)^\eta}(c^\xi)$$

This time the first equation leads to a contradiction and the second implies that $\sigma = \lambda = 1 = [b^\mu]_E(a_\lambda^\lambda)^E$. Again it follows that $\sigma = 1$. Thus we have shown that $\sigma = 1$ so that (18) and (20) yield the following result.

(21) Either $(ab)^\sigma = a^s b^\sigma a^z$ and $(ba)^\sigma = b^\sigma a^z$ or $(ab)^\sigma = b^\sigma a^z$ and $(ba)^\sigma = a^z b^\sigma$.

By (9), this also holds if $ab = ba$ and hence for all $a, b \in G$. In the remainder of the proof we shall show that (21) and (9) imply that for all $a, b \in G$, either $(ab)^\sigma = a^s b^\sigma a^z$, that is, $\sigma$ is an isomorphism, or $(ab)^\sigma = b^\sigma a^z$, that is, $\sigma$ is an anti-isomorphism. By 7.2.5, the other $\phi$-mapping will then be an anti-isomorphism or an isomorphism, respectively. First of all, (21) implies that $(aba)^\sigma \in \{a^s b^\sigma a^z, (a^s)^E b^\sigma, b^\sigma (a^s)^E\}$ and \{(a^s)^E b^\sigma, b^\sigma (a^s)^E\}. By (4), $\sigma$ is bijective and it follows that

(22) $(aba)^\sigma = a^s b^\sigma a^z$ for all $a, b \in G$.

Now suppose, for a contradiction, that $\sigma$ is neither an isomorphism nor an anti-isomorphism. We then claim that there exist elements $u, v, w \in G$ such that

(23) $(uv)^\sigma = u^z v^\sigma \neq v^z u^\sigma$, $(uw)^\sigma = w^z u^\sigma \neq u^z v^\sigma$, and $w^z u^\sigma v^z = v^z u^\sigma w^z$.

To prove this, we first show that the sets $R = \{a \in G|(ag)^\sigma = a^z g^\sigma \text{ for all } g \in G\}$ and $S = \{a \in G|(ag)^\sigma = g^\sigma a^z \text{ for all } g \in G\}$ are subgroups of $G$. For this let $g \in G$ and take $a, b \in R$. Then $(abg)^\sigma = a^z b^\sigma g^\sigma = (ab)^\sigma g^\sigma$ and hence $ab \in R$; furthermore, by (10), $(ga^{-1})^\sigma = ((a^{-1})^\sigma)^{-1} = (g^\sigma)^{-1} = g^\sigma(a^{-1})^\sigma$ and then (21) shows that $(a^{-1})^\sigma = (a^{-1})^\sigma g^\sigma$, that is, $a^{-1} \in R$. If $a, b \in S$, then $(ab)^\sigma = (by)^\sigma a^z = g^\sigma b^\sigma a^z = g^\sigma(ab)^\sigma$ and hence $ab \in S$; furthermore, $(ga^{-1})^\sigma = ((a^{-1})^\sigma)^{-1} = (g^\sigma)^{-1}a^z = (a^{-1})^\sigma g^\sigma$ and then $(a^{-1})^\sigma = g^\sigma(a^{-1})^\sigma$, that is, $a^{-1} \in S$. Thus $R$ and $S$ are subgroups of $G$. If $R = G$, $\sigma$ would be an isomorphism; if $S = G$, $\sigma$ would be an anti-isomorphism. Thus our assumption implies that $R \neq G \neq S$ and, since a group cannot be the set-theoretic union of two proper subgroups, there exists $u \in G$ such that $u \notin R$ and $u \notin S$. Let

$$V = \{g \in G|(ug)^\sigma = u^z g^\sigma \neq g^\sigma u^z\} \quad \text{and} \quad W = \{g \in G|(ug)^\sigma = g^\sigma u^z \neq u^z g^\sigma\}.$$  

Now $V \neq \emptyset$ since $u \notin S$, and $W \neq \emptyset$ since $u \notin R$; further, an element $g \in G$ that does not lie in $V$ or in $W$ satisfies $u^z g^\sigma = g^\sigma u^z$, hence $(ug)^\sigma = (gu)^\sigma$ and therefore $ug = gu$. Thus $G$ is the disjoint union of $C_G(u), V,$ and $W$. So if $uv = wv$ for all $v \in V, w \in W$, we could choose $v \in V$ and investigate the three possibilities for $uv$. From $uv \in C_G(u)$ it would follow that $v \in C_G(u)$, a contradiction. Also $wv \in V$ would imply that $u = uv^{-1} \in \langle V \rangle \subseteq C_G(W)$ and hence $uw = wu$, again a contradiction. It would follow that $uv \in W$ so that, by (22), $(uwv)^\sigma = (uv)^\sigma u^z = u^z v^z u^z = (uwv)^\sigma$; since $\sigma$ is bijective, this would imply that $uw = vu$, a final contradiction. Thus there exist $v \in V,$
$w \in W$ such that $vw \neq wv$, and we claim that the three elements $u, v, w$ satisfy (23). The first two equations are clear since $v \in V$ and $w \in W$. To prove the third, we compute $(uvw)^2$. By (21), $(v(uw))^2 \in \{v^2(uw)^2, (uw)^2v^2\}$ and $(uv)(wu)^2 \in \{(uw)^2v^2, v^2(uw)^2\}$. Since $vw \neq wv$, we have $v^2w^2u^2 \neq w^2v^2u^2$, again by (21); similarly, $v^2w^2u^2 \neq v^2u^2w^2$ and $w^2u^2v^2 \neq w^2v^2u^2$. It follows that $w^2u^2v^2 = (uvw)^2 = v^2u^2w^2$ and this proves (23).

We now take $u, v, w \in G$ satisfying (23) and study $(uvw)^n$. By (21) and (22),

$$(uvu)w^2 \in \{u^2v^2u^2w^2, w^2u^2v^2u^2\} \quad \text{and} \quad ((uv)(uw))^2 \in \{u^2v^2w^2u^2, w^2u^2v^2u^2\}.$$

However, as before, $u^2v^2u^2w^2 \neq u^2v^2w^2u^2$ and $w^2u^2v^2u^2 \neq w^2u^2v^2u^2$ and, by (23), $u^2v^2u^2w^2 = u^2w^2u^2v^2 \neq w^2u^2v^2u^2$ and $w^2u^2v^2u^2 = v^2u^2w^2u^2 \neq u^2v^2w^2u^2$. This is a contradiction. Thus $x$ is an isomorphism or an anti-isomorphism.

**Finitely generated nilpotent groups**

Before we carry out the induction announced above, we remind the reader of some further properties of a torsion-free nilpotent group $G$ of class $c \geq 2$. As for regular $p$-groups, the commutator collecting process yields that for all primes $p > c$ and $i \in \mathbb{N}$,

$$G^p = \langle x^p | x \in G \rangle = \{x^p | x \in G \} \quad \text{and} \quad K_i(G^p) \leq K_i(G)^p.$$

If $L_i(G)/K_i(G)$ is the torsion subgroup of $G/K_i(G)$, then

$$G = L_1(G) > L_2(G) > \cdots > L_c(G) > L_{c+1}(G) = 1 \text{ is a central series.}$$

Indeed, if $Z_i/L_i(G) = Z(G/L_i(G))$, then by (1), $G/Z_i$ is torsion-free and, since $[K_{i-1}(G), G] = K_i(G) \leq L_i(G)$, it follows that $K_{i-1}(G) \leq Z_i$ and then $L_{i-1}(G) \leq Z_i$. Thus $G = L_1(G) \geq \cdots \geq L_{c+1}(G) = 1$ is a central series and $c(G) = c$ implies that $L_i(G) > L_{i+1}(G)$ for $i = 1, \ldots, c$.

In the sequel we shall mainly study torsion-free nilpotent groups which are finitely generated. It is well-known (see Robinson [1982], p. 132) that for such a group $G$,

$$(27) \; L(G) \text{ satisfies the maximal condition}$$

and hence, in particular, every subgroup is finitely generated. Furthermore

$$\bigcap_{n \in \mathbb{N}} G^n = 1 \text{ for every infinite subset } I \text{ of } \mathbb{N}.$$

Indeed, every $x \in \bigcap_{n \in I} G^n$ is contained in $\bigcup_{n \in I} H^n$ where $H = \langle g \in G | g^m = x \text{ for some } m \in \mathbb{Z} \rangle$; by (7) and (27), $H$ is a finitely generated torsion-free abelian group and hence $\bigcap_{n \in I} H^n = 1$.

Finally, if $G = \langle x, y \rangle$ is generated by two elements, then $G/Z_{c-1}(G)$ is a torsion-free abelian group of rank 2 and hence also

$$(29) \; G/G' = \langle xG', yG' \rangle \text{ is torsion-free of rank 2.}$$
Moreover, $G' = K_2(G) = \langle [x, y], K_3(G) \rangle$ (see Huppert [1967], p. 258) and if the cyclic group $G'/K_3(G)$ were finite, it would follow that $L_3(G) \geq G' = L_2(G)$, contradicting (26). Thus $G/G'$ and $G''/K_3(G)$ are torsion-free and hence also

(30) $G/K_3(G)$ is torsion-free.

### 7.2.7 Theorem

Let $G$ be a finitely generated torsion-free nilpotent group, $\varphi$ a projectivity from $G$ to a group $\bar{G}$ and $x$ a $\varphi$-mapping. Then $x$ is an isomorphism or an anti-isomorphism.

The proof of this theorem is long and technical; it will be given in the next three lemmas. We use induction on the class $c$ of $G$. If $G$ is abelian, then by (3), $x$ is an isomorphism; if $c = 2$, Theorem 7.2.6 yields the assertion. So we assume in the sequel that $G$, $\varphi$, $x$ are as in the theorem, that

(31) $c \geq 3$

and that the assertion is true for groups of smaller class. By 7.2.4, $\varphi$ is normalizer preserving. Therefore 5.6.2 and a trivial induction yield that for all $H \leq G$ and $i \in \mathbb{N}$,

(32) $K_i(H)^\varphi = K_i(H^\varphi)$ and hence $L_i(H)^\varphi = L_i(H^\varphi)$.

Furthermore, if $K \leq Z(H)$, then $\varphi$ induces a projectivity $\psi$ in $H/K$ and $x$ induces a map $x^*: H/K \to H^\varphi/K^\varphi$ defined by $(xK)x^* = x^*K^\varphi$ for $x \in H$. Clearly, $x^*$ induces the projectivity $\psi$. And if $K \leq A \leq H$ such that $A/K$ is abelian, then $c(A) \leq 2$ and, by 7.2.5, $x|_A$ is a $\rho$-mapping where $\rho$ is the projectivity induced by $\varphi$ in $A$. By 7.2.6 or (3), $x|_A$ is an isomorphism or an anti-isomorphism and hence the map induced by $x$ or $x^*$ in the abelian group $A/K$ is an isomorphism. Thus (3) holds for $x^*$ and $x^*$ is a $\psi$-mapping. By (27), $H/K$ is finitely generated so that our inductive hypothesis yields the following.

(33) If $H \leq G$, $K \leq Z(H)$ and $H/K$ is torsion-free and of class $c(H/K) < c$, then $x$ induces an isomorphism or an anti-isomorphism in $H/K$.

For every $H \leq G$, we write $\tilde{H} = H/L_c(H)$ and apply (33) to this group. By (26), $L_c(H) \leq Z(H)$ and $H/L_c(H)$ is torsion-free of class $c(\tilde{H}) < c$. Thus by (33),

(34) $x$ induces an isomorphism or an anti-isomorphism in $\tilde{H} = H/L_c(H)$.

### 7.2.8 Lemma

Let $y, a \in G$, $H = \langle y, a \rangle$ and $K = \langle y^r, (y^s a)^t \rangle$ where $r, s, t \in \mathbb{Z}$. If $x$ induces an isomorphism in $\bar{G}$ but not in $\bar{K}$, then $[y, a] \in L_c(G)$, $c(H) = 2$ and $x|_H$ is an anti-isomorphism.

**Proof.** By assumption and (34), $x$ induces in $G/L_c(G)$ an isomorphism and in $K/L_c(K)$ an anti-isomorphism which is not an isomorphism. In particular, $K$ is not cyclic and hence $r \neq 0 \neq t$. Since $L_c(K) \leq L_c(G) \cap K \leq K$, we see that $x$ induces in $K/(L_c(G) \cap K)$ an isomorphism and an anti-isomorphism. It follows that this group is abelian and hence $[y^r, (y^s a)^t] \in L_c(G)$. Since $G/L_c(G)$ is torsion-free, (7) then implies that $[y, y^s a] \in L_c(G)$ and so, finally, $[y, a] \in L_c(G) \leq Z(G)$. Thus $c(H) \leq 2$. Since $x$ does not induce an isomorphism in $\bar{K}$, it follows that $x|_H$ is not an isomorphism. By (33), $x|_H$ is an anti-isomorphism and $H$ is not abelian. \qed
Let $i: \tilde{G} \to \tilde{G}$ be defined by $x' = x^{-1}$ for $x \in \tilde{G}$. By 7.2.5 and (34), one of the two \(\varphi\)-mappings $x$ and $x'$ induces an isomorphism in $\tilde{G}$, the other an anti-isomorphism which is not an isomorphism since $c(\tilde{G}) = c - 1 \geq 2$. We choose the map inducing an isomorphism and come to the main step in the proof of Theorem 7.2.7.

### 7.2.9 Lemma.

Let $\alpha$ be the \(\varphi\)-mapping inducing an isomorphism in $\tilde{G}$ and suppose that $G = N \cdot x$ where $N \leq G$ and $\alpha|_N$ is an isomorphism or an anti-isomorphism. Then $\alpha$ is an isomorphism from $G$ onto $\tilde{G}$.

**Proof.** Let $t \in Z$ and $a, b \in N$. Since $\alpha$ induces an isomorphism in $\tilde{G} = G/\langle x \rangle$, there exist elements $h_i(a)$ and $f(b, a)$ in $L_c(G) \leq Z(G)$ such that

\begin{align*}
(35) \quad (x^t a)^x &= (x^2)^x h_i(a) x \\
(36) \quad (a^x)^{xb} &= (a^x)^x f(b, a).
\end{align*}

We first show in several steps that the lemma will be proved if we can show that $f(1, a) = 1$ for all $a \in N$.

(a) If the assumptions of the lemma imply that $f(1, a) = 1$ for all $a \in N$, then $f(b, a) = 1$ for all $a, b \in N$.

**Proof.** Let $b \in N$. Then $G = N \cdot xb$ and the assumptions of the lemma also hold with $x$ replaced by $xb$. So if these assumptions imply that $f(1, a) = 1$ for all $a \in N$, this will also be true for the function $f^*: N \times N \to L_c(G)$ defined via (36) for $xb$ instead of $x$. This means that $(a^x)^{xb} = (a^x)^x f^*(1, a)^x = (a^x)^x$ and thus $f(b, a) = 1$. Since $b \in N$ was arbitrary, (a) holds.

(b) If $f(b, a) = 1$ for all $a, b \in N$, then $\alpha|_N$ is an isomorphism.

**Proof.** For $a, b \in N$, (35) and (36) together with $f(b, a) = f(1, a) = 1$ and $h_i(b)^a \in Z(\tilde{G})$ imply that

\[(a^x)^a = (a^x)^{xb} = (a^x)^{xb} h_i(b)^a = ((a^x)^x)^{xb} = ((a^x)^x)^{xb}.
\]

If $\alpha|_N$ is an isomorphism, we are done. And if $\alpha|_N$ is an anti-isomorphism, then $(a^x)^a = (b^{-1} a x b)^a = b x (a^x)^a (b^{-1})^{-1} = ((a^x)^a)^{xb}$. For arbitrary $g, y \in G$,

\[(37) \quad (g^y)^x = (g^y)^y = (g^y)^{y^{-1}} \text{ implies that } g^x = g.
\]

Indeed, this assumption yields $[y^2, g^2] = 1$ so that, by (7), $[y^2, g^2] = 1$; thus $g^x = (g^y)^x = (g^y)^x$ and, since $\alpha$ is bijective, $g^x = g$.

Now (37) applied with $g = a^x$ and $y = b$ yields that $[a^x, b] = 1$ and, since $a$ and $b$ are arbitrary elements of $N$, it follows that $N$ is abelian. But then the anti-isomorphism $\alpha|_N$ is also an isomorphism and (b) holds.

(c) If $f(1, a) = 1$ for all $a \in N$, then $(a^x)^2 = (a^x)^{xb}$ for all $a \in N, t \in Z$.  

7.2 Torsion-free nilpotent groups

Proof. By (36), \((a^x)^x = (a^x)^x\) and hence \(a^x = a^{ax^x}^{-1}\) for all \(a \in N\). It follows that \(a^{x^t} = a^{ax^x^t}^{-1}\) for all \(t \in \mathbb{Z}\) and this yields (c).

(d) If \(f(b, a) = 1 = h_i(a)\) for all \(a, b \in N\) and \(t \in \mathbb{Z}\), then \(x\) is an isomorphism.

Proof. For \(a, b \in N\) and \(s, t \in \mathbb{Z}\), (35), (b), and (c) imply that

\[
(x^s ax^t b)^x = (x^{s+t} a^{x^t} b)^x = (x^a)^{s+t}(a^x)^{x^t} b^x
\]

Thus \(x\) is multiplicative and hence an isomorphism.

(e) If \(f(b, a) = 1\) for all \(a, b \in N\), then \(h_i(a) = 1\) for all \(a \in N\) and \(t \in \mathbb{Z}\).

Proof. Let \(t \in \mathbb{Z}\) and \(a \in N\). We put \(y = x^t\) and study \(u_k = a^{x^k} \in N\) and \(v_k = (a^y)^{x^k} \in N\) for \(k \in \mathbb{N}\). By induction on \(k\), we get the well-known formulae

\[(ya)^k = y^k u_k \quad \text{and} \quad (y^2 a^x)^k = (y^2)^k v_k.\]

Clearly, (b) and (c) together with \((x')^x = (x^x)'\) imply that for all \(k \in \mathbb{N}\),

\[(xa)^k = (x^x)^k v_k.\]

We choose a prime \(p > c\), put \(H = \langle y, a \rangle\) and \(K = \langle y^p, (ya)^p \rangle = \langle y^p, u_p \rangle\), and claim that \(x\) induces an isomorphism in \(\hat{K}\). Indeed, otherwise 7.2.8 would imply that \(c(H) = 2\) and \(x|_H\) is an anti-isomorphism. Using (c), we would get

\[(a^x)^{p^r} = (a^x)^x = (y^{-1} ay)^x = y^x a^x (y^x)^{-1} = (a^x)^{p^r};\]

and, by (37), \(a^x = a\). But then \(H\) would be abelian, a contradiction. Thus \(x\) induces an isomorphism in \(\hat{K}\) and hence

\[((ya)^p)^x = (y^p u_p)^x \equiv (y^p)^x u_p = (y^p a^x)^p \pmod{L_3(K)^p}.\]

On the other hand, (35) and \(h_i(a)^x \in Z(\tilde{G})\) imply that

\[((ya)^p)^x = ((x^t a^x)^x)^p = ((x^t)^x a^x h_i(a)^x)^p = (y^p a^x)^p (h_i(a)^x)^p.\]

It follows that \(h_i(a)^p \in L_3(K)\). By (30), \(L_3(K) = K_3(K)\) and, since \(K \leq G^p\), (25) yields that \(L_3(K) \leq L_3(K) \leq K_3(K) \leq K_3(G^p) \leq K_3(G)^p \leq G^p\). By (24), \(h_i(a)^p = g^p\) for some \(g \in G\) and then (6) implies that \(h_i(a) \in G^p\). This holds for all primes \(p > c\); by (28), \(h_i(a) = 1\) and (e) holds.

Now (a), (d), and (e) yield that to prove the lemma, we only have to show that \(f(1, a) = 1\) for all \(a \in N\). To do this, however, we shall need some further steps. We put \(f(1, a) = f(a)\) for \(a \in N\), first derive some general properties of this function \(f: N \to L_3(G)\), then prove the desired result under additional assumptions on \(N\); the
general case follows. First note that the defining equation (36) now reads

\[(40) \ (a^x)^t = (a^x)^t f(a)^t \text{ for all } a \in N.\]

If \( \varphi|_N \) is an isomorphism, then \( ((ab)^x)^t = ((ab)^x)^t f(ab)^t = (a^x)^t (b^x)^t f(ab)^t \) for all \( a, b \in N \) and \( ((ab)^x)^t = (a^x)^t (b^x)^t x^x = (a^x)^t (b^x)^t f(a)^t f(b)^t \) since \( f(a)^t \in Z(\hat{G}) \); if \( \varphi|_N \) is an anti-isomorphism, \( ((ab)^x)^t = (ab)^x f(ab)^t = (b^x)^t (a^x)^t f(ab)^t \) and \( ((ab)^x)^t = (b^x)^t (a^x)^t f(a)^t f(b)^t \). In both cases, \( f(ab)^t = f(a)^t f(b)^t = (f(a) f(b))^t \), by (3). Since \( \varphi \) is bijective, it follows that

\[(41) \ f: N \to Z(G) \text{ is a homomorphism.}\]

Another consequence of (40), via a simple induction, is that

\[(42) \ (a^x)^{xt} = (a^x)^{xt} f(a^{x-t+1}) \text{ for all } a \in N, t \in \mathbb{N}.\]

Indeed, if \( t = 1 \), this is (40); and if (42) holds for \( t - 1 \), then (40), \( L_v(G)^t \leq Z(\hat{G}) \), and (41) yield that

\[ (a^x)^{xt} = ((a^x)^{t-1} f(a^x^{t-1}+\cdots+x) x^t) x^t = (a^x)^{xt} f(a^x^{t-1}+\cdots+x+1)^t. \]

This proves (42) and, raising both sides of this equation to the \( s \)-th power, we obtain

\[(43) \ ((a^x)^{xt})^s = ((a^x)^t)^s f(a^{x-t+1+s})^s \text{ for } a \in N, t \in \mathbb{N}, s \in \mathbb{Z}.\]

For every \( a \in N \), we define by induction \( a_0 = a \) and \( a_{i+1} = [a_i, x] \). We put \( a^{v_i} = f(a_i) \) and claim that for all \( i \geq 0 \),

\[(44) \ v_i: N \to Z(G) \text{ is a homomorphism.}\]

This is clear for \( i = 0 \) since \( v_0 = f \) is a homomorphism by (41). Since \( a_i^x = (a^x)_i \),

\[ a^{v_{i+1}} = f(a_{i+1}) = f(a_i^{-1} a_i^x) = f((a_i)^{-1} f((a_i)^x)) = (a^{v_i})^{-1} (a^x)^{v_i}; \]

therefore if \( v_i \) is a homomorphism, then since \( N^{v_i} \leq Z(G) \), it follows that for all \( a, b \in N \),

\[ (ab)^{v_{i+1}} = ((ab)^x)^{v_i} = (a^{v_i})^{-1} (a^x)^{v_i} (b^{v_i})^{-1} (b^x)^{v_i} = a^{v_i} b^{v_i}. \]

Thus \( v_{i+1} \) is also a homomorphism and (44) holds.

We study more closely the factor \( f(a^{x-t+1}) \) appearing in (42) and first claim that for \( t \geq 1 \),

\[(45) \ f(a^{x-t+1}) = \prod_{i=0}^{c-1} f(a_i)^{(i+1)} \]

For \( t = 1 \), both sides of this equation equal \( f(a) \); so suppose that (45) holds for \( t \). If \( s \in \mathbb{N} \), then \( a_1^{x-1} = [a, x]^{x-1} = [a^{x-1}, x] = a^{-x^t+1} x^t \) and hence \( a^x = a^{x-t} a_1^{x-1} \); fur-
thermore \((a_i)_i = a_{i+1}\). Using (41), we therefore obtain
\[
f(a^{x_1+\cdots+x+1}) = f(a^{x_1+\cdots+x+1})f(a_1^{x_1+\cdots+x+1})f(a)
\]
\[
= \left(\prod_{i=0}^{c-1} f(a_i)^{(i+1)}\right)\left(\prod_{i=0}^{c-1} f(a_{i+1})^{(i+1)}\right)f(a)
\]
\[
= \left(\prod_{i=0}^{c-1} f(a_i)^{(i+1)}+1\right)f(a_1)^{(c+1)}\prod_{i=0}^{c-1} f(a_i)^{(i+1)}
\]
\[
= \prod_{i=0}^{c-1} f(a_i)^{(i+1)}+1\prod_{i=0}^{c-1} f(a_i)^{(i+1)}
\]
since \(a_i \in K_{c+1}(G) = 1\). This proves (45).

For \(0 \leq i \leq c - 1\), we write \(c! \left(\begin{array}{c} t \\ i+1 \end{array}\right)\) as a polynomial in \(t\), that is, in the form
\[
(46) \quad c! \left(\begin{array}{c} t \\ i+1 \end{array}\right) = \sum_{j=1}^{c} \lambda_{ij} t^j \quad \text{where} \quad \lambda_{ij} \in \mathbb{Z}.
\]
Then we obtain from (45)
\[
f(a^{x_1+\cdots+x+1})c! = \prod_{i=0}^{c-1} f(a_i)^{\sum_{j=1}^{c} \lambda_{ij} t^j} = \prod_{j=1}^{c} \prod_{i=0}^{c-1} f(a_i)^{\lambda_{ij} t^j},
\]
that is
\[
(47) \quad f(a^{x_1+\cdots+x+1})c! = \prod_{j=1}^{c} g_j(a)^{t^j} \quad \text{where} \quad g_j(a) = \prod_{i=0}^{c-1} f(a_i)^{\lambda_{ij}}.
\]
By (46), \(\lambda_{01} = c!\) and \(\lambda_{11} = -\frac{1}{2} c!\) so that
\[
(48) \quad g_1(a) = f(a_0)^c f(a_1)^{-c/2} \ldots
\]
We can now prove the desired result in the crucial case.

(f) If \(G = \langle x, b \rangle\) and \(N = \langle b \rangle^G\), then \(f(a) = 1\) for all \(a \in N\) and hence \(x\) is an isomorphism.

Proof. Let \(i \in \mathbb{Z}\) and \(a = b^x\); let \(p > c\) be a prime and put \(K = \langle x^p, a^p \rangle\). Then \(x\) induces an isomorphism in \(\tilde{K}\); indeed, otherwise, by 7.2.8, \(H = \langle x, a \rangle\) would be of class 2 which contradicts (31). Thus \(((a^p)^{x^p})^p \equiv ((a^p)^{x^p})^p (\mod L_p(K)^p)\) and then (43) shows that \(f(a^{x_1^{p+1}+\cdots+x+1})p \in L_c(K)\). By (47),
\[
\prod_{j=1}^{c} g_j(a)^{p^j} = f(a^{x_1^{p+1}+\cdots+x+1})p \in L_c(K).
\]
As in the proof of (e), \(L_c(K) \leq L_3(K) = K_3(K) \leq K_3(G^p) \leq G^{p^3}\) and it follows that \(g_1(a)^{p^j} \ldots g_2(a)^{p^j} \ldots \in G^{p^3}\). Thus \(g_1(a)^{p^j} \in G^{p^3}\) and then (24) and (6) yield that \(g_1(a) \in G^p\). This holds for all \(p > c\) and therefore, by (28), \(g_1(a) = 1\), that is, \(g_1(b^x) = 1\). By (47) and (44), \(g_1\) is a homomorphism from \(N\) to \(Z(G)\) and we have just shown that its kernel contains \(\langle b^x | i \in \mathbb{Z} \rangle = \langle b \rangle^G = N\). Thus
\[
(49) \quad g_1(a) = 1 \quad \text{for all} \quad a \in N.
\]
Now suppose, for a contradiction, that there exists \( a \in N \) such that \( f(a) \neq 1 \). Then since \( a_i \in K_{i+1}(G) = 1 \) for \( i \geq c \), there exists \( k \in \{0, \ldots, c - 1\} \) such that \( f(a_k) \neq 1 \) and \( f(a_i) = 1 \) for all \( i > k \). By (48) with \( a \) replaced by \( a_k \),

\[
g_1(a_k) = f(a_k)^r f(a_{k+1})^{-1/2^k e^1} = f(a_k)^{e^1}
\]

so that (49) implies \( f(a_k)^{e^1} = 1 \). Since \( G \) is torsion-free, it follows that \( f(a_k) = 1 \), the desired contradiction. Thus \( f(a) = 1 \) for all \( a \in N \) and, by (a), (d), and (e), \( \alpha \) is an isomorphism. This proves (f).

We return to the general situation.

(g) Let \( b \in N \). Then (50) or (51) holds.

(50) \( (a^x)^y = (a^y)^{x^y} \) for all \( a \in N \).

(51) \( (a^x)^y = (a^y)^{(x^y)^{-1}} \) and \([xb, a] \in Z(G)\) for all \( a \in N \).

Proof. Let \( y = xb \). For \( a \in N \), define \( H = \langle y, a \rangle = \langle y, M \rangle \) where \( M = \langle a \rangle^H \leq H \) and let \( \psi \) be the projectivity induced by \( \varphi \) in \( H \). By 7.2.5, \( \alpha|H \) is a \( \psi \)-mapping and, since \( M \leq N \), \( \alpha|M \) is an isomorphism or an anti-isomorphism. So if \( \alpha \) induces an isomorphism in \( H \), the assumptions of 7.2.9 are satisfied with \( G \) and \( \alpha \) replaced by \( H \) and \( \alpha|H \); by (f), \( \alpha|H \) is an isomorphism and hence \( (a^x)^y = (a^y)^{x^y} \). And if \( \alpha \) does not induce an isomorphism in \( H \), we apply 7.2.8 with \( K = H = \langle y, a \rangle \), that is, \( r = t = 1 \) and \( s = 0 \); it follows that \([y, a] \in L_i(G) \leq Z(G) \) and \( \alpha|H \) is an anti-isomorphism, that is, \((a^x)^y = (y^{-1}a)^{x^y} = y^x a^x (y^x)^{-1} \). Thus we obtain that either

(52) \( (a^x)^y = (a^y)^{x^y} \) or

(53) \([y, a] \in Z(G)\) and \((a^x)^y = (a^y)^{(x^y)^{-1}}\).

Suppose, for a contradiction, that there exist \( u, v \in N \) such that \((u^x)^y = (u^y)^{x^y} \neq (u^x)^{(x^y)^{-1}} \) and \((v^x)^y = (v^y)^{(x^y)^{-1}} \neq (v^x)^{x^y} \). By (52) and (53) there exists \( e \in \{+1, -1\} \) such that \((a^x)^y = (a^y)^{(x^y)^{e}} \) where \( a = uv \). If \( \alpha|N \) is an isomorphism, it follows that

\[
(u^x)^y (v^x)^{(x^y)^{e-1}} = (u^x)^y (v^x)^{(x^y)^{e}} = ((uv)^x)^y = ((uv)^x)^{(x^y)^e} = (u^x)^{(y^e)} (v^x)^{(e^y)^e}.
\]

For \( e = 1 \), we obtain \((v^x)^{(x^y)^{-1}} = (v^x)^{x^y} \) and if \( e = -1 \), \((u^x)^y = (u^x)^{(y^e)^{-1}} \); neither is the case. Similarly, if \( \alpha|N \) is an anti-isomorphism, we get the same contradiction. So we see that the equations in (52) or (53) are satisfied simultaneously for all \( a \in N \). Thus either (50) holds or every \( a \in N \) satisfies the equation in (51). In the latter case, either \([y, a] \in Z(G)\) by (53), or (52) holds for \( a \) and then, by (37), \([y, a] = 1 \in Z(G)\). Thus (51) holds and this proves (g).

(h) For all \( a \in N \), \( f(a) = 1 \), that is, \((a^x)^y = (a^y)^x\).

Proof. The assertion is that (50) holds for \( b = 1 \). Thus by (g), we may suppose that (51) holds for \( b = 1 \), that is

(54) \( (a^x)^y = (a^y)^{(x^y)^{-1}} \) for all \( a \in N \).
If \([xb, d] \in Z(G)\) for all \(b, d \in N\), then \(G = N \langle x \rangle\) would imply that \(G' \leq Z(G)\) and this would contradict (31). Thus there exist \(b, d \in N\) such that
\[
(55) \quad [xb, d] \notin Z(G).
\]
By (g), such an element \(b\) satisfies (50) and, since \(x\) induces an isomorphism in \(\tilde{G}\), \((xb)^a \equiv x^a b^a \pmod{Z(\tilde{G})}\). It follows that
\[
(56) \quad (ab)^a = (a')^b = x'b' \quad \text{for all} \quad a \in N.
\]
So if \(\alpha|_n\) is an isomorphism, \(((a^x)^b)^+ = (a^x b^a)^a = (b^{-1} a^x b)^a = (b^x)^a b^a = ((a^x)^b)^+\) and hence \((a^x)^a = (a^x)^x\), as desired. Therefore suppose, for a contradiction, that \(\alpha|_n\) is an anti-isomorphism. Then (56) and (54) imply that \((a^x b)^a = (a^x b)^a = (b^{-1} a^x b)^a = b^a(a^x)^a(b^x)^{-1} = (a^x)^{(a^x^{-1} b^x)^{-1}}\) for all \(a \in N\) and hence \((x^a)^2 \equiv (b^a)^{-2} \pmod{C(\tilde{N})^o}\). By (7), \(G/C(\tilde{N}^o)\) is torsion-free and therefore by (6), \(x^a \equiv (b^a)^{-1} \pmod{C(\tilde{N}^o)}\), that is, \(x^a b^x \in C(\tilde{N}^o)\). Now (56) yields \((a^x b)^a = a^a\) and hence \(a^x b = a\) for all \(a \in N\); this contradicts (55). Thus (h) holds and Lemma 7.2.9 follows from (a), (d), (e), and (h).

The following lemma finishes the proof of Theorem 7.2.7.

**Lemma.** \(x\) is an isomorphism or an anti-isomorphism.

**Proof.** Let \(X\) be the set of all the subgroups \(H\) of \(G\) for which \(x|_H\) is an isomorphism or an anti-isomorphism. Since \(G\) is finitely generated, \(L(G)\) satisfies the maximal condition, by (27), and therefore \(X\) contains a maximal element \(N\). We have to show that \(N = G\). So suppose, for a contradiction, that \(N \neq G\). Then since \(G\) is nilpotent, there exists \(x \in N_G(N)\setminus N\); let \(H = \langle N, x \rangle\) and \(\psi\) be the projectivity induced by \(\varphi\) in \(H\). Then \(H \notin X\) and hence, by (33), \(c(H) = c\). By 7.2.5, \(x|_H\) and \(x|_{\tilde{H}}\), where \(g' = g^{-1}\) for all \(g \in \tilde{G}\), are the two \(\psi\)-mappings and (34) implies that \(x|_{\tilde{H}}\) or \(x|_{H}\) induces in \(\tilde{H}\) an isomorphism. By 7.2.9, this map is then an isomorphism from \(H\) onto \(H^o\). It follows that \(H \in X\), a contradiction. Thus \(N = G\) and the lemma follows.

The main theorem

**Theorem (Sadovskii [1964]).** Every projectivity of a nonabelian torsion-free locally nilpotent group is induced by a unique isomorphism.

**Proof.** Let \(G\) be a nonabelian torsion-free locally nilpotent group and let \(\varphi\) be a projectivity from \(G\) to a group \(\tilde{G}\). By 1.5.8, \(\varphi\) is induced by at most one isomorphism. By 1.3.6, we may assume that \(G\) is finitely generated since the set of nonabelian finitely generated subgroups is a local system of subgroups of \(G\). Thus \(G\) is nilpotent. If \(c(G) = 2\), the assertion follows from 7.2.6, and if \(c(G) \geq 3\), then 7.2.5 and 7.2.7 imply that there exists an isomorphism inducing \(\varphi\).

We combine Theorem 7.2.11 and Sadovskii's Approximation Theorem to obtain the following result.
7.2.12 Theorem. Let $G$ be a nonabelian group and let $\mathcal{S}$ be a family of normal subgroups of $G$ such that
(a) for every $X, Y \in \mathcal{S}$ there exists $Z \in \mathcal{S}$ with $Z \leq X \cap Y$,
(b) $\bigcap_{X \in \mathcal{S}} X = 1$, and
(c) $G/N$ is torsion-free and locally nilpotent for every $N \in \mathcal{S}$.
Then every projectivity of $G$ is induced by a unique isomorphism.

Proof. Let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$. By (b) and (c), $G$ is torsion-free and hence 1.5.8 implies that $\varphi$ is induced by at most one isomorphism. Let $\mathcal{S} = \{X \in \mathcal{S} | G' \leq X\}$. Then, clearly, (a) and (c) hold with $\mathcal{S}$ replaced by $\mathcal{S}$. And (b) implies that for $1 \neq g \in G$, there exist $X, Y \in \mathcal{S}$ such that $g \notin X$ and $G' \leq Y$; by (a) there exists $Z \in \mathcal{S}$ such that $Z \leq X \cap Y$. Then $Z \in \mathcal{S}$ and $g \notin Z$; since $G/Z$ is torsion-free, it follows that $\langle g \rangle \cap Z = 1$. By 6.5.1 and 7.2.11, $N^\circ \leq \overline{G}$ for every $N \in \mathcal{S}$ and the projectivity induced by $\varphi$ in $G/N$ is induced by a unique isomorphism from $G/N$ onto $\overline{G}/N^\circ$. By 1.3.8, $\varphi$ is induced by an isomorphism from $G$ to $\overline{G}$. $\square$

It is well-known (see Robinson [1982], p. 159) that if $F$ is a free group, $\bigcap_{i \in N} K_i(F) = 1$ and $F/K_i(F)$ is torsion-free. Thus Theorem 7.2.12 yields another proof for the fact (see 7.1.18) that every projectivity of a nonabelian free group is induced by a unique isomorphism. Another important class of groups which can be approximated by torsion-free nilpotent groups is the class of free polynilpotent groups (see Smelkin [1964]). So we have the following result.

7.2.13 Corollary (Sadovskii [1965a]). Every projectivity of a free polynilpotent group (in particular, of a free soluble group of given derived length) is induced by a unique isomorphism.

Exercises

1. Give a lattice-theoretic characterization of the $n$-th centre of a torsion-free nilpotent group.

2. (Scott [1957]) Let $\alpha$ be a bijective map from the group $G$ to the group $\overline{G}$ such that $(xy)^2 = x^2y^2$ or $(xy)^2 = y^2x^2$ for all $x, y \in G$. Show that $\alpha$ is an isomorphism or an anti-isomorphism. (Hint: First show that $\alpha$ satisfies (9) and (21).)

7.3 Mixed nilpotent groups

We would like to prove for mixed and periodic nilpotent groups analogues of the results for torsion-free nilpotent groups. However, this is too much to expect since there are examples of nilpotent and nonnilpotent groups with isomorphic subgroup lattices and of projectivities between nonisomorphic nilpotent groups. For example,
in 6.2.9 we noted that the semidirect product $\tilde{G} = T\langle z \rangle$ of an abelian group $T$ of type $p^\infty$ and an infinite cyclic group $\langle z \rangle$ with respect to the automorphism $t \mapsto t^{1+p}$ ($t \in T$) is lattice-isomorphic to the direct product $G = T \times \langle z \rangle$. Clearly, $G$ is abelian and $|Z_n(\tilde{G})| = p^n$ for all $n \in \mathbb{N}$ so that $\tilde{G}$ is not nilpotent.

**Finitely generated groups**

We want to show that the situation is better for finitely generated nonperiodic nilpotent groups. Such a group $G$ has a finite torsion subgroup $T(G)$, and if one constructs a central series in $G$ containing $T(G)$, it is well-known (see Robinson [1982], p. 133) that one can take infinite cyclic factor groups above $T(G)$ and cyclic factor groups of prime order below $T(G)$. Thus $L(G)$ has a cyclic modular chain in the following sense.

**7.3.1 Definition.** A modular chain $0 = a_0 \leq \cdots \leq a_n = I$ in a complete lattice $L$ is called cyclic if there exists $k \in \{0, \ldots, n-1\}$ such that $[a_i/a_{i-1}] \cong L(C_2)$ for $i = 1, \ldots, k$ and $[a_i/a_{i-1}] \cong L(C_r)$ for $i = k + 1, \ldots, n$; recall that $C_r$ is the cyclic group of order $r$.

**7.3.2 Theorem.** The group $G$ is finitely generated nonperiodic nilpotent if and only if $L(G)$ has a cyclic modular chain.

**Proof.** Let $1 = H_0 \leq \cdots \leq H_n = G$ be a cyclic modular chain in $L(G)$. We have to show that $G$ is finitely generated, nonperiodic, and nilpotent. For this we shall need the following assertion which we prove by induction on $i = 0, \ldots, n$.

\((*)\) If $x \in G$ is of finite order, then $[\langle H_i, x \rangle / H_i]$ is finite and distributive.

Indeed, for $i = 0$, $[\langle H_i, x \rangle / H_i]$ is finite and distributive. If $[\langle H_i, x \rangle / H_i]$ has this property, then $\langle H_i, x \rangle$ is a cyclic element in $[G/H_i]$ and, since $H_i$ is modularly embedded in this lattice, $[\langle H_{i+1}, x \rangle / H_i]$ is a modular lattice. By 2.1.5, $[\langle H_{i+1}, x \rangle / H_{i+1}] = [H_{i+1} \cup \langle H_i, x \rangle / H_{i+1}]$ is isomorphic to $[\langle H_i, x \rangle / H_i] \cap H_{i+1}]$, and this is an interval in $[\langle H_i, x \rangle / H_i]$, hence is finite and distributive. Thus \((*)\) holds for $i = 0, \ldots, n$.

We now prove the statements on $G$ by induction on $n$, the length of the cyclic modular chain in $L(G)$; let $k$ be as in Definition 7.3.1. If $n = 1$, then $k = 0$ and so $L(G) \cong L(C_\infty)$. By 1.2.6, $G \cong C_\infty$ is finitely generated nonperiodic nilpotent. So let $n > 1$ and suppose that the assertion is correct for groups with cyclic modular chains of smaller lengths. If $k = 0$, then $[H_{i+1} / H_i] \cong L(C_\infty)$ for all $i$ and hence $G$ is torsion-free. Indeed, if $1 \neq x \in G$ had finite order, there would exist a maximal $i \in \{0, \ldots, n\}$ such that $x \notin H_i$; by \((*)\), $[\langle H_i, x \rangle / H_i]$ would be a nontrivial finite interval in $[H_{i+1} / H_i]$, which is impossible in $L(C_\infty)$. Thus by 7.2.2, $H_1 \leq Z(G)$ and the induction assumption implies that $G/H_1$ is finitely generated, nonperiodic and nilpotent. Since $C_\infty \cong H_1 \leq Z(G)$, the group $G$ also has this property.

Therefore let $k > 0$. Then $H_i$ is cyclic of prime order $p$. Let $x \in G \setminus H_{n-1}$. If $x$ had finite order, then by \((*)\), $[\langle H_{n-1}, x \rangle / H_{n-1}]$ would be finite and nontrivial and this
again is impossible since $[G/H_{n-1}] \cong L(C_n)$. Hence $o(x) = \infty$ and $L(<H_1,x>)$ is modular since $H_1$ is modularly embedded in $L(G)$. By 2.4.11, $H_1 \leq <H_1,x>$ and $x$ induces a power automorphism $a \mapsto a^r$ in $H_1$ for which $r \equiv 1 \pmod{p}$. Thus $x$ centralizes $H_1$. Since $G$ is generated by the elements $x \in G\setminus H_{n-1}$, it follows that $H_1 \leq Z(G)$. By induction, $G/H_1$ is finitely generated, nonperiodic and nilpotent; since $|H_1| = p$, the group $G$ also has this property.

An easy consequence of Theorem 7.3.2 is the following lattice-theoretic characterization of the class of nonperiodic locally nilpotent groups.

7.3.3 Theorem. The group $G$ is nonperiodic and locally nilpotent if and only if there exists a cyclic element $X$ in $L(G)$ such that for every finite set of cyclic elements $X_1, \ldots, X_n$ in $L(G)$, the lattice $[X \cup X_1 \cup \cdots \cup X_n/1]$ has a cyclic modular chain.

Proof. If $G$ is a nonperiodic locally nilpotent group, take $x \in G$ of infinite order and put $X = <x>$. Then for every finite set of cyclic elements $X_1, \ldots, X_n$ in $L(G)$, $H = <X, X_1, \ldots, X_n>$ is a nonperiodic finitely generated and hence nilpotent subgroup of $G$. By 7.3.2 there exists a cyclic modular chain in $L(H) \cong \{H/1\}$. Conversely, suppose that $G$ satisfies our condition, and take a finite subset $S$ of $G$. If $X_1, \ldots, X_n$ are the subgroups generated by the elements of $S$ and $H = <X, X_1, \ldots, X_n>$, then $L(H)$ has a cyclic modular chain and, by 7.3.2, $H$ is nilpotent and nonperiodic. In particular, $G$ is nonperiodic, $<S>$ is nilpotent and thus $G$ is locally nilpotent.

It follows from Theorems 7.3.2 and 7.3.3 that the classes of nonperiodic finitely generated nilpotent and of nonperiodic locally nilpotent groups are invariant under projectivities, a result due to Pekelis [1961b]. Note that the order of succession of the cyclic intervals in Definition 7.3.1 is important. Indeed, the subgroup lattice of the direct product $G$ of an infinite cyclic group and a nonabelian group of order $pq$, $p$ and $q$ primes, has a modular chain $1 = H_0 < H_1 < H_2 < H_3 = G$ with $[H_1/H_0] \cong L(C_2)$ and $[H_i/H_{i-1}] \cong L(C_2)$ for $i > 1$; but $G$ is not nilpotent.

Groups with torsion-free subgroups

In the light of Sadovskii's theorem on torsion-free nilpotent groups it is reasonable to expect that Baer's theorem on abelian groups with two independent elements of infinite order might generalize to nilpotent groups. However, the following example shows that this is not the case.

7.3.4 Example (Pekelis [1965]). Let $G = <a, b | [a, b]^3 = [[a, b], a] = [[a, b], b] = 1>$. If we put $c = [b, a]$, then $G' = <c> \leq Z(G) = <a^3> \times <b^3> \times <c>$; thus $G$ is nilpotent of class 2 and possesses two independent elements $a$ and $b$ of infinite order. Every $g \in G$ can be written uniquely in the form $g = zr$ where $z \in Z(G)$ and $r \in R = \{a^ib^j | 0 \leq i, j \leq 2\}$. We define a bijective map $\sigma : G \to G$ by $g^\sigma = z^r r^\sigma$ where $r^\sigma = r$ for all $r \in \{1, a, a^2, b, b^2, ab\}$, $r^\sigma = r^c$ for $r \in \{a^2b, a^b, a^2b^2\}$ and $\sigma|_{Z(G)}$ is the automorphism satisfying $(a^3)^\sigma = a^3$, $(b^3)^\sigma = b^3$, $c^\sigma = c^2$. It is easy to check
that \( \sigma^2 = 1 \) and that \( \sigma \) satisfies the assumptions of Theorem 1.3.1; thus \( \sigma \) induces a nontrivial autoprojectivity \( \varphi \) in \( G \). Since \( \langle a \rangle^\sigma = \langle a \rangle \), \( \langle b \rangle^\sigma = \langle b \rangle \), and \( \langle ab \rangle^\sigma = \langle ab \rangle \), we see that \( \varphi \) cannot be induced by an automorphism of \( G \). \( \square \)

So it is clear that we need stronger assumptions for a nilpotent group \( G \) to obtain that every projectivity of \( G \) is induced by an isomorphism. In this spirit, Pekelis [1967] proved that a nilpotent group of class 2 with a torsion-free subgroup of the same class has this property. On the other hand, he gave an example showing that this assertion does not hold with 2 replaced by 3, and Arshinov [1971] produced similar examples for all \( c \geq 3 \) (see Exercise 2). Further results of this type, mainly for groups with torsion-free direct factors, can also be found in Arshinov [1971]. We state the most interesting general result in this direction without proof.

**7.3.5 Theorem (Yakovlev [1988]).** Let \( n \in \mathbb{N}, n \geq 2. \)

(a) If \( G \) is a nilpotent group of class \( n \) containing a subgroup isomorphic to a free nilpotent group of class \( n \), then \( G \) is strongly determined by its subgroup lattice.

(b) If \( K \) is a torsion free nilpotent group of class \( n \geq 3 \) generated by 2 elements and \( K \) is not a free nilpotent group of class \( n \), then there exist a nilpotent group \( G \) of class \( n \) containing \( K \) as a subgroup and a projectivity of \( G \) which is not induced by an isomorphism.

We finally mention that for a nilpotent group \( G \), the existence of two independent elements of infinite order does not imply that \( G \) is determined by its subgroup lattice.

**7.3.6 Example (Arshinov [1971]).** Let \( A \) be a torsion-free abelian group, \( p \) a prime and \( n \in \mathbb{N} \) such that \( 4 \leq n \leq p \). For \( \gamma_1, \gamma_2 \in \{1, \ldots, p - 1\} \), let \( B_i = G_{\gamma_i} \) be the group of order \( p^n \) constructed in 5.6.7 and, finally, \( G = A \times B_1 \) and \( \overline{G} = A \times B_2 \). By (b) of 5.6.7 there exists a bijective map \( \tau: B_1 \to B_2 \) inducing a projectivity from \( B_1 \) to \( B_2 \) and whose restriction to every maximal subgroup of \( B_1 \) is an isomorphism; let \( \sigma: G \to \overline{G} \) be defined by \( (ab)^\sigma = ab^\tau \) for \( a \in A, b \in B_1 \). The reader may show that \( \sigma \) satisfies the assumptions of Theorem 1.3.1 and therefore induces a projectivity from \( G \) to \( \overline{G} \). By (a) of 5.6.7, \( G \neq \overline{G} \), in general. \( \square \)

**Normalizer preserving projectivities**

By 5.6.2, a normalizer preserving projectivity of a nilpotent group maps central series to central series. We study the projectivities induced in the central factors. For this we need the following result on multilinear mappings.

**7.3.7 Lemma.** Let \( A_1, \ldots, A_i, L, M \) be (additive) abelian group, \( \varphi \) a projectivity from \( L \) to \( M \) and suppose that \( f: (A_1, \ldots, A_i) \to L \) and \( g: (A_1, \ldots, A_i) \to M \) are such that

1. \( f \) and \( g \) are multilinear, that is, additive in every component,
2. \( L = \langle f(x_1, \ldots, x_i) | x_i \in A_i \rangle, M = \langle g(x_1, \ldots, x_i) | x_i \in A_i \rangle \), and
3. \( \langle f(x_1, \ldots, x_i) \rangle^\varphi = \langle g(x_1, \ldots, x_i) \rangle \) for all \( x_i \in A_i \).
Then there exists an isomorphism \( \alpha \) from \( L \) onto \( M \) such that

\[
(4) \quad f(x_1, \ldots, x_t)^\alpha = g(x_1, \ldots, x_t) \quad \text{for all} \quad x_i \in A_i.
\]

**Proof.** We use induction on \( t \). For \( t = 1 \), \( f \) and \( g \) are epimorphisms from \( A_1 \) onto \( L \) and \( M \), respectively, and by (3), \( \text{Ker} f = \text{Ker} g \). Then the map \( \alpha \colon L \to M \) such that \( f(x)^\alpha = g(x) \) (\( x \in A_1 \)) is well-defined and an isomorphism satisfying (4). So let \( t \geq 2 \), and assume that the lemma is correct for smaller numbers of abelian groups \( A_i \). First note that the assertion of the lemma is equivalent to the following.

(5) If \( C \) is a finite subset of \( A = (A_1, \ldots, A_n) \), then \( \sum_{x \in C} f(x) = 0 \) if and only if \( \sum_{x \in C} g(x) = 0 \).

Indeed, if \( \alpha \colon L \to M \) is an isomorphism satisfying (4), then

\[
\left( \sum_{x \in C} f(x) \right)^\alpha = \sum_{x \in C} g(x)
\]

for every finite subset \( C \) of \( A \); in particular, (5) holds. Conversely, suppose that (5) is satisfied. By (2), for every \( w \in L \) there exists a finite subset \( C \) of \( A \) such that \( w = \sum_{x \in C} f(x) \) and we put \( w^\alpha = \sum_{x \in C} g(x) \). Then (5) and (1) imply that \( \alpha \) is well-defined and injective; by (2), \( \alpha \) is surjective and the additivity of \( \alpha \) and (4) follow directly from the definition of \( \alpha \).

Now suppose that \( C \) is a finite subset of \( A \). Every \( x \in C \) has the form \( x = (x_1, \ldots, x_t) \) where \( x_i \in A_i \). For \( i = 1, \ldots, t \), we put \( A_i^* = \langle x_i \mid x \in C \rangle \leq A_i \); furthermore \( A^* = (A_1^*, \ldots, A_t^*) \), \( f^* = f|_{A^*} \), \( g^* = g|_{A^*} \), \( L^* = \langle f^*(a) \mid a \in A^* \rangle \), \( M^* = \langle g^*(a) \mid a \in A^* \rangle \), and consider the projectivity \( \phi^* \) induced by \( \phi \) in \( L^* \). Clearly, (1)–(3) hold for the starred groups and maps. So if we can prove (5) for these, then, since \( C \) is a subset of \( A^* \),

\[
\sum_{x \in C} f(x) = 0 \iff \sum_{x \in C} f^*(x) = 0 \iff \sum_{x \in C} g^*(x) = 0 \iff \sum_{x \in C} g(x) = 0,
\]

as desired. Thus we may assume that all the \( A_i \) are finitely generated. Since \( f \) is multilinear, it follows that \( L \) too is finitely generated and therefore a direct sum of cyclic groups. Since every cyclic group is residually a cyclic primary group, there exist subgroups \( L_i \) of \( L \) (\( i \in I \)) such that \( L/L_i \) is cyclic of prime power order for all \( i \in I \) and \( \bigcap_{i \in I} L_i = 0 \). Let \( M_i = L_i^p \) and define \( f_i \colon A \to L/L_i \) and \( g_i \colon A \to M/M_i \) by

\[
f_i(x) = f(x) + L_i \quad \text{and} \quad g_i(x) = g(x) + M_i.
\]

Then again (1)–(3) hold for \( f_i \), \( g_i \), and the projectivity \( \phi_i \) induced by \( \phi \) in \( L/L_i \); in addition, since \( \bigcap_{i \in I} L_i = 0 \), also \( \bigcap_{i \in I} M_i = 0 \). Thus if (5) holds for cyclic groups of prime power order, then

\[
\sum_{x \in C} f(x) = 0 \iff \sum_{x \in C} f(x) \in L_i \quad \text{for all} \quad i \iff \sum_{x \in C} g(x) \in M_i \quad \text{for all} \quad i \iff \sum_{x \in C} g(x) = 0,
\]

as desired. Therefore we may assume for the proof of the lemma that

(6) \( L \) is cyclic of order \( p^m \), \( p \) a prime, \( m \in \mathbb{N} \).
As a projective image of $L$, $M$ is cyclic of order $q^m$, $q \in \mathbb{P}$. For $k \in \mathbb{N}$ and $x = (x_1, \ldots, x_t) \in A$, \( \langle kf(x) \rangle^\sigma = \langle f(kx_1, x_2, \ldots, x_t) \rangle^\sigma = \langle g(kx_1, x_2, \ldots, x_t) \rangle = \langle kg(x) \rangle \).

Hence $f(x)$ and $g(x)$ have the same order and (2) implies that $p = q$. We may therefore assume that

(7) $M = L$.

Then $\phi$ is the trivial autoprojectivity and (3) becomes

(8) $\langle f(x) \rangle = \langle g(x) \rangle$ for all $x \in A$.

Therefore there exists $k_x \in \mathbb{Z}$ such that $(k_x, p) = 1$ and $g(x) = k_x f(x)$. Let $r_x$ denote the order of $f(x)$ in the group $L$. Then we claim that

(9) $k_x \equiv k_y \pmod{r_y}$ for all $x, y \in A$ such that $r_x \geq r_y > 1$.

This will prove the lemma. Indeed, by (2) there exists $z \in A$ such that $\langle f(z) \rangle = L$ and, if we put $k = k_x$, then $k \equiv k_y \pmod{r_y}$ and hence $kf(y) = k_y f(y) = g(y)$ for all $y \in A$. Thus the map $x: L \to L$ defined by $w^z = kw$ $(w \in L)$ is an automorphism of $L$ satisfying $f(y)^z = g(y)$ for all $y \in A$.

It remains to prove (9). For this take $x = (x_1, \ldots, x_t) \in A$ and $y = (y_1, \ldots, y_t) \in A$ such that $r_x \geq r_y > 1$. Consider the maps $\sigma$, $\tau$ from $A_t$ to $L$ defined by $a^\sigma = f(x_1, \ldots, x_{t-1}, a)$ and $a^\tau = f(y_1, \ldots, y_{t-1}, a)$ for $a \in A_t$. As $f$ is multilinear, $\sigma$ and $\tau$ are homomorphisms; and $A_t^\sigma \neq 0 \neq A_t^\tau$, since $x^\sigma = f(x)$, $y^\sigma = f(y)$, and $r_x \geq r_y > 1$. Therefore $pA_t^\sigma$ and $pA_t^\tau$ are subgroups of index $p$ in $A_t^\sigma$ and $A_t^\tau$, respectively, and it follows that their preimages $\sigma^{-1}(pA_t^\sigma)$ and $\tau^{-1}(pA_t^\tau)$ are subgroups of index $p$ in $A_t$.

Since a group cannot be the set-theoretic union of two proper subgroups, there exists $d \in A_t$ such that $d \notin \sigma^{-1}(pA_t^\sigma)$ and $d \notin \tau^{-1}(pA_t^\tau)$. Then $d^\sigma \notin pA_t^\sigma$ and $d^\tau \notin pA_t^\tau$ so that $\langle d^\sigma \rangle = A_t^\sigma$ and $\langle d^\tau \rangle = A_t^\tau$. Let $u = (x_1, \ldots, x_{t-1}, d)$ and $v = (y_1, \ldots, y_{t-1}, d)$. Then $f(u) = d^\sigma$ and $f(v) = d^\tau$, so that $A_t^\sigma = \langle f(u) \rangle$ and $A_t^\tau = \langle f(v) \rangle$. Since $f(x) = x^\sigma \in A_t^\sigma = \langle f(u) \rangle$ and, similarly, $f(y) = y^\tau \in \langle f(v) \rangle$, it follows that

(10) $r_x \leq r_u$ and $r_y \leq r_v$.

We define $d: A_t \to L$ and $e: A_t \to L$ with respect to $g$ in the same way as $d$, $e$ for $f$, that is, $a^d = f(x_1, \ldots, x_{t-1}, a)$ and $a^e = f(y_1, \ldots, y_{t-1}, a)$ for all $a \in A_t$. By (8), $A_t^d = A_t^e$ is a subgroup $L$ of $L$ and we may apply the lemma in the case $t = 1$ to the homomorphisms $d$ and $e$ from $L$ to $L$. We obtain an isomorphism $\beta: \tilde{L} \to \tilde{L}$ satisfying $a^\sigma d^\sigma a^{-1} = d^e$ for all $a \in A_t$. For $a = x_t$ and $a = d$, this yields $f(x)^d = f(x)$ and $f(u)^d = g(u)$. Since automorphisms of $L$ are multiplications with integers prime to $p$, there exists $i \in \mathbb{N}$ such that $g(x) = if(x)$ and $g(u) = if(u)$. It follows that $k_x f(x) = g(x) = if(x)$ and hence $k_x \equiv i \pmod{r_x}$; similarly, $k_y \equiv i \pmod{r_y}$. Since $r_x \leq r_u$, finally,

(11) $k_x \equiv k_y \pmod{r_x}$.

In the same way, applying the lemma in the case $t = 1$ to $\tau$ and $\tau'$, we obtain

(12) $k_x \equiv k_y \pmod{r_y}$.

Finally, for $d \in A_t$ chosen above, there are multilinear mappings $\bar{f}$ and $\bar{g}$ from $(A_1, \ldots, A_{t-1})$ into $\tilde{L} = \langle f(z_1, \ldots, z_{t-1}, d) \mid z_i \in A_i \rangle$ defined by $\bar{f}(z_1, \ldots, z_{t-1}) = f(z_1, \ldots, z_{t-1}, d)$ and $\bar{g}(z_1, \ldots, z_{t-1}) = g(z_1, \ldots, z_{t-1}, d)$. By the induction assumption
there exists an automorphism \( \delta \) of \( \tilde{L} \) such that \( f(z_1, \ldots, z_{t-1})^\delta = \tilde{g}(z_1, \ldots, z_{t-1}) \) for all \( z_i \in A_i \). In particular,

\[
f(u)^\delta = f(x_1, \ldots, x_{t-1}, d)^\delta = f(x_1, \ldots, x_{t-1})^\delta = \tilde{g}(x_1, \ldots, x_{t-1}) = g(u)
\]

and, similarly, \( f(v)^\delta = g(v) \). Again there exists an integer \( j \) such that \( g(u) = jf(u) \) and \( g(v) = jf(v) \), and it follows that \( k_x \equiv j \pmod{r_x} \) and \( k_v \equiv j \pmod{r_v} \). Thus \( k_x \equiv k_v \pmod{r} \) where \( r = \min(r_x, r_v) \). Now (10) and the assumption \( r_x \geq r_y \) yield that \( r \geq r_y \) and then, by (11) and (12), \( k_x \equiv k_u \equiv k_v \equiv k_y \pmod{r_y} \). This proves (9) and the lemma.

We study properties of a fixed normalizer preserving projectivity between two groups \( G \) and \( \tilde{G} \). It is convenient for this purpose to represent \( G \) and \( \tilde{G} \) as factor groups of an auxiliary group \( F \). In the applications, \( F \) will be a suitable free or relatively free group.

So let \( G, \tilde{G}, F \) be groups, \( \varphi \) a projectivity from \( G \) to \( \tilde{G} \), \( \lambda: F \to G \) and \( \mu: F \to \tilde{G} \) epimorphisms. We say that \( \varphi \) is compatible with the pair \( (\lambda, \mu) \) if \( K^\lambda = K^\mu \) for all \( K \in L(F) \). More generally, we say that \( \varphi \) is compatible with the pair \( (\lambda, \mu) \) on the section \( P/Q \) of \( F \) if \( K^\lambda = K^\mu \) whenever \( Q < K < P \), that is, if \( \varphi \) induces a projectivity from \( P/Q^\lambda \) to \( P/Q^\mu \) which is compatible with the restrictions \( \lambda', \mu' \) of \( \lambda, \mu \) to \( P/Q \).

7.3.8 Remark. If \( \varphi \) is compatible with the pair \( (\lambda, \mu) \), then the map \( \sigma: G \to \tilde{G} \) defined by \( (x^\lambda)^\varphi = x^\mu \) (\( x \in F \)) is an isomorphism from \( G \) onto \( \tilde{G} \) inducing \( \varphi \).

Proof. For every \( K \leq F \), \( K^\lambda = K^\mu \). Since \( \varphi \) is a projectivity, it follows that \( K^\mu = 1 \) if and only if \( K^\lambda = 1 \). Thus \( \operatorname{Ker} \lambda = \operatorname{Ker} \mu \) and \( \sigma \) is an isomorphism. For every \( H \leq G \), there exists \( K \leq F \) such that \( K^\lambda = H \) and then \( H^\varphi = K^\lambda \varphi = K^\mu = H^\mu \). Thus \( \varphi \) is induced by \( \sigma \).

7.3.9 Theorem. Let \( G, \tilde{G}, F \) be groups, \( \lambda: F \to G \) and \( \mu: F \to \tilde{G} \) epimorphisms and \( \varphi \) a normalizer preserving projectivity from \( G \) to \( \tilde{G} \). Let \( P_i/Q_i, \ldots, P_t/Q_t \) be central sections of \( F \), that is, \( [P_i, F] \leq Q_i \) for \( i = 1, \ldots, t \), on each of which \( \varphi \) is compatible with \( (\lambda, \mu) \). Finally, let

\[
P = [P_1, \ldots, P_t] \quad \text{and} \quad Q = [Q_1, P_2, \ldots, P_t][P_1, Q_2, P_3, \ldots, P_t] \ldots [P_1, \ldots, P_{t-1}, Q_t].
\]

Then \( P/Q \) is a central section of \( F \) and \( \varphi \) is compatible with \( (\lambda, \mu) \) on \( P/Q \).

Proof. The theorem is trivial for \( t = 1 \). And it suffices to prove the assertion for \( t = 2 \); the theorem for \( t \) sections will then follow by induction. Indeed, suppose that \( t \geq 3 \) and the theorem holds for \( t - 1 \) sections. Then if \( \tilde{P} = [P_1, \ldots, P_{t-1}] \) and \( \tilde{Q} = [Q_1, P_2, \ldots, P_{t-1}][P_1, Q_2, P_3, \ldots, P_{t-1}] \ldots [P_1, \ldots, P_{t-2}, Q_{t-1}] \), by induction, \( \tilde{P}/\tilde{Q} \) is a central section of \( F \) on which \( \varphi \) is compatible with \( (\lambda, \mu) \); and the theorem for \( t = 2 \) applied to \( \tilde{P}/\tilde{Q} \) and \( P_i/Q_i \), yields the same for \( P^*/Q^* \) where \( P^* = [\tilde{P}, P_t] = \ldots \).
mixed nilpotent groups

\[ [P_1, \ldots, P_t] = P \]

\[ Q^* = [\tilde{Q}, P_1][\tilde{P}, Q] \]

\[ = [Q_1, P_2, \ldots, P_t, \ldots, P_{r-2}, Q_{r-1}, P_r][P_1, \ldots, P_{r-1}, Q_r] = Q, \]

that is, for \( P/Q \).

So suppose that \( t = 2, P = [P_1, P_2] \) and \( Q = [Q_1, P_2][P_1, Q_2] \). By the Three Subgroup Lemma (see (7) of § 1.5), \([P, F] = [P_1, P_2, F] \leq [F, P_1, P_2][P_2, F, P_1] \leq [Q_1, P_2][Q_2, P_1] = Q\), that is, \( P/Q \) is a central section of \( F \). Let \( u, v \in P_1 \) and \( x, y \in P_2 \). Then \([u, x] \in P \) and, since \( P/Q \leq Z(G/Q) \),

\[ (13) \ [uv, x] = [u, x] [v, x] \equiv [u, x] [v, x] \pmod{Q}. \]

Similarly,

\[ (14) \ [u, xy] \equiv [u, x] [u, y] \pmod{Q}. \]

If we choose \( v \in Q_1 \) and \( y \in Q_2 \), then \([v, x] \) and \([u, y] \) lie in \( Q \) so that \([uv, x] = [u, x] \equiv [u, x] \pmod{Q} \). It follows that the map \((P_1/Q_1, P_2/Q_2) \rightarrow P/Q\) sending \((uQ_1, xQ_2)\) to \([u, x]Q\) is well-defined and, by (13) and (14), bilinear. Since \( \lambda \) and \( \mu \) are homomorphisms, the maps

\[ f: (P_1/Q_1, P_2/Q_2) \rightarrow P^\lambda/Q^\lambda; \quad (uQ_1, xQ_2) \mapsto [u^\lambda, x^\lambda]Q^\lambda \]

and

\[ g: (P_1/Q_1, P_2/Q_2) \rightarrow P^\mu/Q^\mu; \quad (uQ_1, xQ_2) \mapsto [u^\mu, x^\mu]Q^\mu \]

are also bilinear and, as \( P = [P_1, P_2] \), their images generate \( P^\lambda/Q^\lambda \) and \( P^\mu/Q^\mu \), respectively. Now \( \phi \) is compatible with \((\lambda, \mu)\) on \( P_1/Q_1 \) and \( P_2/Q_2 \); furthermore, \( \phi \) is normalizer preserving and therefore, by 5.6.2, preserves mixed commutators. It follows that \( P^{\lambda\phi} = [P_1, P_2]^{\phi} = [P_1^{\lambda\phi}, P_2^{\lambda\phi}] = [P_1^{\mu\phi}, P_2^{\mu\phi}] = P^\mu \), similarly \( Q^{\lambda\phi} = Q^\mu \) and

\[ \langle[u, x], Q \rangle^{\lambda\phi} = \langle[\langle u, Q_1 \rangle, \langle x, Q_2 \rangle], Q \rangle^{\lambda\phi} = \langle[\langle u, Q_1 \rangle^{\lambda\phi}, \langle x, Q_2 \rangle^{\lambda\phi}], Q \rangle^{\lambda\phi} = \langle[\langle u, x \rangle^{\lambda\phi}, \langle x, Q_2 \rangle^{\lambda\phi}], Q \rangle \]

Therefore \( \phi \) induces a projectivity \( \tilde{\phi} \) from \( P^\lambda/Q^\lambda \) to \( P^\mu/Q^\mu \) satisfying

\[ \langle f(uQ_1, xQ_2) \rangle^{\tilde{\phi}} = \langle [u^\lambda, x^\lambda]Q^\lambda \rangle^{\tilde{\phi}} = \langle [u^\mu, x^\mu] \rangle \]

By 7.3.7 there exists an isomorphism \( x: P^\lambda/Q^\lambda \rightarrow P^\mu/Q^\mu \) such that \( f(uQ_1, xQ_2)^\mu = g(uQ_1, xQ_2)^\mu \) and hence \((u, x)Q^\mu = ([u, x]Q)^\mu \) for all \( u \in P_1 \), \( x \in P_2 \). Since \( P = [P_1, P_2] \), it follows that \((wQ)^\mu = (wQ)^\mu \) for all \( w \in P \). So if \( Q \leq K \leq P \), then \((K^\lambda/Q^\lambda)^\mu = K^\mu/Q^\mu \) and \((K^\lambda/Q^\lambda)^\mu = K^{\lambda\phi}/Q^{\lambda\phi} \) since \( x \) induces the projectivity \( \tilde{\phi} \). Thus \( K^{\lambda\phi} = K^\mu \) and \( \phi \) is compatible with \((\lambda, \mu)\) on \( P/Q \). \( \square \)
A simple consequence of the above theorem is that a normalizer preserving projectivity from $G$ to $\overline{G}$ which is induced by an isomorphism on $G/G'$, is induced by isomorphisms on every factor $K_i(G)/K_{i+1}(G)$ of the lower central series of $G$ (see Exercise 3). For certain nilpotent groups, we can say a little more.

**Almost free groups of nilpotent varieties**

We remind the reader of some basic properties of varieties of groups (see Robinson [1982], pp. 54–60). Let $W$ be a nonempty set of words in the indeterminates $x_i$ ($i \in \mathbb{N}$). Then for every group $G$, the verbal subgroup of $G$ determined by $W$ is defined to be

$$W(G) = \langle w(g_1, g_2, \ldots) | g_i \in G, w \in W \rangle.$$  

The variety $\mathcal{B}(W)$ determined by $W$ is the class of all groups $G$ such that $W(G) = 1$. Such a variety is called nilpotent (or abelian) if it consists of nilpotent (or abelian) groups. A group $F \in \mathcal{B}$ is called $\mathcal{B}$-free on a subset $X$ of $F$ if for each map $\alpha$ from $X$ to a group $G \in \mathcal{B}$ there exists a unique homomorphism $\beta : F \to G$ extending $\alpha$. If $\overline{F}$ is a free group on a set $\overline{X} \subseteq \overline{F}$, then

$$(16) \ F = \overline{F}/W(\overline{F})$$ is $\mathcal{B}$-free on $X = \{xW(\overline{F}) | x \in \overline{X} \};$$ conversely, every $\mathcal{B}$-free group is of the form $\overline{F}/W(\overline{F})$ for some (absolutely) free group $\overline{F}$.

If $W = \{x_1^{-1}x_2^{-1}x_1x_2\}$, then $W(G) = G'$ for every group $G$, $\mathcal{B}(W)$ is the variety of abelian groups and a free abelian group $\overline{F}/\overline{F}'$ is a direct product of infinite cyclic groups (see Robinson [1982], p. 59). A verbal subgroup in this abelian group $\overline{F}/\overline{F}'$ has the form $(\overline{F}/\overline{F}')^n$ for some nonnegative integer $n$ and therefore, if $F$ is a free group of an abelian variety,

$$(17) \ F = \text{a direct product of isomorphic cyclic groups}.$$ Finally, let $\mathcal{B}$ be a nilpotent variety and $F$ a $\mathcal{B}$-free group; let $c = c(F)$ be the class of $F$. Then a factor group

$$(18) \ G = F/M$$ where $M < K_c(F)$

is called an almost free group of $\mathcal{B}$.

**7.3.10 Theorem** (Barnes and Wall [1964]). Let $\mathcal{B}$ be a nilpotent variety, $G$ a non-abelian almost free group of $\mathcal{B}$ and $\overline{G} \in \mathcal{B}$. If $G$ is finite, assume further that $G$ is not generated by two elements. If there exists a normalizer preserving projectivity from $G$ to $\overline{G}$, then $\overline{G} \simeq G$.

**Proof.** Let $G = F/M$ be as in (18) and let $\phi$ be a normalizer preserving projectivity from $G$ to $\overline{G}$. Since $M < K_c(F)$, we have $c(G) = c(F) = c$ and, as $G$ is not abelian, $c \geq 2$. Thus $K_c(F) \leq F'$ and hence $G/G' \simeq F/F'$. Let $W$ be a set of words in $x_1, x_2, \ldots$ such that $\mathcal{B} = \mathcal{B}(W)$ and let $W^* = W \cup \{x_1^{-1}x_2^{-1}x_1x_2\}$. Then $F = \overline{F}/W(\overline{F})$ for some free group $\overline{F}$ and, by (15), $W^*(\overline{F}) = \overline{F}'W(\overline{F})$. It follows that $\overline{F}/W^*(\overline{F}) = \overline{F}/W(\overline{F})$. Since $\overline{G} \simeq G$, $\overline{F}/W(\overline{F}) = \overline{F}/W^*(\overline{F})$. Therefore, $\overline{G} \simeq G$.
Mixed nilpotent groups

Theorem 7.3.11. Normally our aim is to prove that a given group (for example, an almost free group of a certain nilpotent variety) is determined by its subgroup lattice. In this regard, the above theorem contains three troublesome assumptions, namely that

(a) \( G \) is not generated by two elements if it is finite,
(b) \( G \in \mathfrak{B} \), and
(c) the projectivity \( \varphi \) from \( G \) to \( \overline{G} \) is normalizer preserving.

However, we can say the following:

(a) Barnes and Wall [1964] prove the theorem without the assumption that \( G \) is not a finite 2-generator group. In this case, \( G/G' \) can be the direct product of two isomorphic cyclic groups and \( \varphi \) need not be induced by an isomorphism on \( G/G' \). After an easy reduction this leads to the case that \( G \) is a finite p-group generated by two elements. If \( c(G) \leq 3 \), it is possible to write down generators and relations for \( G \) and \( \overline{G} \) and to see that \( G \simeq \overline{G} \). If \( c(G) \geq 4 \), then \( G/K_{4}(G) \simeq \overline{G}/K_{4}(G) \) and one can show (see Exercise 4) that \( \varphi \) is induced by an isomorphism \( \tau \) on \( G/G'G'' \)
where \( p' = \text{Exp} K_{c}(F) \). The argument then proceeds as in the general case using an isomorphism \( \sigma: G/G' \to \overline{G}/\overline{G}' \) which induces \( \tau \).

(b) Sometimes \( \overline{G} \in \mathfrak{B} \) follows from the fact that \( \varphi \) is normalizer preserving. For example, let \( W = \{ x^{n}_{1}, [x_{1}, x_{2}, \ldots, x_{c+1}] \} \) so that \( \mathfrak{B}(W) = \mathfrak{B}(p^{n}, c) \) is the variety of
nilpotent groups of class at most \( c \) and exponent dividing \( p^n \) (\( p \) a prime). If \( G \in \mathfrak{B}(p^n, c) \) is nonabelian and \( \varphi \) is a normalizer preserving projectivity from \( G \) to \( \overline{G} \), then by 2.2.7, \( \overline{G} \) is a \( p \)-group and so \( \overline{G} \in \mathfrak{B}(p^n, c) \).

(c) Also the assumption that \( \varphi \) is normalizer preserving is not always needed. By 5.6.6, for example, this is the case if \( \text{Exp} \ G = p \). Therefore we get as a corollary to Theorem 7.3.10 that every nonabelian almost free group in \( \mathfrak{B}(p, c) \) is determined by its subgroup lattice. For \( c = 2 \), finally, we obtain the following result.

7.3.12 Theorem. Every nilpotent group of class 2 and exponent \( p \) (a prime) is determined by its subgroup lattice.

Proof. Let \( c(G) = 2 \), \( \text{Exp} \ G = p \) and \( \varphi \) a projectivity from \( G \) to a group \( \overline{G} \). If \( G \) is generated by two elements, then \( |G| = p^3 \) and \( \overline{G} \cong G \); suppose therefore that \( G \) is not generated by two elements. Since \( \text{Exp} \ G = p \), \( G/G' \) is a vector space over \( GF(p) \); let \((g_i G'), g_i \) be a basis of this vector space. By (16) there exists a group \( F \) which is \( \mathfrak{B}(p, 2) \)-free on a set \( \{f_i | i \in I\} \subseteq F \) of the same cardinality. Since \( G \in \mathfrak{B}(p, 2) \), there exists a homomorphism \( \beta: F \to G \) such that \( f_i^\beta = g_i \) for all \( i \in I \). By (19), \( \beta \) is an epimorphism. Thus \( (F')^\beta = G' \) and the basis \( \{(f_i F')_{i \in I}\} \) of \( F/F' \) is mapped to the basis \( \{(g_i G')_{i \in I}\} \) of \( G/G' \) by the epimorphism from \( F/F' \) onto \( G/G' \) induced by \( \beta \). It follows that \( \text{Ker} \beta \leq F' \) and, since \( G \) is not abelian, \( \text{Ker} \beta \leq F' = K_2(F) \). Thus \( G \) is a nonabelian almost free group in \( \mathfrak{B}(p, 2) \). By 2.2.7, \( \overline{G} \) is a \( p \)-group of exponent \( p \), of course. By 5.6.6, \( \varphi \) is normalizer preserving and hence \( c(\overline{G}) = 2 \). Thus \( \overline{G} \in \mathfrak{B}(p, 2) \) and all the assumptions of Theorem 7.3.10 are satisfied. It follows that \( \overline{G} \cong G \). \( \square \)

Exercises

1. In Examples 7.3.4 and 7.3.6, verify that \( \sigma \) satisfies the assumptions of Theorem 1.3.1.

2. (Arshinov [1971]) Let \( p \in \mathcal{P}, 3 \leq n \in \mathbb{N} \) and

\[
N = \langle a_3 \rangle \times \cdots \times \langle a_{n+1} \rangle \times \langle c_1 \rangle \times \cdots \times \langle c_{n-2} \rangle
\]

where \( o(a_i) = \infty \) and \( o(c_i) = p \) for all \( i \). Let \( H = N \langle a_2 \rangle \) and \( G = H \langle a_1 \rangle \) be semidirect products with respect to the automorphisms \( \alpha \) and \( \beta \), respectively, given by \( a_3^\alpha = a_3 c_1, a_3^\beta = a_3 (i > 3), c_i^\alpha = c_i c_{i+1} (i = 1, \ldots, n - 3), c_{n-2}^\alpha = c_{n-2} \) and \( a_i^\beta = a_i a_{i+1} (i = 2, \ldots, n), a_{n+1}^\beta = a_{n+1}, c_i^\beta = c_i (i = 1, \ldots, n - 2) \).

(a) Show that \( G \) is nilpotent of class \( n \) and \( \langle a_1, a_2^\beta \rangle \) is a torsion-free nilpotent subgroup of \( G \) of the same class.

(b) For \( g \in G, g = a_1^r a_2^s b \ (r, s \in \mathbb{Z}, b \in N) \), let \( g^\sigma = g \) if \( rs \equiv 0 \pmod{p} \) and \( g^\sigma = g c_{n-2}^t \) where \( r + s + t \equiv 0 \pmod{p} \) if \( rs \not\equiv 0 \pmod{p} \). Show that \( \sigma: G \to G \) is bijective and induces an autoprojectivity \( \varphi \) of \( G \).

(c) Show that \( \varphi \) is not induced by an isomorphism.
3. (Barnes and Wall [1964]) Let \( \varphi \) be a normalizer preserving projectivity from \( G \) to \( G' \). If \( \varphi \) is induced by an isomorphism on \( G/G' \), show that \( \varphi \) is induced by isomorphisms on \( K_i(G)/K_{i+1}(G) \) for all \( i \geq 1 \). (Hint: Represent \( G \) as a factor group of a free group and study the proof of Theorem 7.3.10.)

4. (Barnes and Wall [1964]) Let \( G \) be a finite \( p \)-group of class 3 generated by two elements and suppose that \( G \) is \( \mathcal{B} \)-free for some variety \( \mathcal{B} \); let \( p' = \text{Exp}_{K_3(G)} \). If \( \varphi \) is a normalizer preserving autoprojectivity of \( G \), show that \( \varphi \) is induced on \( G/G'G'p' \) by an automorphism of \( G/G'G'p' \).

### 7.4 Periodic nilpotent groups

A nilpotent torsion group is the direct product of its primary components, and its subgroup lattice is then the direct product of the subgroup lattices of these components. Therefore we have to study subgroup lattices and projectivities of primary nilpotent groups. We want to use the concepts of Kontorovitch and Plotkin to give a lattice-theoretic characterization of this class of groups where, of course, allowance must be made for the \( P \)-groups. However, for every Tarski \( p \)-group \( G \), \( L(G) \) is modular and therefore has a modular chain \( 1 = H_0 < H_1 = G \) of length 1; but \( G \) is not nilpotent and is lattice-isomorphic to any other (nonprimary) Tarski group. Therefore we have to avoid the Tarski groups, and we do this just as in §6.4. Recall that a lattice \( L \) is permodular if it is modular and every interval of finite length in \( L \) is finite.

#### Permodular chains

7.4.1 Definition. Let \( L \) be a complete lattice and let \( a, a_0, \ldots, a_t \in L \). Then \( a \) is permodularly embedded in \( L \) if \( [a \cup c/O] \) is permodular for all \( c \in C(L) \), and \( O = a_0 < a_1 < \cdots < a_t = I \) is a permodular chain in \( L \) if \( a_{i+1} \) is permodularly embedded in \( [I/a_i] \) for every \( i = 0, \ldots, t - 1 \).

We need some simple inheritance properties of these concepts.

7.4.2 Lemma. Let \( G \) be a \( p \)-group, \( p \) a prime, \( K \) a permutable subgroup of \( G \), \( K < H < G \) and suppose that \( H \) is permodularly embedded in \( [G/K] \).

(a) Then \( H \) is permutable in \( G \).

(b) If \( C \) is a cyclic element in \( [G/K] \), there exists \( c \in G \) such that \( C = K\langle c \rangle \).

(c) If \( N \trianglelefteq G \), then \( NH \) is permodularly embedded in \( [G/NK] \).

Proof. (a) It suffices to prove the assertion in the special case that \( H = K\langle x \rangle \) for some \( x \in G \). Indeed, if \( x \in H \), then \( K\langle x \rangle \) is permodularly embedded in \( [G/K] \); and if all these \( K\langle x \rangle \) are permutable in \( G \), then so is \( H = \langle K\langle x \rangle \mid x \in H \rangle \). So suppose that \( H = K\langle x \rangle \), let \( y \in G \) and put \( T = \langle H, y \rangle \); we have to show that \( H\langle y \rangle = \langle y \rangle H \). Since \( K \) per \( G \), we have that \( [K\langle y \rangle/K] \simeq [\langle y \rangle/\langle y \rangle \cap K] \) is a finite chain and hence
Classes of groups and their projectivities

$K\langle y \rangle$ is cyclic in $[G/K]$. Since $H$ is permodularly embedded in $[G/K]$, it follows that $[K\langle y \rangle \cup H/K] = [T/K]$ is a permodular lattice. In particular, $H \mod [T/K]$ and hence, by (c) of 2.1.6, $H \mod T$. Then $[T/H] \simeq [\langle y \rangle \langle y \rangle \cap H]$ and $[H/K] \simeq [\langle x \rangle \langle x \rangle \cap K]$ are finite chains. So $[T/K]$ has finite length and, as a permodular lattice, is finite. By 6.2.5, $|T:K| < \infty$; thus $T/K$ is a finite $p$-group and $H$ is a subnormal modular subgroup of $T$. By 6.2.10, $H \perp T$; in particular, $H \langle y \rangle = \langle y \rangle H$, as desired.

(b) Since $[C/K]$ satisfies the maximal condition, $C$ is finitely generated modulo $K$ and hence, by 6.2.8, $|K^C : K| < \infty$. Furthermore, $[C/K^C]$ is distributive, and so $C/K^C$ is cyclic. Since $G$ is periodic, $C/K^C$ is finite. Thus $|C : K| < \infty$ and $C/K^C$ is a finite $p$-group. Since $[C/K]$ is distributive, there is exactly one maximal subgroup $D$ of $C$ containing $K$ and every element $c \in C \setminus D$ satisfies $C = K\langle c \rangle$.

(c) Since $N$ and $K$ are permutable in $G$, we have $NK \perp G$. So if $C$ is a cyclic element in $[G/NK]$, then by (b) there exists $c \in G$ such that $C = NK \langle c \rangle$. Since $K$ per $G$, the element $K\langle c \rangle$ is cyclic in $[G/K]$ and, as $H$ is permodularly embedded in this lattice, $[H \cup K\langle c \rangle/K] = [H \cup \langle c \rangle/K]$ is permodular. Thus $[NH \cup C/NK] = [H \cup \langle c \rangle \cup NK/NK] \simeq [H \cup \langle c \rangle \cup NK]$ is permodular and therefore $NH$ is permodularly embedded in $[G/NK]$.

7.4.3 Corollary. Let $G$ be a $p$-group and $1 = H_0 \leq \cdots \leq H_t = G$ be a permodular chain in $L(G)$.

(a) Then $H_i$ is permutable in $G$ for $i = 0, \ldots, t$.

(b) If $N \leq G$, then $1 = NH_0/N \leq \cdots \leq NH_t/N = G/N$ is a permodular chain in $L(G/N)$.

Proof. Clearly, $H_0$ per $G$. If $H_i$ per $G$, then $H_i = K$ and $H_{i+1} = H$ satisfy the assumptions of 7.4.2. Thus $H_{i+1}$ per $G$ and (a) holds. By (c) of 7.4.2, $NH_{i+1}$ is permodularly embedded in $[G/NH_i]$ and this proves (b).

Nilpotent $p$-groups

7.4.4 Lemma. Let $G$ be a $p$-group and suppose that $H$ is permodularly embedded in $L(G)$.

(a) If $\text{Exp } H = p^n (n \in \mathbb{N})$, then $H \leq Z_{2n}(G)$.

(b) If $\text{Exp } H = \infty$, then $H \leq Z(G)$.

Proof. (a) We use induction on $n$. Clearly, every subgroup of $H$ is permodularly embedded in $L(G)$ and thus permutable in $G$ by 7.4.2. So if $M \leq H$ is of order $p$ and $X \leq G$ is cyclic, then $|MX| \leq p |X|$ is finite and $M \leq N_G(X)$. Thus $M \leq N(G)$, the norm of $G$. By 1.5.3, $N(G) \leq Z_2(G)$ and so $\Omega(H) \leq N(G) \leq Z_2(G)$. In particular, the assertion is true for $n = 1$. Let $n \geq 2$ and $N = Z_2(G)$. Then by 7.4.2, $HN/N$ is permodularly embedded in $L(G/N)$ and $\text{Exp}(HN/N) \leq p^{n-1}$. By induction, $HN/N \leq Z_{2(n-1)}(G/N) = Z_{2n}(G)/N$. Thus $H \leq Z_{2n}(G)$ and (a) holds.

(b) Let $x \in G$. Then $\langle H, x \rangle$ is a $p$-group with permodular subgroup lattice. If $S$ is a finite subset of $\langle H, x \rangle$, then by 2.1.5, $L(\langle S \rangle)$ has finite length and hence is finite;
thus $\langle S \rangle$ is finite and $\langle H, x \rangle$ is locally finite. By 2.4.15, a nonabelian locally finite $p$-group with modular subgroup lattice has finite exponent. Thus $\langle H, x \rangle$ is abelian and $H \leq Z(G)$.

The above lemma is the crucial step towards our lattice-theoretic characterization of primary nilpotent groups. As an immediate consequence we get a characterization of nilpotency in $p$-groups.

7.4.5 Theorem. Let $G$ be a $p$-group, $p$ a prime. Then $G$ is nilpotent if and only if $L(G)$ has a permodular chain.

Proof: If $G$ is nilpotent, its ascending central series is a permodular chain in $L(G)$. Conversely, let $1 = H_0 \leq \cdots \leq H_t = G$ be a permodular chain in $L(G)$ and let $N = H_1^0$. By 7.4.4, $N \leq Z(G)$ or $N \leq Z_{2n}(G)$ where $p^n = \text{Exp } H_1$. By 7.4.3, $1 = H_1 N/N \leq \cdots \leq H_t N/N = G/N$ is a permodular chain of length $t - 1$ in $L(G/N)$. By induction $G/N$, and hence also $G$, is nilpotent.

A second important consequence of Lemma 7.4.4 is that projective images of nonabelian nilpotent $p$-groups are nilpotent. We also get an upper bound for the class of such an image.

7.4.6 Theorem (Yakovlev [1965]). Let $p$ be a prime and $G$ a nilpotent $p$-group which is not elementary abelian. If $\overline{G}$ is a group such that $L(\overline{G}) \cong L(G)$, then $\overline{G}$ is a nilpotent primary group and

(a) $c(\overline{G}) = c(G)$ if $\text{Exp } G = p$ or $\text{Exp } G = \infty$,

(b) $c(\overline{G}) \leq 2nc(G)$ if $\text{Exp } G = p^n$, $2 \leq n \in \mathbb{N}$.

Proof. Let $\phi$ be a projectivity from $G$ to $\overline{G}$. As a nilpotent $p$-group, $G$ is locally finite (see Robinson [1982], p. 147). If $G$ is locally cyclic, then so is $\overline{G}$ and we are done; so suppose that $G$ is not locally cyclic. Then by 2.2.7, $\overline{G}$ is a $p$-group. Put $c = c(G)$ and $H_i = Z_i(\overline{G})^\phi$ for $i = 0, \ldots, c$. Then $1 = H_0 \leq \cdots \leq H_c = \overline{G}$ is a permodular chain in $L(\overline{G})$ and, by 7.4.5, $\overline{G}$ is nilpotent.

(a) If $\text{Exp } G = p$, then by 5.6.6, $\phi$ is normalizer preserving and hence $H_i = Z_i(\overline{G})$ for all $i$, that is, $c(\overline{G}) = c$. So let $\text{Exp } G = \infty$. Then we prove $c(\overline{G}) \leq c(G)$ by induction on $c$; application of this result to $\phi^{-1}$ will yield the other inequality. It is well-known (see Robinson [1982], p. 133) that if the centre of a nilpotent group has finite exponent, then so does the whole group. Therefore $\text{Exp } Z(G) = \infty$ and, by 7.4.4, $H_1 \leq Z(\overline{G})$. Thus if $c = 1$, then $\overline{G}$ is abelian and the assertion holds; so let $c > 1$ and suppose that the assertion is true for groups of smaller class. Clearly, $\phi$ induces a projectivity from $G/Z(G)$ to $\overline{G}/H_1$. Therefore if $\text{Exp}(G/Z(G)) = \infty$, the induction assumption implies that $c(\overline{G}/H_1) \leq c - 1$ and hence $c(\overline{G}) \leq c$. Finally, suppose that $\text{Exp}(G/Z(G)) = p^n < \infty$ and let $K = K_c(G)$ be the last nontrivial term of the descending central series of $G$. Since $K^\phi \leq H_1 \leq Z(\overline{G})$, it follows that $\phi$ induces a projectivity from $G/K$ to $\overline{G}/K^\phi$ and $c(G/K) = c - 1$. For $x \in K_{c-1}(G)$ and $y \in G$, we have $[x, y] \in K \leq Z(G)$, and hence $[x, y]^{p^n} = [x^{p^n}, y] = 1$, as $x^{p^n} \in Z(G)$. Since $K$ is generated by these commutators, it follows that $\text{Exp } K \leq p^n$; thus $\text{Exp}(G/K) = \infty$. By induction, $c(\overline{G}/K^\phi) \leq c - 1$ and hence $c(\overline{G}) \leq c$. 


 Classes of groups and their projectivities

(b) We use induction on \( c \) to show that a (nilpotent) \( p \)-group \( \overline{G} \) of exponent \( p^n \) whose subgroup lattice possesses a permodular chain \( 1 = H_0 \leq \cdots \leq H_c = \overline{G} \) of length \( c \) satisfies \( c(\overline{G}) \leq 2nc \). By 7.4.4, \( H_1 \leq Z_{2n}(\overline{G}) = N \) and, in particular, the assertion holds for \( c = 1 \). By 7.4.3, \( 1 = H_1 N / N \leq \cdots \leq H_c N / N = \overline{G} / N \) is a permodular chain of length \( c - 1 \) in \( L(\overline{G} / N) \) and, by induction, \( c(\overline{G} / N) \leq 2n(c - 1) \). Thus \( c(\overline{G}) \leq 2nc \), as desired.

An arbitrary nilpotent torsion group \( G \) is the direct product of its primary components \( G_p \). If \( \varphi \) is a projectivity from \( G \) to a group \( \overline{G} \), then by 1.6.6, \( \overline{G} = \bigoplus_{p \in \mathbb{P}} G_p^\varphi \) with coprime groups \( G_p^\varphi \) and, by 2.2.5 and 7.4.6, these \( G_p^\varphi \) are \( P \)-groups and nilpotent primary groups. However, note that \( \overline{G} \) need not be nilpotent even if all the \( G_p^\varphi \) are nilpotent. And there are direct products of coprime finite \( p \)-groups which are not lattice-isomorphic to any nilpotent group.

7.4.7 Example. Let \( \mathbb{P} = \{p_1, p_2, \ldots \} \).

(a) For every \( n \in \mathbb{N} \), let \( G_n \) be the abelian group of type \((p_n^n, p_n^{n-1})\) and let \( \overline{G}_n = \langle x, y | x^{p_n^n} = y^{p_n^{n-1}} = 1, x^y = x^{1+p_n^{n-1}} \rangle \) where \( p = p_n \). Then \( G = \bigoplus_{n \in \mathbb{N}} G_n \) is abelian and \( \overline{G} = \bigoplus_{n \in \mathbb{N}} \overline{G}_n \) is lattice-isomorphic to \( G \) since every \( \overline{G}_n \) is lattice-isomorphic to \( G_n \) and the direct factors are coprime. Since \( c(\overline{G}_n) = n \), the group \( \overline{G} \) is not nilpotent.

(b) For every \( n \in \mathbb{N} \), let \( H_n \) be a \( p_n \)-group such that every projective image of \( H_n \) has class at least \( n \) (by 7.4.12, we may take any \( p_n \)-group of maximal class \( n + 1 \)). Then every projectivity \( \varphi \) maps \( H = \bigoplus H_n \) to \( \bigoplus H_n^\varphi \), and this group is not nilpotent since \( c(\overline{H}_n^\varphi) \geq n \).

Lattice-theoretic characterization

To give a lattice-theoretic characterization of the class of nilpotent primary groups we combine our concept of permodular embedding with the obvious fact that every element of a group \( G \) has prime power order if and only if for every cyclic element \( C \) of \( L(G) \), the lattice \([C/1]\) is finite and directly indecomposable.

7.4.8 Lemma. Let \( G \) be a group such that

1. \([C/1]\) is finite and directly indecomposable for every cyclic element \( C \) of \( L(G) \) and

2. there exists a nontrivial subgroup of \( G \) which is permodularly embedded in \( L(G) \).

Then there is a prime \( p \) such that either

(a) \( G \) is a \( p \)-group with \( Z(G) \neq 1 \) or

(b) \( G = PQ \) where \( P \) is a normal \( p \)-subgroup of \( G \), \( |Q| \) is a prime dividing \( p - 1 \) and \( Q \) operates fixed-point-freely on \( P \). In this case, if \( G \) is not a \( P \)-group, then every permodularly embedded element of \( L(G) \) is a normal elementary abelian \( p \)-subgroup of \( G \).
Proof. By (1), \( G \) is a torsion group and

(3) every element of \( G \) has prime power order.

Let \( 1 \neq H \leq G \) be permodularly embedded in \( L(G) \) and take a minimal subgroup \( M \) of \( H \). Then

(4) \( |M| = p \) for some prime \( p \).

Let \( x \in G \) and let \( K \) be a nontrivial finite \( p \)-subgroup of \( H \). Then \( K \) is permodularly embedded in \( L(G) \) and so \( [\langle K, x \rangle/1] \) is a permodular lattice. Therefore \( [\langle K, x \rangle/K] \simeq [\langle x \rangle/\langle x \rangle \cap K] \) is a finite chain, hence \( [\langle K, x \rangle/1] \) has finite length and so is finite. Thus \( \langle K, x \rangle \) is a finite group with modular subgroup lattice. By 2.4.4 and (3),

(5) \( \langle K, x \rangle \) is a finite \( p \)-group or a finite nonabelian \( P \)-group.

If \( G \) is a \( p \)-group, then \( M \leq Z_2(G) \) by 7.4.4. Thus \( Z(G) \neq 1 \) and (a) holds. So assume that \( G \) is not a \( p \)-group and suppose first that there exist \( r \)-elements in \( G \) where \( r \) is a prime, \( r > p \). We claim that \( G \) is a \( P \)-group in this case. To show this, let \( R \) be the set of \( r \)-elements in \( G \), and take \( x, y \in R \) such that \( x \neq y \). By (5), \( \langle M, x \rangle \) is a finite \( P \)-group and so \( o(x) = r \) and \( \langle x \rangle^M = \langle x \rangle \) since \( r > p \). Furthermore, the \( P \)-group \( \langle M, x \rangle \) is generated by conjugates of \( M \) and so \( x \in M^G \). Since all conjugates of \( M \) are permodularly embedded in \( L(G) \), \( \langle x \rangle \leq M^G \). Similarly, \( \langle y \rangle \leq M^G \) and so \( \langle x \rangle \langle y \rangle \) is elementary abelian of order at most \( r^2 \). It follows that \( xy = yx \) and \( xy^{-1} \in R \). Thus \( R \) is an elementary abelian \( r \)-group and \( R \leq M^G \). By (3), \( C_G(R) \) is an \( r \)-group, hence \( C_G(R) = R \). Since every subgroup of \( R \) is normal in \( M^G \), we see that \( M \) induces a nontrivial power automorphism in \( R \) and so \( RM \) is a \( P \)-group. Furthermore, \( G/R \) is isomorphic to a subgroup of \( \text{Aut} R \) in which this power automorphism is central. Hence \( RM/R \leq Z(G/R) \) and, again by (3), \( G/R \) is a \( p \)-group. Since \( RM \leq G \), we have shown that

(6) \( M^G = RM \) is a \( P \)-group.

Suppose, for a contradiction, that \( RM < G \) and take \( g \in G \setminus RM \). Since \( G/R \) is a \( p \)-group, \( g \) is a \( p \)-element. If \( \langle M, g \rangle \) were a finite nonabelian \( P \)-group, then \( |\langle M, g \rangle| = r^k p \) for some \( k \) since no other primes are involved in \( G \). But this would imply that \( g \in M^G \), a contradiction. Therefore, by (4), \( \langle M, g \rangle \) is a finite \( p \)-group operating fixed-point-freely on \( R \). Then \( M \) is the only minimal subgroup of \( \langle M, g \rangle \) (see Huppert [1967], p. 502) and hence \( \langle M, g \rangle = \langle g \rangle \) is cyclic. In particular, \( g \in C_g(M) \). Since \( G \) is generated by the elements \( g \in G \setminus RM \), it follows that \( M \leq Z(G) \), contradicting (3). Thus we have shown that \( G = RM \) is a \( P \)-group and (b) holds.

It remains to consider the case that \( H \) is a \( p \)-group where \( p \) is the largest prime involved in \( G \). Let \( N = O_p(G) = \langle x \in G \mid (o(x), p) = 1 \rangle \). Since \( G \) is not a \( p \)-group, \( N \neq 1 \). Let \( K \) be a nontrivial cyclic subgroup of \( H \) and take \( 1 \neq x \in G \) with \( (o(x), p) = 1 \). By (5), \( \langle K, x \rangle \) is a nonabelian \( P \)-group of order \( p^m q \) for some prime \( q < p \). Thus

(7) \( |K| = p, o(x) \) is a prime and \( K \leq \langle K, x \rangle \leq N \).
Since \( x \) was arbitrary, \( K \leq N \). In particular, \( M \leq N \). So if \( P = C_N(M) \), then \( P \leq N \) is a \( p \)-group and \( N/P \) is cyclic of order dividing \( p - 1 \). By (7), \( |N : P| = q \) is a prime. Thus \( N = PQ \) where \( |Q| = q \) and \( Q \) operates fixed-point-freely on \( P \), by (3). Since \( P \) is a characteristic subgroup of \( N \), \( P \triangleleft G \). Every \( p \)-element of \( G/P \) normalizes \( N/P \), a cyclic group of order \( q < p \), and thus centralizes \( N/P \). But \( G/P \) does not contain elements of composite order. This shows that every \( p \)-element of \( G \) is contained in \( P \leq N \) and that \( N = G \). By (7), \( H \) is elementary abelian and normal in \( G \). Thus (b) holds.

7.4.9 Lemma. Let \( G \) be a group such that

(8) every interval in \( L(G) \) is directly indecomposable and

(9) \( L(G) \) has a permodular chain.

Then there is a prime \( p \) such that either

(a) \( G \) is a nilpotent \( p \)-group or

(b) \( G = PQ \) where \( P \) is a normal abelian \( p \)-subgroup of \( G \), \( |Q| \) is a prime dividing \( p - 1 \) and \( Q \) induces nontrivial power automorphisms in \( P \).

Proof. We shall need the following simple fact.

(10) A finite group \( G \) of order \( p^n q \) satisfying (8) has the structure given in (b) if \( p \) and \( q \) are primes such that \( q \) divides \( p - 1 \).

Indeed, if \( P \in \text{Syl}_{p}(G) \) and \( Q = \langle a \rangle \in \text{Syl}_{q}(G) \), then \( P \triangleleft G \) and \( P/\Phi(P) = N_1/\Phi(P) \times \cdots \times N_r/\Phi(P) \) where \( N_i \triangleleft G \) and \( |N_i/\Phi(P)| = p \) for all \( i \) (see 4.1.7). If \( a \) induced different powers in \( N_i/\Phi(P) \) and \( N_2/\Phi(P) \), say, then \( [G/H] = \{G, N_1 H, N_2 H, H\} \) would be the direct product of two chains of length 1 where \( H = N_3 \cdots N_r Q \), a contradiction. Thus \( a \) induces the same power in every \( N_i/\Phi(P) \) and so \( G/\Phi(P) \) is a \( P \)-group. Hence if \( X \) is a proper subgroup of \( P \), there exist maximal subgroups \( M_1 \) and \( M_2 \) of \( G \) with \( X \leq M_1 \cap M_2 \) and \( M_1 \neq P \neq M_2 \). By induction, \( M_1 \) and \( M_2 \) have the structure given in (b) and so \( X \leq \langle M_1, M_2 \rangle = G \). Thus every subgroup of \( P \) is normal in \( G \), that is, \( Q \) induces power automorphisms in \( P \), and \( P \) is abelian since \( p > 2 \). This proves (10).

To prove the lemma, we use induction on the length \( t \) of a permodular chain \( 1 = H_0 \leq H_1 \leq \cdots \leq H_t = G \) in \( L(G) \). By (8), \( G \) is a torsion group and therefore satisfies the assumptions of 7.4.8. If \( G \) is a \( p \)-group for some prime \( p \), then by 7.4.5, \( G \) is nilpotent and (a) holds; if \( G \) is a \( P \)-group, (b) is satisfied. So we may assume that \( G \) is neither a \( p \)-group nor a \( P \)-group. Then by 7.4.8 there are primes \( p \) and \( q \) such that \( q \) divides \( p - 1 \) and \( G = PQ \) where \( P \) is a normal \( p \)-subgroup of \( G \), \( |Q| = q \) and \( Q \) operates fixed-point-freely on \( P \); furthermore, \( H_1 \) is an elementary abelian \( p \)-group and normal in \( G \). By induction, \( H_1 = P \) or \( P/H_1 \) is abelian. In both cases, \( P \) is metabelian and so locally finite. Therefore, if \( x \) and \( y \) are nontrivial elements of \( P \) and \( Q = \langle a \rangle \), then

\[
L = \langle x, x^a, \ldots, x^{aq-1}, y, y^a, \ldots, y^{aq-1} \rangle
\]
7.4 Periodic nilpotent groups

is finite and invariant under \(Q\). Hence \(LQ\) is a finite group of order \(p^nq\) satisfying (8) and, by (10), \(L\) is abelian and \(\langle x \rangle^a = \langle x \rangle\). Thus \(xy = yx\) and since \(x\) and \(y\) are arbitrary, \(P\) is abelian. So \(\langle x \rangle \leq G\) and \(Q\) induces power automorphisms in \(P\).

We come to the desired characterization.

**7.4.10 Theorem.** The group \(G\) is a nilpotent \(p\)-group for some prime \(p\) or a \(P\)-group if and only if it has the following properties.

(i) Every interval in \(L(G)\) is directly indecomposable.

(ii) \(L(G)\) has a permodular chain.

(iii) If \(S \leq T \leq G\) such that \([S/1]\) is a chain of length 2 and \(S\) is maximal in \(T\), then \([T/1]\) is modular or is isomorphic to the subgroup lattice of the dihedral group \(D_8\) of order 8.

**Proof.** Let \(G\) be a nilpotent \(p\)-group. If \([H/K]\) were a directly decomposable interval in \(L(G)\), then, since \(G\) satisfies the normalizer condition, \(L(N_H(K)/K)\) would be directly decomposable, in contradiction to 1.6.5. Thus (i) holds and (ii) follows from 7.4.5. Finally, if \(S\) and \(T\) are as in (iii), then \(T\) is a group of order \(p^3\) with a cyclic subgroup of order \(p^2\). Such a group has modular subgroup lattice or is isomorphic to \(D_8\). Hence (iii) is also satisfied. If \(G\) is a \(P\)-group, \(L(G)\) is isomorphic to the subgroup lattice of a suitable elementary abelian group and therefore also satisfies (i)–(iii).

Conversely, let \(G\) be a group satisfying (i)–(iii). Then by 7.4.9, either \(G\) is a nilpotent \(p\)-group or \(G = PQ\) where \(P\) is a normal abelian \(p\)-subgroup of \(G\), \(|Q|\) is a prime dividing \(p - 1\) and \(Q\) induces nontrivial power automorphisms in \(P\). If \(P\) contained an element \(x\) of order \(p^2\), then \(S = \langle x \rangle \leq \langle x \rangle Q = T\) would satisfy the assumptions of (iii). But \([T/1]\) is not modular since \(T = \langle Q, Q^* \rangle\). Also \([T/1]\) is not isomorphic to \(L(D_8)\) since \(p > 2\). This contradiction shows that \(P\) is elementary abelian and \(G\) is a \(P\)-group.

It should be mentioned that Theorem 7.4.10 is inspired by a lattice-theoretic characterization of finite \(p\)-groups and \(P\)-groups due to Suzuki [1951a]; see Exercises 3 and 4, also Suzuki [1956].

**Finite \(p\)-groups**

Apart from the results of §§ 2.5 and 2.6 on abelian groups, not much is known about the problem: which finite \(p\)-groups are (strongly) determined by their subgroup lattices. So it seems better to ask which classes of \(p\)-groups are invariant under projectivities; by 2.2.6, we may restrict our attention to projectivities between \(p\)-groups. Unfortunately, this question is not a very fruitful one either. It is rather easy to answer, in general. For example, the order, exponent, number of generators, Frattini length of a \(p\)-group are obviously invariant under these projectivities; on the other hand, properties depending on commutator calculus, like class or derived length, are not invariant, as the projectivities between \(p\)-groups with modular sub-
group lattices show. So there are only a few classes which are serious candidates for study. One of these, the class of metacyclic $p$-groups, was handled in 5.2.13. We briefly look at regular $p$-groups and then consider groups of maximal class.

Recall that a finite $p$-group $G$ is regular if for all $x, y \in G$,

$$(11) \quad x^p y^p = (xy)^p \prod_d x_i^p$$

with suitable $d_i \in \langle x, y \rangle'$. This class of groups is not invariant under index preserving projectivities. Indeed, if we put $m = p - 1$ in Exercise 5.5.1, then $c(G) = p - 1$ and hence $G$ is regular (see Huppert [1967], p. 322); in $\overline{G}$, however, $(b^p f_0)^p = b^p f_0$ and, since $\text{Exp} \ G' = p$, this contradicts (11). In any case, since projectivities between $p$-groups satisfy $\Omega_n(G)^p = \Omega_n(\overline{G})$ and $\mathcal{U}_n(G)^p = \mathcal{U}_n(\overline{G})$ for all $n \in \mathbb{N}$, at least the power structure of regular $p$-groups is preserved under these projectivities (see Exercise 5).

### $p$-groups of maximal class

Let $G$ be a finite $p$-group, $|G| = p^n$, $n \geq 2$. Recall that $G$ is said to be of maximal class if $c(G) = n - 1$. Then every factor of the upper and lower central series of $G$, except the uppermost one, has order $p$ and hence for $i = 0, \ldots, n - 2$,

$$(12) \quad Z_i(G) = K_{n-i}(G)$$

is the unique normal subgroup of order $p^i$ of $G$.

We shall use the following characterization (see Huppert [1967], p. 375):

$$(13) \quad G \text{ is of maximal class if and only if there exists } s \in G \text{ such that } |C_G(s)| = p^2.$$  

Let $n \geq 4$ and suppose that $s \in G$ such that $|C_G(s)| = p^2$. Then

$$(14) \quad \langle Z(G), s \rangle \neq Z_2(G).$$

Indeed, since $|Z_2(G)| = p^2$, the equality $\langle Z(G), s \rangle = Z_2(G)$ would imply that $C_G(s) = C_G(Z_2(G))$ is a normal subgroup of index $p$ in $G$; hence $|G| = p^3$, a contradiction. Furthermore, we write $Z = Z(G)$ and claim that

$$(15) \quad |C_G/Z(sZ)| = p^2.$$  

Indeed, by (14), $\langle Z_2(G), s \rangle/Z$ is a subgroup of order $p^2$ of $C_G/Z(sZ)$. So if (15) were false, there would exist $H/Z \leq C_G/Z(sZ)$ containing $\langle Z_2(G), s \rangle/Z$ as a maximal subgroup. Since $\langle Z_2(G), s \rangle/Z$ is central in $C_G/Z(sZ)$, it follows that $H/Z$ is abelian and hence $c(H) = 2$. On the other hand, $|H| = p^4$ and $|C_H(s)| = p^2$; by (13), $c(H) = 3$. This contradiction proves (15).

In general, projectivities do not map $p$-groups of maximal class to $p$-groups of maximal class. For example, if $p > 2$, the nonabelian group of order $p^3$ and exponent $p^2$ has maximal class and is lattice-isomorphic to the abelian group of type $(p^2, p)$. However, the following two theorems show that the majority of groups in this class are invariant under projectivities.

7.4.11 Theorem (Caranti [1979]). Let $G$ be a $p$-group of maximal class, $|G| = p^n$, $n \geq 4$ and let $s \in G$ such that $|C_G(s)| = p^2$ and $o(s) = p$. If $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, then $\overline{G}$ is a $p$-group of maximal class and $Z_i(G)^p = Z_i(\overline{G})$ for all $i$. 


7.4 Periodic nilpotent groups

Proof. By 2.2.6, \( \bar{G} \) is a \( p \)-group. Write \( Z = Z(G) \) and \( S = \langle s \rangle \). Since \( |\langle Z, S \rangle| = p^2 \), the group \( \langle Z, S \rangle^p \) is abelian. Suppose, for a contradiction, that \( |C_{\bar{G}}(S^p)| \geq p^3 \). Then there exists \( K \leq G \) such that \( \langle Z, S \rangle^p \leq K^p \leq C_{\bar{G}}(S^p) \) and \( |K| = p^3 \). Since \( Z \) is the unique minimal normal subgroup of \( G \), we have \( Z^p \leq \bar{G} \), by 5.4.2. It follows that \( \langle Z^p, S^p \rangle \) is central in \( K^p \) and hence \( K^p \) is abelian. But \( |C_{\bar{G}}(S)| = p^2 \) implies that \( K \) is not abelian and so \( K^p \) is of type \((p^2, p)\). Since \( |KZ_2(G) : K| \leq p \), there exists \( H \leq G \) such that \( KZ_2(G) \leq H \) and \( |H| = p^4 \). By (13), \( H \) is of maximal class. Furthermore, by assumption, \( |S| = p \) so that \( \langle Z, S \rangle = \Omega(K) \leq H \). Since \( H \) has only one normal subgroup of order \( p^2 \), it follows that \( \langle Z, S \rangle = Z_2(G) \), contradicting (14). Thus \( |C_{\bar{G}}(S^p)| = p^2 \) and, by (13), \( \bar{G} \) is of maximal class. For \( i = 1, \ldots, n - 2 \), \( Z_i(G) \) is the unique normal subgroup of \( G/Z_{i-1}(G) \) so that by 5.4.2 and a trivial induction, \( Z_i^p(G) = Z_i^p(\bar{G}) \). Since \( Z_i^p(G) = Z_i^p(\bar{G}) \) is the unique normal subgroup of \( G/Z_i(G) \) so that by 5.4.2 and a trivial induction, \( Z_i^p(G) = Z_i^p(\bar{G}) \), it follows that \( Z_i^p(G) = Z_i^p(\bar{G}) \). \( \square \)

7.4.12 Theorem (Caranti [1979]). Let \( G \) be a \( p \)-group of maximal class, \(|G| = p^n, n \geq 4\), and let \( \varphi \) be a projectivity from \( G \) to a group \( \bar{G} \). If \( \bar{G} \) is not a \( p \)-group of maximal class, then

(a) \( c(\bar{G}) = c(G) - 1 \) and \( Z_i(\bar{G}) = Z_{i+1}(G)^p \) for all \( i \geq 1 \),
(b) \( \text{Exp } S_2(G) = p \) and \( |G : \Omega(G)| = p \),
(c) \( |G| \leq p^{n+1} \).

Proof. Again by 2.2.6 and 5.4.2, \( |\bar{G}| = p^n \) and \( Z^p \leq \bar{G} \) where \( Z = Z(G) \).

(a) First consider the case that \( |G| = p^4 \). Suppose, for a contradiction, that \( \bar{G}/Z^p \) is abelian. Then \( \bar{G}/Z^p \) is of type \((p^2, p)\) and therefore contains two cyclic subgroups \( A_i/Z^p \) of order \( p^2 \). Then \( A_i/Z \) is cyclic, hence the \( A_i \) are abelian and \( A_1 \cap A_2 \leq Z(G) \). But this implies that \( |Z(G)| \geq p^2 \), a contradiction. Thus \( \bar{G}/Z^p \) is not abelian. Since \( \bar{G} \) is not of maximal class, it follows that \( c(\bar{G}) = 2 \) and \( Z^p < Z(\bar{G}) \). On the other hand, \( |Z(\bar{G}/Z^p)| = p \) and hence \( Z(\bar{G}) = \Phi(\bar{G}) = Z_2(G)^p \). Thus (a) holds in this case. Now suppose that \(|G| \geq p^5 \) and let \( s \in G \) such that \( |C_{\bar{G}}(s)| = p^2 \). By 7.4.11, \( o(s) = p^2 \) and hence \( Z < \langle s \rangle \). So by (15), \( G/Z \) satisfies the assumptions of Theorem 7.4.11, and therefore \( c(\bar{G}/Z^p) = n - 2 \) and \( Z_i+1(G)^p/Z^p = Z_i(\bar{G}/Z^p) \) for all \( i \geq 1 \). Since \( c(\bar{G}) < n - 1 \), we obtain \( Z^p < Z(\bar{G}) \) and \( Z(\bar{G}/Z^p) = Z(\bar{G})/Z^p \). Thus \( Z_i(\bar{G}/Z^p) = Z_i(\bar{G})/Z_i^p \) for all \( i \geq 1 \) and (a) follows.

(b), (c) We prove both assertions simultaneously and consider a group \( G \) of minimal order for which (b) or (c) is false. Let \( s \in G \) such that \( |C_{\bar{G}}(s)| = p^2 \) and let \( M \) be a maximal subgroup of \( G \) containing \( s \). By (13), \( M \) is of maximal class. By (a), \( Z(\bar{G}) = Z_2(G)^p \leq Z(M)^p \) since \( Z_2(G) \leq \Phi(G) \leq M \); thus \( M^p \) is not of maximal class. If \(|M| \geq p^4 \), the minimality of \( G \) implies that (b) and (c) hold for \( M \), that is, \(|M| \leq p^{n+1} \) and \( \Omega(M) \) is a maximal subgroup of exponent \( p \) of \( M \). Since \( \Omega(M) \leq G \) and \( |G : \Omega(M)| = p^2 \), we have \( \Omega(M) = G' \) and hence

(16) \( \text{Exp } G' = p \) and \(|G| \leq p^{n+2} \).

If \(|M| < p^4 \), then clearly \(|G| = p^4 \leq p^{n+2} \). Let \( t \in G \setminus Z \) be such that \( o(t) = p \) and consider \( H = C_G(t) \). By 7.4.11, \( |H| = p^3 \) and since \( \langle Z, t \rangle \leq \Omega(Z(H)) \), we conclude that \( H \) is abelian and \(|G : \Omega(H)| \leq p^2 \). It follows that \( G' \leq \Omega(H) \) and hence (16) also holds in this case.
If \(|G| = p^{p+2}\), there exists a maximal subgroup \(G_1\) of \(G\) such that \(\Omega(G_1) = K_3(G)\) (see Huppert [1967], p. 370 for \(p > 2\); if \(p = 2\), we can take the cyclic maximal subgroup of \(G\)). But by (16), \(K_2(G) = G' \leq \Omega(G_1)\), a contradiction. Thus \(|G| \leq p^{p+1}\). Therefore by (a), \(c(G) = c(G) - 1 \leq p - 1\) and so \(G\) is regular (see Huppert [1967], p. 322). Then \(\text{Exp} \Omega(G) = p\) and hence also \(\text{Exp} \Omega(G) = p\). Since \(G\) is a counter-example to (b) or (c), it follows that \(|G : \Omega(G)| \neq p\). By (16), \(G' \leq \Omega(G)\), and \(\Omega(G) = G'\) since \(\text{o}(s) = p^2\). By a well-known property of regular \(p\)-groups (see Huppert [1967], p. 327), \(|\mathcal{U}(G)| = |G : \Omega(G)|\) and hence \(|\mathcal{U}(G)| = |G : \Omega(G)| = p^2\). Thus there exists \(x \in G\) such that \(x^p \notin Z\); let \(N = \langle x, G' \rangle\). Then \(\Omega(N) = G'\) and \(N\) is regular since \(|N| \leq p^p\). Therefore \(|\mathcal{U}(N)| = |N : \Omega(N)| = p\) and so \(|x^p^\theta| = \mathcal{U}(N) \leq G\). This contradicts (12).

Caranti [1979] proved that \(|G| \leq p^p\) in 7.4.12(c) and he constructed all the \(p\)-groups of maximal class which are lattice-isomorphic to groups of smaller class. There are two series of such groups, one of which we present in Exercise 7. We mention that the \(2\)-groups of maximal class are the dihedral, generalized quaternion, and semidihedral groups (see Huppert [1967], p. 339), and all these groups are easily seen to be determined by their subgroup lattices since they contain cyclic maximal subgroups and differ in the number of minimal subgroups. So we could have assumed \(p > 2\) in our investigations. Finally, for \(p > 2\), two lattice-isomorphic but nonisomorphic groups of order \(p^4\) and class 3 are the groups 9) and 10) in Exercise 6.

---

**Exercises**

1. If \(H\) is permodular in the group \(G\), and \(C\) is a cyclic element in \([G/H]\), show that there exists \(c \in G\) such that \(C = \langle H, c \rangle\).

2. Let \(G\) be a nilpotent \(p\)-group such that \(\text{Exp} G = \infty\). Show that every projectivity of \(G\) is normalizer preserving.

3. (Suzuki [1951a]) Let \(G\) be a finite group such that \(L(G)\) is lower semimodular and all intervals in \(L(G)\) are directly indecomposable. If \(\Phi(G) = 1\), show that \(G\) is a \(P\)-group. (Hint: By 5.3.11, \(G\) is supersoluble.)

4. (Suzuki [1951a]) Show that a finite group \(G\) has a lower semimodular subgroup lattice all of whose intervals are directly indecomposable if and only if \(G\) is either a \(p\)-group or satisfies (b) of 7.4.9.

5. Let us call a finite \(p\)-group \(G\) an \(\Omega\)-group if for every section \(A\) of \(G\) and all \(n \in \mathbb{N}\), \(\Omega_n(A) = \{a \in A | a^{p^n} = 1\}\). (Thus every regular \(p\)-group is an \(\Omega\)-group.) Show that if \(G\) is an \(\Omega\)-group and \(\varphi\) is a projectivity from \(G\) to a \(p\)-group \(\overline{G}\), then \(\overline{G}\) is an \(\Omega\)-group.

6. It is well-known (see Huppert [1967], p. 346) that for \(p > 3\) there are exactly 15 pairwise nonisomorphic groups of order \(p^4\). Show that among these (in Huppert’s notation) just the following are lattice-isomorphic: 2) and 6), 3) and 7), 4) and 14), 9) and 10), 13) and 15). Note that the groups of maximal class are 9), 10), 12), and 13).
7. (Caranti [1979]) Let $3 \leq n \leq p$ and $G = \langle s, s_1, s_2, \ldots, s_{n-1} \rangle$ with defining relations $s^p = s_{n-1}, s_i^p = 1 \ (1 \leq i \leq n-1), [s_i, s] = s_{i+1} \ (1 \leq i \leq n-2)$ and $[s_i, s_j] = 1 \ (1 \leq i, j \leq n-1)$. Let $\tilde{G}$ be the group obtained, replacing in these relations $[s_{n-2}, s] = s_{n-1}$ by $[s_{n-2}, s] = 1$. Show that $|G| = |\tilde{G}| = p^n$, $c(G) = n-1$, $c(\tilde{G}) = n-2$, and that $G$ and $\tilde{G}$ are lattice-isomorphic.

7.5 Soluble groups

We have seen that the class of soluble groups is invariant under projectivities. However, there are only a few general theorems saying that the members of a certain class of soluble groups are determined (or even strongly determined) by their subgroup lattices. On the contrary, projectivities between nonisomorphic groups of this type occur in abundance. Examples can be found in 4.1.7, 4.2.12, 5.6.8, 5.6.9, and in the literature cited in §5.6. In addition, Yakovlev [1975] constructed a projectivity between two nonisomorphic nonabelian torsion-free soluble groups, and thus showed that Sadovskii’s theorem on torsion-free nilpotent groups does not generalize to soluble groups. More accessible is the question as to which classes of soluble and generalized soluble groups are invariant under projectivities. We study this problem in two rather different situations. First and foremost we investigate formations of finite soluble groups; and then at the end of this section we show that an important class of generalized soluble groups, the class of radical groups, is invariant under projectivities.

Finite soluble groups

We already know classes of finite soluble groups which are invariant under projectivities, and in some cases we have also given lattice-theoretic characterizations of these classes. For the convenience of the reader we give references in the following table. All groups considered are finite.

<table>
<thead>
<tr>
<th>Class of Groups</th>
<th>Reference</th>
<th>Characterization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soluble groups</td>
<td>4.3.4</td>
<td>5.3.5</td>
</tr>
<tr>
<td>Groups of Fitting length $k$, $k \geq 3$</td>
<td>4.3.3</td>
<td></td>
</tr>
<tr>
<td>Groups of $p$-length $l$, $l \geq 2$</td>
<td>4.3.8</td>
<td></td>
</tr>
<tr>
<td>Supersoluble groups</td>
<td>5.3.8</td>
<td>5.3.7 and 5.3.9</td>
</tr>
<tr>
<td>Supersoluble groups inducing automorphism</td>
<td>5.3.11</td>
<td>Groups with lower semimodular subgroup</td>
</tr>
<tr>
<td>groups of at most prime order in every chief factor</td>
<td></td>
<td>lattice</td>
</tr>
</tbody>
</table>

The most important invariants of a finite soluble group $G$ are the derived length, the Fitting length, and the rank of $G$. We have seen that derived length is not preserved by projectivities, and we now show that the rank of $G$ is preserved. Let us
Classes of groups and their projectivities

recall that if \( 1 = G_0 < G_1 < \cdots < G_n = G \) is a chief series of \( G \) with \( |G_i : G_{i-1}| = p_i^{r_i}, \) \( p_i \in \mathbb{P} \) and \( r_i \in \mathbb{N}, \) \( i = 1, \ldots, n, \) then the rank \( r(G) \) of \( G \) is the unordered \( n \)-tuple \( (r_1, \ldots, r_n) \) of the dimensions of the chief factors of \( G. \) By the Jordan-Hölder Theorem, \( r(G) \) is independent of the choice of the chief series. We write \( \mathcal{E}(r) \) for the class of soluble groups of rank \( r = (r_1, \ldots, r_n) \) and define \( \mathcal{S}_k \) to be the class of all soluble groups whose chief factors have dimension at most \( k (k \in \mathbb{N}). \)

7.5.1 Theorem (Schmidt [1972b]). If \( \varphi \) is a projectivity from a finite soluble group \( G \) to a group \( \overline{G}, \) then \( r(\overline{G}) = r(G). \) Thus all the classes \( \mathcal{E}(r) \) and \( \mathcal{S}_k \) are invariant under projectivities.

Proof. We proceed by induction on \( |G|. \) Let \( N \) be a minimal normal subgroup of \( G. \) If \( N^\varphi \) is a minimal normal subgroup of \( \overline{G}, \) then \( N \) and \( N^\varphi \) have the same dimension. By induction, \( r(\overline{G}/N^\varphi) = r(G/N) \) and hence \( r(\overline{G}) = r(G). \) Now suppose that \( N^\varphi \) is not a minimal normal subgroup of \( \overline{G}. \) Then by 5.4.4, \( N \) is cyclic and there exists a normal subgroup \( S \) of \( G \) such that \( N \leq S, S^\varphi \leq \overline{G}, \) and \( S \) and \( S^\varphi \) are hypercyclically embedded in \( G \) and \( \overline{G}, \) respectively. Thus if \( m = \text{the length of } L(S), \) every chief series of \( G \) through \( S \) has \( m \) of its factors below \( S \) and all of these have dimension 1. The same holds for \( S^\varphi \) in \( \overline{G}. \) By induction, \( r(\overline{G}/S^\varphi) = r(G/S) \) and it follows that \( r(\overline{G}) = r(G). \)

The above result generalizes Iwasawa's theorem that the class \( \mathcal{E}_1 \) of supersoluble groups is invariant under projectivities. It is not difficult also to extend the lattice-theoretic characterization 5.3.7 of \( \mathcal{E}_1 \) to the classes \( \mathcal{E}_k \) (see Exercise 1).

Another interesting class of finite soluble groups is the class \( \mathcal{I} \) of Sylow tower groups. Recall that \( G \in \mathcal{I} \) if and only if there exists a chain \( 1 = G_0 < \cdots < G_r = G \) of normal subgroups \( G_i \) of \( G \) such that \( G_{i+1}/G_i \) is a Sylow subgroup of \( G/G_i \) for \( i = 0, \ldots, r - 1. \)

7.5.2 Theorem (Schmidt [1972b]). The class \( \mathcal{I} \) of Sylow tower groups is invariant under projectivities.

Proof. Let \( G \in \mathcal{I} \) and \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G}. \) We use induction on \( |G| \) to show that \( \overline{G} \in \mathcal{I}. \) If \( G = S \times T \) where \( S \) is a P-group and \( (|S|, |T|) = 1, \) then \( \overline{G} = S^\varphi \times T^\varphi, (|S^\varphi|, |T^\varphi|) = 1, \) and \( S^\varphi \) is a P-group. Thus \( S^\varphi \in \mathcal{I} \) and, by induction, \( T^\varphi \in \mathcal{I}; \) since \( (|S^\varphi|, |T^\varphi|) = 1, \) it follows that \( \overline{G} \in \mathcal{I}. \) Now suppose that \( G \) is not P-decomposable and let \( P \neq 1 \) be a normal Sylow p-subgroup of \( G. \) By 4.3.2, \( P^\varphi = Q_q(\overline{G}) \) for some prime \( q. \) If \( P^\varphi \in \text{Syl}_q(\overline{G}), \) then \( \overline{G} \in \mathcal{I}, \) by induction. And if \( P^\varphi \) is not a Sylow q-subgroup of \( \overline{G}, \) then \( \varphi^{-1} \) is singular at \( q \) and by 4.2.6 there exists a normal q-complement \( N^\varphi \) in \( \overline{G}. \) By induction, \( N^\varphi \in \mathcal{I} \) and then also \( \overline{G} \in \mathcal{I}. \)

The types of the Sylow towers in \( G \) and \( \overline{G} \) can of course differ. Indeed, the number of primes dividing \( |G| \) can be twice the number of primes dividing \( |G|; \) for example, if \( G \) and \( \overline{G} \) are direct products of coprime P-groups. But also if \( G \) is not P-decomposable, the number of primes involved in \( |G| \) and \( |\overline{G}| \) can be different: Theorem 4.1.6 shows that the nonabelian group of order 63 and exponent 21 and the
7.5 Soluble groups

Dihedral group of order 42 are lattice-isomorphic. By Example 4.1.7(b) there are lattice-isomorphic groups of order $11^3 \cdot 7$ and $11^3 \cdot 19$ with minimal normal subgroups of order $11^3$. This shows that the class of groups with a Sylow tower with respect to the natural ordering of the primes is not invariant under projectivities. This contradicts Theorem 6.2 in Schmidt [1987]; a corrected version of this "theorem" is given in Exercise 2.

To obtain deeper results, we need some simple facts from the theory of formations.

**Formations of finite soluble groups**

A *formation* is a class $\mathcal{F}$ of soluble groups with the following properties:

1. If $N \trianglelefteq G \in \mathcal{F}$, then $G/N \in \mathcal{F}$.

2. If $N_1, N_2 \trianglelefteq G$ such that $G/N_i \in \mathcal{F}$ $(i = 1, 2)$, then $G/(N_1 \cap N_2) \in \mathcal{F}$.

A formation $\mathcal{F}$ is called *saturated* if $G/\Phi(G) \in \mathcal{F}$ implies $G \in \mathcal{F}$.

It follows from (2) that if $\mathcal{F}$ is a formation, then in every finite soluble group $G$ there exists a unique smallest normal subgroup whose factor group lies in $\mathcal{F}$; this is called the $\mathcal{F}$-*residual* $G_{\mathcal{F}}$. It is the intersection of all the normal subgroups $N$ of $G$ such that $G/N \in \mathcal{F}$. Furthermore it is well-known that if $\mathcal{F}$ is saturated, then in every finite soluble group $G$ there exists a canonical conjugacy class of subgroups $S$ of $G$, called $\mathcal{F}$-*projectors*, defined by the condition that $SN/N$ is $\mathcal{F}$-maximal in $G/N$ for every normal subgroup $N$ of $G$ (see Robinson [1982], p. 272). We describe a construction for formations due to W. Gaschütz and give some examples.

For every prime $p$, let $\mathcal{R}(p)$ be a class of groups. Define $\mathcal{F}$ to be the class of all finite soluble groups $G$ such that $G/C_G(H/K) \in \mathcal{R}(p)$ for every chief factor $H/K$ of order divisible by $p$ of $G$. It is clear that $\mathcal{F}$ satisfies (1). And since the chief factors of $G/(N_1 \cap N_2)$ are $G$-isomorphic to those of $G/N_1$ or $G/N_2$, it follows that $G/(N_1 \cap N_2) \in \mathcal{F}$ if $G/N_1$ and $G/N_2$ are in $\mathcal{F}$. Thus $\mathcal{F}$ is a formation, called the *formation defined locally by the classes* $\mathcal{R}(p)$. If all the $\mathcal{R}(p)$ are formations, then $\mathcal{F}$ is saturated (see Robinson [1982], p. 269).

**7.5.3 Examples.** All groups considered are finite and soluble.

(a) The class $\mathfrak{A}$ of abelian groups clearly is a formation. Since $G/\Phi(G) \in \mathfrak{A}$ for every $p$-group $G$, the class $\mathfrak{A}$ is not saturated.

(b) If $\mathcal{R}(p) = \{1\}$ for all primes $p$, the formation defined locally by the $\mathcal{R}(p)$ is the class of groups with central chief factors, that is, the class $\mathfrak{N}$ of nilpotent groups.

(c) Let $\mathfrak{X}$ be a formation, $\mathcal{R}(p) = \mathfrak{X}$ for all primes $p$ and let $\mathcal{F}$ be the formation defined locally by the $\mathcal{R}(p)$. If $G \in \mathcal{F}$, then $G/F(G) \in \mathfrak{X}$ since $F(G)$, the Fitting subgroup of $G$, is the intersection of the centralizers of the chief factors of $G$ (see Robinson [1982], p. 129). Thus $G \in \mathfrak{N}\mathfrak{X}$, the class of all groups with nilpotent $\mathfrak{X}$-residual. Conversely, if $G \in \mathfrak{N}\mathfrak{X}$, then $G/F(G) \in \mathfrak{X}$ and hence $G \in \mathcal{F}$. Thus $\mathcal{F} = \mathfrak{N}\mathfrak{X}$. Of particular interest in the theory of finite soluble groups are the class $\mathfrak{N}\mathfrak{A}$ of nilpotent-by-abelian groups and the formations $\mathfrak{N}\mathfrak{A}^s$, $s \in \mathbb{N}$, of groups of Fitting length at most $s$. 

(d) It is easily seen that the classes $\mathcal{E}_k, k \in \mathbb{N}$, are formations. Of these, only the formation $\mathcal{E}_1$ of supersoluble groups is saturated: it is defined locally by the formations $\mathfrak{A}_p$ of abelian groups of exponent dividing $p - 1$ (see Huppert [1967], pp. 712–715).

(e) For every prime $p$, let $\mathfrak{Z}_p$ be the class of groups consisting of the trivial group and all the cyclic groups of prime order $q$ dividing $p - 1$. Since $\mathfrak{Z}_p \subseteq \mathfrak{A}_p$, the formation defined locally by these classes $\mathfrak{Z}_p$ consists of those supersoluble groups inducing automorphism groups of at most prime order in their chief factors. By 5.3.11, this is the class $\mathfrak{V}_L$ of groups with lower semimodular subgroup lattice.

We come to our main result.

7.5.4 Theorem (Schmidt [1974], [1987]). For every prime $p$, let $\mathfrak{F}(p)$ be a class of finite soluble groups such that

1. $\mathfrak{Z}_p \subseteq \mathfrak{F}(p)$ and

2. if $X$, $Y$ are lattice-isomorphic irreducible subgroups of $GL(n, p)$, $n \in \mathbb{N}$, and $X \in \mathfrak{F}(p) \setminus \mathfrak{Z}_p$, then $Y \in \mathfrak{F}(p)$.

Then the formation $\mathfrak{F}$ defined locally by the classes $\mathfrak{F}(p)$ is invariant under projectivities.

Proof. Let $G \in \mathfrak{F}$ and $\varphi$ be a projectivity from $G$ to a group $\tilde{G}$. We use induction on $|G|$ to show that $\tilde{G} \in \mathfrak{F}$. Suppose first that $G$ is $P$-decomposable, that is, $G = S \times T$ where $S$ is a $P$-group and $(|S|, |T|) = 1$. Then by 1.6.6, $\tilde{G} = S^* \times T^*$; furthermore $T \simeq G/S \in \mathfrak{F}$ and hence by induction, $\tilde{G}/S^* \simeq T^* \in \mathfrak{F}$. Therefore if $H/K$ is a chief factor of $\tilde{G}$ of order a power of $p$ such that $K > S^*$, then $\tilde{G}/C_{\tilde{G}}(H/K) \in \mathfrak{F}(p)$. Also if $H \leq S^*$, then $\tilde{G}/C_{\tilde{G}}(H/K) \in \mathfrak{Z}_p \subseteq \mathfrak{F}(p)$ since $S^*$ is a $P$-group. Thus $\tilde{G} \in \mathfrak{F}$ and we may assume that $G$ is not $P$-decomposable.

Now let $N$ be a minimal normal subgroup of $G$. If $N^*$ is not a minimal normal subgroup of $\tilde{G}$, then by 5.4.4 there exists a minimal subgroup $M$ of $Z(G)$ such that $M^* \leq Z(\tilde{G})$; let $|M^*| = q$. By induction, $\tilde{G}/M^* \in \mathfrak{F}$; also, $\tilde{G}/C_{\tilde{G}}(M^*) = 1 \in \mathfrak{F}(q)$ and hence $\tilde{G} \in \mathfrak{F}$. So suppose that $N^*$ is a minimal normal subgroup of $\tilde{G}$ and let $|N| = p^n$. Then by induction, $\tilde{G}/N^* \in \mathfrak{F}$. If $n \geq 2$ or $n = 1$ and $\varphi$ and $\varphi^{-1}$ are regular at $p$, then by 5.4.5, $C_{\tilde{G}}(N^*) = C_{\tilde{G}}(N^*)$ and $\varphi$ induces a projectivity from $X = G/C_G(N)$ to $Y = \tilde{G}/C_{\tilde{G}}(N^*)$. Since $|N| = p^n = |N^*|$, both groups are irreducible subgroups of $GL(n, p)$ and $X \in \mathfrak{F}(p)$ since $\tilde{G} \in \mathfrak{F}$. If $X \notin \mathfrak{Z}_p$, then by (4), $Y = \tilde{G}/C_{\tilde{G}}(N^*) \in \mathfrak{F}(p)$ and hence $\tilde{G} \in \mathfrak{F}$. And if $X \in \mathfrak{Z}_p$, then $|X|$ divides $p - 1$ and the irreducibility of $X$ implies $n = 1$ (see Huppert [1967], p. 165). Since $Y \leq GL(1, p) \simeq C_{p-1}$ is lattice-isomorphic to $X$, the subgroup $Y$ is cyclic of prime order dividing $p - 1$ (or $Y = 1$) and hence $Y \in \mathfrak{Z}_p \subseteq \mathfrak{F}(p)$, by (3). Again it follows that $\tilde{G} \in \mathfrak{F}$.

It remains to consider the case that $N^* \leq \tilde{G}$, $|N| = p$ and $\varphi$ or $\varphi^{-1}$ is singular at $p$; let $|N^*| = q$. If $\varphi^{-1}$ is singular at $q$, then by 4.2.6 there exists a normal $q$-complement with abelian factor group in $\tilde{G}$, since $\tilde{G}$ is $P$-indecomposable. Then $N^*$ is a central chief factor so that $\tilde{G}/C_{\tilde{G}}(N^*) = 1 \in \mathfrak{F}(q)$ and $\tilde{G} \in \mathfrak{F}$. So suppose that $\varphi^{-1}$ is regular at $q$. Then $p = q$, $\varphi$ is singular at $p$ and by 4.2.6 there exists a normal
p-complement $K$ in $G$ such that $K^p \leq \bar{G}$ and $\bar{G}/K^p$ is cyclic or a $P$-group. It follows that $\bar{G}/C_{\bar{G}}(N^p) \in \mathcal{J}_p \subseteq \mathcal{F}(p)$ and again $\bar{G} \in \mathcal{F}$, as desired. □

Theorem 7.5.4 and Example 7.5.3(c) show that if $\mathcal{X}$ is a formation of finite soluble groups satisfying (3) and (4) in place of $\mathcal{F}(p)$, then $\mathcal{X} = \mathcal{N} \mathcal{X}$ is invariant under projectivities. Now, obviously, $\mathcal{N} \mathcal{X}$ satisfies (3) and (4) and a trivial induction yields that $\mathcal{N}^s \mathcal{X}$ is invariant under projectivities for all $s \in \mathbb{N}$. We give examples of formations $\mathcal{X}$ with this property. The formation $\mathcal{U}$ of abelian groups clearly satisfies (3). By Schur's Lemma, every irreducible subgroup of $GL(n, p)$ has cyclic centre. And since the class of cyclic groups is invariant under projectivities, it follows that $\mathcal{U}$ satisfies (4). Thus the class $\mathcal{N} \mathcal{U}$ is invariant under projectivities although $\mathcal{N}$ and $\mathcal{U}$ are not. By 1.6.6 and 2.2.6, every projective image of a nilpotent group with cyclic centre is nilpotent and therefore $\mathcal{U}$ satisfies (4). Thus we get that for $t \geq 2$, the formations $\mathcal{N}^t$ are invariant under projectivities, a result already known from 4.3.3. Finally, by 7.5.1, the formations $\mathcal{S}_k$ satisfy (3) and (4). So we have the following result.

7.5.5 Corollary. If $\mathcal{X}$ is a formation of finite soluble groups satisfying (3) and (4) in place of $\mathcal{F}(p)$, then $\mathcal{N}^s \mathcal{X}$ is invariant under projectivities for every $s \in \mathbb{N}$. In particular, the saturated formations $\mathcal{N}^s \mathcal{U}$, $\mathcal{N}^s \mathcal{S}_k$ and $\mathcal{N}^t$ ($s, k \geq 1$; $t \geq 2$) are invariant under projectivities.

Of course, the classes $\mathcal{F}(p) = \mathcal{J}_p$ also satisfy (3) and (4) and are the smallest classes with this property. In fact, the following holds and will be used later.

7.5.6 Remark. Let $\mathcal{F} \neq \{1\}$ be a formation defined locally by classes $\mathcal{F}(p)$. If $\mathcal{F}$ is invariant under projectivities, then $\mathcal{J}_p \subseteq \mathcal{F}(p)$ for every prime $p$. Thus the formation $\mathcal{M}_L$ of groups with lower semimodular subgroup lattice is the smallest nontrivial formation which is defined locally and is invariant under projectivities.

Proof. Let $1 \neq G \in \mathcal{F}$ and $p \in \mathbb{P}$. Then there exists $N \leq G$ such that $G/N$ is cyclic of prime order. Since $G/N \in \mathcal{F}$ and $\mathcal{F}$ is invariant under projectivities, it follows that $C_p \in \mathcal{F}$; thus $1 \in \mathcal{F}(p)$. Furthermore, $C_p \times C_p \in \mathcal{F}$ and hence for every prime $q$ dividing $p - 1$, the nonabelian group of order $pq$ lies in $\mathcal{F}$. Therefore $C_q \in \mathcal{F}(p)$ and hence $\mathcal{J}_p \subseteq \mathcal{F}(p)$. Now 7.5.3(e) shows that $\mathcal{M}_L \subseteq \mathcal{F}$. □

Residuals and projectors

We want to show now that every projectivity between finite soluble groups maps $\mathcal{F}$-residual to $\mathcal{F}$-residual and $\mathcal{F}$-projectors to $\mathcal{F}$-projectors if $\mathcal{F}$ is a formation which is invariant under projectivities. In the case of the $\mathcal{F}$-residual, we need an additional assumption which will now be explained. For short, let us say that $(G, H, K)$ is a $P$-hypercentral triple if $H, K$ are normal subgroups of $G$ such that $K \leq H$ and

$$G/K = S_1/K \times \cdots \times S_r/K \times T/K$$
where \( 0 \leq r \in \mathbb{Z} \) and for all \( i, j \in \{1, \ldots, r\} \),

5. \( S_i/K \) is a \( P \)-group,

6. \( (|S_i/K|, |S_j/K|) = 1 = (|S_i/K|, |T/K|) \) for \( i \neq j \),

7. \( H/K = S_1/K \times \cdots \times S_r/K \times (H \cap T)/K \), and

8. \((H \cap T)/K\) is hypercentrally embedded in \( G \).

A formation \( \mathcal{F} \) is called \( P \)-hypercentrally closed if for every \( P \)-hypercentral triple \((G, H, K)\), \( G/H \in \mathcal{F} \) implies that \( G/K \in \mathcal{F} \). The formations studied above have this property.

7.5.7 Lemma. If \( \mathcal{F} \) is a formation defined locally by classes \( \mathcal{F}(p) \) such that \( \mathcal{F}_p \subseteq \mathcal{F}(p) \) for every prime \( p \), then \( \mathcal{F} \) is \( P \)-hypercentrally closed.

Proof. Let \((G, H, K)\) be a \( P \)-hypercentral triple and suppose that \( G/H \in \mathcal{F} \). We have to show that \( G/K \in \mathcal{F} \) and may assume without loss of generality that \( K = 1 \). Then \( G \) is soluble; let \( X/Y \) be a chief factor of \( G \) such that \( |X/Y| \) is a power of the prime \( p \). Then \( X/Y \) is \( G \)-isomorphic either to a chief factor of \( G/H \), and so \( G/C_G(X/Y) \in \mathcal{F}(p) \) since \( G/H \in \mathcal{F} \), or to a chief factor contained in \( H \). By (7) and (8), in the latter case, \( X/Y \) is central or contained in some \( S_i \); in both cases, \( G/C_G(X/Y) \in \mathcal{F} \). Thus in any case, \( G/C_G(X/Y) \in \mathcal{F}(p) \) and \( G \in \mathcal{F} \).

7.5.8 Theorem (Schmidt [1987]). Let \( \mathcal{F} \) be a formation which is invariant under projectivities and \( P \)-hypercentrally closed. If \( G \) is a finite soluble group and \( \phi \) a projectivity from \( G \) to a group \( \overline{G} \), then \( (G)'' = G \).

Proof. Let \( G/N = H, H^\circ = (N^\circ)^\overline{G} \) and \( K^\circ = (N^\circ)^{\overline{G}} \). By 5.4.7, \((G, H, K)\) is a \( P \)-hypercentral triple. Since \( G/N \in \mathcal{F} \) and \( \mathcal{F} \) is a formation, \( G/H \in \mathcal{F} \) and, since \( \mathcal{F} \) is \( P \)-hypercentrally closed, \( G/K \in \mathcal{F} \). But \( N \) is the smallest normal subgroup of \( G \) with factor group in \( \mathcal{F} \). It follows that \( N = K \) and thus \( N^\circ = K^\circ \leq \overline{G} \). Since \( \mathcal{F} \) is invariant under projectivities, \( \overline{G}/N^\circ \in \mathcal{F} \) and therefore \( (G^\circ)^{\overline{G}} = N^\circ \geq \overline{G} \). If we apply this result to the soluble group \( \overline{G} \) and \( \varphi^{-1} \) in place of \( G \) and \( \varphi \), we obtain \( (G^\circ)^{\overline{G}} \varphi^{-1} \geq G^\circ \). Thus \( (G^\circ)^{\overline{G}} = \overline{G} \), as desired.

7.5.9 Corollary. If \( \mathcal{F} \) is a formation defined locally by classes \( \mathcal{F}(p) \) satisfying (3) and (4), then \( (G^\circ)^{\overline{G}} = \overline{G} \) for every projectivity \( \varphi \) from a soluble group \( G \) to a group \( \overline{G} \).

Proof. By 7.5.4 and 7.5.7, \( \mathcal{F} \) is invariant under projectivities and \( P \)-hypercentrally closed. Now 7.5.8 yields the assertion.

Note that the above corollary improves Theorem 7.5.4 and applies to all the formations in Corollary 7.5.5. For \( \mathcal{F} \)-projectors, the situation is even better. They exist in every soluble group if and only if \( \mathcal{F} \) is saturated; and in this case, they behave well.
7.5 Soluble groups

7.5.10 Theorem (Schmidt [1987]). Let $\mathcal{F}$ be a saturated formation which is invariant under projectivities. If $S$ is an $\mathcal{F}$-projector of the soluble group $G$ and $\varphi$ a projectivity from $G$ to a group $\tilde{G}$, then $S^\varphi$ is an $\mathcal{F}$-projector of $\tilde{G}$.

Proof. If $\mathcal{F} = \{1\}$, there is nothing to be shown; so suppose that $\mathcal{F} \neq \{1\}$. It is well-known (see Huppert [1967], p. 710) that $\mathcal{F}$ is defined locally by formations $\mathcal{F}(p)$. By 7.5.6, $\mathcal{F}_p \subseteq \mathcal{F}(p)$ for all primes $p$ and, by 7.5.7, $\mathcal{F}$ is $P$-hypercentrally closed. Now let $N^\varphi \leq G$. We have to show that $S^\varphi N^\varphi / N^\varphi$ is $\mathcal{F}$-maximal in $G / N^\varphi$. Since $S \in \mathcal{F}$ and $\mathcal{F}$ is invariant under projectivities, $S^\varphi \in \mathcal{F}$ and hence $S^\varphi N^\varphi / N^\varphi \simeq S^\varphi / S^\varphi \cap N^\varphi \in \mathcal{F}$.

Let $M \leq G$ such that $S^\varphi N^\varphi \leq M^\varphi$ and $M^\varphi / N^\varphi$ is $\mathcal{F}$-maximal in $G / N^\varphi$. If we put $H = N^G$ and $K = N_G$, then by 5.4.7, $(G, H^\varphi, K^\varphi)$ is a $P$-hypercentral triple. Since $M^\varphi / N^\varphi \in \mathcal{F}$ and $N^\varphi \leq M^\varphi \cap H^\varphi \leq M^\varphi$, we have $M^\varphi H^\varphi / H^\varphi \simeq M^\varphi / M^\varphi \cap H^\varphi \in \mathcal{F}$. Also $(M^\varphi H^\varphi, H^\varphi, K^\varphi)$ is a $P$-hypercentral triple and $\mathcal{F}$ is $P$-hypercentrally closed; it follows that $M^\varphi H^\varphi / K^\varphi \in \mathcal{F}$. Thus $MH/K \in \mathcal{F}$. The choice of $M$ implies that $S^\varphi K^\varphi \leq S^\varphi N^\varphi \leq M^\varphi$ and hence $SK \leq MH$. Since $S$ is an $\mathcal{F}$-projector, $SK/K \in \mathcal{F}$-maximal in $G/K$. It follows that $SK = MH$ and then $S^\varphi N^\varphi \geq S^\varphi K^\varphi \geq M^\varphi$. Thus $S^\varphi N^\varphi = M^\varphi$ and $S^\varphi N^\varphi / N^\varphi$ is $\mathcal{F}$-maximal in $G / N^\varphi$. This shows that $S^\varphi$ is an $\mathcal{F}$-projector of $\tilde{G}$. □

Lattice-theoretic characterizations of the formations studied in 7.5.5 are not known; in fact, this is an interesting problem even for $\mathfrak{Hi}$ or $\mathfrak{N}^2$. On the other hand such characterizations are known for $\mathfrak{M}_L$ and $\mathfrak{S}_1$, and, more generally, $\mathfrak{S}_k$ (see Exercise 1). Then it is possible, under the usual assumptions on $\mathcal{F}$, to give lattice-theoretic characterizations of the $\mathcal{F}$-residual and of $\mathcal{F}$-projectors (see Exercise 5).

A different approach is used by Hauck and Kurzweil [1990] to characterize the prefrattini subgroups discovered by Gaschütz in 1962. They show that for a subgroup $H$ of a finite soluble group $G$, all the subgroups $K \in [G/H]$ which are minimal with respect to the property that the interval $[G/K]$ is complemented are conjugate in $G$; furthermore they identify these groups as the $H$-prefrattini subgroups introduced by Kurzweil [1989]. For $H = 1$, one obtains the prefrattini subgroups, which are therefore characterized in the subgroup lattice of $G$.

Further results on intervals in finite soluble groups are contained in Kurzweil [1985] and Heineken [1987].

### Infinite soluble and generalized soluble groups

Some of the results of Chapters 4 and 5 have been generalized to infinite groups. By 6.6.4, the class of soluble groups is invariant under projectivities, however a lattice-theoretic characterization of this class is not known. In § 6.4 we gave lattice-theoretic characterizations of the classes of hypoabelian, hyperabelian, finitely generated soluble, polycyclic, and supersoluble groups, and mentioned that the classes of hypercyclic and of $SN$-groups can also be characterized.

Some rather special classes of infinite soluble groups were characterized by Plotkin [1957] and Pekelis [1961a]. Intervals in hyperabelian groups were studied by Plaumann, Strambach and Zacher [1985], and Stonehewer and Zacher [1988].
We finish this section by showing that another important class of generalized soluble groups, the class of radical groups, is invariant under projectivities. Actually, we prove a somewhat stronger result on the iterated Hirsch-Plotkin radicals which is a direct generalization of Theorem 4.3.3 on the iterated Fitting subgroups of finite groups.

### Radical groups

Recall that the Hirsch-Plotkin radical $R(G)$ of a group $G$ is the unique maximal normal locally nilpotent subgroup of $G$. It is well-known (see Robinson [1982], p. 344) that

(9) $R(G)$ contains all the ascendant locally nilpotent subgroups of $G$.

Furthermore, since $R(G)$ is locally nilpotent, the elements of finite order in $R(G)$ form a characteristic subgroup $T = T(R(G))$, the torsion subgroup of $R(G)$. Clearly,

(10) $R(G)/T$ is torsion-free and $T$ is a direct product of $p$-groups.

If $G$ is finite, $R(G) = F(G)$ and so the following result generalizes Lemma 4.3.2(b).

7.5.11 Lemma. Let $\varphi$ be a projectivity from $G$ to $\bar{G}$ such that $R(G)^\varphi \neq R(\bar{G})$. Then $G$ is periodic and $P$-decomposable, that is, $G = H \times K$ where $H \in P(n, p)$ for some $n \in \mathbb{N} \cup \{\infty\}$, $p \in P$, and $H$ and $K$ are coprime; furthermore, $\varphi$ or $\varphi^{-1}$ is singular at $p$.

Proof. We assume that the conclusions of the lemma do not hold and show that then

(11) $R(G)^\varphi \leq R(\bar{G})$;

by symmetry, it will follow that $R(G)^\varphi = R(\bar{G})$, the desired contradiction.

Let $R = R(G)$ and suppose first that $R$ is not periodic. Then by 7.3.3, $R^\varphi$ is locally nilpotent. Let $T = T(R)$ be the torsion subgroup of $R$ and let $W = \langle x \in G | o(x) = \infty \rangle$. By (10), $R/T$ is torsion-free. Since $R$ is generated by the elements outside $T$, we have $R \leq W$. By 6.5.1, $T^\varphi \leq W^\varphi$ and $\varphi$ induces a projectivity $\tilde{\varphi}$ from $W/T$ to $W^\varphi/T^\varphi$. If $R/T$ is abelian, then by 6.6.5, $(R/T)^\varphi$ is permutable in $(W/T)^\varphi$. And if $R/T$ is nonabelian, then by 7.2.11, $\tilde{\varphi}$ is induced by an isomorphism on $R/T$ and 6.6.6(c) shows that $(R/T)^\varphi$ is permutable in $(W/T)^\varphi$. In any case, it follows from 6.2.10 that $R^\varphi$ is ascendant in $W^\varphi$. Since $W^\varphi = \langle x \in \bar{G} | o(x) = \infty \rangle \leq \bar{G}$, the subgroup $R^\varphi$ is ascendant in $\bar{G}$. By (9), $R^\varphi \leq R(\bar{G})$, as desired.

Now let $R$ be periodic and suppose, for a contradiction, that (11) does not hold. By (10), $R$ is a direct product of locally nilpotent $p$-groups and, by 1.6.6, $R^\varphi$ is the direct product of the images of these groups. Since $R^\varphi \not\leq R(\bar{G})$, there exists a $p$-component $S$ of $R$ such that $S^\varphi \not\leq R(\bar{G})$. By (9), either $S^\varphi$ is not locally nilpotent and hence by 2.2.7,

(12) $S$ is an elementary abelian $p$-group and $S^\varphi$ is a nonabelian $P$-group;
or $S^o$ is not ascendant in $\overline{G}$ and hence, by 6.2.10, in particular,

(13) $S^o$ is not permutable in $\overline{G}$.

We show first that $G$ is a torsion group. So suppose, for a contradiction, that there exists an element $x$ of infinite order in $G$. Then by 6.6.6 (or 6.2.12), $S^o$ is permutable in $\overline{G}$ and hence (12) is satisfied. Let $P^o$ be the Sylow $p$-subgroup of $S^o$ and $L = S\langle x \rangle$. By 6.5.1, $S^o \leq L^o$ and hence $P^o \leq L^o$ since $P^o$ is characteristic in $S^o$; again by 6.5.1, $P \leq L$. Thus $\varphi$ induces a projectivity from $L/P$ to $L^o/P^o$ and 6.5.11 applied to this projectivity yields that $|S/P| = |S^o/P^o|$. But $|S/P| = p \neq |S^o/P^o|$, a contradiction. Thus

(14) $G$ is periodic.

We want to show next that (12) is satisfied. So assume that (13) holds and let $H = S^\overline{G}$, $N = S_{\overline{G}}$. Then by 6.6.6 applied to the normal $p$-subgroup $S$ of $G$, $G/N = H/N \times K/N$ where $H/N$ and $K/N$ are coprime, $H/N \in P(n, p)$ for some $n \in \mathbb{N} \cup \{\infty\}$, $|S/N| = p$ and $|S^o/N^o| = q \neq p$. Since we assume that the conclusions of the lemma do not hold, $N \neq 1$. By 2.2.7, $S$ is either locally cyclic or elementary abelian. In the latter case, (12) holds, as desired. So suppose that $S$ is locally cyclic. Then $S$ is finite since it contains the maximal subgroup $N$. It follows that the Sylow $p$-subgroup of $H$ is a nilpotent normal subgroup of $G$; hence it is contained in $R(G)$ and therefore is $S$. Thus $H$ is finite, $\varphi$ is singular at $p$ on $H$ and, since $S$ is cyclic of order at least $p^2$, 4.2.6 implies that there exists a normal $p$-complement in $H$. But $S < H$ and hence $H/N$ is a nonabelian group in $P(n, p)$, a contradiction.

It remains to consider the case that (12) is satisfied. Then there exists $M \leq S$ such that $|M| = p$ and $|M^o| \neq p$. We claim that

(15) $M \leq G$.

Since $M^o$ is not permutable in the $P$-group $S^o$, and hence also not in $\overline{G}$, it will follow from 6.6.6 that $G$ satisfies the conclusions of the lemma. This will contradict the choice of $G$.

To prove (15), suppose, for a contradiction, that $M$ is not normal in $G$ and take $x \in G$ such that $M^x \neq M$ and $o(x) = s$ is a prime power. Then

$$W = \langle M, M^x, \ldots, M^{x^{s-1}} \rangle \langle x \rangle$$

is a finite group since all the $M^x$ are minimal subgroups of the abelian group $S$ and their join is invariant under $\langle x \rangle$. Clearly, $\varphi$ induces a $p$-singular projectivity in $W$. Since $M$ is a nonnormal and $S \cap W \geq M$ is a normal $p$-subgroup of $W$, it is clear that (a) of 4.2.6 cannot be satisfied by this projectivity. Thus there exists a normal $p$-complement $C$ in $W$ with abelian factor group $W/C$. If $x$ is a $p$-element, $(S \cap W) \langle x \rangle$ is a $p$-subgroup of $W$ and hence is abelian; and if $x$ is a $p'$-element, then $x \in C$ and $[M, x] \leq S \cap C = 1$. In both cases, $M^x = M$, a contradiction. This proves (15) and the lemma.

Recall that the upper Hirsch-Plotkin series of a group $G$ is the ascending series

$$1 = R_0(G) \leq R_1(G) \leq \cdots$$

in which $R_{s+1}(G)/R_s(G)$ is the Hirsch-Plotkin radical of
G/R, (G) for every ordinal \( \alpha \). This series becomes stationary at a certain ordinal \( \gamma \) and the term \( R, (G) \) is then called the Hirsch-Plotkin hyperradical \( \overline{R}(G) \) of \( G \). Finally, \( G \) is called radical if \( \overline{R}(G) = G \). We come to our main result.

7.5.12 Theorem (Zacher [1982a]). If \( \varphi \) is a projectivity from the group \( G \) to a group \( \overline{G} \), then \( R_n(G) = R_n(\overline{G}) \) for all \( n \in \mathbb{N} \) such that \( n \geq 2 \).

Proof. Suppose that the theorem is false. Then there exists a smallest integer \( n \geq 2 \) for which there is a projectivity \( \varphi \) between two groups \( G \) and \( \overline{G} \) such that \( R_n(G) \neq R_n(\overline{G}) \). If \( G \) is periodic and \( \{S_1, S_2, \ldots\} \) is the set of \( P \)-subgroups which are coprime direct factors of \( G \), then \( G = (S_1 \times S_2 \times \cdots) \times K \) where \( K \) is \( P \)-indecomposable. Since \( n \geq 2 \), \( R_n(G) = (S_1 \times S_2 \times \cdots) \times R_n(K) \). By 1.6.6, \( \overline{G} = (S^1_1 \times S^2_2 \times \cdots) \times K^\circ \) and then \( R_n(\overline{G}) = (S^1_1 \times S^2_2 \times \cdots) \times R_n(K^\circ) \). It follows that \( R_n(K^\circ) \neq R_n(\overline{G}) \). Thus we may assume without loss of generality that \( G = K \) is \( P \)-indecomposable if \( G \) is periodic. Then 7.5.11 yields that

\[
R(G) = R(\overline{G}); \text{ write } R(G) = R.
\]

Let \( \tilde{\varphi} \) be the projectivity induced by \( \varphi \) in \( G/R \). Since

\[
R_{n-1}(G/R)^\circ = (R_n(G)/R)^\circ = R_n(G)/R^\circ \neq R_n(\overline{G})/R^\circ = R_{n-1}(\overline{G}/R^\circ),
\]

the minimality of \( n \) implies that \( n = 2 \). And by 7.5.11 applied to \( \tilde{\varphi} \), \( G/R \) is periodic and \( G/R = H/R \times K/R \) where \( H/R \) and \( K/R \) are coprime, \( H/R \in P(m, p) \) for some \( m \in \mathbb{N} \cup \{\infty\}, p \in P, \) and \( \tilde{\varphi} \) or \( \tilde{\varphi}^{-1} \) is singular at \( p \). Since the situation is symmetric in \( G \) and \( \overline{G} \), we may assume that \( \tilde{\varphi} \) is singular at \( p \). Then if \( H/R \) is elementary abelian, there exist \( x, y \in H \) such that

\[
o(xR) = p = o(yR) \text{ and } |\langle xR \rangle^\circ| = p \neq q = |\langle yR \rangle^\circ|;
\]

and if \( H/R \) is not abelian, there exist \( x, y, z \in H \) such that

\[
o(xR) = p \neq o(yR) = o(zR) \text{ and } |\langle yR \rangle^\circ| = p \neq q = |\langle xR \rangle^\circ| = |\langle zR \rangle^\circ|.
\]

Now suppose first that \( R \) is periodic. Then in both cases we may choose \( x \) as a \( p \)-element and want to show that \( \langle x \rangle \leq H \). For this let \( w \in H \) and consider \( W = \langle x, y, w \rangle \). Every finitely generated subgroup of \( R \) is a finitely generated nilpotent torsion group and therefore is finite; thus \( R \) is locally finite and hence so is \( H \) (see Robinson [1982], pp. 133 and 411). Thus \( W \) is finite and \( \varphi \) induces a \( p \)-singular projectivity in \( W \). By 4.2.6, either every \( p \)-subgroup of \( W \) is normal in \( W \) or \( W \) has a normal \( p \)-complement. In the first case, \( \langle x \rangle^w = \langle x \rangle \), as desired. In the second case, \( WR/R \approx W/W \cap R \) also has a normal \( p \)-complement and hence is abelian. Therefore (17) holds and the Sylow \( p \)-subgroups of \( W \) are not cyclic. Then \( |\langle x \rangle| = p = |\langle x \rangle^\circ| \) and, by 4.2.10, \( x \in Z(W) \). So again \( \langle x \rangle^w = \langle x \rangle \) and, since \( w \in H \) was arbitrary, it follows that \( \langle x \rangle \leq H \). Thus \( \langle x \rangle \) is a subnormal nilpotent subgroup of \( G \) and, by (9), \( \langle x \rangle \leq R \). This contradicts (17) or (18).

It remains to consider the case that \( R \) is not periodic; let \( T = T(R) \). Then \( \varphi \) induces a projectivity from \( G/T \) to \( \overline{G}/T^\circ \) and since our final argument only concerns this projectivity, we may assume that \( T = 1 \). Then \( R \) is torsion-free. Let \( u \in H \backslash R \).
Since $H/R \in P(m, p)$, we obtain $u^r \in R$ for some prime $r$. If $o(u)$ is finite, it follows that $o(u) = r$. Take $1 \neq w \in R$ and consider $W = \langle w, w^*, \ldots, w^{r-1} \rangle \langle u \rangle$. Since $R$ is locally nilpotent, $\langle w, w^*, \ldots, w^{r-1} \rangle = W \cap R$ is a nontrivial nilpotent normal subgroup of $W$. Hence $W$ has a nontrivial torsion-free abelian normal subgroup and by 6.5.12,

(19) $|\langle u \rangle^o| = |\langle u \rangle|$.

If $o(u)$ is infinite and $\varphi$ is induced by an isomorphism on $R$, then $\varphi$ is index preserving on $\langle u^r \rangle \leq R$ and hence, by 6.5.10, on $\langle u \rangle$ also. But $|\langle yR \rangle^o| \neq |\langle yR \rangle|$ in (17) and (18). Therefore it follows from (19) that $o(y)$ is infinite and that $\varphi$ is not induced by an isomorphism on $R$. By 7.2.11 and 2.6.10, $R$ is abelian of rank 1. Now if (17) holds, then by 6.5.12, there is no $p$-element in $H$ and hence $o(x) = o(y) = \infty$. Furthermore, by 6.5.10, $\varphi$ maps $p$-indices in $\langle x \rangle$ to $p$-indices in $\langle x \rangle^o$ and $p$-indices in $\langle y \rangle$ to $q$-indices in $\langle y \rangle^o$. But this is impossible since $\langle x \rangle \cap \langle y \rangle \neq 1$. Similarly, if (18) holds and $o(yR) = r = o(zR)$, then $\varphi$ maps $r$-indices in $\langle y \rangle \cap \langle z \rangle$ to $p$-indices and $q$-indices in $(\langle y \rangle \cap \langle z \rangle)^o$, the same contradiction.

By an obvious transfinite induction, we get the result announced above.

7.5.13 Corollary (Pekelis [1972b], [1976]). If $\varphi$ is a projectivity from the group $G$ to a group $\overline{G}$, then $R(G)^\varphi = \overline{R(G)}$. In particular, the class of radical groups is invariant under projectivities.

**Exercises**

1. (Schmidt [1987]) For $k \in \mathbb{N}$, let us call a lattice $L$ with least element $0$ and greatest element $1$ *poly-k-modular* if there exist elements $x_0, \ldots, x_r \in L$ such that $0 = x_0 \leq \cdots \leq x_r = 1$, $x_i \mod L$ and $[x_{i+1}/x_i]$ is a modular lattice of length at most $k$ ($i = 0, \ldots, r - 1$). Show that a group $G$ lies in $\mathcal{S}_k$ if and only if $L(G)$ is poly-$k$-modular.

2. For every ordering $<$ of the set $\mathbb{P}$ of primes, denote by $\mathcal{X}_<$ the class of groups with a Sylow tower with respect to $<$; thus $G \in \mathcal{X}_<$ if and only if there exists a chain $1 = G_0 \leq \cdots \leq G_r = G$ of normal subgroups $G_i$ of $G$ such that $G_i/G_{i-1}$ is a Sylow $q_i$-subgroup of $G/G_{i-1}$ for $i = 1, \ldots, r$ and $q_r < q_{r-1} < \cdots < q_1$. Show that $\mathcal{X}_<$ is not invariant under projectivities. [Hint: Suppose that $\mathcal{X}_<$ is invariant under projectivities and prove the following assertions.

(a) If $q \mid p - 1$, then $q < p$.

(b) If $q < p < r$, then $o_q(p) \neq o_r(p)$; here $o_q(p)$ is the order of $p$ modulo $q$, that is, the smallest natural number $n$ such that $p^n \equiv 1 \pmod{q}$.

(c) There is no ordering of $\mathbb{P}$ satisfying (a) and (b). (Use a computer to produce a table of all $o_q(p)$ for $p, q < 250$.)]

3. (Schmidt [1973]) For $p \in \mathbb{P}$, let $\mathcal{Q}_p$ be the formation of abelian groups with square-free exponent dividing $p - 1$ and let $\mathcal{Q}$ be the saturated formation defined locally by the $\mathcal{Q}_p$. 
(a) Show that $\mathcal{M}_L \subset \mathfrak{Q} \subset \mathfrak{S}_1$.
(b) Show that $\mathfrak{Q}$ is the smallest nontrivial saturated formation which is invariant under projectivities.

4. Show that not every saturated formation containing $\mathcal{M}_L$ is invariant under projectivities.

5. (Schmidt [1987]) Let $\mathfrak{F}$ be a formation of finite soluble groups and $\mathfrak{L}$ a class of lattices such that for every group $X$, we have $X \in \mathfrak{F}$ if and only if $L(X) \in \mathfrak{L}$. Assume further that $\mathfrak{F}$ is $P$-hypercentrally closed and that $[I/x] \in \mathfrak{L}$ for all $x \mod L \in \mathfrak{L}$. Let $G$ be a finite soluble group.
(a) Show that $G_\mathfrak{F}$ is the smallest modular subgroup $M$ of $G$ such that $[G/M] \in \mathfrak{L}$.
(b) Show that a subgroup $S$ of $G$ is an $\mathfrak{F}$-projector of $G$ if and only if for every $M \mod G$, we have that $[S \cup M/M] \in \mathfrak{L}$ and $[T/M] \not\in \mathfrak{L}$ for all $T \leq G$ such that $S \cup M < T$.

6. (Schmidt [1987]). Let $k \in \mathbb{N}$ and $G$ be a soluble group.
(a) Show that the $\mathfrak{S}_k$-residual of $G$ is the smallest modular subgroup $M$ of $G$ with $[G/M]$ poly-$k$-modular.
(b) Show that the subgroup $S$ of $G$ is an $\mathfrak{S}_k$-projector of $G$ if and only if for every $M \mod G$, the interval $[S \cup M/M]$ is poly-$k$-modular and $[T/M]$ is not poly-$k$-modular for all $T \leq G$ such that $S \cup M < T$.

### 7.6 Direct products of groups

In 1951 Suzuki showed that the direct product of a finite simple group with itself is determined by its subgroup lattice. We use his method to prove a generalization of this result and also study projectivities of direct products of groups more systematically.

#### General properties

If $G = \bigoplus_{\lambda \in \Lambda} G_\lambda$ and $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, the first question to ask is whether $\overline{G} = \bigoplus_{\lambda \in \Lambda} G_\lambda^\varphi$. It is clear that this is false in general: every projectivity from a finite abelian to a nonabelian group is a counterexample. On the other hand, by 1.6.6, the assertion is true in the important case where the $G_\lambda$ are coprime. Other positive results follow from our general theorems on projective images of normal subgroups. We prove an additional assertion of this type.

#### 7.6.1 Lemma. Let $G = H \times K$ and suppose that $X \leq K$ such that $X \cap N(K) = 1$ where $N(K)$ is the norm of $K$. If $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, then $H^\varphi$ is normalized by $X^\varphi$.

**Proof.** Suppose, for a contradiction, that $H^\varphi$ is not normalized by $X^\varphi$ and take $x \in X^\varphi$ such that $(H^\varphi)^x \neq H^\varphi$. Then $M = H^\varphi x^{-1}$ is a modular subgroup of $G$ sat-
isfying \( M \cap K = H^{\varphi^{-1}} \cap K^{\varphi^{-1}} = (H \cap K)^{\varphi^{-1}} = 1 \). For every \( A \leq K \), therefore, \( A = A \cup (M \cap K) = (A \cup M) \cap K \leq A \cup M \) since \( M \mod G \) and \( K \leq G \). Thus \( M \) normalizes \( A \) and it follows that \( (H \cup M) \cap K \leq N(K) \). Now \( H^{\varphi} \cup M^{\varphi} = H^{\varphi} \cup H^{\varphi x} \) is contained in \( H^{\varphi} \cup X^{\varphi} \) and hence \( H \cup M \leq H \times X \). Since \( M \neq H \), we finally obtain that \( 1 \neq (H \cup M) \cap X \geq (H \cup M) \cap K \leq N(K) \), and this contradicts our assumption on \( X \).

In the following theorem we collect an obvious corollary of Lemma 7.6.1 and some consequences of our results on projective images of normal subgroups.

**7.6.2 Theorem.** Let \( G = \bigoplus_{\lambda \in \Lambda} G_{\lambda} \) with subgroups \( G_{\lambda} (\lambda \in \Lambda) \) and let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). Then \( \overline{G} = \bigoplus_{\lambda \in \Lambda} G_{\lambda}^{\varphi} \) if every \( G_{\lambda} \) has one of the following properties.

(i) \( Z(G_{\lambda}) = 1 \).

(ii) \( G_{\lambda} \) is perfect and finite.

(iii) \( G_{\lambda} \) is generated by elements of infinite order and order 2.

**Proof.** We have to show that \( G_{\lambda}^{\varphi} \) is normalized by \( G_{\mu}^{\varphi} \) for every \( \lambda, \mu \in \Lambda \); then all the \( G_{\lambda}^{\varphi} \) are normal subgroups of \( \overline{G} \) and \( \overline{G} = \bigoplus_{\lambda \in \Lambda} G_{\lambda}^{\varphi} \). For this we clearly may assume that \( \lambda \neq \mu \) and \( G = G_{\lambda} \times G_{\mu} \). Suppose first that \( Z(G_{\mu}) = 1 \). Then by 1.4.3, \( N(G_{\mu}) = 1 \) and 7.6.1 yields that \( G_{\lambda}^{\varphi} \) is normalized by \( G_{\mu}^{\varphi} \). If \( G_{\mu} \simeq G_{\lambda} \) is a finite perfect group, then by 6.5.7 and (c) of 5.4.9, \( G_{\lambda}^{\varphi} \leq \overline{G} \). Finally, suppose that \( G_{\mu} = \langle x | x \in X \rangle \) where \( X \leq G_{\mu} \) and \( o(x) \in \{2, \infty\} \) for every \( x \in X \). Let \( x \in X \) and put \( H = \langle G_{\lambda}, x \rangle = G_{\lambda} \times \langle x \rangle \).

If \( o(x) = \infty \), then \( G_{\lambda}^{\varphi} \leq H^{\varphi} \) by 6.5.1. And if \( o(x) = 2 \) and \( G_{\mu}^{\varphi} \) is not normal in \( H^{\varphi} \), then by 6.5.3 there exists \( K \leq G_{\lambda} \) such that \( H^{\varphi} / K^{\varphi} \) are contained in \( P(2,p) \) for some prime \( p \). But \( \langle x \rangle K / K \) is a normal subgroup of order 2 in \( H/K \). Thus \( p = 2 \) and \( H^{\varphi} / K^{\varphi} \) is elementary abelian of order 4. This contradiction shows that \( G_{\lambda}^{\varphi} \leq H^{\varphi} \).

Since \( G_{\mu}^{\varphi} = \langle \langle x \rangle^{\varphi} | x \in X \rangle \), it follows that \( G_{\lambda}^{\varphi} \) is normalized by \( G_{\mu}^{\varphi} \).

We show next that projectivities of direct products sometimes preserve indices and normalizers.

**7.6.3 Lemma.** Let \( G = H \times K \) be a finite group and \( p \) a prime dividing \( |H| \) and \( |K| \). If \( G \) admits a \( p \)-singular projectivity, then \( G \) has elementary abelian \( p \)-subgroups and a normal \( p \)-complement. Furthermore, in one of the two groups \( H \) or \( K \), the \( p \)-Sylow \( p \)-subgroup is a direct factor.

**Proof.** Let \( \varphi \) be a \( p \)-singular projectivity from \( G \) to a group \( \overline{G} \), and let \( P \in \text{Syl}_p(G) \) such that \( |P^\varphi| \neq |P| \). Since \( p \) divides \( |H| \) and \( |K| \), \( P \) is not cyclic and hence elementary abelian, by 2.2.6.

Suppose, for a contradiction, that \( G \) does not possess a normal \( p \)-complement. Then by 4.2.6, \( G = S \times T \) where \( (|S|, |T|) = 1 \) and \( S \) is a \( P \)-group containing \( P \) as a proper normal subgroup. Let \( |S : P| = q \) and \( Q \in \text{Syl}_q(S) \). Then \( Q \in \text{Syl}_q(G) \) and \( |Q| = q \). It follows that \( Q \) is contained in one of the two direct factors of \( G = H \times K \). So \( Q \leq H \), say, and then \( P \cap K \leq C_p(Q) = 1 \) since \( S \) is a \( P \)-group. But \( P \cap K \) is a \( p \)-Sylow \( p \)-subgroup of \( K \), a contradiction. Thus \( G \) has a normal \( p \)-complement \( N \).

We show next that projectivities of direct products sometimes preserve indices and normalizers.
Let $P_0^p$ be the Sylow $p$-subgroup of $P^p$. Then $P_0$ is a maximal subgroup of $P$ and, by 4.2.10, $P_0 \leq Z(G)$. If $P \cap K \leq P_0$, then $P \cap K \leq Z(K)$ and hence $K = (P \cap K) \times (N \cap K)$; and if $P \cap K \not\leq P_0$, then $P = P_0(P \cap K) \leq C_6(H)$ and it follows that $H = (P \cap H) \times (N \cap H)$.

It follows from 7.6.3, or simply from the fact that a nonabelian $P$-group is directly indecomposable, that a projectivity $\varphi$ of a direct product $G = H \times K$ of two isomorphic finite groups $H$ and $K$ is index preserving if $G^\varphi = H^\varphi \times K^\varphi$. Zacher [1981] proved that if $G$ is infinite, it is at least true that $\varphi$ induces index preserving projectivities in the direct factors. We shall need not this but a similar result on normalizers.

7.6.4 Lemma. Let $G = H \times K$, $H \simeq K$ and suppose that $\varphi$ is a projectivity from $G$ to a group $\widetilde{G}$ such that $\widetilde{G} = H^\varphi \times K^\varphi$. Then $H^\varphi \simeq K^\varphi$ and the projectivity $\psi$ induced by $\varphi$ in $H$ is normalizer preserving. In particular, $(X')^\varphi = (X^\psi)'$ and $Z(X)^\varphi = Z(X^\psi)$ for every subgroup $X$ of $H$.

Proof. Clearly, $\varphi$ maps diagonals with respect to $H$ and $K$ onto diagonals with respect to $H^\varphi$ and $K^\varphi$. By 1.6.2, $H^\varphi \simeq K^\varphi$ and hence $\varphi^{-1}$ satisfies the assumptions of the lemma. Therefore to prove that $\psi$ is normalizer preserving, it suffices to show that for every $X \leq H$, the inclusion $N_H(X)^\varphi \leq N_{H^\varphi}(X^\varphi)$ holds; application of this result to $\varphi^{-1}$ will yield the other inclusion.

So let $X \leq H$, $N = N_H(X)$, $\varepsilon: H \to K$ be an isomorphism, $M = N^\varepsilon$, and consider $L = N \times M \leq G$. By 1.6.2, $D = \{x\varepsilon^y|x \in N\}$ is a diagonal in $L$ and, since $X \leq L$, we see that $XD$ is a subgroup of $L$ such that $XD \cap N = X$. Since $\widetilde{G} = H^\varphi \times K^\varphi$, we have $L^\varphi = N^\varphi \times M^\varphi$, and hence $M^\varphi$ centralizes $X^\varphi$. Also, $X^\varphi = (XD)^\varphi \cap N^\varphi \leq (XD)^\varphi$ so that $D^\varphi$ normalizes $X^\varphi$. Since $L^\varphi = D^\varphi \cup M^\varphi$, it follows that $X^\varphi \leq L^\varphi$. In particular, $N_H(X)^\varphi = N^\varphi \leq N_{H^\varphi}(X^\varphi)$, as desired. Thus $\psi$ is normalizer preserving. By 5.6.4, $\psi$ is also centralizer preserving and, by 5.6.2 and 5.6.3, $(X')^\psi = (X^\varphi)'$ and $Z(X)^\psi = Z(X^\varphi)$ for all $X \leq H$.

Note that if $\widetilde{G}$ is not the direct product of $H^\varphi$ and $K^\varphi$, then $\varphi$ in general neither preserves normalizers nor indices. This is shown by the obvious example of $P$-groups.

The direct product of two isomorphic groups

The basic tools in the study of projectivities of a direct product $G = H \times K$ of two isomorphic groups $H$ and $K$ are the diagonals; these are the subgroups $D$ of $G$ such that $D \cap H = 1 = D \cap K$ and $DH = G = DK$. By 1.6.2, these subgroups are in one-to-one correspondence with the isomorphisms from $H$ to $K$, and hence also with the automorphisms of $H$. It follows that a projectivity $\varphi$ from $G$ to a group $\widetilde{G}$ such that $\widetilde{G} = H^\varphi \times K^\varphi$ induces a bijective map $i$ from $\text{Aut} \ H$ to $\text{Aut} \ H^\varphi$. We study this map and want to show first that it induces an isomorphism $i^*$ from $\text{Aut} \ H/Pot \ H$ onto $\text{Aut} \ H^\varphi/Pot \ H^\varphi$. This is particularly interesting if $Z(H) = 1$. For in this case, $Pot \ H = 1$.
and $Z(H^\sigma) = 1$ so that $i = i^*$ is an isomorphism from $\text{Aut } H$ onto $\text{Aut } H^\sigma$. Hence $(\text{Inn } H)^r$ and $\text{Inn } H^\sigma$ are normal subgroups of $\text{Aut } H^\sigma$ isomorphic to $H$ and $H^\sigma$, respectively. We shall give an example to show that $(\text{Inn } H)^r \neq \text{Inn } H^\sigma$, in general. However, our main result will be that $(\text{Inn } H)^r \cap \text{Inn } H^\sigma$ is at least abelian. This will imply that $(\text{Inn } H)^r = \text{Inn } H^\sigma$ and hence $H \cong H^\sigma$ if $H$ has trivial centre and is perfect.

So let $G = H \times K$ and $\varepsilon: H \to K$ be a fixed isomorphism. By 1.6.2, for every isomorphism $\delta$ from $H$ to $K$,

1. $D(\delta) = \{xx^\delta | x \in H\}$

is a diagonal in $G$ (with respect to $H$ and $K$) and every diagonal has this form. For $\sigma \in \text{Aut } H$, let $\hat{\sigma}$ be the autoprojectivity of $G$ induced by the automorphism $\hat{\sigma}$ of $G$ defined by

2. $\hat{\sigma}: xy \to x^{\sigma}y$ for $x \in H$, $y \in K$.

Clearly, $\hat{\sigma}$ is an autoprojectivity of $G$ fixing $H$ and every subgroup of $K$. In particular, it has to map diagonals onto diagonals. Also

3. $D(\tau\varepsilon)^\delta = D(\sigma^{-1}\tau\varepsilon)$

since $(xx^{\tau\varepsilon})^\delta = x^{\sigma}\tau = x^{\sigma}(x^{\tau\varepsilon})^{-1}$ for $x \in H$ and $\sigma \in H$. We study images of diagonals under an autoprojectivity of $G$ fixing $H$ and every subgroup of $K$.

**7.6.5 Lemma.** Let $\psi$ be an autoprojectivity of $G$ such that $H^\psi = H$ and $Y^\psi = Y$ for all $Y \subseteq K$; let $\sigma, \tau \in \text{Aut } H$.

(a) If $D^\psi = D$ for some diagonal $D$, then $X^\psi = X$ for all $X \subseteq D$ and all $X \subseteq H$.

(b) If $X^\psi = X$ for all $X \subseteq H$ and $D(\sigma\varepsilon)^\psi = D(\tau\varepsilon)$, then $\sigma\tau^{-1} \in \text{Pot } H$.

(c) If $D(\varepsilon)^\psi = D(\sigma\varepsilon)$, then $D(\tau\varepsilon)^\psi = D(\sigma\tau\varepsilon)$ for some $\sigma \in \text{Pot } H$.

**Proof.** (a) For every $X \subseteq D$, by Dedekind's law, $X = XH \cap D = (H \cup (XH \cap K)) \cap D$, and this subgroup is clearly invariant under $\psi$. Similarly, if $X \subseteq H$, then $X = XK \cap H = (XK \cap D) \cup K \cap H$ and it follows that $X^\psi = X$.

(b) Let $\alpha = \sigma\tau^{-1}$ and $\mu = \psi \tau^{-1}$. By (3), $D(\sigma\varepsilon)^\mu = D(\tau\varepsilon)^{\tau^{-1}} = D(\sigma\varepsilon)$ and then (a) implies that $X^\mu = X$ for all $X \subseteq H$. Since $\alpha = \mu\psi$, it follows that $X^\mu = X$ for all $X \subseteq H$. Thus $\alpha \in \text{Pot } H$.

(c) This time, let $\mu = \psi \hat{\sigma}$. By (3), $D(\varepsilon)^{\mu} = D(\varepsilon)$ and hence again $X^\mu = X$ for all $X \subseteq H$. Then (b) implies that $D(\tau\varepsilon)^{\mu} = D(\tau\varepsilon)$ where $\tau(\tau\varepsilon)^{-1} = \tau\varepsilon^{-1} \tau^{-1} \in \text{Pot } H$. Thus $\alpha \in \text{Pot } H$ and, by (3), $D(\tau\varepsilon)^{\mu} = D(\tau\varepsilon)^{\tau^{-1}} = D(\sigma\tau\varepsilon)$.

Now suppose that $\varphi$ is a projectivity from $G$ to a group $\overline{G}$ such that $\overline{G} = H^\varphi \times K^\varphi$; put $H^\varphi = \overline{H}$ and $K^\varphi = \overline{K}$. Then $D(\varepsilon)^{\varphi}$ is a diagonal in $\overline{G}$ with respect to $\overline{H}$ and $\overline{K}$ and hence $D(\varepsilon)^{\varphi} = D(\varepsilon')$ for some isomorphism $\varepsilon'$ from $\overline{H}$ onto $\overline{K}$. For $\sigma \in \text{Aut } H$, $D(\sigma\varepsilon)^{\varphi}$ is a diagonal in $\overline{G}$, and hence there exists a unique $\sigma' \in \text{Aut } \overline{H}$ such that $D(\sigma\varepsilon)^{\varphi} = D(\sigma'\varepsilon')$; define $\sigma' = \sigma^r$. Then by 1.6.2, $i$ is a bijective map from $\text{Aut } H$ onto $\text{Aut } \overline{H}$ and we show that it induces an isomorphism in $\text{Aut } H/\text{Pot } H$.

**7.6.6 Theorem (Suzuki [1951a]).** Let $G = H \times K$, $H \cong K$ and let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$ such that $\overline{G} = H^\varphi \times K^\varphi$; put $H^\varphi = \overline{H}$ and $K^\varphi = \overline{K}$. Let $\varepsilon$ be an
isomorphism from $H$ onto $K$, $D(\varepsilon)^\sigma = D(\varepsilon')$ and let $i$ be the map from Aut $H$ onto Aut $H$ defined by

(4) $D(\sigma \varepsilon)^\sigma = D(\sigma' \varepsilon')$ for $\sigma \in$ Aut $H$.

Then $i$ induces an isomorphism $i^*$ from Aut $H$/Pot $H$ onto Aut $H$/Pot $H$.

Proof. Let $\sigma, \tau \in$ Aut $H$. If $\alpha = \sigma^{-1} \in$ Pot $H$, then $\mu = \varphi^{-1} \alpha \varphi$ is an autoprojectivity of $G$ such that $X^\mu = X$ for all subgroups $X$ of $H$ and $K$. Furthermore, by (3) and (4),

$$D(\sigma' \varepsilon')^\mu = D(\sigma \varepsilon)^\sigma = D(\tau \varepsilon)^\tau = D(\tau' \varepsilon').$$

Now (b) of 7.6.5 yields that $\sigma'(\tau')^{-1} \in$ Pot $H$. Conversely, $\sigma'(\tau')^{-1} \in$ Pot $H$ implies $\sigma^{-1} \in$ Pot $H$, since $i^{-1}$ is constructed from $\varepsilon'$ and $\varphi^{-1}$ in the same way as $i$ from $\varepsilon$ and $\varphi$. Thus $i$ induces a bijective map $i^*$ from Aut $H$/Pot $H$ onto Aut $H$/Pot $H$. For $\psi = \varphi^{-1} \alpha^{-1} \varphi$, $D(\varepsilon')^{\psi} = D(\sigma \varepsilon)^{\psi} = D(\sigma' \varepsilon')$, by (3), and hence by (c) of 7.6.5 there exists $\beta \in$ Pot $H$ such that $D(\sigma' \varepsilon' \beta) \varepsilon' = D(\tau' \varepsilon')^\psi = D(\sigma \varepsilon)^{\sigma} = D((\sigma \tau)' \varepsilon')$. Thus $(\sigma \tau)' = \sigma' \tau' \beta$ and $i^*$ is an isomorphism.

The above theorem is the essence of Suzuki's method. If $H$ is a nonabelian simple group, then by 6.4.2 and 6.5.4, $H^\sigma$ is also simple and $\overline{G} = H^\sigma \times K^\sigma$. Hence the assumptions of Theorem 7.6.6 are satisfied and, furthermore, Pot $H = 1$ and Inn $H$ is the unique minimal normal subgroup of Aut $H$. It follows that $i = i^*$ is an isomorphism and $H \simeq$ (Inn $H)^\sigma = $ Inn $H^\sigma = K^\sigma$. Thus we get the theorem, proved by Suzuki [1951a] in the finite case and by Zacher [1981] in general, that $G$ is determined by its subgroup lattice if $H$ is a nonabelian simple group. We want to prove a more general result, and for this we have to study the map $i$ more closely. We mention in passing that $i^*$ is independent of the choice of $\varepsilon$ and that, in general, $i$ is not an isomorphism. This can be seen, for example, if $H$ is a cyclic group of prime order $p \geq 5$.

7.6.7 Lemma. Suppose that the hypotheses of Theorem 7.6.6 are satisfied and let $X \leq H$ and $\alpha \in$ Aut $H$. Then

(a) $(X^\alpha)^\sigma = (X^\alpha)^\varepsilon$,
(b) $X^\varepsilon = X$ if and only if $(X^\alpha)^\varepsilon = X^\sigma$, and
(c) $[X, x]^\sigma = [X^\sigma, x^\varepsilon]$ if $X^\varepsilon = X$.

In particular, $[H, x]^\sigma = [\overline{H}, x^\varepsilon]$ and $C_H(x)^\sigma = C_{\overline{H}}(x^\varepsilon)$.

Proof. (a) Clearly, $(X \times X^\varepsilon) \cap D(\varepsilon)$ is a diagonal in $X \times X^\varepsilon \leq G$. Since $\overline{G} = \overline{H} \times \overline{K}$, it follows that $(X \times X^\varepsilon)^\sigma = X^\sigma \times (X^\varepsilon)^\sigma$ and hence $((X \times X^\varepsilon) \cap D(\varepsilon))^\sigma = (X \times (X^\varepsilon)^\sigma) \cap D(\varepsilon')$ is a diagonal in $X^\sigma \times (X^\varepsilon)^\sigma$. It follows that $(X^\sigma)^\varepsilon = (X^\sigma)^\varepsilon$.

(b) Let us define $D(X, x, \varepsilon) = D(\varepsilon x) \cap (X \times X^\varepsilon)$. Then by (a) and (4),

(5) $D(X, x, \varepsilon)^\sigma = D(\varepsilon x)^\sigma \cap (X^\sigma \times (X^\varepsilon)^\sigma) = (X^\varepsilon \times (X^\varepsilon)^\varepsilon) \cap (X^\sigma \times (X^\varepsilon)^\varepsilon) = D(X^\sigma, x^\varepsilon, \varepsilon')$.

By 1.6.2, $D(X, x, \varepsilon)$ is a diagonal in $X \times X^\varepsilon$ if and only if the map $x \mapsto x^\varepsilon$ ($x \in X$) is an isomorphism from $X$ onto $X^\varepsilon$. This is the case if and only if $X^\varepsilon = X$. Similarly, $D(X^\sigma, x^\varepsilon, \varepsilon')$ is a diagonal in $X^\sigma \times (X^\varepsilon)^\varepsilon$ if and only if $(X^\sigma)^\varepsilon = X^\sigma$. And finally, since
φ is a projectivity, \(D(X, \alpha, \epsilon)\) is a diagonal in \(X \times X^e\) if and only if \(D(X, \alpha, \epsilon) = D(X^e, \alpha^e, \epsilon')\) is a diagonal in \(X^e \times (X^e)^o = X^o \times (X^o)^e\). Summarizing, we obtain (b).

(c) Suppose that \(\alpha, \beta \in \text{Aut} H\) such that \(X^o = X = X^\beta\) and let \(N \leq X\). Then we claim that

\[(6) \ D(X, \alpha, \epsilon) \leq D(X, \beta, \epsilon)N\] if and only if \([X, \alpha^e] = D(X, \alpha, \epsilon)\] is a diagonal in \(X^o \times (X^o)^e = X^o \times (X^o)^e\). Summarizing, we obtain (b).

To prove (c), we apply (6) with \(N = [X, \alpha]\) and \(\beta = \text{id}_H\), the trivial automorphism; note that \(N \leq X\), by (6) of § 1.5. Thus by (6), \(D(X, \alpha, \epsilon) \leq D(X, \text{id}_H, \epsilon)N\). By 7.6.4, \(N^o \leq X^o\) and, since \(\phi\) is a projectivity, using (5) we get that \(D(X^o, \alpha^e, \epsilon') \leq D(X^o, \text{id}_H, \epsilon)N^o\). Now (4) shows that \((\text{id}_H)^e = \text{id}_H^e\) and, by (b), \((X^o)^e = X^o\). Hence (6) for \(G = H \times K\) yields that \([X^o, \alpha^e] \leq N^o = [X, \alpha]^o\). If we apply this result to \(\phi^e\) and \(i^e\), we obtain that \([X, \alpha] \leq [X^o, \alpha^e]^o\) and (c) follows. Now \(X = H\) and \(X = C_H(x)\) satisfy the assumption of (c). It follows that \([H, \alpha]^o = [H, \alpha']^o\] and \([C_H(x)^o, \alpha^e] = [C_H(x), x]^o\) = 1. Thus \(C_H(x)^o \leq C_H(x')^o\) and, if we apply this result to \(\phi^e\) and \(i^e\), we get the other inclusion. □

We come to our main result.

7.6.8 Theorem (Schmidt [1981]). Let \(G = H \times K\) where \(H \approx K\) and \(Z(H) = 1\) and suppose that \(\phi\) is a projectivity from \(G\) to a group \(\bar{G}\). Put \(H^o = H\) and \(K^o = K\), let \(\sigma\) be the natural isomorphism from \(H\) onto \(\text{Inn} H\), that is, \(x^\sigma = z^{-1}xz\) for \(x, z \in H\); similarly \(\tau\) for \(\bar{H}\).

(a) Then \(\bar{G} = H \times K\), \(\bar{H} \approx K\), \(Z(\bar{H}) = 1\) and the map \(i\) constructed in 7.6.6 is an isomorphism from \(\text{Aut} H\) onto \(\text{Aut} \bar{H}\).

(b) If \(N\) is a characteristic subgroup of \(H\) or a normal subgroup of \(H\) contained in \(H^e\), then \(N^o \approx N^o / N\cap N^o\) is abelian. In particular, \((\text{Inn} H)^e \approx \text{Inn} \bar{H}(/(\text{Inn} H)^e) \cap \text{Inn} \bar{H}\) is abelian.

(c) The maximal perfect subgroup of \(H\) is isomorphic to the maximal perfect subgroup of \(\bar{H}\).

Proof. (a) By 7.6.2, \(\bar{G} = H \times K\) and then 7.6.4 implies that \(\bar{H} \approx K\) and \(Z(\bar{H}) = 1\). It follows from 1.4.3 that \(\text{Pot} H = 1 = \text{Pot} \bar{H}\) and, by 7.6.6, \(i = i^e\) is an isomorphism from \(\text{Aut} H\) onto \(\text{Aut} \bar{H}\).

(b) Let \(X \leq H\), \(\Sigma = X^\sigma \cup X^\sigma\), \(\Delta = X^\sigma \cap X^\sigma\), and suppose that \(X^\sigma \leq \Sigma\) and \(X^\sigma \leq \Sigma\). Then \(\Sigma/\Delta = X^\sigma/\Delta \times X^\sigma/\Delta\) and we show that

\[(7) \ \Sigma/\Delta\] is abelian.

For this let \(\alpha \in X^\sigma\) and \(x \in X^\sigma\); let \(D \leq X\) such that \(D^\sigma = \Delta\). For \(z \in \bar{H}\) and \(\beta \in \text{Aut} \bar{H}\),

\[z^{[x, \beta]} = (x^{-1}(xz^{-1})^\beta)^{x^\beta} = (x^{-1}(x^\beta)^{-1}z x^{-1}x^\beta = z^{[x, \beta]}\]
so that \([x', \beta] = [x, \beta]^t\), a well-known formula. It implies that \([x, x']^t = [x', x']^t \in [X^\sigma, X^\sigma] \leq \Delta\) since \(X^\sigma\) and \(X^\sigma\) are normal subgroups of \(\Sigma\). Therefore \([x, x']^t \in \Delta^t = D^\sigma\) for all \(x \in X^\sigma\) and hence \([X^\sigma, x']^t \leq D^\sigma\). Since \(x \in X^\sigma\), we have \(X^\sigma = X\) and, by (c) of 7.6.7, it follows that \([X, x] \leq D\). This holds for all \(x \in X^\sigma\); thus \(X' = [X, X^\sigma] \leq D\). By 7.6.4, \((X^\sigma)^t = (X'^t)^t \leq D^\sigma\) and hence \(X^\sigma / D^\sigma\) is abelian. So, finally, \(X^\sigma / D^\sigma = X^\sigma / \Delta\) is abelian. If we apply this result to \(\varphi^{-1}\) and \(t^{-1}\), we obtain that \(X^\sigma / X^\sigma t = X^\sigma / \Delta\) is abelian. Thus \(X^\sigma / X^\sigma t \cap X^\sigma = X^\sigma / \Delta\) is abelian and (7) holds.

Now if \(N\) is a characteristic subgroup of \(H\), then by (b) of 7.6.7, \(N^\sigma\) is characteristic in \(\bar{H}\) and hence \(N^\sigma_{t'}\) and \(N^\sigma_{t'}\) are normal subgroups of \(\text{Aut} \bar{H}\). By (7), \(N^\sigma_{t'} N^\sigma_{t' n t'} / N^\sigma_{t'} \) is abelian. In particular, \((\text{Inn} H)' \cap \text{Inn} \bar{H}\) is abelian and hence \((H')^\sigma_{t'}\) and \((H')^t\) are contained in \(\Delta = (\text{Inn} H)^t \cap \text{Inn} \bar{H}\). Thus if \(N\) is a normal subgroup of \(H\) contained in \(H'\), then by 7.6.4, \(N^\sigma\) is a normal subgroup of \(\bar{H}\) contained in \(H'\). It follows that \(N^\sigma_{t'}\) and \(N^\sigma_{t'}\) are normal subgroups of \(\Delta \geq N^\sigma_{t'} N^\sigma_{t'}\). By (7), \(N^\sigma_{t'} N^\sigma_{t'} / N^\sigma_{t'} \cap N^\sigma_{t'}\) is abelian.

(c) Let \(S\) be the maximal perfect subgroup of \(H\). Then \(S\) is characteristic in \(H\) and, by 7.6.4 (or 6.4.5), \(S^\sigma\) is the maximal perfect subgroup of \(\bar{H}\). It follows from (b) that \(S^\sigma t = S^\sigma t \cap S^\sigma t = S^\sigma t\) and hence \(S^\sigma = S^\sigma t^{-1} \simeq S\).

7.6.9 Corollary. If \(H\) is a perfect group with trivial centre and \(K \simeq H\), then \(G = H \times K\) is determined by its subgroup lattice.

Proof. By (a) of 7.6.8, a projective image \(G^\sigma\) of \(G\) satisfies \(G^\sigma = H^\sigma \times K^\sigma\) where \(H^\sigma \simeq K^\sigma\) and, by (c), \(H^\sigma \simeq H\). Thus \(G^\sigma \simeq G\).

The main idea in Theorem 7.6.8 is to try to prove that \((\text{Inn} H)' = \text{Inn} \bar{H}\); since \(H \simeq \text{Inn} H\) and \(H \simeq \text{Inn} \bar{H}\), this implies that \(\bar{H} \simeq H\). We were able to do this when \(H = H'\); it can also be proved if this hypothesis is replaced by the assumption that \(H\) is generated by involutions (see Zacher [1981]). We leave this as an exercise for the reader, and remark that in 7.7.8 we shall prove \(\bar{H} \simeq H\) in this situation using...
quite different methods. We want to show now that 7.6.9 does not hold without the assumption that \( H \) is perfect so that in the situation of Theorem 7.6.8, in general, \((\text{Inn } H)' \neq \text{Inn } \overline{H}\).

7.6.10 Example. Let \( q \geq 7 \) and \( p \) be primes such that \( q \mid p - 1 \), and let \( r \in \mathbb{N} \) such that \( r \neq 1 \pmod{p} \) and \( r^q \equiv 1 \pmod{p} \). Recall that in 5.6.8 for every \( \mu \in \{2, \ldots, q - 1\} \), we defined the Rottländer group

\[
G_\mu = \langle x, y, a \mid x^p = y^p = a^q = [x, y] = 1, a^{-1}xa = x^r, a^{-1}ya = y^{r''} \rangle
\]

and proved that all the \( G_\mu \) are lattice-isomorphic, but \( G_\mu \cong G_\nu \) if and only if \( \mu = \nu \) or \( \mu \nu \equiv 1 \pmod{q} \). We claim that if \( \mu \neq q - 1 \neq \nu \), then \( G_\mu \times G_\nu \) and \( G_\nu \times G_\nu \) also have isomorphic subgroup lattices.

Proof. Let \( H = \langle x_1, x_2, a \rangle \cong G_\mu \cong K = \langle x_3, x_4, b \rangle \) such that \( o(x_i) = p, x_ix_j = x_jx_i \) for all \( i, j \) and \( x_i^a = x_i^b, x_i^a = x_i^b, x_3^b = x_4^b = x_4^a \). Let \( G = H \times K = NA \) where \( N = \langle x_1, x_2, x_3, x_4 \rangle \) and \( A = \langle a, b \rangle \), and put \( N_i = \langle x_i \rangle \) for \( i = 1, \ldots, 4 \). We determine the centralizers and eigenspaces in \( N \) of the subgroups of order \( q \) of \( A \). Since \( p \not\equiv 0 \pmod{q} \), we obtain \( CN(a) = N_3 \times N_4, CN(b) = N_1 \times N_2 \) and \( CN(ab^\lambda) = 1 \) for \( 0 < \lambda < q \). Since \( \mu \neq 0 \pmod{q} \), the other eigenspaces of \( a \) are \( N_1 \) and \( N_2 \), those of \( b \) are \( N_3 \) and \( N_4 \), and those of \( ab \) are \( N_1 \times N_3 \) and \( N_2 \times N_4 \). Since \( \mu \neq q - 1, \mu^2 \neq 1 \pmod{q} \) and there exists \( \mu' \in \{2, \ldots, q - 2\} \) such that \( \mu \neq \mu' \) and \( \mu \mu' \equiv 1 \pmod{q} \). Then the eigenspaces of \( ab^\mu \) are \( N_1, N_2 \times N_3, N_4 \) and those of \( ab^\mu \) are \( N_1 \times N_4, N_2, N_3 \). Finally, if \( \lambda \not\in \{1, \mu, \mu'\} \), all the exponents \( r, r^\mu, r^\lambda, r^{\mu \lambda} \) are pairwise incongruent modulo \( p \), and hence \( N_1, N_2, N_3, N_4 \) are the eigenspaces of \( ab^\lambda \). This eigenspace situation is more or less independent of \( \mu \). Let \( \overline{H} = \langle x_1, x_2, c \rangle \cong G_\nu \cong K = \langle x_3, x_4, d \rangle \) where \( x_1^c = x_1^d, x_2^c = x_2^d, x_3^d = x_4^d = x_4^c \), and define \( \overline{G} = \overline{H} \times \overline{K} = NB \) where \( B = \langle c, d \rangle \); let \( v \in \{2, \ldots, q - 2\} \) such that \( vv' \equiv 1 \pmod{p} \). Then the identity \( \sigma \) on \( N \) and every projectivity \( \tau \) from \( A \) to \( B \) such that \( \langle a \rangle^\tau = \langle c \rangle, \langle b \rangle^\tau = \langle d \rangle, \langle ab \rangle^\tau = \langle cd \rangle, \langle ab^\nu \rangle^\tau = \langle cd^\nu \rangle \) satisfy the assumptions of Theorem 4.1.6. Indeed, since \( q \mid p - 1 \), a subspace \( P \) of \( N \) is invariant under an element of \( A \) or \( B \) if and only if it is a direct sum of subspaces of eigenspaces of this element. By 4.1.6, there exists a projectivity from \( G \) to \( \overline{G} \).

It is easy to see that for the projectivity constructed above, \((\text{Inn } H)' = (\text{Inn } \overline{H})'\) in the notation of 7.6.8. It is an open problem whether this holds in general.

**Direct products of isomorphic groups**

The Fundamental Theorem of Projective Geometry states that every isomorphism of the lattice of subspaces of a vector space of dimension \( n \geq 3 \) onto the lattice of subspaces of another vector space is induced by a semilinear map between the two spaces. In particular, the ground fields are isomorphic. This theorem suggests the following general question.
Classes of groups and their projectivities

Given an algebraic structure $\mathcal{U}$ closed with respect to direct products, does there exist an integer $n = n(\mathcal{U})$ such that the $n$-fold direct product of every member of $\mathcal{U}$ is determined by its lattice of substructures?

The $P$-groups show that the cyclic groups of prime order $p > 2$ are counter-examples to this conjecture for the algebraic structure “group”; and there are also less trivial examples (see Exercise 7). Therefore we have to make additional assumptions on the projectivities considered. The most natural one is that they preserve the direct decomposition. This leads to the following two problems.

7.6.11 Problem. Let $\mathfrak{X}$ be a class of groups. Does there exist an integer $n$ such that whenever $X \in \mathfrak{X}$, $G = X_1 \times \cdots \times X_n$ with $X_i \cong X$ for all $i = 1, \ldots, n$, and $\varphi$ is a projectivity from $G$ to a group $\widetilde{G}$ satisfying $\widetilde{G} = X_1^\varphi \times \cdots \times X_n^\varphi$, then

(A) $X_1^\varphi \cong X_1$ (and hence $G \cong \widetilde{G}$), or even

(B) $\varphi$ is induced by an isomorphism?

In particular, does there exist such an integer for the class $\mathfrak{X}$ of all groups?

Clearly when $n = 1$ (A) or (B) is satisfied precisely when every group in $\mathfrak{X}$ is determined or strongly determined by its subgroup lattice. So the two problems in 7.6.11 can be considered as natural generalizations of the main problems studied in this chapter. We want to discuss them briefly without giving proofs since most of the results known are rather special and require long and technical computations.

Problem (A) is wide open. Example 7.6.10 shows that the Rottländer groups need at least three direct factors. But there is no example known in which $n = 3$ would not suffice. So it might be true that, as in the Fundamental Theorem of Projective Geometry, $n = 3$ will solve Problem (A) for the class $\mathfrak{X}$ of all groups. This was proved by Baer for abelian groups (see 2.6.7 and 2.6.10, and note that the assumptions in 7.6.11 imply that $\widetilde{G}$ is abelian). It is also proved in 7.6.9 for perfect groups with trivial centre; for these groups and for abelian groups with elements of infinite order, even $n = 2$ suffices. Another class of groups is handled by Schmidt [1982] who proves that if $X$ is a finite group with a proper elementary abelian normal Hall subgroup $N$ such that $C_X(N) = N$, then $n = 3$ suffices. Note that the Rottländer groups are covered by this theorem.

Problem (B) is solved for the class $\mathfrak{X}$ of all groups. There are groups, even with trivial centre, such that no integer $n$ has the required property.

7.6.12 Example (Schmidt [1982]). Let $p > 2$ be a prime and $n \in \mathbb{N}$.

(a) Let $G = A_1B_1 \times A_2B_2$ be a finite group with elementary abelian normal $p$-subgroups $A_i, (p, |B_i|) = 1 = (|B_1|, |B_2|)$ and $C_A_i(B_i) = 1$ for $i = 1, 2$. Let $N = A_1 \times A_2, H = B_1 \times B_2$, take $s \in \mathbb{N}$ such that $0 \neq s \neq 1 \pmod{p}$, and define $\sigma: N \to N$ by $(xy)^\sigma = xy^s$ for $x \in A_1, y \in A_2$. Finally, for $U \leq G$, that is $U = MK^z$ where $z \in N, M \leq N, K \leq N_{H}(M)$ (see 4.1.5), define $U^\sigma = MK^{z^\sigma}$. Then $\varphi$ is an autoprojectivity of $G$ which induces the trivial autoprojectivity in $N$ and in $H$ and which is not induced by an automorphism of $G$.

(b) Let $q$ and $r$ be different primes dividing $p - 1$ and let $X$ be the direct product of a nonabelian group of order $pq$ and a nonabelian group of order $pr$. If
G = X_1 \times \cdots \times X_n where X_i \simeq X for i = 1, \ldots, n, then there exists an autoprojectivity \phi of G satisfying X_i^\phi = X_i for all i which is not induced by an automorphism of G. Clearly, |X| = p^2qr and Z(X) = 1.

Proof. (a) First note that N is an elementary abelian normal Hall subgroup of G with complement H. Since (|B_1|, |B_2|) = 1, every subgroup K of H has the form K = (K \cap B_1) \times (K \cap B_2), and hence C_n(K) = C_n(K \cap B_1) \cap C_n(K \cap B_2) = C_{A_1}(K \cap B_1) \times C_{A_2}(K \cap B_2). Since \sigma fixes every subgroup of A_1 and A_2, it follows that C_n(K)^\sigma = C_n(K). If M \leq N is invariant under K, then by 4.1.3 and (1) of §1.5, M = [M, K] \times C_M(K) and [M, K] = [M, K \cap B_1][M, K \cap B_2]^\sim. Since [M, K \cap B_2] \leq A_2 and [M, K \cap B_1] \leq A_1, we obtain that [M, K]^\sigma = [M, K]. Thus if C_n(K) \leq M, then M = [M, K] \times C_n(K) and hence M^\sigma = M.

Now let U_i \leq G (i = 1, 2), that is U_i = M_i K_i^\sigma_i where z_i \in N, M_i \leq N and K_i \leq N H(M_i), and suppose that U_1 \leq U_2. Then by 4.1.5, K_1 \leq K_2, M_1 \leq M_2 and z_1 z_2^{-1} \in C_n(K_1) M_2. Therefore C_n(K_2) \leq C_n(K_1) and, since \sigma is an isomorphism,

\[ z_1(z_2^{-1})^{-1} = (z_1 z_2^{-1})^\sigma \in (C_n(K_1) C_n(K_2) M_2)^\sigma = C_n(K_1) C_n(K_2) M_2 = C_n(K_1) M_2. \]

Again by 4.1.5, M_1 K_1^{s_1} \leq M_2 K_2^{s_2} and hence \phi is well-defined and order preserving. The map constructed with respect to \sigma^{-1} in the same way as \phi with respect to \sigma is the inverse of \phi. Thus \phi is a projectivity which clearly fixes every subgroup of N and H. An automorphism \mu of G inducing \phi therefore would have to fix H and to induce a power automorphism in N; on the other hand, it would satisfy H^\mu = (H^2)^\mu = (H^2)^\mu = H^{2^\mu} and, since C_n(H) = 1, it would follow from 4.1.1 that z^s = z^2u for all z \in N. But, since s \neq 1 (mod p), \sigma is not a power automorphism.

(b) Let X_i = M_i Q_i \times L_i R_i where |M_i| = |L_i| = p, |Q_i| = q and |R_i| = r for all i = 1, \ldots, n. Then A_1 = M_1 \times \cdots \times M_n, A_2 = L_1 \times \cdots \times L_n, B_1 = Q_1 \times \cdots \times Q_n and B_2 = R_1 \times \cdots \times R_n satisfy the assumptions of (a). The autoprojectivity \phi constructed there fixes every subgroup of N and H, hence every M_i, L_i, Q_i, R_i and so, finally, all the X_i.

Similar examples of groups of order \( p^n q^e \) with nontrivial centre are given by Schenke [1987b]; see Exercise 8. Although these examples destroy any hope for a general theorem, there are positive results for interesting classes of groups. First of all note that in Problem (A) every integer greater than n also has the desired property; but this is not so clear for Problem (B). Baer's theorems mentioned above show that (B) holds for every \( n \geq 2 \) if \( X \) consists of abelian groups with elements of infinite order, and for every \( n \geq 3 \) if \( X \) is the class of all abelian groups. In 7.7.6 we shall prove that (B) holds for \( n = 2 \) if \( X \) is the class of dihedral groups. Again Schmidt [1982] proves that every \( n \geq 3 \) satisfies (B) for the class of all finite groups \( X = NH \) with normal elementary abelian \( p \)-subgroup \( N \) and abelian \( q \)-group \( H \) operating faithfully on \( N \), \( p \) and \( q \) being different primes. Also Schenke [1987], [1987b] studies finite \( p \)-groups and proves that (B) holds for every

(8) \( n \geq 2 \) if \( X \) has class at most 4 and exponent \( p \),

(9) \( n \geq p - 2 \) if \( X \) is metabelian of exponent \( p \),

(10) \( n \geq 3 \) if \( X \) is of class 2 and \( p \neq 2 \).
In addition, for every prime \( p \geq 7 \), he constructs a group of class 5 and exponent \( p \) for which \( n = 2 \) does not satisfy (B). And he shows that for every \( n \in \mathbb{N} \) there exists a prime \( p \) and a metabelian group \( X \) of exponent \( p \) such that \( n \) does not satisfy (B) for \( X \). This shows that although the bound \( p - 2 \) in (9) might not be best possible, there is no integer \( n \) satisfying (B) for all metabelian groups of exponent \( p \) and all primes \( p \).

The methods of Schenke and Schmidt are quite different. In both cases, the results follow from more general investigations. Schmidt considers under which conditions a projectivity \( \varphi \) of a finite group \( G = NH \) with elementary abelian normal Hall subgroup \( N \) and complement \( H \) is induced by an isomorphism. He shows that this is true in a certain minimal situation and then examines how to extend isomorphisms inducing \( \varphi \) on subgroups of the form \( NH_i, H_i \leq H \). In this way he is able to show that \( \varphi \) is induced by an isomorphism if \( H \) is an abelian \( q \)-group with three independent elements of maximal order and \( C_H(N) = 1 \). This implies the result mentioned above.

Schenke’s method is more closely related to the given problem. He uses Baer’s ideas to study a projectivity \( \varphi \) from a direct product \( G = H \times K \) of two \( p \)-groups \( H \) and \( K \) of equal exponent to a \( p \)-group \( \tilde{G} = H^* \times K^* \). His main tools are Baer maps; these are maps \( \alpha: G \to \tilde{G} \) for which there exist \( x \in H, y \in K \) with \( o(x) = o(y) = \text{Exp } G \) such that for all \( a \in H \) and \( b \in K \),

\[
(11) \quad a^x = f(a; y, y^x, \varphi), \quad b^y = f(b; x, x^y, \varphi) \quad \text{and} \quad (ab)^y = a^xb^y
\]

where \( f \) is the map defined in 2.6.2. In the situation of 7.6.11, Schenke shows that every Baer map \( \alpha \) induces \( \varphi \), and that for every automorphism \( \sigma \) of \( X_i, \sigma_i^{-1}\sigma \) is an automorphism of \( X_i^\sigma \) if \( \sigma_i \) is the restriction of \( \sigma \) to \( X_i \). Using this property, he is able to handle the minimal situation that \( X \) is the nonabelian group of order \( p^3 \) and exponent \( p \). Then he uses induction to show that under the assumptions of (8)–(10) there is a Baer map which is an isomorphism.

**Wreath products**

A well-known construction which uses direct products of isomorphic groups is the wreath product of two groups \( A \) and \( B \). To define this, let \( N \) be the set of functions \( f: B \to A \) satisfying \( f(b) = 1 \) for all but a finite number of elements \( b \in B \). With the obvious multiplication, \( f_1f_2(b) = f_1(b)f_2(b) (b \in B), N \) is a group, and an action of \( B \) on \( N \) is established as follows: if \( f \in N \) and \( b \in B \), then \( f^b \) is the function defined by the equation

\[
(12) \quad f^b(c) = f(cb^{-1}) \quad \text{for } c \in B.
\]

It is easy to check that, with this definition, \( B \) acts as a group of automorphisms on \( N \). The semidirect product of \( N \) with \( B \) acting as above is the (standard restricted) wreath product of \( A \) with \( B \) and is denoted by \( A \wr B \); the normal subgroup \( N \) is called the base group of the wreath product. The following properties of \( A \wr B = NB \) are easy to prove and are, in fact, well-known (see Suzuki [1982], pp. 268–279).
For \( b \in B \), let \( A_b = \{ f \in N | f(c) = 1 \text{ for all } b \neq c \in B \} \). Then

\[(13) \quad N = \bigoplus_{b \in B} A_b, \quad A_b \cong A \text{ and } (A_b)^c = A_{bc} \text{ for all } b, c \in B.\]

Conversely, this property characterizes the wreath product.

\[(14) \quad \text{If } G = MC \text{ where } M = \bigoplus_{c \in C} A_c \text{ and } (A_c)^d = A_{cd} \text{ for all } c, d \in C, \text{ then } G \cong M_1 \, \wr \, C.\]

As a consequence we get the following two properties which are basic for inductive proofs.

\[(15) \quad \text{If } X \subseteq A_b (b \in B) \text{ and } C \subseteq B, \text{ then } \langle X, C \rangle \cong X \, \wr \, C.\]

\[(16) \quad \text{If } C \subseteq B \text{ and } T \text{ is a left transversal to } C \text{ in } B, \text{ then } NC \cong A \, \wr \, C \text{ where } A = \bigoplus_{t \in T} A_t.\]

We now briefly report the known results on projectivities of wreath products without giving proofs. So let \( G = A \, \wr \, B \) with nontrivial groups \( A, B \) and let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). First of all, the image \( N^\varphi \) of the base group \( N \) is a normal subgroup of \( G \) (see Menegazzo [1973]). However, in general, \( \overline{G} \) need not be a wreath product. For example, if \( |A| = 29 \) and \( |B| = 3 \), then \( |N| = 29^3 \) and, since \( B \) centralizes the “diagonal” \( \{(a, a, a) | a \in A\} \) of \( N \) but does not centralize \( N \), it follows (see 4.1.7) that \( N = N_1 \times N_2 \) where \( |N_1| = 29, |N_2| = 29^2, N_1 = C_N(B) \) and \( B \) operates irreducibly on \( N_2 \). Since \( 5|29^2 - 1 \), a group \( C \) of order 5 can operate irreducibly on \( N_2 \) and, by 4.1.6, \( G = N_1 \times N_2 B \) is lattice-isomorphic to \( G^* = N_1 \times N_2 C \). Clearly, \( G^* \) is not a wreath product. On the other hand, there is the following positive result.

7.6.13 Theorem (Menegazzo [1973]). Let \( G = A \, \wr \, B \) where \( A \neq 1 \) and \( 2 < |B| < \infty \) and let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \).

(a) Then \( \overline{G} = N^\varphi B^\varphi, N^\varphi \leq \overline{G}, N^\varphi = \bigoplus_{b \in B} A^\varphi_b \) and \( A^\varphi_b \cong A^\varphi \) for all \( b, c \in B \).

(b) If \( A \) is locally finite and \( |B^\varphi| = |B| \), then \( N^\varphi = \bigoplus_{b \in B} (A^\varphi_b)^b \) and hence \( \overline{G} \cong A^\varphi \, \wr \, B^\varphi \).

Here (b) is an immediate consequence of (a). Indeed, since \( A^\varphi_b \leq N^\varphi \) and \( N^\varphi = (A_1 \cup B)^\varphi \cap N^\varphi = (A^\varphi_b \cup B^\varphi) \cap N^\varphi = (A^\varphi_b)^B \), one only has to show that \( A^\varphi_b \cap (A^\varphi_b)^b | 1 \neq b \in B^\varphi | = 1 \). For this one may assume that \( A \) is finite, then (a) and the assumption in (b) imply that \( |N^\varphi| = |A^\varphi_b|^B | = |A^\varphi_b||B^\varphi| \), and this yields the assertion. To prove (a), one has to show that \( [A^\varphi_b, A^\varphi_c] = 1 \) for all \( b, c \in B \) such that \( b \neq c \). Properties (15) and (16) reduce this to the case where \( A \) is cyclic of prime power order and \( |B| = q \) or \( 4, q \) a prime, \( q \neq 2 \). Here \( N^\varphi \) is abelian and, in general, \( G \) is even determined by its subgroup lattice (see Exercises 9 and 10). It is an open problem to give precise conditions under which \( \overline{G} \cong G \) in 7.6.13. For torsion-free groups, the situation is better.

7.6.14 Theorem (Arshinov and Sadovskii [1973]). The wreath product \( G = A \, \wr \, B \) of two nontrivial torsion-free groups \( A \) and \( B \) is strongly determined by its subgroup lattice.
Sketch of proof. Let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). First consider the case that \( A \) and \( B \) are infinite cyclic. Then \( G \) is residually torsion-free nilpotent (see Smelkin [1964]), and hence the family \( \mathcal{F} \) of all normal subgroups \( X \) of \( G \) with nonabelian torsion-free nilpotent factor group \( G/X \) satisfies the assumptions (18) and (19) of Sadovskii’s Approximation Theorem in §1.3. By 6.5.1 and 7.2.11, if \( X \in \mathcal{F} \), then \( X^\varphi \leq \overline{G} \) and \( \varphi \) is induced by a unique isomorphism on \( G/X \). Thus by 1.3.8, \( \varphi \) is induced by an isomorphism from \( G \) to \( \overline{G} \). This proves Theorem 7.6.14 in the special case that \( A \cong C_x \cong B \).

If \( A \) and \( B \) are arbitrary torsion-free groups, then by 7.6.2 and 6.5.1, \( N^\varphi = Dr A_c^e \leq \overline{G} \). Let \( b, c \in B \). Since there are diagonals in \( A_b \times A_c \), there exist diagonals in \( A_b^e \times A_c^e \) and hence all the \( A_b^e \) are isomorphic. By (15), if \( 1 \neq a \in A_c \) and \( 1 \neq b \in B \), then \( \langle a, b \rangle \simeq \langle a \rangle \wr \langle b \rangle \) is strongly determined by its subgroup lattice, as we have just seen. By 1.5.8, \( Pot \langle a, b \rangle = 1 \) and hence \( \varphi \) is induced on \( \langle a, b \rangle \) by a unique isomorphism \( \nu(a, b) \colon \langle a, b \rangle \to \langle a, b \rangle^\varphi \). So, if we fix \( a \in A_c \), we obtain a map \( \sigma \colon B \to B^\varphi \) defined by \( b^\sigma = b^{\nu(a, b)} \) and satisfying \( \langle b \rangle^\varphi = \langle b^\sigma \rangle \) for all \( b \in B \). If we fix \( b \in B \), we can define maps \( \tau_c \colon A_c \to A_c^\varphi (c \in B) \) by \( a^\tau = a^{\nu(a, b)} \) for \( a \in A_c \), and these can be put together to a map \( \tau \colon N = Dr A_c \to N^\varphi = Dr A_c^e \). It is not difficult to show that \( \sigma \) and \( \tau \) are independent of the choices of \( a \in A_c \) and \( b \in B \), and that they are, in fact, isomorphisms satisfying \( \langle b^{-1}ab \rangle^\varphi = \langle (b^\sigma)^{-1}a^ib^\sigma \rangle \) for all \( a \in N, b \in B \). Thus there is an isomorphism \( \omega \colon G \to \overline{G} \) such that \( \omega|_N = \tau \) and \( \omega|_B = \sigma \), and it is possible to show that the projectivity \( \varphi \) is induced by \( \omega \).

Direct products of lattice-isomorphic groups

Finally we study the following problem. If \( X \) is a group which has only finitely many pairwise nonisomorphic projective images—call them \( X_1, \ldots, X_n \)—is \( \overline{G} = X_1 \times \cdots \times X_n \) determined by its subgroup lattice? The following example shows that this is not the case.

7.6.15 Example. Let \( p > 2 \) be a prime and \( X = X_1 \) be the abelian group of type \((p^2, p)\). Then \( n = 2, X_2 = \langle c, d \rangle | c^{p^2} = d^p = 1, [c, d] = c^p \rangle \) is the nonabelian group of order \( p^3 \) and exponent \( p^2 \), and we claim that the group \( G = X_1 \times X_2 \) is not determined by its subgroup lattice.

Proof. Let \( A = X_1 \times \langle c^p, d \rangle \leq G \) and \( \alpha \colon G \to G \) be defined by \( x^\alpha = x^{1+p} \) for all \( x \in G \). Since \( G' = \langle c^p \rangle \leq Z(G) \), it follows from (4) of §1.5 that

\[
(xy)^{1+p} = x^{1+p}y^{1+p}[y, x]^{1+p} = x^{1+p}y^{1+p}
\]

for all \( x, y \in G \), that is,

\(17\) \( \alpha \) is a power automorphism of \( G \).

Therefore the situation is similar to the proof of Theorem 2.5.9: here \(|G : A| = p\) so that \( s = 1 = m \), but \( G \) is not abelian. Nevertheless we can construct a crossed
isomorphism of $G$ in the same way as in that proof. We put $r = 1 + p$, $\mu = \mu_r$, write $x \in G$ in the form $x = ae^{i(x)}$ with $a \in A$ and $1 \leq i(x) \leq p$, and define

$$f(x) = \alpha^j$$

for $j \in \mathbb{Z}$ such that $\mu(j) \equiv i(x) \pmod{p}$.

We copy Baer's argument literally and obtain that $f(x)$ is well-defined,

$$(18) \quad f(x) = \alpha^j$$

and $f: G \to \text{End} \ G$ satisfies (2)–(4) of §2.5 and (d) of 2.5.8. By 2.5.2 and 2.5.8, there is a new operation $\circ$ defined by

$$x \circ y = x^{f(y)}y$$

for $x, y \in G$ such that $G^* = (G, \circ)$ is a group and the identity is an $f$-isomorphism inducing a projectivity from $G$ to $G^*$. Clearly, $i(c) = 1$ and $\mu(1) = 1$ so that $f(c) = \alpha$. By (19) and (20), the inverse of an element of $A$ is the same in $G$ and $G^*$. Let $b$ be the inverse of $c$ in $G^*$, that is, $1 = b \circ c = b^{f(c)}c$. If $a$ is an element of order $p^2$ in $X_1$, then

$$b \circ a \circ c \circ a^{-1} = (ba)^{f(c)}ca^{-1} = b^{f(c)}a^{f(c)}ca^{-1} = b^{f(c)}ca^{1+p}a^{-1} = a^p$$

and

$$b \circ d^{-1} \circ c \circ d = (bd^{-1})^{f(c)}cd = b^{f(c)}(d^{-1})^{1+p}cd = b^{f(c)}d^{-1}cd = b^{f(c)}cc^p = c^p$$

since $o(d) = p$. Thus the commutator subgroup of $G^*$ contains $a^p$ and $c^p$ and, since $|G'| = p$, it follows that $G^* \neq G$.

However, there is a positive result for a large class of finite groups.

7.6.16 Theorem (Schmidt [1980b]). Let $X$ be a finite group such that $Z(X) = 1$ or $X = X'$, and let $G = X_1 \times \cdots \times X_n$ where $X_1, \ldots, X_n$ are all the pairwise nonisomorphic projective images of $X$. Then $G$ is determined by its subgroup lattice.

Proof. First note that, by 1.6.10, every finite group with infinitely many pairwise nonisomorphic projective images has a nontrivial cyclic direct factor. Thus $X$ indeed has only finitely many such images and $G$ is well-defined. Let $\phi$ be a projectivity from $G$ to a group $\overline{G}$. We want to show that

$$(21) \quad \overline{G} = X_1^\phi \times \cdots \times X_n^\phi.$$  

If $X$ is perfect, then by 5.3.4, every $X_i$ is perfect and (21) follows from 7.6.2. Now suppose that $Z(X) = 1$ and, for a contradiction, that $X_i^\phi$ is not normal in $\overline{G}$ for some $i$. Then there exists $k \in \{1, \ldots, n\}$ such that $X_k^\phi$ is not normalized by $X_i^\phi$. And, since $X_k$ is generated by its elements of prime power order, there exists a cyclic subgroup $C$ of prime power order $p'$ of $X_k$ such that $X_k^\phi$ is not normalized by $C^\phi$. Clearly, $p$ divides $|X_i|$ since otherwise by 1.6.6, $(X_i \times C)^\phi = X_i^\phi \times C^\phi$. If $\phi$ were singular at $p$, then by 7.6.3 applied to $H = X_i$ and $K = \text{Dr} X_j$, the group $G$ would have a normal $p$-complement and, for some $j \in \{1, \ldots, n\}$, $X_j = P \times Q$ where $1 \neq P \in \text{Syl}_p(X_j)$. Let
σ be a projectivity from $X_j$ to $X$. Then, again by 1.6.6, $X = P^\sigma \times Q^\sigma$ and $Z(P^\sigma) = 1$ since $Z(X) = 1$. By 2.2.6, $P^\sigma$ would be a nonabelian group in $P(m, p)$ for some $m$. But the definition of $G$ implies that $X$ is isomorphic to a subgroup of $G$ and hence would have a normal $p$-complement. This contradiction shows that $\varphi$ is not singular at $p$.

Let $D = \Omega(C)$ be the minimal subgroup of $C$. By 4.3.5, $X_i^\rho \unlhd (X_i \times D)^\rho$ and hence, in particular, $D < C$. Furthermore, by 7.6.1 applied to $X_i \times X_k$, we have $C \cap N(X_k) \neq 1$ and hence $D \leq N(X_k)$. Let $\tau$ be a projectivity from $X_k$ to $X$. By 1.4.3, $N(X) = 1$, and hence there exists a subgroup $M$ of $X_k$ such that $M^D = M$ but $M^\tau$ is not normalized by $D^\tau$. Again by 4.3.5, $\tau$ is singular at $p$. Since $C$ is cyclic of order at least $p^2$, 4.2.6 shows that there exists a normal $p$-complement $N$ in $X_k$ with cyclic factor group such that $N^\tau \unlhd X$. If $P$ is a Sylow $p$-subgroup of $MD$ containing $D$, then $P = (M \cap P)D$; since $P$ is cyclic and $M \cap D = 1$, it follows that $P = D$. Thus $M = MD \cap N$ and then $M^\tau = (M^\tau \cap D^\tau) \cap N^\tau \unlhd M^\tau \cap D^\tau$. This final contradiction shows that $X_i^\rho \unlhd \overline{G}$ for all $i$ and (21) follows.

All the $X_i^\rho$ are projective images of $X$. If two of them, $X_i^\rho$ and $X_j^\rho$, say, were isomorphic, then by 1.6.2 there would exist diagonals in the group $X_i^\rho \times X_j^\rho = (X_i \times X_j)^\rho$, and hence also in $X_i \times X_j$. It would follow that $X_i \simeq X_j$, contradicting our assumption. Therefore $X_1^\rho, \ldots, X_n^\rho$ are pairwise nonisomorphic projective images of $X$ and, since $X$ possesses only $n$ of these, it follows that the $X_i^\rho$ are isomorphic to the $X_j$ in some arrangement. Thus $\overline{G} = X_1^\rho \times \cdots \times X_n^\rho \simeq X_1 \times \cdots \times X_n = G$, as required.

### Exercises

1. (Lukács and Pálfy [1968]) If $G = H \times K$, $H \simeq K$ and $L(G)$ is modular, show that $G$ is abelian. (Do not use the results of § 2.4.)
2. Show that the isomorphism $i^*$ in 7.6.6 is independent of the choice of $\varepsilon$.
3. Let $X$ be a finite group such that $Z(X) = 1$ and let $G = H \times K$ where $H \simeq \text{Aut} X \simeq K$. Show that $G$ is determined by its subgroup lattice.
4. Let $G = H \times K$ and define

$$R(H, K) = \{\sigma \in P(G) | H^\sigma = H \text{ and } X^\sigma = X \text{ for all } X \leq K\},$$

$$S(H, K) = \{\sigma \in P(G) | X^\sigma = X \text{ for all } X \leq H \text{ and all } X \leq K\}.$$ 

(a) Show that $S(H, K) \unlhd R(H, K)$ and $R(H, K)/S(H, K)$ is isomorphic to a subgroup of $P(H)$ containing $PA(H)$.
(b) If $H \simeq K$, show that $R(H, K)/S(H, K) \simeq PA(H)$.
5. (Zacher [1981]) If the group $H$ in Theorem 7.6.8 is generated by involutions, show that $(\text{Inn } H)^t = \text{Inn } H$. Deduce that $\overline{G} \simeq G$.
6. Show that for the Rottländer groups $G_\mu$, we have $L(G_\mu \times G_\mu) \neq L(G_{q-1} \times G_{q-1})$ if $2 \leq \mu \leq q - 2$.

In the next two exercises let $3 \leq n \in \mathbb{N}$, $p$ and $q$ be different primes, $X_1 = N_1H_1$ where $N_1$ is an elementary abelian normal $p$-subgroup of $X_1$ and $H_1$ is a $q$-group. With the obvious notation, assume that $X_i = N_iH_i$ are isomorphic to $X_i$ ($i = 2, \ldots, n$) and let $G = X_1 \times \cdots \times X_n$, $N = N_1 \times \cdots \times N_n$, $H = H_1 \times \cdots \times H_n$. 

**Note:** The content is extracted from a document discussing classes of groups and their projectivities. The text provides a detailed explanation of projectivities and their properties, along with exercises that involve modular lattices and the isomorphism of certain groups. The exercises include showing that a group is abelian under certain conditions, demonstrating the independence of isomorphisms from the choice of a parameter, and working with Rottländer groups and their properties. The final two exercises involve conditions for the isomorphism of certain lattice elements and involve the construction of groups with specific properties. The document is a comprehensive resource for understanding group theory and its applications.
7. (Schmidt [1982]) Assume in addition that \( H_1 \) is abelian of exponent \( q^r \), \( r \geq 2 \) and \( r \geq 3 \) in case \( q = 2 \), and that \( C_{H_1}(N_1) = \Omega(H_1) \). Show that there exists a semidirect product \( \tilde{G} = N \tilde{H} \) lattice-isomorphic to \( G \) in which \( \tilde{H} \) is a nonabelian \( M \)-group. (Hint: Use 4.1.9.)

8. (Schenke [1987b]) Assume that \( 2 < q | p - 1 \), \( |N_1| = p \), \( H_1 \) is the nonabelian group of order \( q^3 \) and exponent \( q \) and \( |H_1 : C_{H_1}(N_1)| = q \). Show that \( G \) has an autoprojectivity \( \varphi \) which satisfies \( X_i^{\varphi} = X_i \) for all \( i \) and is not induced by an automorphism. (Hint: Use 4.1.9 to construct an autoprojectivity of \( G \) which is trivial on \( G/C_H(N) \) and induced on \( H_1 \) by a suitable automorphism of \( H_1 \).)

9. (Menegazzo [1973]) Let \( G = A \wr B \) where \( A \) is cyclic of order \( p^n, |B| = q, p \) and \( q \) primes, \( n \in N \), and assume that \( \varphi \) is a projectivity from \( G \) onto a group \( \tilde{G} \); let \( N \) be the base group of \( G \).
   (a) If \( p \neq q \), show that \( N^\varphi \cong N \); if in addition \( |B^\varphi| = q \), show that \( \tilde{G} \cong G \).
   (b) If \( p = q \neq 2 \), show that \( \tilde{G} \cong G \).
   (c) If \( p = q = 2 \) and \( [D^\varphi, B^\varphi] = 1 \) where \( D = \{(a, a) | a \in A\} \) is the diagonal in \( N \), show that \( \tilde{G} \cong G \).

10. (Menegazzo [1973]) (a) Show that \( G = A \wr B \) is determined by its subgroup lattice if \( A \) is cyclic of order \( 2^n \) \( (n \in N) \) and \( |B| = 4 \).
    (b) Show that \( C_8 \wr C_2 \) is not determined by its subgroup lattice.

11. (Zacher [1981]) Show that for every group \( H \) there exists a group \( K \) such that \( H \times K \) is determined by its subgroup lattice. (Hint: Take a suitable free group \( K \)).

### 7.7 Groups generated by involutions

The following is a general idea to prove that a group \( G \) is determined by its subgroup lattice. It is clear that if \( \varphi \) is a projectivity from \( G \) to a group \( \tilde{G} \), then \( \tilde{G} \) operates on \( L(G) \) via the map \( \tau \) sending every \( x \in \tilde{G} \) to the autoprojectivity \( \tau(x) \) of \( G \) given by

\[
(1) \quad H^{\tau(x)} = H^{\varphi x \varphi^{-1}} \text{ for } H \leq G.
\]

So one could try to prove that \( \tilde{G} \) is isomorphic to \( G \) by showing that \( G \) and \( \tilde{G} \) operate in the same way on \( L(G) \). Unfortunately, this is much too difficult. To simplify matters, however, one could restrict oneself to a suitable subset \( \Delta \) of \( L(G) \) and to a system \( D \) of generators of \( G \) and try to prove that for every \( d \in D \) and \( \langle x \rangle = \langle d \rangle^\varphi \), the elements \( x \) and \( d \) operate in the same way on \( \Delta \). For this, \( \Delta \) would have to be a union of conjugacy classes of subgroups of \( G \); otherwise \( G \) would not operate on \( \Delta \). Furthermore, it seems that this can only work for elements \( d \) and \( x \) which are the unique generators of the subgroups they generate, that is, for involutions. We shall show in this section that this idea works and give some applications.

The most interesting will be to show that certain multiply transitive permutation groups and classical groups are determined by their subgroup lattices. In addition, an application to lattice-simple groups will be given in §7.8.
2-singular projectivities

To prove these results, we first of all have to guarantee that \(|\langle d \rangle^\sigma| = 2\) if \(d \in D\) is an involution. For any prime \(p\) and a projectivity \(\varphi\) between arbitrary groups \(G\) and \(\overline{G}\), let us say that \(\varphi\) is \(p\)-regular if it maps every subgroup of order \(p\) of \(G\) to a subgroup of order \(p\) in \(\overline{G}\). Note that for finite groups this is equivalent to our definition of \(p\)-regularity in §4.2. So we have to study 2-singular projectivities of groups generated by involutions, and we start with groups generated by two involutions. Now if \(G = \langle d, e \rangle\) where \(o(d) = o(e) = 2\) and \(o(de) = n \in \mathbb{N} \cup \{\infty\}\), then \((de)^n = dded = ed = (de)^{-1}\) so that \(G\) is the semidirect product of a cyclic group \(\langle a \rangle = \langle de \rangle\) of order \(n\), and a cyclic group \(\langle d \rangle\) of order 2 with respect to the automorphism given by \(a^d = a^{-1}\); such a group is called a dihedral group of order \(2n\). Note that \((a^d)^2 = a^d a^{-1} = 1\) for all \(i \in \mathbb{Z}\) so that every element in \(G \setminus \langle a \rangle\) has order 2.

7.7.1 Lemma. Let \(n \in \mathbb{N} \cup \{\infty\}\), \(G\) be a dihedral group of order \(2n\), that is, \(G = \langle d, e \rangle\) where \(o(d) = o(e) = 2\) and \(o(de) = n\), and let \(\varphi\) be a projectivity from \(G\) to a group \(\overline{G}\); put \(\langle d \rangle^\sigma = \langle x \rangle\) and \(\langle e \rangle^\sigma = \langle y \rangle\).

(a) If \(n = \infty\), then \(\varphi\) is 2-regular, \(\langle de \rangle^\sigma = \langle xy \rangle\) and \(\overline{G} \simeq G\).

(b) If \(n = p\) is a prime, then \(\overline{G} \in P(2, p)\). If \(\varphi\) is 2-regular, then \(\langle de \rangle^\sigma = \langle xy \rangle\).

(c) If \(n\) is neither infinite nor a prime, then \(\langle de \rangle^\sigma\) is a cyclic normal subgroup of order \(n\) in \(\overline{G}\) and \(o(x) = o(y) = q\) for some prime \(q\). If \(q = 2\), then \(\varphi\) is 2-regular, \(\langle de \rangle^\sigma = \langle xy \rangle\) and \(\overline{G} \simeq G\). If \(q > 2\), then either \(q\) does not divide \(n\) and \(x\) operates fixed-point-freely on \(\langle de \rangle^\sigma\) or \(n = qn'\) where \((n', q) = 1\).

Proof. (a) If \(n = \infty\), \(\langle de \rangle\) is the unique cyclic maximal subgroup of \(G\). Since every projectivity maps cyclic subgroups to cyclic subgroups, \(\langle de \rangle^\sigma\) is the unique cyclic maximal subgroup of \(\overline{G}\), and by 6.5.11, \(\varphi\) is 2-regular. In particular, \(o(x) = o(y) = 2\), \(G = \langle x, y \rangle = \langle xy, x \rangle\) is an infinite dihedral group and \(\langle de \rangle^\sigma = \langle xy \rangle\).

(b) That \(\overline{G} \in P(2, p)\) follows from 2.2.5. If \(\varphi\) is 2-regular, then \(\langle de \rangle^\sigma = \langle xy \rangle\) since \(\langle de \rangle\) and \(\langle xy \rangle\) are the only minimal subgroups of \(G\) and \(\overline{G}\) of order different from 2 (if \(p > 2\)) or different from \(\langle d \rangle\), \(\langle e \rangle\), \(\langle x \rangle\), \(\langle y \rangle\) (if \(p = 2\)).

(c) Again, \(\langle de \rangle\) is the unique cyclic maximal subgroup of \(G\); hence \(\langle de \rangle^\sigma\) is a cyclic normal subgroup of \(\overline{G}\) and \(o(x) = |\overline{G}/\langle de \rangle^\sigma| = o(y)\) is a prime \(q\). Let \(|\langle de \rangle^\sigma| = m\). We have to show that \(m = n\).

First suppose that \(q = 2\). Then \(\overline{G}\) is generated by the involutions \(x\) and \(y\) and hence is a dihedral group with cyclic maximal subgroup \(\langle xy \rangle\). It follows that \(\langle xy \rangle = \langle de \rangle^\sigma\). Since every element in \(\overline{G}/\langle xy \rangle\) has order 2, the number of minimal subgroups of \(\overline{G}\) not contained in \(\langle xy \rangle\) is \(m\). Thus \(m = n\) and \(\overline{G} \simeq G\). Clearly, \(\varphi\) is 2-regular. Indeed, if \(n\) is even, this follows from 2.2.6 since the Sylow 2-subgroups of \(G\) are noncyclic. And if \(n\) is odd, the Sylow 2-subgroups of \(G\) are the complements to \(\langle de \rangle\) in \(G\); they are mapped to the complements to \(\langle xy \rangle\) in \(\overline{G}\) and hence to subgroups of order 2.

Now let \(q > 2\). If \(q\) does not divide \(m\), then \(x\) operates fixed-point-freely on \(\langle de \rangle^\sigma\) since every nontrivial fixed element \(z \in \langle de \rangle^\sigma\) would yield a cyclic group \(\langle xz \rangle^\sigma^{-1}\) of composite order whose preimage \(\langle xz \rangle^\sigma^{-1}\) would be a dihedral group, a contradiction. Thus there exist exactly \(m\) complements to \(\langle de \rangle^\sigma\) in \(\overline{G}\). The number of
complements to $\langle de \rangle$ in $G$ is $n$ and it follows that $m = n$. Finally, suppose that $q$ divides $m$ and let $Q^o$ be the Sylow $q$-subgroup of $\langle de \rangle^o$. Then $Q^o \langle x \rangle$ is a noncyclic $q$-group whose preimage $Q \langle d \rangle$ is not a $q$-group. By 2.2.6, $Q \langle d \rangle \in P(r, q)$ for some $r \in \mathbb{N}$ and hence $|Q| = q$ since $Q$ is cyclic and $Q \leq Q \langle d \rangle$. Let $R^o$ be the complement to $Q^o$ in $\langle de \rangle^o$. Then the dihedral group $R \langle d \rangle$ is mapped by $\varphi$ to $R^o \langle x \rangle$ and $(|R^o|, q) = 1$. By (b) or the case of (c) just considered, $|R^o| = |R| = q$. It follows that $m = |R^o| = |Q^o| = |R|$, $q = n$. Since $|Q^o| = q$, finally, $n = qn'$ where $(n', q) = 1$. 

The structure of finite groups with 2-singular projectivities is well-known. By 4.2.6, such a group $G$ is either $P$-decomposable, that is, $G = S \times T$ where $S$ is a $P$-group of order $2p^n$ for some prime $p > 2$, $n \in \mathbb{N}$, and $(|S|, |T|) = 1$, or $G$ has a normal 2-complement $K$ with cyclic factor group $G/K$ such that $K^o \leq G$. A similar result for arbitrary groups is not known. Even the most moderate conjecture that a group $G$ generated by involutions with a 2-singular projectivity is either a $P$-group or has a normal subgroup $K$ such that $|G : K| = 2$, $K^o \leq G$ and every element in $K$ has infinite or finite odd order has not been confirmed yet. An immediate consequence would be that all subgroups of order 2 of $G$ are mapped onto subgroups of the same order if $G$ is not a $P$-group. We can prove this much weaker result and it will suffice for our applications.

7.7.2 Lemma. Let $G$ be a group generated by involutions and $\varphi$ a projectivity from $G$ to a group $\bar{G}$. If there exist involutions $a, b \in G$ such that $|a^o| = q$, $|b^o| = p$ and $q < p$. Then $\langle a, b \rangle$ is a dihedral group of order $2p$ and $\langle a, b \rangle^o$ is a nonabelian group of order $pq$.

Proof. Let $D$ be the set of involutions in $G$. If $a \in D$, then $|a^o|$ is a prime; let $q$ be the smallest prime occurring among the $|a^o|$ for $a \in D$. We study the groups $\langle a, b \rangle$ and $\langle a, b, c \rangle$ where $a, b, c \in D$ and first of all note the following immediate consequence of 7.7.1.

(2) Let $a, b \in D$ such that $|a^o| = q$, $|b^o| = p$ and $q < p$. Then $\langle a, b \rangle$ is a dihedral group of order $2p$ and $\langle a, b \rangle^o$ is a nonabelian group of order $pq$.

Indeed, $\langle a, b \rangle$ is a dihedral group of order $2r$ for some $r \in \mathbb{N} \cup \{\infty\}$ and $|a^o| \neq |b^o|$. By 7.7.1, $r$ is a prime and $\langle a, b \rangle^o \in P(2, r)$. Since $p$ and $q$ divide the order of $\langle a, b \rangle^o$, this group is nonabelian of order $pq$, $r = p$, and $\langle a, b \rangle$ is a dihedral group of order $2p$.

(3) Let $a, b \in D$ such that $|a^o| = q$, $|b^o| = p$ and $q < p$. If $c \in D$ such that $c \notin \langle a, b \rangle$, then $\langle a, b, c \rangle^o$ is a $P$-group of order $p^2q$, $\langle a, b, c \rangle \in P(3, p)$ and $\langle ab, ac, bc \rangle$ is elementary abelian of order $p^2$.

To prove this, we first show that $H = \langle a, b, c \rangle$ is finite. If $|c^o| = r > q$, then by (2), $\langle a, b \rangle^o$ and $\langle a, c \rangle^o$ are nonabelian of order $pq$ and $rq$, respectively. It follows that $\langle a \rangle^o$ normalizes $\langle b \rangle^o$ and $\langle c \rangle^o$ and hence also $\langle b \rangle^o \cup \langle c \rangle^o = \langle b, c \rangle^o$. Since $|\langle b \rangle^o| = p > q \geq 2$, the projectivity $\varphi$ is 2-singular on the dihedral group $\langle b, c \rangle$. By 7.7.1, $\langle b, c \rangle^o$ is finite; hence so is $\langle b, c \rangle^o \langle a \rangle^o = H^o$ and $H$. Now suppose that $|c^o| = q$. Then by (2), $\langle b \rangle^o$ is normalized by $\langle a \rangle^o$ and $\langle c \rangle^o$ and hence also by $\langle a, c \rangle^o$. If $\langle a, c \rangle^o$ were to contain an element of infinite order, it would follow from
6.5.11 that \( p = |\langle b \rangle^\sigma| = |\langle b \rangle| = 2 \), a contradiction. Therefore \( \langle a, c \rangle \) is a finite dihedral group, and \( \langle b \rangle^\sigma \langle a, c \rangle^\sigma = H^\sigma \) and \( H \) are finite. Thus, in all cases, \( H = \langle a, b, c \rangle \) is a finite group generated by involutions in which \( \varphi \) induces a 2-singular projectivity. If there existed a normal 2-complement \( K \) in \( H \) such that \( K^\sigma \leq H^\sigma \), then \( q = |\langle a \rangle^\sigma| = |H^\sigma : K^\sigma| = |\langle b \rangle^\sigma| = p \), a contradiction. By 4.2.6, \( H \) is a \( P \)-group of order \( 2r^a \) for some prime \( r \). Since \( c \notin \langle a, b \rangle \), we have \( n = 2 \); thus \( H \in P(3, r) \) and therefore also \( H^\sigma \in P(3, r) \). Since \( p \) and \( q \) divide \( |H^\sigma| \) and \( q < p \), it follows that \( r = p \), \( |H^\sigma| = p^2q \) and \( H \in P(3, p) \). Now \( ab, ac, bc \) are contained in the normal subgroup of order \( p^2 \) of \( H \) and, since \( H \) is generated by \( a \) and these three elements, it follows that \( \langle ab, ac, bc \rangle \) is an elementary abelian of order \( p^2 \). This proves (3).

(4) Let \( b, c \in D \) such that \( |\langle b \rangle^\sigma| = p > q, |\langle c \rangle^\sigma| > q \) and \( b \neq c \). Then \( \langle b, c \rangle^\sigma \) is elementary abelian of order \( p^2 \).

To prove this, take an element \( a \in D \) such that \( |\langle a \rangle^\sigma| = q \). Then by (2), \( \langle a, b \rangle^\sigma \) is nonabelian of order \( pq \). Therefore \( \langle b \rangle^\sigma \) is the unique minimal subgroup of order different from \( q \) in \( \langle a, b \rangle^\sigma \) and hence \( c \notin \langle a, b \rangle \). By (3), \( \langle a, b, c \rangle^\sigma \) is a \( P \)-group of order \( p^2q \) and \( \langle b, c \rangle^\sigma = \langle b \rangle^\sigma \cup \langle c \rangle^\sigma \) is the elementary abelian normal subgroup of order \( p^2 \) of \( \langle a, b, c \rangle^\sigma \).

To complete the proof of the lemma, we fix an involution \( b \in D \) such that \( |\langle b \rangle^\sigma| = p > q \) and show that

(5) \( A = \langle ab | a \in D \rangle \) is an elementary abelian \( p \)-group.

Since \( (ab)^b = ba = (ab)^{-1} \) for all \( a \in D \), it will follow that \( b \) inverts a system of generators of the abelian group \( A \) and hence every element of \( A \). Hence \( G = \langle a | a \in D \rangle = A \langle b \rangle \) will be a nonabelian \( P \)-group.

To prove (5), we show that all the generators \( ab (b \neq a \in D) \) of \( A \) have order \( p \) and any two of them commute. For this let \( a, c \in D \) be such that \( a \neq b \neq c \), and suppose first that \( \langle a \rangle^\sigma \) or \( \langle c \rangle^\sigma \) has order \( q \); let \( |\langle a \rangle^\sigma| = q \), say. Then by (2), \( \langle a, b \rangle^\sigma \) is a dihedral group of order \( 2p \) and hence \( o(ab) = p \). If \( c \in \langle a, b \rangle^\sigma \), then \( \langle cb \rangle = \langle ab \rangle \) is the subgroup of order \( p \) in \( \langle a, b \rangle^\sigma \), that is, \( cb \) has order \( p \) and commutes with \( ab \). If \( c \notin \langle a, b \rangle^\sigma \), then by (3), \( \langle ab, ac, bc \rangle \) is elementary abelian of order \( p^2 \); again \( ab \) and \( cb \) have order \( p \) and commute. Now suppose that \( |\langle a \rangle^\sigma| > q \) and \( |\langle c \rangle^\sigma| > q \). By (4), \( \langle b, a \rangle^\sigma \) and \( \langle b, c \rangle^\sigma \) are elementary abelian of order \( p^2 \) and then so is \( \langle a, c \rangle^\sigma \) if \( a \neq c \). Thus \( \langle a \rangle^\sigma, \langle b \rangle^\sigma, \langle c \rangle^\sigma \) are subgroups of order \( p \) in \( \tilde{G} \) centralizing each other and therefore generating an elementary abelian subgroup of order \( p^3 \) or \( p^2 \) of \( \tilde{G} \). It follows that \( \langle a, b, c \rangle \) is a \( P \)-group of order \( 2p^2 \) or \( 2p \) and the elements \( ab \) and \( cb \) have order \( p \) and commute. This proves (5) and the lemma.

It is not difficult to generalize the above lemma to the situation that \( G \) is not generated by involutions; then \( G = S \times T \) where \( S = \langle a \in G | a^2 = 1 \rangle \) is a nonabelian \( P \)-group and \( S \) and \( T \) are coprime (see Exercise 2). Conversely, if \( G \) is such a group and \( S \in P(n, p) \), there exist autoprojectivities \( \varphi \) of \( S \), and hence of \( G \), such that \( |\langle a \rangle^\sigma| = p \neq 2 = |\langle b \rangle^\sigma| \) for certain involutions \( a, b \in S \). We note an immediate consequence of Lemma 7.7.2.

7.7.3 Corollary. If \( G \) is a group containing two commuting involutions, then every projectivity of \( G \) is 2-regular.
Proof. These two involutions generate a four group \( H \) and hence the subgroup \( S \) generated by all the involutions in \( G \) cannot be a nonabelian \( P \)-group. Thus if \( \varphi \) is a projectivity of \( G \), then by 7.7.2 there exists a prime \( q \) such that \( |\langle a \rangle^\varphi| = q \) for every involution \( a \in S \). Since \( |H^\varphi| = 4 \), it follows that \( q = 2 \) and \( \varphi \) is 2-regular.

We want to compare the operation of an involution and its projective images on the subgroup lattice. The next lemma takes care of the fixed points under this operation.

7.7.4 Lemma. Let \( G \) be a group generated by involutions, \( \varphi \) a projectivity from \( G \) to a group \( \overline{G} \) and suppose that \( G \) is not a \( P \)-group.

(a) If \( a \in G \) is an involution, \( \langle a \rangle^\varphi = \langle x \rangle \) and \( H \leq G \) such that \( H^a = H^o \), then \( \langle H^\varphi \rangle^x = H^\varphi \).

(b) If \( N \leq G \), then \( N^\varphi \leq \overline{G} \).

Proof. Since \( G \) is generated by involutions, (b) of course follows from (a). To prove (a), suppose, for a contradiction, that \( \langle H^\varphi \rangle^x \neq H^\varphi \) and let \( T = H \langle a \rangle \). Then \( |T : H| = 2 \) and by 6.5.3 there exist a prime \( p \) and a normal subgroup \( K \) of \( T \) contained in \( H \) such that \( |T/K| = 2p \), \( K^\varphi \leq T^\varphi \) and \( T^\varphi/K^\varphi \) is a nonabelian group in \( P(2, p) \). By 7.7.2 there exists a prime \( q \) such that \( |\langle d \rangle^\varphi| = q \) for every involution \( d \) in \( G \). So if \( U/K \) is a subgroup of order 2 of \( T/K \), then \( U = (K \langle a \rangle^t) = K \langle a^t \rangle \) for some \( t \in T \); hence \( U^\varphi = K^\varphi \langle a^t \rangle^\varphi \) and \( |U^\varphi/K^\varphi| = |\langle a^t \rangle^\varphi| = q \). It follows that \( H^\varphi/K^\varphi \) is the subgroup of order \( p \) in \( T^\varphi/K^\varphi \), a contradiction.

Involutions and conjugacy classes

We can now show that the idea described at the beginning of this section indeed works. We present it in its most general form.

7.7.5 Theorem (Schmidt [1980a]). Let \( G \) be a group, \( D \) a set of involutions in \( G \), \( \Delta \) a set of subgroups of \( G \) and \( \varphi \) a projectivity from \( G \) to a group \( \overline{G} \) with the following properties.

(6) \( G = \langle d | d \in D \rangle \).

(7) \( \Delta^D = \Delta \) (that is, \( H^d \in \Delta \) for all \( H \in \Delta, d \in D \)).

(8) If \( d \in D \), \( H \in \Delta \) and \( \langle d \rangle^\varphi = \langle x \rangle \), then \( \langle H^\varphi \rangle^x = \langle H^d \rangle^\varphi \).

(a) Then \( G/\bigcap_{H \in \Delta} N_G(H) \) is isomorphic to \( \overline{G}/\bigcap_{H \in \Delta} N_{\overline{G}}(H^\varphi) \).

(b) Let \( \bigcap_{H \in \Delta} N_G(H) = 1 \). If \( G \) is finite or \( D^G = D \), then \( \overline{G} \) is isomorphic to \( G \).

Proof. (a) For \( y \in \overline{G} \) and \( H \leq G \), let \( H^{\varphi(y)} = H^{\varphi(y)^{-1}} \). If \( d \in D \), \( H \in \Delta \), and \( \langle x \rangle = \langle d \rangle^\varphi \), then \( H^{\varphi(x)} = H^d \in \Delta \), by (8) and (7). Since \( G = \langle d | d \in D \rangle \), the group \( \overline{G} \) is generated by these elements \( x \), and it follows that \( \Delta^\varphi = \Delta \) for all \( g \in G \) and \( \Delta^{\varphi(y)} = \Delta \) for all \( y \in \overline{G} \). Thus \( G \) and \( \overline{G} \) operate on \( \Delta \) via the homomorphisms \( \varphi: G \to \text{Sym} \Delta \) given by
$H^{(g)} = H^g (g \in G)$ and $\mu: \overline{G} \to \text{Sym} \Delta$ defined by $H^{\mu(y)} = H^{(y)}$ ($y \in \overline{G}$) for $H \in \Delta$. By (8), $\nu(d) = \mu(x)$ for every $d \in D$ and $\langle x \rangle = \langle d \rangle^\phi$. Since $G$ is generated by these involutions, it follows that $G^\nu = \overline{G}^\mu$. Thus $G/Ker \nu \simeq G^\nu = \overline{G}/\text{Ker} \mu$; since Ker $\nu = \bigcap_{H \in \Delta} N_G(H)$ and Ker $\mu = \bigcap_{H \in \Delta} N_{\overline{G}}(H^\phi)$, (a) follows.

(b) By (a), $G$ is isomorphic to $\overline{G}/\bigcap_{H \in \Delta} N_{\overline{G}}(H^\phi)$. If $G$ is finite, it follows that $G \simeq \overline{G}$ since the finite group $\overline{G}$ cannot admit a projectivity onto a proper factor group.

Now let $D^G = D$ and suppose, for a contradiction, that $\overline{G}$ is not isomorphic to $G$; then Ker $\mu \neq 1$. For $d \in D$ and $\langle x \rangle = \langle d \rangle^\phi$, $\mu(x) = \nu(d)$. Since $\nu$ is a monomorphism, it follows that $o(\mu(x)) = 2$, and hence $o(x) = 2$. Therefore, if $G$ were a $P$-group, it would follow that $\overline{G} \simeq G$, a contradiction; thus $G$ is not a $P$-group. Then also $G$ is not a $P$-group and is generated by involutions. By 7.7.2, $\phi$ and $\phi^{-1}$ are 2-regular and by 7.7.4, $K = (\text{Ker} \mu)^{\phi^{-1}} \subseteq G$. Since $Z(G) = 1$ and $G = \langle d | d \in D \rangle$, there exists $d \in D$ such that $C_K(d) \neq K$. Let $u \in K$ such that $u^d \neq u$ and let $v = u^{-d}u$. Then $v^d = u^{-1}u^d = v^{-1}$ and hence $\langle v, d \rangle$ is a dihedral group of order $2m$ where $m = o(v) \neq 1$. Since $K \leq G$, we have $v \in K$ and $o(v) \neq 2$; indeed, otherwise $\langle v \rangle^\phi$ would be a subgroup of order 2 of $\overline{G}$ normalizing every $H^\phi (H \in \Delta)$ and 7.7.4 applied to $\phi^{-1}$ would yield that $v \in \bigcap_{H \in \Delta} N_G(H) = 1$, a contradiction. Thus $d$ and $e = d^\phi$ are two different involutions in $D$ (here we use that $D^G = D$) and $de \in \langle v \rangle \leq K$. Let $\langle d \rangle^\phi = \langle x \rangle$ and $\langle e \rangle^\phi = \langle y \rangle$. Since $\phi$ is 2-regular, 7.7.1 shows that $\langle de \rangle^\phi = \langle xy \rangle$ and hence $xy \in \text{Ker} \mu$. For every $H \in \Delta$, also $H^\phi \in \Delta$ and so by (8), $H^\phi = (H^\phi)^{xy} = ((H^d)^\phi)^y = (H^{de})^\phi$, that is $H = H^{de}$. It follows that $de \in \bigcap_{H \in \Delta} N_G(H) = 1$ and hence $d = e$. This contradiction shows that $G \ncong \overline{G}$.

To apply Theorem 7.7.5, we have to choose a set $D$ of involutions and a suitable set $\Delta$ of subgroups of $G$ satisfying (6)–(8). Here (6) and (7) have to be assumed, that is, we have to assume that $G$ is generated by (these) involutions and for $\Delta$ we have to take a union of conjugacy classes of subgroups of $G$, and then we have to try to prove that (8) holds. In view of Lemma 7.7.1 and our discussion on projective images of conjugacy classes in § 5.6, there are two situations in which this could perhaps be possible, namely if

(i) $\Delta = \{ \langle d \rangle | d \in D \}$ or

(ii) $\Delta$ is a conjugacy class of maximal subgroups of $G$ or, in the language of the theory of permutation groups, $G$ is a primitive (or multiply transitive) permutation group on a set $\Omega$ and $\Delta$ is the set of stabilizers of the points.

We start with the first possibility and need the following result which is interesting in its own right.

**7.7.6 Lemma.** Let $n \in \mathbb{N} \cup \{ \infty \}$. If $S$ and $T$ are dihedral groups of order $2n$, then $G = S \times T$ is strongly determined by its subgroup lattice.

**Proof.** Let $\phi$ be a projectivity from $G$ to a group $\overline{G}$. We have to show that $\phi$ is induced by an isomorphism. By 7.7.3, $\phi$ is 2-regular and then 7.7.1 implies that if $d, e$ are involutions in $G$ and $\langle d \rangle^\phi = \langle x \rangle, \langle e \rangle^\phi = \langle y \rangle$, then

$$
(9) \quad \langle de \rangle^\phi = \langle xy \rangle \quad \text{and} \quad o(de) = o(xy);
$$
it follows that \( \langle d, e \rangle^o \simeq \langle d, e \rangle \). This holds in particular for \( S \) and \( T \) and by 7.6.2,

(10) \( \overline{G} = S^o \times T^o \) where \( S^o \simeq S \) and \( T^o \simeq T \); thus \( \overline{G} \simeq G \).

We fix the following notation. Let \( S = \langle a, s \rangle \) where \( o(a) = n, o(s) = 2 \) and \( a^s = a^{-1} \). Then \( s \) and \( as \) are involutions generating \( S \). Therefore if \( \langle s \rangle^o = \langle u \rangle \) and \( \langle as \rangle^o = \langle cu \rangle \) where \( c \in S^o \), then by (9), \( \langle a \rangle^o = \langle c \rangle \) and \( o(c) = o(a) = n \); furthermore \( S^o = \langle c, u \rangle \) and \( c^u = c^{-1} \). Let \( Z_n = \mathbb{Z} \) be the ring of integers if \( n = \infty \) and \( Z_n = \mathbb{Z}/(n) \) if \( n \in \mathbb{N} \). Then every involution in \( S \) not contained in \( \langle a \rangle \) can be written uniquely in the form \( a^i s \) where \( i \in Z_n \); similarly for the involutions in \( S^o \setminus \langle c \rangle \). Since \( \langle a \rangle^o = \langle c \rangle \), for every \( i \in Z_n \) there exists a unique \( j \in Z_n \) such that \( \langle a^i s \rangle^o = \langle c^j u \rangle \). Thus we obtain a bijective map \( v: Z_n \to Z_n \) satisfying

(11) \( \langle a^i s \rangle^o = \langle c^v(i) u \rangle \) for all \( i \in Z_n \).

Since \( \langle s \rangle^o = \langle u \rangle \) and \( \langle as \rangle^o = \langle cu \rangle \),

(12) \( v(0) = 0 \) and \( v(1) = 1 \).

We handle \( T \) and \( T^o \) in the same way. Let \( T = \langle b, t \rangle \) where \( o(b) = n, o(t) = 2 \) and \( b^t = b^{-1} \); let \( \langle t \rangle^o = \langle v \rangle \) and \( \langle bt \rangle^o = \langle dv \rangle \). Then \( T^o = \langle d, v \rangle \), \( o(d) = n \) and \( d^v = d^{-1} \). Let \( \mu: Z_n \to Z_n \) be defined by

(13) \( \langle d^v(i) t \rangle^o = \langle d^{v(i)} v \rangle \) for all \( j \in Z_n \).

Then as above

(14) \( \mu(0) = 0 \) and \( \mu(1) = 1 \).

We want to show that \( v \) and \( \mu \) are the identity on \( Z_n \). For this let \( i, j \in Z_n \). Then \( \langle a^i s \rangle^o = \langle c^{v(i)} u \rangle \) and \( \langle b^j t \rangle^o = \langle d^{v(j)} v \rangle \) and therefore by (9),

(15) \( \langle a^i b^j s t \rangle^o = \langle c^{v(i)} d^{v(j)} uw \rangle \).

For \( i = j = 0 \), we obtain that \( \langle st \rangle^o = \langle uv \rangle \) and then by (15) and (9),

(16) \( \langle a^i b^j \rangle^o = \langle c^{v(i)} d^{v(j)} \rangle \).

Now (15) and (14) imply that \( \langle a^i bst \rangle^o = \langle c^{v(i)} duv \rangle \) and (15), (12), and (14) yield that

(17) \( v(i) = i = \mu(i) \) for all \( i \in Z_n \).

On the other hand, by (16) and (14), \( \langle a^{i-1} b \rangle^o = \langle c^{v(i-1)} d \rangle \). Thus \( \langle c^{v(i-1)} d \rangle = \langle c^{v(i-1)} d \rangle \) and, since \( o(c) = o(d) = n \), it follows that \( v(i - 1) = v(i) - 1 \). This holds for all \( i \in Z_n \). Since \( v(0) = 0 \), a trivial induction yields that \( v \) is the identity. In exactly the same way it may be proved that \( \mu \) is the identity; thus we have shown that

(18) \( v(i) = i = \mu(i) \) for all \( i \in Z_n \).

Now let \( x: G \to \overline{G} \) be the isomorphism satisfying \( a^x = c \), \( s^x = u \), \( b^x = d \), and \( t^x = v \). We want to show that \( H^o = H^x \) for all \( H \leq G \) and it suffices to do this for cyclic \( H \). So let \( H = \langle g \rangle \), \( g = a^i b^j s^h t^k \) where \( i, j \in Z_n \) and \( h, k \in \{0, 1\} \). If \( h = k = 1 \) or \( h = k = 0 \), then \( \langle g \rangle^o = \langle g \rangle^x \) by (15) and (17), or (16) and (17) respectively. So let
Classes of groups and their projectivities

$h = 1, k = 0$ (the case $h = 0, k = 1$ is similar). Then $g = a'sb' \in \langle a's \rangle \times \langle b' \rangle$ and $g^2 = b'^2$ since $a's$ is an involution. So if $\langle b'^2 \rangle = \langle b' \rangle$, then $\langle g \rangle = \langle a's \rangle \times \langle b' \rangle$. By (11) and (17), $\langle a's \rangle^\varphi = \langle c'u \rangle = \langle a's \rangle^x$ and, since $\langle b' \rangle^\varphi = \langle b' \rangle^x$ as already shown, it follows that $\langle g \rangle^\varphi = \langle g \rangle^x$. And if $\langle b'^2 \rangle \neq \langle b' \rangle$, then $\langle g \rangle$ is the unique subgroup different from $\langle a's \rangle \langle b'^2 \rangle$ and $\langle b' \rangle$ contained properly between $\langle a's \rangle \times \langle b' \rangle$ and $\langle b'^2 \rangle$. Since these four groups are mapped in the same way by $\varphi$ and $\alpha$, it follows that $\langle g \rangle^\varphi = \langle g \rangle^x$. Thus $\varphi$ is induced by $\alpha$. \qed

We can now give our first general application of Theorem 7.7.5.

7.7.7 Theorem (Schmidt [1980a]). Let $F$ be a subgroup of the group $G$ with the following properties.

(18) $Z(F) = 1$ and $F \notin P(n, 3)$ for all $n \in \mathbb{N} \cup \{\infty\}$.
(19) $F$ is generated by a set $D$ of involutions satisfying $DF = D$.
(20) Let $d, e \in D$ and $S = \langle d, e \rangle$. If $o(de) \notin \{1, 2, 3, 4, 6, \infty\}$, then there exists a subgroup $T$ of $C_G(S)$ isomorphic to $S$ or to an infinite dihedral group and satisfying $S \cap T = 1$.

If $\varphi$ is a projectivity from $G$ to a group $\overline{G}$, then $F^\varphi$ is isomorphic to $F$.

Proof. We verify the assumptions of Theorem 7.7.5 for $F$, the projectivity $\psi$ from $F$ to $F^\varphi$ induced by $\varphi$, $D$ and $\Delta = \{\langle d \rangle | d \in D\}$. By (19), (6) and (7) hold. We have to show that (8) is satisfied; then, since $\bigcap_{H \in \Delta} N_F(H) = \bigcap_{d \in D} C_F(d) = Z(F) = 1$ and $DF = D$, it will follow from 7.7.5 (b) that $F \simeq F^\varphi = F^\psi$.

We show first that $\varphi$ is 2-regular. For this let $d, e \in D$. If $o(de) \notin \{1, 2, 3, 4, 6, \infty\}$, then by (20) there exist two commuting involutions in $G$ and hence $\varphi$ is 2-regular, by 7.7.3. The same is true if $o(de) = 2, 4, 6$. So assume that $o(de) \in \{3, \infty\}$ for any two different elements $d, e \in D$. Since $F = \langle d | d \in D \rangle$ and $Z(F) = 1$, we see that $|D| \geq 2$. So if the group $G_0$ generated by the involutions in $G$ were a $P$-group, it would lie in $P(m, 3)$ for some $m \in \mathbb{N} \cup \{\infty\}$ and, as $F \leq G_0$, this would contradict (18). Thus $G_0$ is not a $P$-group and by 7.7.2 there exists a prime $q$ such that $|H^\varphi| = q$ for every subgroup $H$ of order 2 of $G$. Suppose, for a contradiction, that $q \neq 2$. Then by 7.7.1, $o(de) = 3$ and $\langle d, e \rangle$ is nonabelian of order 6. Therefore $\langle d, e \rangle^\varphi$ lies in $P(2, 3)$ and contains three subgroups of order $q \neq 2$. Thus $q = 3$, $\langle d, e \rangle^\varphi$ is elementary abelian of order 9 and so $\langle d \rangle^\varphi$ and $\langle e \rangle^\varphi$ are commuting subgroups of order 3 in $\overline{G}$. This holds for every pair $d, e$ of different elements in $D$ and, since $D$ generates $F$, it follows that $F^\varphi$ is an elementary abelian 3-group. But then $F \notin P(n, 3)$ for some $n$, contradicting (18). Thus $q = 2$ and

(21) $\varphi$ is 2-regular.

To prove (8) for $\psi$, let $d \in D, H = \langle e \rangle \in \Delta, \langle d \rangle^\varphi = \langle x \rangle$, and $S = \langle d, e \rangle$. Suppose first that $o(de) \notin \{1, 2, 3, 4, 6, \infty\}$. Then by (20) there exists $T \leq C_G(S)$ such that $S \cap T = 1$ and $T \simeq S$ or $T$ is an infinite dihedral group. If $T \simeq S$, then by 7.7.6, $\varphi$ is induced by an isomorphism on $\langle S, T \rangle \simeq S \times T$. In particular,

(22) there exists an isomorphism $\alpha: S \to S^\varphi$ such that $X^\alpha = X^\varphi$ for all $X \leq S$.\hfill\qed
We show that this is also true if \( T \) is an infinite dihedral group. Indeed, by 7.6.2 and 7.7.1, \( (S \times T)^\varphi = S^\varphi \times T^\varphi \) and \( T^\varphi \cong T \). Let \( N \leq T \) such that \( T/N \cong S \). Then \( \varphi \) induces a projectivity from \( \langle S, T \rangle/N \cong S \times (T/N) \) onto \( \langle S, T \rangle^\varphi/N^\varphi \) and by 7.7.6 there exists an isomorphism \( \gamma: SN/N \rightarrow (SN)^\varphi/N^\varphi \) such that \( (V/N)^\varphi = V^\varphi/N^\varphi \) for all \( N \leq V \leq SN \). If \( \beta: S \rightarrow SN/N \) and \( \delta: S^\varphi N^\varphi/N^\varphi \rightarrow S^\varphi \) are the natural isomorphisms, then \( \alpha = \beta \gamma \delta \) is an isomorphism from \( S \) onto \( S^\varphi \) satisfying \( X^\varphi = X^\beta \delta = (XN/N)^\delta = (X^\varphi N^\varphi/N^\varphi)^\delta = X^\varphi \) for every \( X \leq S \). Thus (22) also holds in this case, and it is clear that (22) implies (8). Indeed, since \( d \in S \) and \( H \leq S \), the equalities \( \langle x \rangle = \langle d \rangle^\varphi = \langle d \rangle^x \) imply that \( x = d^x \). Then \( (H^\varphi)^x = (H^\varphi)^x = (H^\delta)^x = (H^d)^x = (H^d)^\varphi = (H^d)^\varphi \), as desired.

Now suppose that \( o(de) \in \{1, 2, 3, 4, 6, \infty \} \). If \( o(de) = 1 \), then \( H = \langle d \rangle \) and so \( (H^d)^\varphi = H^\varphi = (H^\varphi)^x \). If \( o(de) = 2 \), \( S \) and \( S^\varphi \) are elementary abelian of order 4 and hence again \( (H^d)^\varphi = H^\varphi = (H^\varphi)^x \). If \( o(de) = 4 \), then \( S \) and \( S^\varphi \) are dihedral groups of order 8. Here \( H \) and \( H^d \) are the unique minimal subgroups of \( S \) which together with

\[ \langle d \rangle \text{ generate } S. \] 

Then \( H^\varphi \) and \( (H^d)^\varphi \) have the same property in \( S^\varphi \) with respect to \( \langle x \rangle \) and hence are conjugate under \( x \). Exactly the same argument applies if \( o(de) = 6 \); here 4 of the 6 involutions in \( S \setminus \langle de \rangle \) together with \( d \) generate subgroups of order 6, 4, and 2 of \( S \). Similarly, if \( o(de) = \infty \), \( S \) and \( S^\varphi \) are infinite dihedral groups. Since every element in \( S \setminus \langle de \rangle \) has the form \( (de)^i d \) \((i \in \mathbb{Z})\), there are exactly two subgroups of order 2 in \( S \) which together with \( \langle d \rangle \) generate \( S \), namely \( \langle (de)^i d \rangle = H^d \) and \( \langle (de)^{-1} d \rangle = H \). Their images have the same property in \( S^\varphi \) with respect to \( \langle d \rangle^\varphi = \langle x \rangle \) and hence are conjugate under \( x \). Thus \( (H^\varphi)^x = (H^d)^\varphi \), as desired. Finally, suppose that \( o(de) = 3 \). Then, since \( \varphi \) is 2-regular, \( S^\varphi \) is nonabelian of order 6 and \( H^\varphi \) and \( (H^d)^\varphi \) are the unique subgroups of order 2 different from \( \langle d \rangle^\varphi \) in \( S^\varphi \). Thus \( (H^\varphi)^x = (H^d)^\varphi \) and (8) holds in all cases.

In general, we shall use Theorem 7.7.7 in the situation that \( F = G \). However, there will also be an application in 7.8.17 in which \( F < G \) and, of course, we have the following general consequence.

**7.7.8 Corollary.** Let \( H \) be a group generated by involutions and with trivial centre. If \( K \cong H \) or \( K \) is an infinite dihedral group, then \( G = H \times K \) is determined by its subgroup lattice.
Proof. Let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). Then by 7.6.2 and 7.7.3, \( \overline{G} = H^\varphi \times K^\varphi \) and \( \varphi \) is 2-regular. We apply 7.7.7 with \( F = H \) to prove that \( H^\varphi \simeq H \). It will also follow that \( K^\varphi \simeq K \) if \( K \simeq H \); and by 7.7.1, \( K^\varphi \simeq K \) if \( K \) is an infinite dihedral group. So, in both cases, \( \overline{G} \simeq H \times K = G \), as desired.

By assumption, \( Z(H) = 1 \). If \( H \in P(n, 3) \) for some \( n \), then by 2.2.5, \( H^\varphi \in P(n, 3) \) and, since \( \varphi \) is 2-regular, it follows that \( H^\varphi \simeq H \). So we may assume that \( H \notin P(n, 3) \). Thus (18) holds for \( F = H \) and (19) is satisfied if we take for \( D \) the set of all involutions in \( H \). Finally, \( S = \langle d, e \rangle \leq H \) for all \( d, e \in D \). So if \( K \simeq H \), there exists \( T \leq K \leq C_G(S) \) such that \( T \simeq S \); and if \( K \) is an infinite dihedral group, we may choose \( T = K \). In both cases, (20) is satisfied and by 7.7.7, \( H^\varphi \simeq H \).

Holmes [1971] has shown that for two lattice-isomorphic Rottländer groups \( H_1 \) and \( H_2 \), the groups \( H_1 \times K \) and \( H_2 \times K \) are lattice-isomorphic if \( K \) is an infinite dihedral group.

### Multiply transitive permutation groups

If \( G \) is a permutation group on a set \( \Omega \) and \( \alpha \in \Omega \), we write \( G_\alpha \) for the stabilizer of \( \alpha \) in \( G \) and \( \alpha^G \) for the orbit of \( \alpha \) under \( G \), that is, \( G_\alpha = \{ g \in G | g\alpha = \alpha \} \) and \( \alpha^G = \{ g\alpha | g \in G \} \). Then it is well-known that

\[
(23) \quad G_\alpha^g = G_{g\alpha} \quad \text{for all} \quad g \in G \quad \text{and} \quad |\alpha^G| = |G : G_\alpha|.
\]

So if \( G \) is transitive on \( \Omega \), the set \( \Delta = \{ G_\alpha | \alpha \in \Omega \} \) of stabilizers of the points of \( \Omega \) is a class of conjugate subgroups of \( G \). Recall that \( G \) is said to be \( k \)-transitive on \( \Omega \) \((k \in \mathbb{N}, k \leq |\Omega|)\) if for any two ordered \( k \)-tuples \((\alpha_1, \ldots, \alpha_k)\) and \((\beta_1, \ldots, \beta_k)\) consisting of distinct elements of \( \Omega \), there exists \( g \in G \) such that \( \alpha_i^g = \beta_i \) for \( i = 1, \ldots, k \). Clearly, for \( k \geq 2 \), every \( k \)-transitive group is \((k - 1)\)-transitive, and the stabilizer \( G_\alpha \) of a point \( \alpha \) in a \( k \)-transitive group \( G \) is \((k - 1)\)-transitive on \( \Omega \setminus \{ \alpha \} \).

Now let \( G \) be 2-transitive on \( \Omega \) and assume that \( |\Omega| \geq 3 \). We put \( \Delta = \{ G_\alpha | \alpha \in \Omega \} \) and want to look out for the assumptions of Theorem 7.7.5. Clearly (6) has to be assumed. If \( G_\alpha < M \leq G \), there exists \( x \in M \) such that \( \alpha^x \neq \alpha \) and, since \( G_\alpha \) is transitive on \( \Omega \setminus \{ \alpha \} \), it follows that \( M \) is transitive on \( \Omega \). Thus for \( g \in G \), there exists \( y \in M \) such that \( \alpha^{gy} = \alpha \); hence \( gy \in G_\alpha \leq M \) and so \( g = (gy)y^{-1} \in M \). Therefore \( M = G \) and this shows that

\[
(24) \quad \Delta \text{ is a conjugacy class of maximal subgroups of } G.
\]

In particular, (7) holds. Moreover, since \( G_\alpha \) is transitive on \( \Omega \setminus \{ \alpha \} \) and \( |\Omega| \geq 3 \), we have \( G_\alpha \neq 1 \). Since \( G \) is faithful on \( \Omega \), it follows that \( N_G(G_\alpha) = G_\alpha \) and

\[
(25) \quad \bigcap_{\alpha \in \Omega} N_G(H) = \bigcap_{\alpha \in \Omega} G_\alpha = 1.
\]

Furthermore, if \( \Omega \) is finite, (23) shows that

\[
(26) \quad |G_\alpha : G_{\beta\alpha}| = |\Omega| - 1 = |G : G_\alpha| - 1 \quad \text{for} \ \alpha \neq \beta \in \Omega.
\]

If \( G \in P(n, p) \) for some prime \( p \) and \( n \in \mathbb{N} \cup \{ \infty \} \), then, since every \( p \)-subgroup of \( G \) is normal in \( G \) and \( G_\alpha \) has trivial core, it follows that \( |G_\alpha| = q \) is the smaller prime
involved in \( G \) and so \( |G| = pq \). By (26), \( q = p - 1 \) and hence \( p = 3 \). Thus we have shown:

(27) If \( G \) is a \( P \)-group, then \( |\Omega| = 3 \) and \( G \cong S_3 \).

Now suppose that \( |\Omega| \geq 4 \) and \( \varphi \) is a projectivity from \( G \) to a group \( \overline{G} \); consider \( H = G_a \in \Delta \). If \( H^\varphi \trianglelefteq \overline{G} \), then, since \( H \) is a maximal subgroup of \( G \), it would follow that \( |\overline{G} : H^\varphi| \) is a prime and, by 6.5.3, \( G/H_G \) would be a \( P \)-group. But since \( H_G = 1 \), this would contradict (27). Thus \( H^\varphi \) is not normal in \( \overline{G} \) and hence \( N_{\overline{G}}(H^\varphi) = H^\varphi \). So we have the following:

(28) If \( |\Omega| \geq 4 \), then \( N_{\overline{G}}(H^\varphi) = H^\varphi \) for all \( H \in \Delta \) and \( \bigcap_{H \in \Delta} N_{\overline{G}}(H^\varphi) = 1 \).

Now 7.7.5 and (23)–(28) suggest the following procedure to prove that \( G \) is determined by its subgroup lattice.

7.7.9 Remark. Let \( G \) be a doubly transitive permutation group on a set \( \Omega \), \( |\Omega| \geq 4 \), and assume that \( G \) is generated by a set \( D \) of involutions. If we want to prove that \( G \) is determined by its subgroup lattice and \( \varphi \) is a given projectivity from \( G \) to a group \( \overline{G} \), we put \( \Delta = \{ G_a \mid a \in \Omega \} \) and try to verify the assumptions of Theorem 7.7.5. By assumption and (24), (6) and (7) are satisfied. So we have to prove (8); then 7.7.5(a) together with (25) and (28) will yield that \( \overline{G} \cong G \). To do this, we let \( d \in D \), \( H = G_a \in \Delta \) and \( \langle d \rangle^\varphi = \langle x \rangle \). If \( d \in H \), then \( x \in H^\varphi \) and hence \( (H^\varphi)^x = H^\varphi = (H^d)^\varphi \), as desired. So we are left with the case that \( d \not\in H \), that is, \( x^d = \beta \) with \( x \neq \beta \in \Omega \). Since \( d \) is an involution, it follows that \( \beta^d = x \) and hence by (23),

(29) \( G_x^d = G_\beta \), \( G_\beta^d = G_x \), and \( G_\alpha^d = G_\alpha \).

By (27), \( G \) is not a \( P \)-group and then 7.7.4 implies that

(30) \((G_\alpha^\varphi)^x = G_\alpha^\varphi\).

Finally, \( x \notin G_x^d = N_{\overline{G}}(G_x^\varphi) \) by (28) since \( d \notin G_x \), thus

(31) \((G_x^\varphi)^x \neq G_\varphi^d\).

Since \( H = G_x \) and \( H^d = G_\beta \), we have to show that \((G_x^\varphi)^x = G_\beta^\varphi\); then (8) will hold.

\( \square \)

If \( G \) is 3-transitive, this is quite easy since the stabilizers \( G_x \) and \( G_\beta \) are characterized in the interval \([G/G_\beta]\).

(32) Let \( G \) be triply transitive on \( \Omega \), \( |\Omega| \geq 4 \) and let \( x, \beta \in \Omega \) such that \( x \neq \beta \). Then \([G/G_\beta]\) has precisely 3 atoms, namely \( G_x \), \( G_\beta \), and a subgroup \( X \) satisfying \( |X : G_\beta| = 2 \).

Proof. Since \( G_x \) is 2-transitive on \( \Omega \setminus \{ x \} \), \( G_{x\beta} \) is a maximal subgroup of \( G_x \) and, similarly, of \( G_\beta \). Furthermore, since \( G \) is 2-transitive, there exists \( g \in G \) such that \( x^g = \beta \) and \( \beta^g = x \). Then \( g \notin G_{x\beta} \), but \( g^2 \in G_{x\beta} \) and, by (23), \( G_{x\beta} = (G_x \cap G_\beta)^g = G_x^g \cap G_\beta^g = G_x \cap G_\beta = G_{x\beta} \). It follows that \( |\langle g, G_{x\beta} \rangle : G_{x\beta}| = 2 \) and, since \( g \notin G_x \) and \( g \notin G_\beta \), \( \langle g, G_{x\beta} \rangle \) is a third atom in \([G/G_{x\beta}]\). Therefore to prove (32) we have to show
that if $X$ is an atom in $[G/G_{\alpha\beta}]$ and $G_{\alpha} \neq X \neq G_{\beta}$, then $X = \langle g, G_{\alpha\beta} \rangle$. Since $G_{\alpha\beta}$ is maximal in $G_{\alpha}$ and $G_{\beta}$, we obtain $X_{\alpha} = X \cap G_{\alpha} = G_{\alpha\beta} = X \cap G_{\beta} = X_{\beta}$. If $X$ were transitive on $\Omega$, there would exist $x \in X$ such that $\alpha^x = \beta$ and hence by (23), $G_{\alpha\beta}^x = X_{\alpha}^x = X_{\beta}^x$. It would follow that $X_{x} = G_{\alpha\beta} \leq X$ and the transitivity of $X$ would imply that $G_{\alpha\beta} = 1$. But since $G$ is 3-transitive, $G_{\alpha\beta}$ is transitive on $\Omega \setminus \{x, \beta\}$ and $|\Omega \setminus \{x, \beta\}| \geq 2$, a contradiction. Therefore $X$ is not transitive on $\Omega$. Since $G_{\alpha\beta} \leq X$ is transitive on $\Omega \setminus \{x, \beta\}$ and $X_{x} = G_{\alpha\beta} = X_{\beta}$, it follows that $\alpha^x = \beta$ and $\beta^x = \alpha$ for every $x \in X \setminus G_{\alpha\beta}$. Then $xg \in G_{\alpha\beta}$ and hence $x \in \langle g, G_{\alpha\beta} \rangle$. Thus $X = \langle g, G_{\alpha\beta} \rangle$, as desired.

We can now give our first application of Theorem 7.7.5 to multiply transitive permutation groups.

7.7.10. Theorem. Every triply transitive permutation group of degree at least 4 which is generated by involutions is determined by its subgroup lattice.

Proof. Let $G$ be 3-transitive on the set $\Omega$, $|\Omega| \geq 4$, $D$ the set of involutions in $G$ and $\varphi, \Delta, d, x, \alpha, \beta$ as in Remark 7.7.9. We have to show that $(G_{\alpha}^x)^x = G_{\beta}^x$. By (32) there are precisely 3 subgroups of $G$ containing $G_{\alpha\beta}$ as a maximal subgroup, namely $G_{\alpha}^x$, $G_{\beta}^x$, and $\langle d, G_{\alpha\beta} \rangle^x$. Since, by (30), $G_{\alpha\beta}^x$ is normalized by $x$, these subgroups have to be permuted by $x$. Now $x \in \langle d, G_{\alpha\beta} \rangle^x$ and, by (31), $(G_{\alpha}^x)^x \neq G_{\beta}^x$. It follows that $(G_{\alpha}^x)^x = G_{\beta}^x$, as desired.

The most interesting groups satisfying the assumptions of Theorem 7.7.10 are the symmetric and alternating groups. More generally, if for every set $\Omega$ and infinite cardinal $A$ we define $\text{Sym}(\Omega, A) = \{g \in \text{Sym} \Omega | |\{x \in \Omega | x^g \neq x\}| < A\}$, then these groups too fall under Theorem 7.7.10. We collect these and some other examples in the following corollary. For the finite symmetric and alternating groups, Exercises 9 and 10 show some other methods to prove the desired result.

7.7.11 Corollary. The following groups are determined by their subgroup lattices:

(a) $\text{Sym} \Omega$ and, more generally, $\text{Sym}(\Omega, A)$ for every set $\Omega$ with $|\Omega| \geq 4$ and every infinite cardinal $A$.

(b) $\text{Alt} \Omega$, $|\Omega| \geq 4$.

(c) $\text{PGL}(2, F)$ where $F$ is a field, $|F| \geq 3$.

(d) The five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$.

Proof. (a) Every permutation can be decomposed into cycles, every finite cycle is a product of transpositions and

$$(\ldots, -1, 0, 1, \ldots) = [(0, 1)(-1, 2)(-2, 3)\ldots][(0, 2)(-1, 3)(-2, 4)\ldots].$$

Thus $\text{Sym}(\Omega, A)$ is generated by involutions and, of course, 3-transitive on $\Omega$ if $|\Omega| \geq 4$.

(b) As shown in § 1.4, $A_4$ is determined by its subgroup lattice. In addition for $|\Omega| \geq 5$, $\text{Alt} \Omega$ is 3-transitive and generated by involutions since it is simple and contains involutions.
7.7 Groups generated by involutions

(c) It is well-known that $\text{PGL}(2, F)$ is sharply 3-transitive on the projective line (see Huppert [1967], p. 151 or (33) below). We leave it as an exercise for the reader to show that every element in this group is even the product of two involutions.

(d) The Mathieu group $M_n$ is 3-transitive of degree $n$ and simple (see Huppert and Blackburn [1982b], pp. 297–303), and hence is generated by involutions.

We come now to doubly transitive permutation groups generated by involutions. Here we need additional properties to prove that such a group is determined by its subgroup lattice. Some of these occur in the following groups.

7.7.12 Example. Let $V$ be a vector space of dimension $n \geq 2$ over the field $F$. Then the general linear group $\text{GL}(V)$ operates on the set $\Omega$ of 1-dimensional subspaces of $V$ and the kernel of this operation is the group of scalar transformations of $V$. Let $G = \text{PSL}(n, F) = \text{SL}(V)/Z$ where $Z$ is the set of scalar transformations of determinant 1, and let $\alpha, \beta, \gamma$ be three distinct elements of $\Omega$. Then we claim that

(a) $G$ is a doubly transitive permutation group on $\Omega$ and

(b) $G_{ab}$ fixes at most one further point of $\Omega$, except when $n = 2$ and $|F| = 3$.

Furthermore, if $n \geq 3$, then

(c) $G_{ab}$ has exactly 4 orbits on $\Omega$ and

(d) there exists an involution $t \in G$ such that $t = (\alpha \beta)(\gamma)$ and $G = \langle t^x \mid x \in G \rangle$.

Proof. Let $\delta, \epsilon \in \Omega$ such that $\delta \neq \epsilon$ and let $\alpha = \langle u \rangle$, $\beta = \langle v \rangle$, $\delta = \langle w \rangle$, $\epsilon = \langle z \rangle$. Then $u, v$ and $w, z$ are linearly independent and there exists $\sigma \in \text{SL}(V)$ such that $u^\sigma = w$, $v^\sigma = cz$ with suitable $c \in F$. Then $g = \sigma Z$ satisfies $\alpha^g = \delta$, $\beta^g = \epsilon$ and thus $G$ is 2-transitive on $\Omega$.

To prove the other assertions, suppose first that $n = 2$ and $|F| \geq 4$. Then there exist $u, v \in V$ and $c \in F$ such that $\alpha = \langle u \rangle$, $\beta = \langle v \rangle$, $\gamma = \langle u + v \rangle$, and $0 \neq c^2 \neq 1$. Let $\sigma \in \text{SL}(V)$ be defined by $u^\sigma = cu$, $u^\sigma = c^{-1}v$. Then $g = \sigma Z \in G_{ab}$ and $\gamma^g \neq \gamma$; thus (b) holds in this case. We mention in passing that if $\delta \in \Omega \setminus \{\alpha, \beta\}$, then $\delta = \langle au + v \rangle$ for some $a \in F \setminus \{0\}$ and there exists $\sigma \in \text{GL}(V)$ satisfying $u^\sigma = au$, $v^\sigma = v$ so that $\alpha^\sigma = \alpha$, $\beta^\sigma = \beta$, and $\gamma^\sigma = \delta$; this shows that $\text{PGL}(V)_{ab}$ is transitive on $\Omega \setminus \{\alpha, \beta\}$ and hence

(33) $\text{PGL}(V)$ is triply transitive on $\Omega$ if $n = 2$.

Now assume that $n \geq 3$ and define $\Gamma_{ab} = \{\delta \in \Omega \setminus \{\alpha, \beta\} \mid \delta \leq \alpha + \beta\}$ and $\Delta_{ab} = \{\delta \in \Omega \setminus \{\alpha, \beta\} \mid \delta \leq \alpha + \beta\}$. If $\gamma, \delta \in \Gamma_{ab}$, we may again choose $u, v \in V$ such that $\alpha = \langle u \rangle$, $\beta = \langle v \rangle$, $\gamma = \langle u + v \rangle$, $\delta = \langle au + v \rangle$ for some $a \in F \setminus \{0\}$; also there exists $w \in V$ such that $u, v, w$ are linearly independent. Then there are $\sigma, \tau \in \text{SL}(V)$ such that $u^\sigma = au$, $v^\sigma = v$, $w^\sigma = a^{-1}w$ and $u^\tau = v$, $v^\tau = u$, $w^\tau = -w$, $\tau^2 = 1$. And if $\gamma, \delta \in \Delta_{ab}$, then $\alpha = \langle u \rangle$, $\beta = \langle v \rangle$, $\gamma = \langle w \rangle$, $\delta = \langle z \rangle$ where $u, v, w, u, v, z$ are linearly independent. Then there are $\sigma, \tau \in \text{SL}(V)$ satisfying $u^\sigma = u$, $v^\sigma = v$, $w^\sigma = cz$ for suitable $c \in F$, $u^\tau = v$, $v^\tau = u$, $w^\tau = -w$, and $\tau^2 = 1$. In both cases, $g = \sigma Z \in G_{ab}$ and satisfies $\gamma^g = \delta$, whereas $t = \tau Z$ is an involution in $G$ such that $\alpha^t = \beta$, $\beta^t = \alpha$, and $\gamma^t = \gamma$. It follows that $\{x\}, \{\beta\}, \Gamma_{ab}$, and $\Delta_{ab}$ are the orbits of $G_{ab}$ on $\Omega$ and since $|\Delta_{ab}| > 1$ this also implies (b). Finally, since $G$ is simple (see Robinson [1982], p. 72), the conjugates of $t = (\alpha\beta)(\gamma) \ldots$ generate $G$. 

\[\square\]
We now show that if \( G \) is a finite 2-transitive group generated by involutions, then (b) of 7.7.12 yields that \( G \) is determined by its subgroup lattice.

7.7.13 Theorem (Schmidt [1975b]). Let \( G \) be a doubly transitive permutation group on a finite set \( \Omega, |\Omega| = n \geq 4 \), such that the stabilizer \( G_{a\beta} \) of two distinct points \( a, \beta \in \Omega \) fixes at most one further point. If \( G \) is generated by involutions, then \( G \) is determined by its subgroup lattice.

Proof. Let \( \varphi \) be a projectivity from \( G \) to a group \( \bar{G} \), \( D \) the set of involutions in \( G \) and \( \Delta = \{ G_x | x \in \Omega \} \). We first prove that

(34) \((\Delta^\varphi)^g = \Delta^\varphi \) for all \( g \in \bar{G} \).

For this we have to show that \( H^{\alpha(g)} = H^{\alpha(g)a} \in \Delta \) for all \( H \in \Delta \) and \( g \in \bar{G} \). Since the stabilizers of the points are maximal subgroups, their images generate \( \bar{G} \), and hence it suffices to show that \( H^{\alpha(g)} \in \Delta \) for all \( g \in G_{a\beta} \) (\( x \in \Omega \)). Clearly, \( G_{a\beta}^{\alpha(g)} = G_x \in \Delta \) and for \( x \neq \beta \in \Omega \), we have \( G_{a\beta}^{\alpha(g)} = (G^g \cap G_x)^{\alpha(g)} = G_{a\beta}^{\alpha(g)} \cap G_x \). If \( G \) were \( P \)-decomposable, it would be a \( P \)-group since it is generated by involutions; but this contradicts (27).

Thus \( G \) is not \( P \)-decomposable and, by 5.6.10, \( \tau(g) \) is index preserving. Thus

\[
|G_{a\beta}^{\alpha(g)} : G_{a\beta}^{\alpha(g)} \cap G_x| = |G_{a\beta}^{\alpha(g)} : G_{a\beta}^{\alpha(g)}| = |G_{a\beta} : G_{a\beta}| = n - 1,
\]

by (26). This shows that the orbit of \( x \) under \( G_{a\beta}^{\alpha(g)} \) has length \( n - 1 \), and hence there exists a unique point \( \gamma \in \Omega \) not contained in this orbit. It follows that \( G_{a\beta}^{\alpha(g)} \leq G_{a\gamma} \), and then \( G_{a\beta}^{\alpha(g)} = G_{a\gamma} \), since both groups are maximal subgroups of \( G \). Thus \( \Delta^{\alpha(g)} = \Delta \) and (34) holds.

To prove the theorem, we have to show that \( (G_{a\beta}^\gamma)^x = G_{a\beta}^\gamma \) where \( d, x, \alpha, \beta \) are as in Remark 7.7.9. By (30) and (31), \( (G_{a\beta}^\gamma)^x = G_{a\beta}^\gamma \) and \( (G_{a\beta}^\gamma)^x \neq G_{a\beta}^\gamma \). Since \( (\Delta^\varphi)^x = \Delta^\varphi \), it follows that \( x \) permutes the \( G_{a\gamma}^\gamma (\gamma \in \Omega) \) containing \( G_{a\beta} \). If \( G_{a\beta} \) does not fix a third point of \( \Omega \), then \( G_x \) and \( G_{a\gamma} \) are the unique elements of \( \Delta \) containing \( G_{a\beta} \), and therefore \( (G_{a\beta}^\gamma)^x = G_{a\beta}^\gamma \). So suppose that there exists \( \gamma \in \Omega \) such that \( x \neq \gamma \neq \beta \) and \( G_{a\beta} \) fixes \( \gamma \). Then by assumption, \( G_x \), \( G_{a\beta} \), and \( G_{a\gamma} \) are the unique elements of \( \Delta \) containing \( G_{a\beta} \). By (29), \( G_{a\beta}^g = G_{a\beta}^\gamma \), and hence \( d \) operates on \( \{ G_x, G_{a\beta}, G_{a\gamma} \} \). Since \( G_x^d = G_{a\beta}^d \) and \( G_{a\beta}^d = G_{a\beta} \), it follows that \( G_{a\beta} = G_{a\gamma} \). Then (24) implies that \( d \in G_{a\gamma} \) and so \( x \in G_{a\gamma}^\gamma \). Therefore \( (G_{a\gamma}^\gamma)^x = G_{a\gamma}^\gamma \) and hence again \( (G_{a\beta}^\gamma)^x = G_{a\beta}^\gamma \), as desired.

By 7.7.12, the groups \( \text{PSL}(n, q), n \geq 2, q \) a prime power, \( q \geq 4 \) if \( n = 2 \), satisfy the assumptions of Theorem 7.7.13. In fact, it is known that in every finite simple 2-transitive permutation group the stabilizers of two points fix at most one further point. Thus the unitary groups \( \text{PSU}(3, q^2), q \geq 3 \) a prime power, the symplectic groups \( \text{Sp}(2m, 2), m \geq 3 \), the Suzuki groups, the Ree groups, the Higman-Sims group and Conway's group (3) also fall under our theorem.

Futhermore note that the proof of (34) did not use our additional assumption on \( G_{a\beta}^\gamma \); nor did it really require that \( G \) be generated by involutions. Thus, in general, if \( G \) is a finite doubly transitive permutation group of degree at least 4 and \( \varphi \) is a projectivity from \( G \) to a group \( \bar{G} \), then \( \bar{G} \) operates on \( \Delta \) and it is possible to show that \( \bar{G} \) is 2-transitive on \( \Delta \). A consequence of this for soluble doubly transitive groups is given in Exercise 5.
We now show that for a possibly infinite 2-transitive permutation group $G$, properties (c) and (d) of 7.7.12 yield that $G$ is determined by its subgroup lattice.

7.7.14 Theorem (Schmidt [1980a]). A doubly transitive permutation group $G$ on a set $\Omega$, $|\Omega| \geq 4$, is determined by its subgroup lattice if it has the following three properties:

1. $G$ is generated by involutions having fixed points on $\Omega$.
2. If $\alpha, \beta, \gamma$ are three distinct elements of $\Omega$, there exists $s \in G$ such that $s = (\alpha)(\beta\gamma)\ldots$.
3. For $\alpha, \beta \in \Omega$ such that $\alpha \neq \beta$, $G_{\alpha \beta}$ has exactly 4 orbits on $\Omega$.

Proof. Let $G$ be a group satisfying (35)–(37), $D$ the set of involutions in $G$ having fixed points on $\Omega$ and $\phi, \Delta, d, \alpha, \beta, \gamma$ as in Remark 7.7.9. We have to show that $(G_{\gamma})^x = G_{\gamma}$. By (31), $(G_{\gamma})^x \neq G_{\gamma}$; let $F = G_{\gamma}^{\phi^{-1}}$. Since $d \in D$, there exists $r \in D$ such that $d = (\alpha\beta)(\gamma)$ and by (36) there exists $s \in G$ such that $s = (\alpha)(\beta\gamma)\ldots$ and hence $(sd)^3 \in T$; it follows that $W/T$ is a dihedral group of order 6. Therefore $d$ and $d^r$ are involutions such that $W = \langle T, d, d^r \rangle$ and again by 7.7.4, $T^\phi \leq W$. Thus $\phi$ induces a projectivity from $W/T$ onto $W^\phi/T^\phi$, and hence

$(38) W^\phi/T^\phi$ is either elementary abelian of order 9 or dihedral of order 6.

Suppose, for a contradiction, that $|W^\phi/T^\phi| = 9$. Then $(\langle T, d \rangle)^\phi = \langle T, d \rangle^\phi$, and hence by (30), $x$ normalizes $(T, s, G_{\alpha \beta})^x = \langle T, s, G_{\alpha \beta} \rangle^x = S^x$. Since $s = (\alpha)(\beta\gamma)\ldots$ and $S^x = S$, we have $G_{\alpha \beta} < S < G_{\alpha \beta}$ and so $S \cap S^d \leq G_{\alpha \beta} \cap G_{\beta} = G_{\alpha \beta}$. Therefore $S$ is not normal in $\langle S, d \rangle$ and, by 6.5.3, $\langle S, d \rangle/S \langle S, d \rangle \in P(2, p)$ for some prime $p$. It follows that $G_{\alpha \beta} = S \cap S^d \leq S$, and hence by (23), $G_{\alpha \beta} = G_{\alpha \beta}^x = G_{\alpha \beta}$. Thus $G_{\alpha \beta}$ fixes $\gamma$ and therefore, by (37), has the four orbits $\{x\}, \{\beta\}, \{\gamma\}$, and $\Omega \setminus \{\alpha, \beta, \gamma\} = \Gamma$ on $\Omega$. The orbits of $F \geq G_{\alpha \beta}$ on $\Omega$ are joins of these orbits of $G_{\alpha \beta}$. Since $\gamma^d = \gamma$, we have $x \in G_{\gamma}$ and so

$F_\gamma = (F \cap G_{\gamma})^F = F^\phi \cap G_{\gamma} = (G_{\gamma})^F \cap (G_{\gamma})^x = (G_{\gamma})^x = (G_{\alpha \beta})^x = G_{\alpha \beta}$,

by (30). Thus $F_\gamma = G_{\alpha \beta}$ and, since $G_{\alpha \beta} < S < F$, it follows that $|\gamma F| = |\gamma : G_{\alpha \beta}| \geq 4$. Thus $\gamma F \cap \Gamma \neq \emptyset$ and hence $\Gamma \leq \gamma F$. Also $\beta \in \gamma F$ since $s = (\alpha)(\beta\gamma)\ldots$ and $S \leq F$. Next $F \neq G_{\gamma}$, so $\Omega \setminus \{\alpha\}$ is not an orbit of $F$ and, finally, $\gamma F = \Omega$. Let $g \in G$ such that $\gamma^g = \alpha$. Then $G_{\alpha \beta}^g = F_\gamma = F_\gamma = F_\gamma = F_\gamma = G_{\gamma} \geq S$. However this is impossible since $G_{\alpha \beta}^g$ has 4 orbits on $\Omega$ whereas $S$ has at most 3 since it contains $G_{\alpha \beta}$ and $S = (\beta, \gamma)\ldots$.

This contradiction shows that $W^\phi/T^\phi$ is dihedral of order 6. Again by 7.7.4, $(T, d)^{\phi^{-1}} \leq W^\phi$ and hence $o(x) = (T, d)^\phi$. Then $\phi$ induces a projectivity from $W/T$ onto $W^\phi/T^\phi$, and hence $(30)$ implies that $(S^\phi)^x = (S^x)^\phi$. Therefore if $S = G_{\alpha \beta}$, we are done; so suppose that $S \neq G_{\alpha \beta}$. By 7.7.2, $\phi$ is 2-regular, hence $G_{\alpha \beta}$ is generated by involutions and not a $P$-group. Since $(G_{\alpha \beta})^x = F^\phi$ and $x$ is an involution, $(G_{\alpha \beta} \cap F^\phi)^x = G_{\alpha \beta} \cap F^\phi$ and then 7.7.4 yields that $(G_{\alpha \beta} \cap F)^d = G_{\alpha \beta} \cap F$. It follows that $G_{\alpha \beta} \cap F = G_{\alpha \beta} \cap G_{\alpha \beta}^d = G_{\alpha \beta}$, on the other hand, by (30), $G_{\alpha \beta} \leq G_{\alpha \beta} \cap F$ and thus $G_{\alpha \beta} = G_{\alpha \beta} \cap F = F$. Now let $\{x\}, \{\beta\}, \Gamma_1$, and $\Gamma_2$ be the orbits of $G_{\alpha \beta}$ on $\Omega$, and let $\gamma \in \Gamma_1$, say. Since
Classes of groups and their projectivities

$s^d = (\beta)(x\gamma) \ldots \in S^d = S^{\pi x \pi^{-1}} \leq F$, we see that $\Gamma_1 \subseteq \alpha^F$. If $\alpha^F = \{x\} \cup \Gamma_1$, then $F_\alpha = G_{\alpha}$ is transitive on $\alpha^F \setminus \{x\}$ and hence $F$ is 2-transitive on $\alpha^F$; but as $F_\alpha < S^d < F$, this contradicts (24). If $\beta \in \alpha^F$, there exists $g \in F$ such that $\alpha^g = \beta$ and then $G_{\alpha^g} = F_\alpha = F_\beta \geq S^d$. This is impossible since $G_{\alpha^g}$ has 4 orbits on $\Omega$ whereas $S^d$ has at most 3. Since $\alpha^F$ is a join of orbits of $G_{\alpha^g}$, the only remaining possibility is that $\alpha^F = \{x\} \cup \Gamma_1 \cup \Gamma_2$. Then $\Omega \setminus \{\alpha^F\} = \{\beta\}$ is invariant under $F$, that is $F = G_{\alpha}$. Thus $(G_{\alpha})^F = G_{\alpha}^F$, as desired.

7.7.15 Corollary. If $n \geq 3$ and $F$ is any field, then $PSL(n, F)$ is determined by its subgroup lattice.

Proof. This follows from 7.7.12 and 7.7.14.

If $F$ is a field in which $-1$ is not a square, it is easy to see that $PSL(2, F)$ does not contain involutions with fixed points on $\Omega$. Therefore these groups do not satisfy the assumptions of Theorem 7.7.14. However it can be shown, using 7.7.5 directly, that $PSL(2, F)$ also is determined by its subgroup lattice if $|F| \geq 3$; see Schmidt [1980a] where this result and 7.7.15 are proved for arbitrary skew-fields $F$. Yakovlev [1986] studies the groups $EL_n(R)$ generated by all transvections of dimension $n$ over an associative ring $R$ with identity. He shows that such a group is determined by its subgroup lattice if $n \geq 4$ and the additive group of $R$ either contains an element of infinite order or is generated by elements of prime order.

Classical groups

The methods of this section can also be applied to the other classical groups, that is the symplectic, orthogonal, and unitary groups over fields. We only state the results and give some brief comments on the proofs; for details see Schmidt [1980a].

7.7.16 Theorem. Let $V$ be a finite-dimensional nonsingular symplectic, orthogonal, or unitary vector space over the field $F$. In any of the following cases, $G$ is determined by its subgroup lattice.

(A) $G = PSp(V)$, $V$ symplectic, $\dim V \geq 12$ if char $F \neq 2$, $\dim V \geq 4$ if char $F = 2$.

(B) $G = PO(V)$, $V$ orthogonal, $\Ind V \geq 12$ if char $F \neq 2$, $\Ind V \geq 6$ if (char $F = 2$ or) $-1$ is a square in $F$.

(C) $G = PSU(V)$, $V$ unitary, $\Ind V \geq 6$ if char $F \neq 2$, $\Ind V \geq 2$ if char $F = 2$.

Sketch of proof. In all cases, $G = \tilde{G}/Z$ where $\tilde{G}$ is the group of all isometries of $V$ and $Z = Z(\tilde{G})$. First let char $F \neq 2$ and recall that the index of $V$ is the dimension of a maximal isotropic subspace of $V$. Thus our assumptions imply the existence of hyperbolic planes $H$ in $V$, that are subspaces $H = \langle u, v \rangle$ such that $(u, u) = 0 = (v, v)$ and $(u, v) = 1$. For every such $H$, we let $\sigma_H$ be the linear map on $V$ satisfying $x^{\sigma_H} = -x$ for $x \in H$ and $x^{\sigma_H} = x$ for $x \in H^\perp$. Since $V = H \oplus H^\perp$, $\sigma_H$ is an isometry of $V$ and $\sigma_H Z$ is a well-defined involution in $G$. We let $\mathfrak{S}$ be the set of all hyperbolic planes in $V$, $D = \{\sigma_H Z | H \in \mathfrak{S}\}$ and verify the assumptions of Theorem 7.7.7 for $G$ in place of...
F. Since $G$ is simple, $G = \langle d \mid d \in D \rangle$; so (18) and (19) are satisfied. If $d = \sigma_d Z$ and $e = \sigma_e Z$ are elements in $D$ and $S = \langle d, e \rangle$, then $S$ is trivial on $H^\perp \cap K^\perp$ and, since $\text{ind } V$ is big enough, it is possible to find subspaces $X, Y$ of $V$ and an isometry $\rho$ of $V$ such that $H + K \leq X, X \perp Y$ and $X^\rho = Y$. Then it is easy to see that $T = S^\rho$ satisfies (20). So by 7.7.7, $G$ is determined by its subgroup lattice. If $\text{char } F = 2$, we can work with transvections, that is to say, maps $\sigma$ of the form $x^\sigma = x + \lambda(x, v)v$ for certain $\lambda \in F$ and $v \in V$ satisfying $(v, v) = 0$. Here $\sigma Z$ is an involution in $G$ and $\sigma$ fixes elementwise the hyperplane $\langle v \rangle^\perp$. That is the reason why our method yields better results in this case.

Every finite classical simple group is determined by its subgroup lattice; see 7.8.1 and 7.8.2.

Finite Coxeter groups

We finish this section with a result of quite a different flavour. Recall that a Coxeter group is a group $G$ generated by a set $S$ of involutions such that the relations

$$ (39) \quad (st)^{m(s, t)} = 1 \text{ for } (s, t) \in I $$

are defining relations for $G$; here, for $s, t \in S, m(s, t)$ is the order of $st$ and $I$ is the set of pairs $(s, t)$ for which $m(s, t)$ is finite. The number $|S|$ is called the rank of $G$; so Coxeter groups of rank 2 are just the dihedral groups.

7.7.17 Theorem (Uzawa [1986]). Every finite Coxeter group $G$ of rank $r \geq 3$ is determined by its subgroup lattice.

Proof. Let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$ and let $S$ be as above. It is well-known (see Suzuki [1982], p. 359) that every Coxeter group of rank $r \geq 3$ contains two commuting involutions (even in $S$). By 7.7.3, $\varphi$ is 2-regular and then 7.7.1 shows that $\varphi(st) = \varphi(xy)$ if $s, t \in S, \langle s \rangle^\varphi = \langle x \rangle$ and $\langle t \rangle^\varphi = \langle y \rangle$. Thus $\overline{G}$ is generated by a set of involutions satisfying the relations (39). Since these are defining relations for $G$, there exists an epimorphism from $G$ onto $\overline{G}$. But a finite group cannot be lattice-isomorphic to a proper factor group and it follows that $G \simeq \overline{G}$. 

Exercises

1. (Uzawa [1986]) Let $G$ be the dihedral group of order $2n$ and $n = p_1^{e_1} \cdots p_r^{e_r}$ the prime factorization with $p_1 < \cdots < p_r$. Show that $G$ is determined by its subgroup lattice if and only if one of the following holds:

(a) $n$ is even,

(b) $n$ is odd, $e_1 > 1$ and $\gcd(p_1 - 1, \ldots, p_r - 1) = 2$, or

(c) $n$ is odd, $e_1 = 1$ and $\gcd(p_1, p_2 - 1, \ldots, p_r - 1) = 1$. 

2. (Schmidt [1980a]) Let $G$ be a group and $\varphi$ a projectivity from $G$ to a group $\bar{G}$. If there exist involutions $a, b \in G$ such that $|\langle a \rangle|^p \neq |\langle b \rangle|^p$, show that $G = S \times T$ where $S$ is a nonabelian $P$-group generated by involutions and $S$ and $T$ are coprime.

3. (Schmidt [1980a]) Let $G$ be a group, $D$ a set of involutions and $\Delta$ a set of subgroups of $G$ with the following properties.
   
   (a) $G = \langle \langle d \rangle | d \in D \rangle$ and $G \not\cong P(n,3)$ for all $n \in \mathbb{N} \cup \{\infty\}$.
   
   (b) $\Delta^G = \Delta$ and $\bigcap_{H \in \Delta} N_G(H) = 1$.

   (c) If $a \in D$ and $H \in \Delta$, then $K^a = K$ for all $K \in \Delta \setminus \{H, H^a\}$ such that $H \cap H^a \leq K \leq \langle H, H^a \rangle$.

   Show that if there exists a projectivity $\varphi$ from $G$ to a group $\bar{G}$ such that $(\Delta^G)^\varphi = \Delta^\varphi$, then $\bar{G} \simeq G$.

4. (Schmidt [1975b]) Let $G$ be a finite doubly transitive permutation group on the set $\Omega$, $|\Omega| \geq 4$, and let $\varphi$ be a projectivity from $G$ to a group $\bar{G}$. Show that $\bar{G}$ can be regarded as a doubly transitive permutation group on $\Delta = \{G_a | a \in \Omega\}$.

5. (Schmidt [1975b]) Show that for $p' \geq 4$, the group $\Gamma(p')$ of all semilinear mappings $x \mapsto ax^a + b$ ($a \neq 0, x \in \text{Aut } GF(p')$)

   on $GF(p')$ is determined by its subgroup lattice. (Hint: Use Exercise 4 and Huppert's theorem on soluble doubly transitive permutation groups; see Huppert and Blackburn [1982b], p. 379.)

6. (Schmidt [1975b]) Let $p$ and $r$ be primes, $p \equiv 1 \pmod{r}$, $r > 2$, $\Omega = GF(p')$ and $S = \Gamma(p')$. Let $T = \{x \mapsto x + b | b \in \Omega\}$, $M = \{x \mapsto ax | 0 \neq a \in \Omega\}$ and $A = \{x \mapsto x^a | a \in \text{Aut } \Omega\}$.

   (a) Show that $S$ contains precisely $r + 1$ subgroups of index $r$, namely $TM$, a subgroup containing $A$ and $r - 1$ other subgroups, all 2-transitive on $\Omega$.

   (b) Show that any two of these $r - 1$ remaining subgroups are lattice-isomorphic but not isomorphic.

7. (Schmidt [1980a]) Show that a doubly transitive permutation group $G$ on a set $\Omega$, $|\Omega| \geq 4$, is determined by its subgroup lattice if it has the following two properties.

   (a) $G$ is generated by involutions having fixed points on $\Omega$.

   (b) If $\alpha$, $\beta$, $\gamma$ are three distinct elements of $\Omega$, there exists $s \in G$ such that $s = (\alpha)(\beta)\ldots$ and $G_s = \langle s, G_{s^2} \rangle$.

8. (Holmes [1971]) Show that if $H_1$ and $H_2$ are lattice-isomorphic Rottländer groups and $K$ is an infinite dihedral group, then $H_1 \times K$ and $H_2 \times K$ are lattice-isomorphic. (Hint: Use 1.6.1.)

9. (a) Show that the symmetric group $S_n$ is the only group of order $n!$ which contains a core-free subgroup of index $n$. Use 4.2.6 and 5.4.11 to conclude that $S_n$ is determined by its subgroup lattice if $n \geq 4$.

   (b) Give a similar proof for $A_n$, $n \geq 5$.

10. Show that if $D$ is the set of transpositions in the symmetric group $S_n$ and $d, e \in D$, then $o(de) \in \{1, 2, 3\}$. Use Theorem 7.7.7 to conclude that $S_n$ is determined by its subgroup lattice if $n \geq 4$. 
7.8 Finite simple and lattice-simple groups

Many problems in group theory were solved by the classification of finite simple groups. Among these is one of the most interesting problems on subgroup lattices of groups.

7.8.1 Theorem. Every nonabelian finite simple group is determined by its subgroup lattice.

Proof. Let $G$ be a nonabelian finite simple group and let $\varphi$ be a projectivity from $G$ to a group $\overline{G}$. By 5.3.2 and 4.2.8, $\overline{G}$ is a simple group of the same order as $G$. Using the classification of finite simple groups, Kimmerle, Lyons, Sandling and Teague [1990] have shown that the only pairs of nonisomorphic finite simple groups of the same order are $PSL(3,4)$ and $PSL(4,2)$ and, in the Lie notation, $B_n(q)$ and $C_n(q)$ for some $n \geq 3$ and some odd $q$. In the same paper they show that $PSL(3,4)$ and $PSL(4,2)$ have different numbers of elements of order 5, and that $B_n(q)$ and $C_n(q)$ have different numbers of involutions if $n \geq 3$ and $q$ is odd. Since $\varphi$ is index preserving, this cannot happen for $G$ and $\overline{G}$. It follows that $G \approx \overline{G}$. (Note that all the exceptional groups mentioned above are classical simple groups, so that the methods of §7.7 show that they are determined by their subgroup lattices; see Remark 7.8.2 below.)

Elementary proofs

Unfortunately, a direct proof of Theorem 7.8.1 is not known. But more elementary proofs are available for certain classes of finite simple groups. For doubly transitive simple groups, in particular the alternating and the projective special linear groups, Theorem 7.7.13 yields the desired result. But the methods of §7.7 also work under weaker assumptions than 2-transitivity and therefore it is possible to handle all the classical finite simple groups in this way. We only sketch this briefly; for details see Schmidt [1977b].

7.8.2 Remark. (a) A primitive permutation group $G$ on a finite set $\Omega$ is determined by its subgroup lattice if it has the following four properties.

(i) $G$ is generated by involutions.

(ii) The stabilizer $G_\alpha$ of a point $\alpha \in \Omega$ has precisely two orbits on $\Omega \setminus \{\alpha\}$ (that is, $G$ is a rank 3 group) and these have different lengths; let $\Lambda_\alpha$ be the larger orbit.

(iii) $G = \langle G_\alpha \mid \alpha \in \Omega, \beta \in \Lambda_\alpha \rangle$.

(iv) The stabilizer of two different points fixes at most one further point.

The proof of this theorem uses 7.7.5 and elementary properties of rank 3 groups.

(b) Let $V$ be a nonsingular symplectic, orthogonal, or unitary vector space of dimension $n$ over the field $GF(q)$ with $q$ elements, and assume that one of the following holds:

(A) $V$ symplectic, $n \geq 4$, $q \neq 3$, $G = PSp(V) = PSp(n,q)$.

(B) $V$ orthogonal, $n \geq 7$, $q$ odd, $G = P\Omega(V) = P\Omega(n,q)$. 
(C) \( V \) orthogonal, \( n = 2m \geq 8, q \) even, \( G = P\Omega(V) = P\Omega(n,q) \).

(D) \( V \) unitary, \( n \geq 4, q \) a square, \( G = PSU(V) = PSU(u,q) \).

In any of these cases, \( G \) is a primitive permutation group on the set \( \Omega = \{ \langle v \rangle | 0 \neq v \in V, (v,v) = 0 \} \), respectively \( \Omega = \{ \langle v \rangle | 0 \neq v \in V, f(v) = 0 \} \) in case (C) where \( f \) is the quadratic form associated to \( V \). By Witt's theorem, the stabilizer \( G_\alpha \) of a point \( \alpha = \langle v \rangle \in \Omega \) has the orbits \( \Lambda_1 = \{ \langle w \rangle | (v, w) = 0 \} \) and \( \Lambda_2 = \{ \langle w \rangle | (v, w) = 1 \} \), and \( G \) also satisfies the other assumptions in (a).

(c) The classical simple groups not included in (A)–(D) are isomorphic either to groups on the list or to groups \( PSL(2,q) \) and are therefore covered by (a) or Theorem 7.7.13. The only exceptions are the groups \( PSp(2n,3) \) in which the stabilizer of two points fixes two further points; they are handled in Exercise 1. Thus all the classical finite simple groups are covered by Theorem 7.7.5 and its consequences.

An immediate consequence of Theorem 7.7.7 is that every finite simple group generated by a conjugacy class \( D \) of \( \{3,4\} \)-transpositions, that is, satisfying \( o(de) \leq 4 \) for all \( d, e \in D \), is determined by its subgroup lattice. This covers all the Chevalley and Steinberg groups over \( GF(2) \) and the three Fischer groups.

Finally, there is a short general argument for arbitrary groups of Lie type, which, however, uses a deep theorem of Tits'.

7.8.3 Theorem (Li [1983]). Every finite simple group \( G \) of Lie type of rank \( n \geq 2 \) is determined by its subgroup lattice.

Proof. Let \( \varphi \) be a projectivity from \( G \) to a group \( \overline{G} \). Then \( \overline{G} \) operates on \( L(G) \) via the map \( \tau \), sending every \( x \in \overline{G} \) to the autoprojectivity \( \tau(x) \) of \( G \) defined by \( H^{\tau(x)} = H^{x_\varphi} \) for \( H \leq G \). Let \( p \) be the characteristic of the ground field and \( B \) the normalizer of a Sylow \( p \)-subgroup of \( G \); recall that the parabolic subgroups of \( G \) are the subgroups containing some conjugate of \( B \), and that the set \( \Delta \) of all parabolic subgroups together with the dual of the inclusion relation is the building of \( G \). By 4.2.8, every autoprojectivity of \( G \) is index preserving and hence maps Sylow \( p \)-subgroups to Sylow \( p \)-subgroups. Since the normalizer of a Sylow \( p \)-subgroup \( P \) is the largest subgroup of \( G \) containing \( P \) but no other Sylow \( p \)-subgroup, \( \tau(x) \) permutes the normalizers of the Sylow \( p \)-subgroups and therefore maps parabolic subgroups to parabolic subgroups. So \( \tau(x) \) induces an automorphism \( \sigma(x) \) of the building \( \Delta \) of \( G \). If \( x \in (B^\varphi)^\circ \), then \( \tau(x) \) fixes every subgroup containing \( B^\varphi \), and hence \( \sigma(x) \) is type preserving. Since \( \overline{G} \) is generated by the \( (B^\varphi)^\circ \), we conclude that \( \sigma \) is a homomorphism from \( \overline{G} \) into the group of all type preserving automorphisms of \( \Delta \). By a well-known theorem of Tits [1974], this group contains a normal subgroup \( G^* \cong G \) with soluble factor group. Since \( \overline{G} \) is simple, it follows that \( \overline{G} \) is isomorphic to a subgroup of \( G \). But \( G \) and \( \overline{G} \) are lattice-isomorphic finite groups; thus \( \overline{G} \cong G \), as desired.

Unfortunately, all these partial results cannot prove 7.8.1. No simple direct proof of this theorem, without using the classification of finite simple groups, is known; it would be highly desirable to have such a proof even if it used the Feit-Thompson Theorem.
The second main problem, whether or not every nonabelian finite simple group is strongly determined by its subgroup lattice, is much easier to solve. This is equivalent to asking the question if, for every nonabelian finite simple group $G$,

(1) $P(G) = PA(G)$.

Indeed, (1) is satisfied for every group $G$ which is strongly determined by its subgroup lattice. Conversely, suppose that (1) holds for every nonabelian finite simple group $G$. Then, since every projective image $\overline{G}$ of $G$ is simple, 1.4.3 and (1) would imply that

$$Aut \overline{G} \cong PA(\overline{G}) = P(\overline{G}) = P(G) = PA(G) \cong Aut G;$$

and, since a nonabelian simple group is isomorphic to the unique minimal normal subgroup of its automorphism group, it would follow that $\overline{G} \cong G$. So we would obtain, without using 7.8.1 or the classification of finite simple groups, that $G$ is determined by its subgroup lattice, and (1) then says that every projectivity of $G$ is induced by an isomorphism. We mention in passing that the weaker property

(2) $PI(G) \leq P(G),$

for every nonabelian finite simple group $G$, would suffice to give an elementary proof of Theorem 7.8.1 (see Exercise 2). Metelli [1971] proved that all the minimal simple groups, that is, nonabelian finite simple groups all of whose proper subgroups are soluble, satisfy (1) and therefore also (2). However, we are now going to show that neither property holds for arbitrary finite simple groups. For this, surprisingly enough, it suffices to study the alternating groups. But for completeness sake we will also treat the finite symmetric groups and give some brief comments on infinite symmetric and alternating groups.

### Symmetric and alternating groups

In the sequel let $n \geq 4$, $\Omega = \{1, \ldots, n\}$ and $G = \text{Sym} \Omega = S_n$ or $G = \text{Alt} \Omega = A_n$; write

$$G_i = \{g \in G | i^g = i\} \quad \text{and} \quad \Delta = \{G_i | i \in \Omega\}$$

so that $G_i$ is the stabilizer of the point $i \in \Omega$ in $G$ and $\Delta$ is the set of all stabilizers. We want to investigate the group $P(G)$ of autoprojectivities of $G$. The idea is to show that (except when $n = 6$) $P(G)$ operates on $\Delta$, and then to study this operation. For this purpose we have to establish some basic properties of $\Delta$.

#### 7.8.4 Lemma. If $M \leq G$ such that $|G:M| = n$, there exists $\alpha \in \text{Aut} G$ such that $G^\alpha = M$.

**Proof.** Let $\{Mx_1, \ldots, Mx_n\}$ with $x_n = 1$ be the set of cosets of $M$ in $G$ and consider the permutation representation $\alpha: G \to S_n$ of $G$ on this set: $g^\alpha$ maps $i \in \Omega$ to $j \in \Omega$ if and only if $Mx_i g = Mx_j$. Since $A_n$ is simple for $n \geq 5$, $\bigcap_{x \in G} M^x = 1$; this also holds for
n = 4 since |M| = 3 or 6 in that case. So α is a monomorphism and, since G is the unique subgroup of its order in Sn, it follows that G* = G, that is, α ∈ Aut G. Now g ∈ M if and only if Mg = M and this holds if and only if nα = n. Thus M* = Gn, as desired.

Let D be the set of 3-cycles in Sn. Since (12n) ∈ A(n-1) and An-1 is a maximal subgroup of An, a trivial induction yields that

(3) An = ⟨(123), (124), ..., (12n)⟩.

A product of two 3-cycles has one of the following four types


Again a simple induction yields the following result.

(5) If 1 ≤ m ≤ n - 3 and x1, ..., xm ∈ D such that o(xixj) = 2 for i ≠ j, then M = ⟨x1, ..., xm⟩ has at least n - m - 2 fixed points on Ω.

Indeed, this is obvious for m = 1; so suppose that m ≥ 2 and ⟨x1, ..., x_(m-1)⟩ has at least n - (m - 1) - 2 = n - m - 1 fixed points. Since o(xixm) = 2, we see from (4) that two of the points moved by xm are also moved by x1. It follows that ⟨x1, ..., xm⟩ has at least (n - m - 1) - 1 fixed points.

7.8.5 Lemma. If n ≠ 6, G has only one conjugacy class of subgroups of index n (namely Δ).

Proof. Assume first that G = An and, since the assertion is obvious for n = 4, that n ≥ 5. We show that

(6) D* = D for all α ∈ Aut G.

To see this, first note that by (4), D* is a conjugacy class of elements of order 3 of G such that o(de) ≤ 5 for all d, e ∈ D. Suppose, for a contradiction, that D* ≠ D. Then there exists x ∈ D* \ D. Since o(x) = 3 and x ∉ D, the cycle decomposition of x contains at least two 3-cycles. If x has a fixed point, so that we may assume x = (123)(456)(7)..., then for g = (34)(67) ∈ G, y = x^g = (124)(357)(6)... ∈ D* and xy = (1473256)... has order divisible by 7, a contradiction. On the other hand, if x has no fixed points, then n ≠ 6 implies that x has the form (123)(456)(789)..., say; once again, if g = (34)(67), then y = x^g = (124)(357)(689)... ∈ D* and now xy = (147932586)... has order divisible by 9. This contradiction shows that D* = D.

Now let M be a subgroup of index n in G. By 7.8.4 there exists x ∈ Aut G such that G* = M and, by (3), Gn = An-1 = ⟨(123), (124), ..., (12n-1)⟩. If xi = (12i + 2)^α, then by (6) and (4), xi ∈ D and o(xixj) = o((12i + 2)(12j + 2)) = 2 for i ≠ j. Thus by (5), the group M = G* = ⟨x1, ..., xn-3⟩ has at least n - (n - 3) - 2 = 1 fixed points on Ω. So M ≤ Gi for some i and then M = Gi since both groups have the same order. This proves the lemma for G = An.

If G = Sn and M ≤ G such that |G : M| = n, then |An : M ∩ An| = n or n/2. Since the simple group An does not admit a homomorphism into the symmetric group Sk for k < n, it follows that |An : M ∩ An| = n. So M ∩ An = Gi ∩ An for some i, as we have
just shown. Now \( A_n \trianglelefteq G \), so \( M \neq G_i \) implies that \( M \cap A_n = G_i \cap A_n \leq M \cup G_i = G \), a contradiction. Thus \( M = G_i \), as desired. \( \square \)

7.8.6 Lemma. If \( n = 6 \), \( G \) has exactly two conjugacy classes \( \Gamma \) and \( \Delta \) of subgroups of index 6; for \( M \in \Gamma \) and \( N \in \Delta \), \( |M : M \cap N| = 6 \).

Proof. Let \( S = S_5 \) and \( T = \langle (12345), (1243) \rangle \leq S \). Then \( |T| = 20 \) and hence \( |S : T| = 6 \). Thus the permutation representation \( \beta \) of \( S \) on the cosets of \( T \) is a homomorphism from \( S \) into \( G = S_6 \) with \( \text{Ker} \beta = \bigcap_{x \in S} T^x = 1 \). It follows that \( S^\beta \cong S = S_5 \), and so \( |G : S^\beta| = 6 \). If \( \{ Tx_1, \ldots, Tx_6 \} \) are the cosets of \( T \) in \( S \), then the stabilizer of \( i \) in \( S^\beta \) is \( S^\beta \cap G_i = (T^x)^\beta \), and hence \( S^\beta \cap G_i \cong T \). Since \( G_i \cap G_j \cong S_4 \) for \( i \neq j \), this shows that \( S^\beta \not\cong \Delta = \{ G_i | i \in \Omega \} \). Clearly, \( S^\beta \cap A_6 \) is a subgroup of index 6 in \( A_6 \) which intersects \( G_i \) in a subgroup of order 10. So there exist at least two conjugacy classes of subgroups of index 6, both in \( S_6 \) and in \( A_6 \).

Now let \( G = S_6 \) or \( A_6 \) and \( M, N \subseteq G \) such that \( |G : M| = |G : N| = 6 \). We claim that

\( (7) \ |M : M \cap N| = 6 \) if \( M \) and \( N \) are not conjugate.

To see this, consider the operation of \( M \) on the set \( \Lambda \) of cosets of \( N \) in \( G \). The stabilizer of the coset \( N \) in \( M \cap N \) and hence \( |M : M \cap N| \leq |\Lambda| = 6 \). By 7.8.4, \( M \cong S_5 \) or \( A_5 \) and so \( |M : M \cap N| \geq 5 \). Also \( |M : M \cap N| = 5 \) would imply that \( M \) has one orbit of length 5 and therefore also one fixed point on \( \Lambda \). Thus \( M \leq N^x \) for some \( x \in G \) and, since both groups have the same order, it would follow that \( M = N^x \), contradicting our assumption. So \( |M : M \cap N| = 6 \) and \( (7) \) holds.

Now let \( M_1, \ldots, M_k \) be representatives of the conjugacy classes of subgroups of index 6 in \( G \); thus \( k \geq 2 \) as we have seen. Since \( 3||M_i|| \), there exists \( x_i \in M_i \) such that \( o(x_i) = 3 \). If \( x_i \) were conjugate to \( x_j \) for some \( i \neq j \), then \( x_i^g = x_j \in M_i^g \cap M_j \) for some \( g \in G \); but by \( (7) \), \( |M_i^g \cap M_j| \) is not divisible by 3, a contradiction. Since \( G \) has only two conjugacy classes of elements of order 3, with representatives (123) and (123)(456), we obtain that \( k = 2 \). The second assertion of 7.8.6 follows from \( (7) \). \( \square \)

7.8.7 Remark. By 4.2.8, every autoprojectivity \( \sigma \) of \( G \) is index preserving. So 7.8.5 shows that for \( n \neq 6 \), \( \sigma \) induces a permutation \( \bar{\sigma} \) of \( \Delta \). The map \( \sigma \rightarrow \bar{\sigma} \) is clearly a homomorphism from \( P(G) \) into \( \text{Sym} \Delta \cong S_n \) with kernel

\[ K = \{ \sigma \in P(G) | G_i^\sigma = G_i \text{ for all } i \in \Omega \} .\]

By the homomorphism theorem, \( P(G)/K \) is isomorphic to a subgroup of \( S_n \). \( \square \)

To study the kernel \( K \), we need the following simple result.

7.8.8 Lemma. Let \( n, k, q \) be natural numbers such that \( k^q \equiv 1 \) (mod \( n \)) and \( k^r \neq 1 \) (mod \( n \)) for \( 1 \leq r < q \).

(a) If \( x = (1, \ldots, n) \) is a cycle of length \( n \) and \( s : \Omega \rightarrow \Omega \) is defined by \( i^s \equiv ik \) (mod \( n \)) for \( i \in \Omega = \{1, \ldots, n\} \), then \( s \in S_n \), \( o(s) = q \) and \( x^s = x^k \).

(b) If \( k = n - 1 \) in (a), then \( s \in A_n \) if and only if \( n \equiv 1 \) (mod \( 4 \)) or \( n \equiv 2 \) (mod \( 4 \)).

(c) If \( y \in S_n \) and \( \tau \in \text{Aut} \langle y \rangle \), there exists \( t \in S_n \) such that \( o(t) = o(\tau) \) and \( y^t = y^\tau \).
Proof. (a) Clearly, \( i^r \equiv ik' \pmod{n} \); since \( k' \equiv 1 \pmod{n} \) for \( 1 \leq r < q \), we have \( o(s) = q \) and \( i^{r+1} \equiv ik^{q-1} \pmod{n} \). Thus \( i^{r+1}x^s \equiv (ik^{q-1} + 1)k \equiv i + k \equiv i^r \pmod{n} \) and hence \( s^{-1}xs = x^k \).

(b) If \( k = n - 1 \), then \( s \) interchanges \( i \) and \( n - i \) for all \( i = 1, \ldots, n - 1 \) and hence \( s \) is a product of \( (n-1)/2 \) or \( (n-2)/2 \) transpositions according as \( n \) is odd or even. These numbers are even if and only if \( n \equiv 1 \) (mod 4) or \( n \equiv 2 \) (mod 4), respectively.

(c) Let \( y = y_1 \ldots y_d \) be the cycle decomposition of \( y \) and suppose that \( y^i = y^k = y_1^k \ldots y_d^k \), \( k \in \mathbb{N} \). If \( y_i \) is a cycle of length \( m \) and \( q \) is the smallest natural number satisfying \( k^q \equiv 1 \pmod{m} \), then \( q|o(\tau) \). By (a) there exists \( s_i \in S_n \), operating only on the \( m \) points moved by \( y_i \), such that \( o(s_i) = q \) and \( y_i^q = y_i^k \). Then \( t = s_1 \ldots s_d \in S_n \) satisfies \( y^t = y^k = y^i \) and \( o(t) = o(\tau) \).

7.8.9 Lemma. If \( G = S_n \) and \( \sigma \in P(G) \) such that \( (G_i)^\sigma = G_i \) for all \( i \in \Omega \), then \( \sigma = 1 \).

Proof. We have to show that \( \langle g \rangle^\sigma = \langle g \rangle \) for every \( g \in G \) and use induction on the number \( v(g) \) of points moved by \( g \) to prove this first for involutions \( g \). If \( g \) is a transposition \( (ij) \), then \( \langle g \rangle = \bigcap_{i \neq k \neq j} G_k \) and hence \( \langle g \rangle^\sigma = \langle g \rangle \). So suppose that \( v(g) > 2 \). Then the cycle decomposition of \( g \) yields involutions \( g_i \) such that \( v(g_i) \leq v(g) \) and \( g = g_1g_2 = g_2g_1 \). By the induction assumption, \( \langle g_i \rangle ^\sigma = \langle g_i \rangle \) and hence \( \langle g_1, g_2 \rangle ^\sigma = \langle g_1, g_2 \rangle \); thus the third subgroup \( \langle g \rangle \) of order 2 of the four-group \( \langle g_1, g_2 \rangle \) is invariant under \( \sigma \).

Now let \( g \in G \) such that \( o(g) > 2 \). By 7.8.8 there exists \( s \in G \) such that \( s^2 = 1 \) and \( g^s = g^{-1} \). Then \( H = \langle g, s \rangle \) is generated by involutions and hence \( H^\sigma = H \). Since every element in \( H \setminus \langle g \rangle \) has order 2, each maximal subgroup of \( H \) different from \( \langle g \rangle \) is generated by involutions. Thus \( \sigma \) fixes all these maximal subgroups and hence also \( \langle g \rangle \).

7.8.10 Theorem (Suzuki [1951a], Zacher [1965]). Let \( n \in \mathbb{N}, n \geq 4 \).

(a) If \( n \neq 6 \), \( P(S_n) = P \cdot A(S_n) = PI(S_n) \cong S_n \).

(b) \( P(S_6) = P \cdot A(S_6), PI(S_6) \cong S_6, |P(S_6)/PI(S_6)| = 2 \).

(c) Every projectivity of \( S_n \) is induced by a unique isomorphism.

Proof. (a) By 7.8.7 and 7.8.9, \( P(S_n) \) is isomorphic to a subgroup of \( S_n \). On the other hand, since \( Z(S_n) = 1 \), it follows from 1.4.3 that \( PI(S_n) \cong S_n \). Thus \( P(S_n) = PI(S_n) \cong S_n \).

(b) By 7.8.6, \( G = S_6 \) has two conjugacy classes \( \Gamma \) and \( \Delta \) of subgroups of index 6. If \( M, N \in \Delta \) and \( \sigma \in P(G) \), then \( M \cap N \simeq S_4 \) and, since \( \sigma \) is index preserving, \( M^\sigma \cap N^\sigma = (M \cap N)^\sigma \) has order 24. By 7.8.6, \( M^\sigma \) and \( N^\sigma \) are conjugate. It follows that \( \Delta^\sigma = \Delta \) or \( \Delta^\sigma = \Gamma \), and hence \( |P(G) : L| \leq 2 \) if \( L = \{ \tau \in P(G) | \Delta^\tau = \Delta \} \). By 7.8.9, \( L \) operates faithfully on \( \Delta \) and so is isomorphic to a subgroup of \( S_6 \). On the other hand, \( S_6 \simeq PI(G) \leq L \) and hence \( L = PI(G) \simeq S_6 \). By 7.8.4, \( PI(G) < PA(G) \) and so, finally, \( PA(G) = P(G) \) and \( |P(G) : PI(G)| = 2 \).

(c) If \( \phi \) is a projectivity from \( G = S_n \) to a group \( \overline{G} \), then by 7.7.11, \( \overline{G} \cong G \). By (a) or (b), \( \phi \) is induced by an isomorphism \( \sigma \) which is unique, by 1.4.2 and 1.4.3. □
Note that by 1.4.3, $PA(S_n) \cong \text{Aut } S_n$; thus 7.8.10(a) implies that $\text{Aut } S_n \cong S_n$ for $n \neq 6$. It is well-known (see Huppert [1967], p. 199) that $A_6 \cong \text{PSL}(2,9)$. Therefore $S_6$ is a subgroup of index 2 of $\text{Aut } A_6 \cong \text{PGL}(2,9)$, and hence this group operates as a group of automorphisms on $S_6$. So 7.8.10(b) implies that $P(S_6) = PA(S_6) \cong \text{Aut } S_6 \cong \text{PGL}(2,9)$.

It is quite obvious that we could handle the alternating groups in the same way as the symmetric groups if we could prove the analogue of Lemma 7.8.9. However this is only possible for certain integers $n$.

**7.8.11 Lemma.** Let $n \geq 5$, $G = A_n$ and $\sigma \in P(G)$ such that $(G_i)^\sigma = G_i$ for all $i \in \Omega$. If $x \in G$ such that $o(x) = p'$ ($p \in \mathbb{P}$, $r \in \mathbb{N}$) and $(x)^\sigma \neq (x)$, then

(a) $p = 3$,
(b) $x$ fixes at most one point of $\Omega$,
(c) $x$ is a cycle (of length $3'$),
(d) $r$ is odd.

**Proof.** (a) We show first in several steps that most cyclic subgroups of $G$ are invariant under $\sigma$. So let $g \in G$.

(8) If $g$ is a 3-cycle, then $(g)^\sigma = (g)$.

Indeed, if $g = (i,j,k)$, then $(g)$ is the intersection of all the $G_i$ with $m \in \Omega \setminus \{i,j,k\}$.

(9) If $g^2 = 1$, then $(g)^\sigma = (g)$.

As in the proof of 7.8.9, we use induction on $v(g)$ to prove this. If $v(g) = 0$, then $g = 1$, while $v(g) = 2$ is impossible since $G = A_n$. So let $v(g) = 4$ and $g = (12)(34)$, say. Since $n \geq 5$, the subgroups $H = \bigcap_{i \geq 5} G_i$ and $K = \langle (125) \rangle$ are invariant under $\sigma$. Clearly, $H \cong A_5$ and $\langle (125), (12)(34) \rangle = N_H(K)$ is invariant under $\sigma$ since it is the unique subgroup of order 6 between $H$ and $K$. The same argument applies to the group $\langle (345), (12)(34) \rangle$, and it follows that $\sigma$ also fixes the intersection $\langle (12)(34) \rangle$ of these two groups. Now let $v(g) > 4$. Then the cycle decomposition of $g$ yields involutions $g_i \in G$ such that $4 \leq v(g_i) < v(g)$ and $g = g_1g_2 = g_2g_1$. By induction, $(g_i)^\sigma = (g_i)$ and hence $(g_1, g_2)^\sigma = (g_1, g_2)$; therefore the third subgroup $(g)$ of order 2 of the four-group $\langle g_1, g_2 \rangle$ is invariant under $\sigma$.

(10) If there exists an involution $s \in G$ such that $g^s = g^{-1}$, then $(g)^\sigma = (g)$.

Indeed, $(g, s)$ and all maximal subgroups of $(g, s)$ different from $(g)$ are generated by involutions; thus $\sigma$ fixes all these groups and hence also $(g)$.

(11) If $g^3 = 1$, then $(g)^\sigma = (g)$.

Again we use induction on $v(g)$ to prove this. By (8), (11) holds if $v(g) = 3$. If $v(g) = 6$, then $g = (123)(456)$, say, and $s = (12)(45) \in G$ satisfies $g^s = g^{-1}$; thus (10) implies that $(g)^\sigma = (g)$. Finally, if $v(g) > 6$, the cycle decomposition of $g$ yields elements $g_i \in G$ of order 3 with disjoint supports such that $g = g_1g_2g_3$. By induction, $(g_1)^\sigma = (g_1)$, $(g_2)^\sigma = (g_2)$, $(g_1, g_2, g_3)$ are invariant under $\sigma$. Since $(g_1, g_2, g_3)$ and $(g_1, g_2, g_3)$ are different elementary abelian groups of order 9 containing $g$, it follows that
Classes of groups and their projectivities

Let $k \geq 2$ and $g = g_1 \ldots g_m$ be the cycle decomposition of $g$. Since every cycle of even length is an odd permutation, $m$ is even. By 7.8.8 there exist involutions $s_i \in S_n$ operating on the points moved by $g_i$ such that $g_i^s = g_i^{-1}$; let $s = s_1 \ldots s_m$. If one of the $g_i$ is a transposition, then either $s \in G$ or $s g_i \in G$, and $g^s = g^{-1} = g^{s^m}$ since $g_i$ centralizes $g$; by (10), $\langle g \rangle^s = \langle g \rangle$. If none of the $g_i$ is a transposition, then $\nu(g_i) \equiv 0 \pmod{4}$ and hence, by (b) of 7.8.8, $s_i \not\in G$ for $i = 1, \ldots, m$. Since $m$ is even, it follows that $s \in G$ and $\langle g \rangle^s = \langle g \rangle$, again by (10).

(13) If $o(g) = p^k$ and $p > 3$, then $\langle g \rangle^s = \langle g \rangle$.

We use induction on $o(g)$ to prove this. So suppose that (13) holds for elements of smaller order than $g$ and let $r$ be an automorphism of order $p - 1$ of $\langle g \rangle$. By 7.8.8 there exists $t \in S_n$ such that $o(t) = p - 1$ and $g^t = g^{-1}$. Since $p > 3$ and $|S_n : G| = 2$, we have $\langle t \rangle \cap G \neq 1$; let $s \in \langle t \rangle \cap G$ be of prime order $q$, say. Then $\langle g, s \rangle$ and all maximal subgroups of $\langle g, s \rangle$ different from $\langle g \rangle$ are generated by subgroups of order $q$. By (9), (11), or induction, all these groups are invariant under $\sigma$ and then so is $\langle g \rangle$. This proves (13); clearly, (12) and (13) imply (a).

(b) If $g \in G$ fixes two points $i$ and $j$ of $\Omega$, and $s \in S_n$ is the involution satisfying $g^s = g^{-1}$ constructed in 7.8.8, then $s$ or $(i,j)s$ is an involution in $G$ inverting $g$. Thus (10) implies that $\langle g \rangle^s = \langle g \rangle$ and this proves (b).

(c) We show first that the cycle decomposition of $x$ contains at most two cycles. To see this, suppose that $g \in G$ such that $o(g) = 3^r$ and $g = g_1 g_2 g_3$ where the $g_i \neq 1$ have disjoint supports. Then $o(g)$ is the least common multiple of the $o(g_i)$ and so $3^r = o(g) = o(g_2) \geq o(g_i)$ ($i = 1, 3$), say. Let $S = \langle g_1 g_2 \rangle \cup \langle g_3 \rangle$ and $T = \langle g_1 \rangle \cup \langle g_2 g_3 \rangle$. If $y \in S \cap T$, then $y = (g_1 g_2)^i g_3^j = g_3^k (g_2 g_3)^m$ for $i, j, k, m \in \mathbb{N}$. Since the product of the $g_i$ is direct, it follows that $i \equiv m \pmod{3^r}$ and $g_1^i = g_3^k$. Thus $y = (g_1 g_2 g_3)^i \in \langle g \rangle$ and so $S \cap T = \langle g \rangle$. The 3-elements $g_1, g_3, g_1 g_2, g_2 g_3$ all have more than one fixed point on $\Omega$; therefore by (b), $\sigma$ fixes $S$ and $T$ and hence $\langle g \rangle$.

Now let $g = g_1 g_2$ with disjoint cycles $g_1$ of length $3^r$ and $g_2$ of length $3^k$. If $r = k$, the involutions $s_i$ inverting $g_i$ constructed in 7.8.8 are either both odd or both even; in any case, $s = s_1 s_2 \in G$ and by (10), $\langle g \rangle^s = \langle g \rangle$. So let $r > k$. Consider the semidirect product $H = N \langle b \rangle$ of an elementary abelian group $N = \langle a_1, \ldots, a_{3^{r-1}} \rangle$ of order $3^{3^{r-1}}$ and a cyclic group $\langle b \rangle$ of order $3^{r-1}$ with respect to the operation $a_i b = a_{i+1}$ (i = 1, ..., $3^{r-1} - 1$), $a_{3^{r-1}} b = a_1$ (note that $H \cong C_3 \wr C_3^{r-1}$; see (14) of § 7.6). Then $c = a_1 b$ satisfies $c^{3^{r-1}} = a_1 \ldots a_{3^{r-1}}$ and hence $o(c) = 3^r$. If $M$ is a complement to $\Omega(\langle c \rangle)$ in $N$, then $M \langle c \rangle = H$ and $M \cap \langle c \rangle = 1$; furthermore, $M_\Omega = 1$ since $Z(H) = \Omega(\langle c \rangle)$. Thus $H$ operates faithfully on the $3^r$ cosets of $M$ in $H$ and $c$ is a cycle of length $3^r$. Since all cycles of length $3^r$ in $S_n$ are conjugate, there exists a subgroup $S \cong C_3 \wr C_3^{r-1}$ of $G$ containing $g_1$ and having the same support as $g_1$. Let $A$ be the base group of $S$ and $T = A \langle g \rangle$. Then $S = A \langle g_1 \rangle$; and $T \cap \langle g_1, g_2 \rangle = \langle g \rangle (A \cap \langle g_1, g_2 \rangle) = \langle g \rangle$ since $A$ is elementary abelian and intersects $\langle g_2 \rangle$ trivially so that $A \cap \langle g_1, g_2 \rangle = \Omega(\langle g \rangle)$. Since $r > k$, we have $T \cap \langle g_2 \rangle = \langle g \rangle \cap \langle g_2 \rangle = 1$ and $T \langle g_2 \rangle = \langle A, g_1, g_2 \rangle = S \times \langle g_2 \rangle$. Thus $T$ is isomorphic to $S$ and hence is generated by elements of order at most $3^{r-1}$. Since $n \geq 3^r + 3^k$, every such element either

\[ \langle g \rangle = \langle g_1 \rangle \cup \langle g_2 g_3 \rangle \cap \langle g_1 g_2 \rangle \cup \langle g_3 \rangle \] is invariant under $\sigma$. 

(12) If $o(g) = 2^k$, then $\langle g \rangle^s = \langle g \rangle$. 

Since every cycle of even length is an odd permutation, $m$ is even. By 7.8.8 there exist involutions $s_i \in S_n$ operating on the points moved by $g_i$ such that $g_i^s = g_i^{-1}$; let $s = s_1 \ldots s_m$. If one of the $g_i$ is a transposition, then either $s \in G$ or $s g_i \in G$, and $g_i^s = g_i^{-1} = g_i^{s^m}$ since $g_i$ centralizes $g$; by (10), $\langle g \rangle^s = \langle g \rangle$. If none of the $g_i$ is a transposition, then $\nu(g_i) \equiv 0 \pmod{4}$ and hence, by (b) of 7.8.8, $s_i \not\in G$ for $i = 1, \ldots, m$. Since $m$ is even, it follows that $s \in G$ and $\langle g \rangle^s = \langle g \rangle$, again by (10).
has two fixed points on $\Omega$—as do $g_1$ and $g_2$—or has three cycles in its cycle decomposition. By (b) and the first part of the proof of (c), $\sigma$ fixes $T$ and $\langle g_1, g_2 \rangle$, and hence also $T \cap \langle g_1, g_2 \rangle = \langle g \rangle$. Thus $x$ is a cycle.

(d) If $r$ were even, then $3^r \equiv 1 \pmod{4}$ and hence by 7.8.8 there exists an involution $s \in G$ inverting the cycle $x$ of length $3^r$. By (10), $\langle x \rangle^e = \langle x \rangle$, a contradiction. Thus $r$ is odd.

7.8.12 Theorem (Schmidt [1977a]). If $n \geq 5$, $n \neq 6$ and not of the form $n = 3^r$ or $n = 3^r + 1$ where $r$ is odd, then $P(A_n) = P(A_6) \approx S_6$; furthermore $P(A_6) = P(A_6) \approx PGL(2, 9)$. Every projectivity of these alternating groups is induced by a unique isomorphism.

Proof. Let $G = A_n$ and $K = \{ \sigma \in P(G) | G^i = G_i \text{ for all } i \in \Omega \}$. If $K \neq 1$, there would exist $\sigma \in K$ and $x \in G$ of prime power order such that $\langle x \rangle^\sigma \neq \langle x \rangle$. By 7.8.11, $x$ would then be a cycle of length $3^r$, $r$ odd, with at most one fixed point, and it would follow that $n = 3^r$ or $n = 3^r + 1$, a contradiction. Thus $K = 1$ and by 7.8.7, $P(G)$ is isomorphic to a subgroup of $S_n$. On the other hand, $S_n$ is a subgroup of $\text{Aut } A_n$, and it follows that $P(G) = PA(G) \approx S_n$. The proofs of the other statements are similar to the corresponding proofs for $S_n$ in 7.8.10 and are left to the reader.

Using Sadovskii's Local Theorem, Corollary 1.3.7, we can extend the results of 7.8.10 and 7.8.12 to infinite sets.

7.8.13 Corollary. If $X$ is an infinite set, then the alternating group $\text{Alt } X$ and the group of finitary permutations $\text{Sym}(X, N_0)$ are strongly determined by their subgroup lattices.

Zacher [1977] has shown that for infinite $X$, every normal subgroup of $\text{Sym } X$ is strongly determined by its subgroup lattice; see Exercise 7.

We now treat the cases $n = 3^r$ and $n = 3^r + 1$, $r$ odd.

7.8.14 Lemma. Let $n = 3^r$ or $n = 3^r + 1$ ($r \geq 2$) and suppose that $X$ is a cyclic subgroup of order $3^r$ in $G = S_n$. If $X \leq H \leq G$, then $O_3(H) = 1$.

Proof. Suppose that the lemma is false and choose a minimal counterexample $H \leq G$; write $H_i$ for the stabilizer of the point $i \in \Omega$ in $H$. Then $H = QX$ where $Q \neq 1$ is a normal $3'$-subgroup of $H$. If $q$ is a prime dividing $|Q|$, then by 4.1.3 there exists an $X$-invariant Sylow $q$-subgroup of $Q$, and the minimality of $H$ implies that $Q$ is a $q$-group. If $n = 3^r$, then $X$ is transitive on $\Omega$ and hence so is $H$. Therefore $|H : H_i| = 3^r$ and so $q \leq H_i$ for all $i \in \Omega$. It follows that $Q = 1$, a contradiction. Thus $n = 3^r + 1$. If $H$ is not transitive on $\Omega$, then $H$ has orbits of lengths $3^r$ and 1 and, as above, $Q = 1$. So $H$ is transitive on $\Omega$ and then $3^r + 1 = n = q^m$ for some $m$ since $X$ is contained in the stabilizer $H_i$ of some point $i \in \Omega$. It follows that $q = 2$ and $m \leq 2$, since $3^r + 1 \equiv 2 \text{ or 4 (mod 8)}$. Thus $r \leq 1$, contradicting our assumption $r \geq 2$. \qed
7.8.15 Theorem. Let $n = 3^r$ or $n = 3^r + 1$, $r$ odd, $r \geq 3$ and let $G = A_n$. Then $PA(G)$ and $PI(G)$ are not normal in $P(G)$.

Proof. Let $x = (12 \ldots 3^r)$ be a cycle of length $3^r$ in $G$ and $X = \langle x \rangle$. If $y \in C_{S_n}(X)$ and $i^y = 1$, then $i^y = 1^{x^i y} = 1^{x^{x^i}} = i$ for all $i \in \{1, \ldots, 3^r\}$, and hence $y = 1$. Since $X \leq C_{S_n}(X)$, this shows that $C_{S_n}(X)$ operates regularly on $\{1, \ldots, 3^r\}$ and so has order $3^r$. Thus $C_{S_n}(X) = X$. Therefore $N_{S_n}(X)/X$ and $N_G(X)/X$ are isomorphic to subgroups of $Aut X$, and this group is cyclic of order $2 \cdot 3^{r-1}$ (see Huppert [1967], p. 84). By 7.8.8, $N_{S_n}(X)/X \cong Aut X$; since $r$ is odd, $3^r \equiv 3 \pmod{4}$ and therefore the involution $s$ satisfying $x^s = x^{-1}$ constructed in 7.8.8 is not contained in $G$. So $N_G(X)/X$ is cyclic of order $3^r - 1$. Let $H$ be the subgroup of order $3^r + 1$ between $X$ and $N_G(X)$. Then $X$ is a cyclic subgroup of index $3$ in $H$, and hence the structure of $H$ is well-known. By 2.3.4 and 2.3.5, for example, $H$ is an $M$-group and $|H : \Omega_{r-1}(H)| = 3$. So $H$ has $3$ cyclic subgroups of order $3^r$; let $\Lambda$ be the set of these cyclic maximal subgroups of $H$. Then we claim the following.

(14) If $Y \in \Lambda$ and $Y < M \leq G$, then $H \leq M$.

To prove this, suppose, for a contradiction, that $H \not\leq M$. If $Y = \langle y \rangle$, then $y$ is a cycle of length $3^r$ since $n \leq 3^r + 1$. So $Y$ is conjugate to $X$ in $S_n$ and hence $N_G(Y)/Y \cong N_G(X)/X$ is cyclic of order $3^{r-1}$. Thus $H$ is the unique subgroup of $N_G(Y)$ in which $Y$ is a maximal subgroup. Since $H \not\leq M$, it follows that $Y = N_M(Y)$ and hence $Y$ is a Sylow $3$-subgroup of $M$ contained in the centre of its normalizer. By a theorem of Burnside (see Robinson [1982], p. 280) there exists a normal $3$-complement $Q$ in $M$. By 7.8.14, $Q = 1$ and hence $Y = M$, a contradiction. Now we can construct auto-projectivities of $G$ which are not induced by automorphisms.

(15) If $\tau$ is a permutation of $\Lambda$, then $\sigma: L(G) \to L(G)$ defined by $Y^\sigma = Y^\tau$ for $Y \in \Lambda$ and $Y^\sigma = Y$ for $Y \not\in \Lambda$ is an autoprojectivity of $G$.

Of course, $\sigma$ is bijective. Let $U < V \leq G$. If $U$, $V \not\in \Lambda$, then $U^\sigma = U < V = V^\sigma$. If $V \in \Lambda$, then $U^\sigma = U \leq \Phi(V) = \Phi(H) < V^\sigma$; and if $U \in \Lambda$, then by (14), $H \leq V$ and hence $U^\sigma \leq H \leq V = V^\sigma$. Thus in all cases, $U < V$ implies that $U^\sigma < V^\sigma$. The same holds for $\sigma^{-1}$ and so $\sigma$ is a projectivity.

An automorphism $\alpha$ inducing this projectivity $\sigma$ has to fix every involution in $G$. Since $G$ is generated by involutions, it follows that $\alpha = 1$; but this is impossible if $\tau \neq 1$. Thus $\sigma$ is not induced by an automorphism and hence $P(G) \neq PA(G)$. But we can improve on this. Since $G$ is simple, there exists $g \in G$ such that $H^\iota \neq H$. Let $\pi$ be the autoprojectivity of $G$ induced by the inner automorphism induced by $g$; so $\pi \in PI(G)$. Then $X^{\pi^{-1} \iota} \not\leq \Lambda$ and hence $X^{\pi^{-1} \iota \pi^{-1} \sigma} = X^{\sigma^{-1} \iota \pi^{-1} \pi} = X^{\sigma^{-1}} \neq X$ if we choose $\tau \in Sym \Lambda$ such that $X^\iota \not\leq X$. Thus $\sigma^{-1} \pi^{-1} \sigma \pi \neq 1$. On the other hand, if $U \leq G$ such that $|U| = 2$, then $U^{\sigma^{-1} \pi^{-1} \sigma} = U^\pi \neq U$, since $\sigma$ fixes all subgroups of order $2$. So again an automorphism $\alpha$ of $G$ inducing the projectivity $\sigma^{-1} \pi^{-1} \sigma \pi$ would have to fix every involution in $G$ and would therefore be the identity, a contradiction. Thus $\sigma^{-1} \pi^{-1} \sigma \pi \not\in PA(G)$ and, since $\pi \in PI(G) \leq PA(G)$, this shows that $PI(G)$ and $PA(G)$ are not normal in $P(G)$.

The following theorem gives more information about the structure of $P(A_n)$ in the exceptional cases; the proof is left to the reader (see Exercises 4–6).
7.8 Finite simple and lattice-simple groups

7.8.16 Theorem (Schmidt [1977a]). Let \( n = 3^r \) or \( n = 3^r + 1 \), \( r \) odd, \( r \geq 3 \) and let \( G = A_n \). Write \( K = \{ \sigma \in P(G) | G_i^\sigma = G_i \text{ for all } i \in \Omega \} \), and let \( L \) be the set of all \( \sigma \in P(G) \) fixing every noncyclic subgroup of \( G \). Then \( K \) and \( L \) are normal subgroups of \( P(G) \) and

(a) \( P(G)/K \cong S_n \),
(b) \( K/L \) is isomorphic to a subgroup of a direct product of groups isomorphic to \( S_3 \) (it is not known whether \( K \neq L \)),
(c) \( L \) is the direct product of \( (3^r - 1)!/2 \cdot 3^r \) (if \( n = 3^r \)) or \( (3^r - 1)!(3^r + 1)/2 \cdot 3^r \) (if \( n = 3^r + 1 \)) groups isomorphic to \( S_3 \).

Simple groups of Lie type

A large number of simple Chevalley groups have been shown to be strongly determined by their subgroup lattices. This was done for the simple groups \( PSL(2, q) \) by Metelli [1968], [1969], and for \( PSL(3, 3) \) and the Suzuki groups in Metelli [1971]. For a Chevalley group \( G \) of rank at least 2, \( P(G) \) operates as a group of automorphisms on the building \( \Delta \) of \( G \), as was shown in the proof of Theorem 7.8.3; and if \( K \) is the kernel of this operation, it follows from Tits' theorem that \( P(G)/K \cong Aut G \). So it remains to study this kernel \( K \). It was proved by Völklein [1986a] that \( K = 1 \) for the groups of type \( B_1, C_1, D_2, 2 D_2, 3 D_4, G_2, F_4 \) if \( p > 3 \) and of type \( E_7, E_8 \) if \( p > 7 \). Similar results have been obtained by Costantini [1989b] for simple algebraic groups over the algebraic closure of the prime field \( GF(p) \). These groups are strongly determined by their subgroup lattices for all odd primes with the sole exception of the groups of type \( A_2 \). These groups are in fact also exceptional in the finite case. Völklein [1986a], [1986b] and Costantini [1990] show that the groups \( PSL(3, q) \) in general are not strongly determined by their subgroup lattices; \( PSL(3, 17) \) is the smallest example of this kind (see Costantini [1989a]).

Lattice-simple groups

A group \( G \) is called lattice-simple if for every subgroup \( H \) of \( G \) such that \( 1 < H < G \), there exists \( \sigma \in P(G) \) such that \( H^\sigma \neq H \); that is, \( G \) does not contain any nontrivial proper \( P(G) \)-invariant subgroup. Obvious examples of such groups are the direct products of isomorphic simple groups: these groups are even characteristically simple (see Robinson [1982], p. 84). In particular, every elementary abelian group and therefore, by 2.2.3, every \( P \)-group is lattice-simple. By 1.2.7, the subgroup lattice of a cyclic group of square-free order is a direct product of chains of length one, and hence such groups are lattice-simple. We now show that, conversely, every finite lattice-simple group is one of the examples mentioned above.

7.8.17 Theorem (Suzuki [1951a], Schmidt [1978]). The finite group \( G \) is lattice-simple if and only if it has one of the following properties.

(i) \( G \) is a \( P \)-group.
(ii) \( G \) is cyclic of square-free order.
(iii) \( G \) is a direct product of isomorphic (nonabelian) simple groups.
Proof. It remains to be shown that every finite lattice-simple group $G$ has one of the properties (i)–(iii). To see this, consider the set $\mathcal{M}$ of all modular subgroups of prime order in $G$ and let $L = \langle M | M \in \mathcal{M} \rangle$. Clearly, $L$ is $P(G)$-invariant and hence $L = G$ or $L = 1$.

Suppose first that $L = G$. If there exists $M \in \mathcal{M}$ which is not permutable in $G$, then by 5.1.9, $G = M^G \times K$ where $M^G$ is a $P$-group and $(|M^G|, |K|) = 1$. By 4.2.4, $M^G$ is $P(G)$-invariant. It follows that $G = M^G$ and (i) holds. So suppose that every $M \in \mathcal{M}$ is permutable in $G$. Then by 5.2.9, $L = \langle M^G | M \in \mathcal{M} \rangle$ is the product of nilpotent normal subgroups, and hence $G = L$ is nilpotent. Since $\Phi(G)$ is $P(G)$-invariant, $\Phi(G) = 1$. Therefore if $G$ is a $p$-group, (i) holds. If $G$ is not a $p$-group and $P$ is a nontrivial Sylow $p$-subgroup of $G$, there exists $\sigma \in P(G)$ such that $P^\sigma \neq P$. Since $P$ is the unique Sylow $p$-subgroup of $G$, it follows that $P^\sigma$ is not a $p$-group. But $P^\sigma$ is nilpotent and hence by 2.2.6, $P$ is cyclic. So $G$ is cyclic and of square-free order since $\Phi(G) = 1$. Thus (ii) holds.

Now suppose that $L = 1$, that is, $G$ has no modular subgroup of prime order. Let $N$ be a minimal normal subgroup of $G$. Then $N$ is not cyclic and hence by 5.4.4, $N^\sigma$ is a minimal normal subgroup of $G$ for every $\sigma \in P(G)$. Clearly, $M = \langle N^\sigma | \sigma \in P(G) \rangle$ is $P(G)$-invariant and hence $M = G$; it follows that $G = N \times N_{\sigma_1} \times \cdots \times N_{\sigma_r}$ for certain $\sigma_i \in P(G)$. As a minimal normal subgroup, $N$ is a direct product of isomorphic simple groups; since it is a direct factor of $G$, it follows that $N$ is simple. By 7.8.1, all the $N_{\sigma_i}$ are isomorphic to $N$ and so $G$ satisfies (iii). However, we need not use the classification of finite simple groups here; using the Feit-Thompson Theorem only, we can verify the assumptions of Theorem 7.7.7 for $N$ and $\sigma = \sigma_i (i = 1, \ldots, r)$ in place of $F$ and $\varphi$. Indeed, since $N$ is simple, $Z(N) = 1$ and $N$ is generated by involutions. Let $D$ be the set of all involutions in $N$, let $d, e \in D$ and $S = \langle d, e \rangle$. By 4.2.8, $\sigma$ is index preserving since $G$ is a direct product of simple groups. So 7.7.1 shows that $S^\sigma \simeq S$ and, clearly, $S^\sigma \leq N^\sigma \leq C_G(S)$. Thus $T = S^\sigma$ satisfies (20) of § 7.7. By Theorem 7.7.7, $N^\sigma \simeq N$ and $G$ satisfies (iii).

Exercises

1. (Schmidt [1977b]) Show that for $n \geq 2$, the group $G = PSp(2n, 3) = Sp(2n, 3)/Z(Sp(2n, 3))$ satisfies the assumptions of Theorem 7.7.5 if one takes $D = \{ \sigma Z(Sp(2n, 3)) | \sigma^2 = 1 \neq \sigma \in Sp(V) \}$ and $\Delta = \{ G_\alpha | \alpha \in \Omega \}$ in the notation of 7.8.2(b).

2. Let $G$ and $\overline{G}$ be nonabelian finite simple groups such that $PI(G) \leq P(G)$ and $PI(\overline{G}) \leq P(\overline{G})$. If $L(\overline{G}) \simeq L(G)$, show that $\overline{G} \simeq G$ (without using 7.8.1, of course).

In the next three exercises let $n = 3^r$ or $n = 3^r + 1$, $r$ odd, $r \geq 3$ and $G = A_n$.

3. Show that $C_{P(G)}(PI(G)) \neq 1$ (compare with the well-known result that $C_{Aut_X}(Inn X) = 1$ if $Z(X) = 1$).

4. Let $S \in Syl_3(G)$ and write $K(S)$ for the set of all $\sigma \in P(S)$ fixing every subgroup of exponent at most $3^{r-1}$ of $S$. Let $\sigma \in K(S)$ and $X \leq S$ such that $X^\sigma \neq X$.

(a) Show that $X$ is metacyclic of exponent $3^r$.

(b) If $X$ is not cyclic, show that there exist $K(S)$-invariant subgroups $U, V, W$ of $S$ such that $U < V < W, U < X < W$, and $|W/U| = 9$. 
5. If $H \leq G$ and $\sigma \in K$ (defined in 7.8.7) such that $H^\sigma \neq H$, show that $H$ is a meta-cyclic 3-group of exponent $3^r$.

6. Prove Theorem 7.8.16.

7. (Zacher [1977]) Let $X$ be an infinite set and $G$ a nontrivial normal subgroup of $\text{Sym} X$. Show that every projectivity of $G$ is induced by a unique isomorphism. (Hint: Consult Scott [1964], pp. 305–315 for the basic properties of $\text{Sym} X$. In particular, note that $G = \text{Alt} X$ or $G = \text{Sym}(X, A)$ for some infinite cardinal $A$ so that by 7.7.11, $G$ is determined by its subgroup lattice.)
Chapter 8

Dualities of subgroup lattices

We say that a group $G$ has a dual if there exists a duality from its subgroup lattice onto the subgroup lattice of a group $\bar{G}$, that is, a bijective map $\delta: L(G) \to L(\bar{G})$ such that for all $H, K \in L(G)$, $H \leq K$ if and only if $K^\delta \leq H^\delta$. Not every group has a dual, for instance the quaternion group has none, and it is an interesting problem to determine all groups with duals.

In 1939 Baer proved that every group with dual is a torsion group and that an abelian group has a dual if and only if it is a torsion group whose primary components are finite. In 1951 Suzuki determined the nilpotent and the finite soluble groups with duals. It turned out that the latter are precisely the projective images of finite abelian groups. In 1961 Zacher showed that every finite group with dual is soluble and determined the infinite soluble groups with duals. Again these are projective images of abelian groups; as torsion groups, they are locally finite. In 1971 Zacher proved conversely that every locally finite group with dual is soluble. Thus the structure of these groups is known and we present it in this chapter.

It should be mentioned that all these results will be proved using elementary methods, except the last one, that every locally finite group with dual is soluble. This proof uses the Feit-Thompson Theorem. Finally, the Tarski groups are examples of groups with duals which are not locally finite and the structure of an arbitrary group with dual is not known.

8.1 Abelian groups with duals

In this section we determine the abelian groups with duals and also give some general results on dualities between subgroup lattices. First of all, we have the following "dual" to Theorem 1.1.2.

8.1.1 Lemma. Let $\delta$ be a bijective map of a lattice $L$ to a lattice $\bar{L}$. Then the following properties are equivalent.

(a) For all $x, y \in L$, $x \leq y$ if and only if $x^\delta \geq y^\delta$.

(b) $(x \cap y)^\delta = x^\delta \cap y^\delta$ for all $x, y \in L$.

(c) $(x \cup y)^\delta = x^\delta \cap y^\delta$ for all $x, y \in L$.

Furthermore, if $\delta$ satisfies (a) and $S$ is a subset of $L$ such that $\bigcap S$ exists, then $\bigcup S^\delta$ exists and $(\bigcap S)^\delta = \bigcup S^\delta$; similarly $(\bigcup S)^\delta = \bigcap S^\delta$ if $\bigcup S$ exists.
A bijective map \( \delta: L \to \tilde{L} \) with one and therefore all of the properties (a)–(c) of 8.1.1 is called a \textit{duality} from \( L \) to \( \tilde{L} \). For brevity, if \( G \) and \( \tilde{G} \) are groups and \( \delta: L(G) \to L(\tilde{G}) \) is a duality, we also call \( \delta \) a duality from \( G \) onto \( \tilde{G} \); and we say that \( G \) has a dual if there exists a duality from \( G \) to some group \( \tilde{G} \). It is clear that not every group has a dual; for instance the quaternion group and a quasicyclic group have none, since a group \( G \) with a maximal subgroup containing every proper subgroup of \( G \) is cyclic. It is also not difficult to see that the infinite cyclic group has no dual. We prove a more general result.

### 8.1.2 Theorem (Baer [1939b]). If a group \( G \) has a dual, then \( G \) is a torsion group.

\textit{Proof.} Suppose, for a contradiction, that \( z \) is an element of infinite order in \( G \). Let \( Z = \langle z \rangle \) and \( Z_i = \langle z^{2^i} \rangle \) for \( i \in \mathbb{N} \). Then \( Z > Z_1 > Z_2 > \cdots \) is a descending chain of subgroups of \( G \) such that \( \bigcap_{i \in \mathbb{N}} Z_i = 1 \). By 8.1.1, \( Z^\delta < Z_1^\delta < Z_2^\delta < \cdots \) is an ascending chain of subgroups of \( \tilde{G} \) whose join is \( 1^\delta = \tilde{G} \). Consider the subgroup \( W = \langle z^{3^\delta} \rangle \) of \( Z \). Since \( Z \) covers \( W \), we see that \( Z^\delta \) is a maximal subgroup of \( W^\delta \) and therefore \( W^\delta = \langle Z^\delta, w \rangle \) for some \( w \in W^\delta \setminus Z^\delta \). Since \( \tilde{G} = \langle Z_i^\delta | i \in \mathbb{N} \rangle \) and the join of an ascending chain of subgroups is the set-theoretical union of these subgroups, there exists \( k \in \mathbb{N} \) such that \( w \in Z_k^\delta \). It follows that \( W^\delta = \langle Z^\delta, w \rangle \leq \langle Z^\delta, Z_k^\delta \rangle = Z_k^\delta \) and hence \( W \geq Z_k \). But \( z^{2^k} \not\in \langle z^{3^n} \rangle = W \), a contradiction. \( \square \)

**Finite abelian groups**

We want to show next that every finite abelian group \( A \) has a dual. For this we have to consider the character group of \( A \).

### 8.1.3 Lemma. Let \( A \) be a finite abelian group, written multiplicatively, and let \( A^* = \text{Hom}(A, \mathbb{C}^*) \) be the set of all homomorphisms from \( A \) into the multiplicative group \( \mathbb{C}^* \) of complex numbers. For \( \sigma, \tau \in A^* \), define \( \sigma \circ \tau \in A^* \) by \( x^{\sigma \circ \tau} = x^{\sigma \tau} (x \in A) \).

(a) Then \( (A^*, \circ) \) is a group isomorphic to \( A \); it is called the character group of \( A \).

(b) If \( 1 \neq x \in A \), there exists \( \sigma \in A^* \) such that \( x^\sigma \neq 1 \).

\textit{Proof.} (a) It is trivial to verify that \( (A^*, \circ) \) is an abelian group. As a finite abelian group, \( A = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle \) for certain \( a_i \in A \). Suppose that \( o(a_i) = n_i \) and let \( \epsilon_i \) be a primitive \( n_i \)-th root of unity in \( \mathbb{C} \). For every \( y = a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} \in A \), we define a map
Dualities of subgroup lattices

\[ \chi_y : A \to \mathbb{C}^* \text{ by} \]

\[ (a_1^{x_1} \cdots a_n^{x_n})^{x_Y} = e_1^{x_1y_1} \cdots e_n^{x_ny_n} \quad (x_i \in \mathbb{Z}). \]

The reader may easily verify that \( \chi_y \in A^* \) and that the map \( \chi : A \to A^* \) sending \( y \in A \) to \( \chi_y \) is a homomorphism. If \( \sigma \in A^* \), then \( (a_i^{\sigma})^{x_i} = (a_i^{\sigma}) = 1^\sigma = 1 \) for all \( i = 1, \ldots, n \). Therefore \( a_i^\sigma \) is an \( n_i \)-th root of unity in \( \mathbb{C} \) and there exists \( y_i \in \mathbb{Z} \) such that \( a_i^\sigma = e_i^{y_i} \).

It follows that

\[ (a_1^{x_1} \cdots a_n^{x_n})^{x_Y} = e_1^{x_1y_1} \cdots e_n^{x_ny_n} = (a_1^{x_1} \cdots a_n^{x_n})^{x_Y} \]

where \( y = a_1^{y_1} \cdots a_n^{y_n} \in A \). Thus \( \chi \) is surjective. And if \( z = a_1^{y_1} \cdots a_n^{y_n} \in \ker \chi \), then \( 1 = a_i^{y_i} = e_i^{y_i} \) for \( i = 1, \ldots, n \). Since \( e_i \) is a primitive \( n_i \)-th root of unity, it follows that \( n_i \) divides \( z_i \) and hence \( a_i^{y_i} = 1 \). Thus \( z = 1 \) and \( \chi \) is injective. So, finally, \( \chi \) is an isomorphism between \( A \) and \( A^* \).

\[ \begin{align*}
\chi & : A \to \mathbb{C}^* \\
\chi(y) & = a_1^{y_1} \cdots a_n^{y_n} \\
\chi & \text{ is a homomorphism} \end{align*} \]

(b) Let \( x = a_1^{x_1} \cdots a_n^{x_n} \). Then there exists \( i \in \{1, \ldots, n\} \) such that \( a_i^{x_i} \neq 1 \) and, since \( o(a_i) = o(e_i) \), it follows that \( \sigma = \chi_{a_i} \) satisfies \( x^\sigma = e_i^{y_i} \neq 1 \).

8.1.4 Theorem (Baer [1937]). A finite abelian group \( A \) is self-dual, that is, there exists a duality from \( A \) onto \( A \).

\[ X = \{ x \in A : x^\sigma = 1 \text{ for all } \sigma \in S \} \quad \text{and} \quad S^\top = \{ a \in A : a^\sigma = 1 \text{ for all } \sigma \in S \}. \]

Of course, \( X^\perp \) and \( S^\top \) are subgroups of \( A^* \) and \( A \), respectively, so that \( \perp : L(A) \to L(A^*) \) and \( \top : L(A^*) \to L(A) \) are well-defined maps. If \( x \in X \) and \( \sigma \in X^\perp \), then \( x^\sigma = 1 \). This shows that \( x \in (X^\perp)^\top \) and hence \( X \leq (X^\perp)^\top \). If \( z \in A \setminus X \), then \( zX \neq 1 \) in \( A/X \) and by (b) of 8.1.3 there exists \( \tau \in (A/X)^* \) such that \((zX)^\tau \neq 1\). So if \( x : A \to A/X \) is the natural epimorphism, then \( x = x(x^\tau) \) satisfies \( X = x^\tau = 1 = 1 \) for all \( x \in X \) and \( z^\tau = (zX)^\tau \neq 1 \). Thus \( x \in X^\perp \) and hence \( z \notin (X^\perp)^\top \). This shows that \((X^\perp)^\top = X \) and that \( \perp \) is injective; for, \( X_1^\perp = X_2^\perp \) implies \( X_1 = (X_1^\perp)^\top = (X_2^\perp)^\top = X_2 \). Since \( A \) and \( A^* \) are isomorphic, \( |L(A)| = |L(A^*)| \) and it follows that \( \perp \) is bijective. Clearly, \( X \leq Y \) if and only if \( X^\perp \geq Y^\perp \). Thus \( \perp \) is a duality from \( A \) onto \( A^* \). And if \( \rho \) is the projectivity induced by an isomorphism from \( A^* \) to \( A \), it is obvious that \( \delta = \perp \rho \) is a duality from \( A \) onto \( A \).

8.1.5 Lemma. (a) Suppose that \( L_0, \ldots, L_n \) are lattices and that for \( i = 1, \ldots, n \) the mapping \( \sigma_i : L_{i-1} \to L_i \) is a duality or an isomorphism. Then \( \rho = \sigma_1 \cdots \sigma_n \) is an isomor-
8.1 Abelian groups with duals

Let $G$ and $\bar{G}$ be groups and $\delta$ a duality from $G$ onto $\bar{G}$. If $\sigma \in P(G)$, then $\delta^{-1} \sigma \delta \in P(\bar{G})$; if $\tau \in P(\bar{G})$, then $\delta \tau \delta^{-1} \in P(G)$. In particular, if $x \in G$, then the map $\nu : L(G) \to L(\bar{G})$ given by $H^\nu = ((H^\delta)^\tau)^\delta$ for $H \leq G$ is an autoprojectivity of $\bar{G}$; similarly, for $u \in \bar{G}$, the map $\mu : L(G) \to L(G)$ given by $K^\mu = ((K^u)^\delta)^\delta$ for $K \leq G$ is an autoprojectivity of $G$. We call $\nu$ the autoprojectivity of $G$ induced by $x \in G$ (via $\delta$) and usually write $\nu = \delta^{-1} x \delta$; similarly, $\mu = \delta u \delta^{-1}$ is the autoprojectivity of $G$ induced by $u \in \bar{G}$ (via $\delta$).

Proof. (a) As a product of bijective maps, $\rho$ is bijective. Every duality among the $\sigma_i$ inverts the order relation. So it will finally be preserved if the number of dualities among the $\sigma_i$ is even, and it will be inverted if this number is odd.

(b) Application of (a) to $\delta^{-1} \sigma \delta$ and $\delta \tau \delta^{-1}$ yields the first statement of (b). Then if we apply this to the autoprojectivities of $G$ and $\bar{G}$ induced by the inner automorphisms given by $x$ and $u$, respectively, we get the second statement.

8.1.6 Lemma. Let $\delta$ be a duality from $G$ onto $\bar{G}$, $1 \leq H \leq K \leq G$ and suppose that $H \leq K$ and $K^\delta \leq H^\delta$. Then $\delta$ induces a duality from $K/H$ onto $H^\delta/K^\delta$. In particular, if $N \leq G$, then $\delta$ induces a duality from $G/N$ onto $N^\delta$.

Proof. Clearly, the restriction $\beta$ of $\delta$ to $[K/H]$ is a duality from $[K/H]$ onto $[H^\delta/K^\delta]$. If $\alpha : L(K/H) \to [K/H]$ and $\gamma : [H^\delta/K^\delta] \to L(H^\delta/K^\delta)$ are the natural isomorphisms, then by 8.1.5, $\alpha \beta \gamma$ is a duality from $K/H$ onto $H^\delta/K^\delta$ and $(X/H)^{\delta \gamma} = X^\delta/K^\delta$ for $H \leq X \leq K$. This proves the first statement of the lemma. If $H = N \subseteq G = K$, then $K^\delta = 1 \leq H^\delta$ and so $\delta$ induces a duality from $G/N$ onto $N^\delta$.

The following result is an important special case of the above situation.

8.1.7 Lemma. Let $\delta$ be a duality from $G$ onto $\bar{G}$ and let $X \leq G$. If $X$ is invariant under $P(G)$, then $X^\delta$ is invariant under $P(\bar{G})$ and $\delta$ induces dualities in $X$ and in $G/X$.

Proof. If $\tau \in P(\bar{G})$, then by 8.1.5, $\delta \tau \delta^{-1} \in P(G)$. Since $X$ is invariant under $P(G)$, we have $X = X^{\delta \tau \delta^{-1}}$ and then $X^\delta = (X^\delta)^\tau$. Thus $X^\delta$ is invariant under $P(\bar{G})$. In particular, $X \leq G$ and $X^\delta \leq \bar{G}$. By 8.1.6, $\delta$ induces dualities from $G/X$ onto $X^\delta$ and from $X$ onto $\bar{G}/X^\delta$.

We finally reduce our main problem to the study of groups with directly indecomposable subgroup lattices.

8.1.8 Lemma. Let $(G_A)_{A \in \Lambda}$ be a family of coprime torsion groups and let $G = \bigoplus_{A \in \Lambda} G_A$.

(a) If there exists a duality $\delta$ from $G$ onto a group $\bar{G}$, then $\bar{G} = \bigoplus_{A \in \Lambda} \bar{G}_A^\delta$ where $\bar{G}_A = \bigcup_{\mu \neq \delta} G_\mu$ and the $\bar{G}_A^\delta$ are coprime torsion groups. In particular, $\delta$ induces a duality from $G/G_A \cong G_\delta$ onto $\bar{G}_A^\delta$, that is, every $G_A$ has a dual.

(b) Conversely, if every $G_A$ is self-dual, then so is $G$.
Dualities of subgroup lattices

Proof. (a) By 8.1.1, \( \bigcup_{\lambda \in \Lambda} \hat{G}^\delta_\lambda = \left( \bigcap_{\lambda \in \Lambda} \hat{G}_\lambda \right)^\delta = 1^\delta = \bar{G} \) and \( \left( \bigcup_{\mu \neq \lambda} \hat{G}_\mu \right) \cap \hat{G}_\lambda^\delta = \left( \left( \bigcap_{\mu \neq \lambda} \hat{G}_\mu \right) \cup \hat{G}_\lambda \right)^\delta = (G_\lambda \cup \hat{G}_\lambda)^\delta = G^\delta = 1 \). Since \( G_\lambda \) and \( \hat{G}_\lambda \) are coprime and \( G = G_\lambda \times \hat{G}_\lambda \), it follows that \( \hat{G}_\lambda \) is the unique complement to \( G_\lambda \) in \( G \). If \( x \in G_\lambda^\delta \), then \( \delta x \delta^{-1} \) is an autoprojectivity of \( G \) fixing \( G_\lambda \) and hence also \( \hat{G}_\lambda \). It follows that \( (\hat{G}_\lambda^\delta)^\delta = \hat{G}_\lambda^\delta \). Thus \( \hat{G}_\lambda^\delta \subseteq \bar{G} \) and \( \bar{G} = \bigcup_{\lambda \in \Lambda} \hat{G}_\lambda^\delta \). If two of these groups, \( \hat{G}_\lambda^\delta \) and \( \hat{G}_\mu^\delta \), say, were to contain elements of the same prime order \( p \), there would exist a subgroup \( P \) of order \( p \) of \( G \) neither contained in \( G_\lambda^\delta \) nor in \( \hat{G}_\lambda^\delta \). But then \( P^\delta^{-1} \) would be a maximal subgroup of \( G \) neither containing \( G_\lambda \) nor \( \hat{G}_\lambda \) and this would contradict 1.6.4. Thus the \( \hat{G}_\lambda^\delta \) are coprime.

(b) Suppose that \( (L_\lambda)_{\lambda \in \Lambda} \) is a family of lattices, \( L = \bigcup_{\lambda \in \Lambda} L_\lambda \) and, for every \( \lambda \in \Lambda, \delta_\lambda \) is an autoduality of \( L_\lambda \). For \( f \in L \) define \( f^\delta \in L \) by \( f^\delta(\lambda) = f(\lambda)^{\delta_\lambda} (\lambda \in \Lambda) \). Since all the \( \delta_\lambda \) are bijective, so is \( \delta : L \to L \). Further \( f \leq g \) with \( f, g \in L \), if and only if \( f(\lambda) \leq g(\lambda) \) for all \( \lambda \in \Lambda; \) moreover this is the case if and only if \( f(\lambda)^{\delta_\lambda} \geq g(\lambda)^{\delta_\lambda} \) for all \( \lambda \in \Lambda \), that is, \( f^\delta \geq g^\delta \). Thus \( \delta \) is an autoduality of \( L \). Now by 1.6.4, \( L(G) \cong \bigcup_{\lambda \in \Lambda} L(G_\lambda) \). Since every \( L(G_\lambda) \) has an autoduality, so does \( \bigcup_{\lambda \in \Lambda} L(G_\lambda) \) and then also \( L(G) \).

We remark that part (a) of Lemma 8.1.8 follows from a more general property of dualities between lattices (see Exercise 2) together with 1.6.4 and 1.6.5. It is an open problem whether (b) holds under the weaker assumption that every \( G_\lambda \) has a dual.

Infinite abelian groups

By 8.1.8 we need only study abelian \( p \)-groups; the crucial case is handled by

8.1.9 Lemma. An infinite elementary abelian \( p \)-group has no dual.

Proof. Let \( P \) be an infinite elementary abelian \( p \)-group and let \( B = \{ a_\lambda | \lambda \in \Lambda \} \) be a basis of \( P \); write \( r = |\Lambda| \). Then \( P = \bigcup_{\lambda \in \Lambda} \langle a_\lambda \rangle \) and every element of \( P \) is a product of finitely many different elements of \( B^* = \{ a_\lambda^k | \lambda \in \Lambda, 0 \leq k \leq p - 1 \} \). Hence there exists an injective map from \( P \) into the set of finite subsets of \( B^* \) and it follows that \( |P| \leq |\mathbb{N}| |p| |B| = |B| = r \). In particular, \( P \) has at most \( r \) cyclic subgroups; on the other hand, \( P \) contains all the \( \langle a_\lambda \rangle (\lambda \in \Lambda) \) and therefore \( P \) has precisely \( r \) minimal subgroups. Every maximal subgroup \( M \) of \( P \) determines exactly \( p - 1 \) nontrivial homomorphisms of \( P \) into a cyclic group \( Z \) of order \( p \) having \( M \) as their kernel. Thus the number of maximal subgroups of \( P \) is \( |\text{Hom}(P, Z)| \). Since \( B \) is a basis of \( P \), every map from \( B \) into \( Z \) can be extended to a unique homomorphism from \( P \) to \( Z \). Therefore \( |\text{Hom}(P, Z)| = p^{|B|} = 2^r \) and we have shown that

(1) \( P \) has \( r \) minimal and \( 2^r \) maximal subgroups.

Now suppose that \( \delta \) is a duality from an elementary abelian \( p \)-group \( G \) onto a group \( \bar{G} \). If \( 1 \neq u \in \bar{G} \), then by 8.1.6, \( \delta \) induces a duality from \( G/\langle u \rangle^{\delta^{-1}} \) onto \( \langle u \rangle \). Thus
8.1 Abelian groups with duals

$G/\langle u \rangle^{\delta^{-1}}$ is an elementary abelian $p$-group with distributive subgroup lattice and hence is cyclic of order $p$. So

(2) every nontrivial element of $\overline{G}$ is of prime order.

Let $1 \neq v \in \overline{G}$ such that $\langle u \rangle \neq \langle v \rangle$ and put $W = \langle u \rangle^{\delta^{-1}} \cap \langle v \rangle^{\delta^{-1}}$. By (2), $\langle u \rangle^{\delta^{-1}}$ and $\langle v \rangle^{\delta^{-1}}$ are two different maximal subgroups of $G$, and hence $G/W$ is elementary abelian of order $p^2$. Again by 8.1.6, $\delta$ induces a duality from $G/W$ onto $W^\delta = \langle u, v \rangle$ and, since $G/W$ is self-dual, $\langle u, v \rangle$ is a projective image of $G/W$. By 2.2.5,

(3) $\langle u, v \rangle \in P(2, p)$ if $1 \neq u, v \in \overline{G}$ and $\langle u \rangle \neq \langle v \rangle$.

Let $H = \{x \in \overline{G} | o(x) \text{ is a power of } p\}$. If $x, y \in H$, then by (2), either $|\langle x, y \rangle|$ divides $p$ or $x \neq 1 \neq y$ and $\langle x \rangle \neq \langle y \rangle$. In this case, (3) implies that $\langle x, y \rangle$ is elementary abelian of order $p^2$ since a nonabelian group in $P(2, p)$ has only one subgroup of order $p$. In any case, we see that $o(x)$ divides $p$, $xy^{-1} \in H$ and $xy = yx$. Thus

(4) $H$ is an elementary abelian $p$-subgroup of $\overline{G}$.

Clearly, $H \leq \overline{G}$. By 8.1.6, $\delta$ induces a duality from $H^{\delta^{-1}}$ onto the $p'$-group $\overline{G}/H$, and (3) applied to this duality yields that $\overline{G}/H$ is cyclic of prime order.

Now suppose, for a contradiction, that $G$ is infinite. Then $H$ too is infinite and $\delta$ induces a duality $\delta_0$ from the infinite elementary abelian $p$-group $P = G/H^{\delta^{-1}}$ onto $H$. Let $r$ be the number of minimal subgroups of $P$. Then by (1), $P$ has $2^r$ maximal subgroups. These are mapped by $\delta_0$ onto the minimal subgroups of $H$. Therefore, again by (1), $H$ has $2^{2^r}$ maximal subgroups and these are mapped by $\delta_0^{-1}$ onto the minimal subgroups of $P$. It follows that $r = 2^{2^r}$, a contradiction.

It follows from 8.1.9 that every abelian $p$-group with dual is finite. Indeed, we prove a much more general result.

8.1.10 Lemma. Every locally finite $p$-group with dual is finite.

Proof. Let $G$ be a locally finite $p$-group and $\delta$ a duality from $G$ to some group $\overline{G}$. Since finite $p$-groups are nilpotent, $G$ is locally nilpotent. Therefore every maximal subgroup of $G$ is normal in $G$ (see Robinson [1982], p. 345) and hence $G/\Phi(G)$ is elementary abelian. By 8.1.6, $G/\Phi(G)$ has a dual and therefore is finite. Thus $G = H\Phi(G)$ for some finitely generated subgroup $H$ of $G$. Since $G$ is locally finite, $H$ is finite. If $H < G$, then $H^\delta > 1$ and by 8.1.2 there would exist a subgroup $M^\delta$ of prime order contained in $H^\delta$. Then $M$ would be a maximal subgroup of $G$ containing $H$ and it would follow that $G = H\Phi(G) \leq M$, a contradiction. Thus $G = H$ is finite.

We can now prove our final result on abelian groups with duals.

8.1.11 Theorem (Baer [1939b]). An abelian group $G$ has a dual if and only if $G$ is a torsion group and every primary component of $G$ is finite. In this case, $G$ is even self-dual and every dual of $G$ is lattice-isomorphic to $G$. 

Dualities of subgroup lattices

Proof. Suppose first that $G$ has a dual. Then by 8.1.2, $G$ is a torsion group and therefore is the direct product of its primary components. By 8.1.8, every such component has a dual and hence is finite, by 8.1.10. Conversely, let $G = \operatorname{Dr} G_p$ with finite abelian $p$-groups $G_p$. By 8.1.4, every $G_p$ is self-dual and then so is $G$, by 8.1.8. Now 8.1.5 shows that if $\delta$ is a duality from $G$ to a group $\bar{G}$ and $\vartheta$ is an autoduality of $G$, then $\vartheta \delta$ is a projectivity from $G$ to $\bar{G}$.

Exercises

1. (Baer [1937]) In the notation of the proof to Theorem 8.1.4, show that for every $X < A$, $X = A*/X \cong A/X^\delta$ and $A/X \cong X^\delta$.

2. Let $(L_\lambda)_{\lambda \in \Lambda}$ be a family of complete lattices; write $I_\lambda$, $O_\lambda$ for the greatest and least elements of $L_\lambda$, respectively. Let $L = \operatorname{Dr} L_\lambda$ and, for all $\lambda \in \Lambda$, define $g_\lambda \in L$ by $g_\lambda(\mu) = I_\mu$ for $\mu \neq \lambda$ and $g_\lambda(\lambda) = O_\lambda$. If $\delta$ is a duality from $L$ onto a lattice $\bar{L}$, and $O$ is the least element of $\bar{L}$, show that the map $\varphi$ sending every $x \in L$ to the function $x^\varphi$ defined by $x^\varphi(\lambda) = x \cap g_\lambda^\delta (\lambda \in \Lambda)$ is an isomorphism from $L$ onto $\operatorname{Dr} [g_\lambda^\delta/O]$.

8.2 The main theorem

By 8.1.5, every projective image of a group with dual has a dual. Therefore the results of §8.1 and Chapter 2 yield that the following groups have duals.

8.2.1 Theorem. Let $G = \operatorname{Dr} G_\lambda$ with finite coprime groups $G_\lambda$, and suppose that every $G_\lambda$ either is a $P$-group or a nonhamiltonian $p$-group with modular subgroup lattice. Then $G$ is self-dual.

Proof. By 2.2.3 or 2.5.9, $G_\lambda$ is lattice-isomorphic to a finite abelian group. By 8.1.4, every $G_\lambda$ is self-dual and then so is $G$, by 8.1.8.

The aim of this chapter is to prove that, conversely, every locally finite group $G$ with dual has the above structure. We state this result in a form which also describes the image of $G$ under the duality.

8.2.2 Main Theorem (Suzuki, Zacher). Let $G$ be a locally finite group and $\delta$ a duality from $G$ to a group $\bar{G}$. Then there exist subgroups $G_\lambda$ of $G$ with the following properties.

(a) $G = \operatorname{Dr} G_\lambda$ and the $G_\lambda$ are coprime.

(b) $\bar{G} = \bigoplus_{\lambda \in \Lambda} G_\lambda$ where $\bar{G}_\lambda = \bigcup_{\mu \neq \lambda} G_\mu$ and the $\bar{G}_\lambda$ are coprime.

(c) For every $\lambda \in \Lambda$, there are primes $p$, $q$ (not necessarily distinct) such that
8.2 The main theorem

(1) \( G_x \) is a cyclic \( p \)-group, \( \hat{G}_x^q \) is a cyclic \( q \)-group; or

(2) \( G_x \) and \( \hat{G}_x^q \) are in \( P(n, p) \) for some \( n \in \mathbb{N} \); or

(3) \( G_x \) and \( \hat{G}_x^q \) are finite nonhamiltonian \( p \)-groups with modular subgroup lattices.

As mentioned in the introduction of this chapter, Suzuki [1951a] proved this theorem for finite soluble groups and Zacher [1961a] extended it to arbitrary soluble groups; later Zacher [1961b], [1966], [1971] showed that, respectively, every finite, locally soluble, and, finally, locally finite group with dual is soluble. We shall prove directly in § 8.3 that an arbitrary soluble group with dual has the structure given in 8.2.2, and then in §§ 8.4 and 8.5 we shall study finite and locally finite groups. In addition, we shall prove in § 8.5 the following result on arbitrary groups with dual. Recall that \( G^L \) is the largest locally finite normal subgroup of the group \( G \); let \( G^\delta \) (respectively \( G^\circ \)) be the join of all finite (respectively soluble) normal subgroups of \( G \) and write \( G^\delta \) (respectively \( G^\circ \)) for the intersection of all subgroups of finite index (respectively normal subgroups with soluble factor group) of \( G \).

8.2.3 Theorem (Stonehewer and Zacher [1994]). Let \( \delta \) be a duality from the group \( G \) to the group \( \hat{G} \). Then

(a) \( G'' = G^\delta = G^\circ \) is a perfect group and has no proper subgroup of finite index,

(b) \( G^{L\delta} = G^\delta = G^\circ \),

(c) \( (G'')^\delta = \overline{G^\delta} \) and \( (G^\circ)^\delta = \overline{G''} \),

(d) \( Z(G'') = G'' \cap G^\delta \) and hence \( G''G^\delta/Z(G'') = G''/Z(G'') \times G^\delta/Z(G'') \), and

(e) \( G''/Z(G'') \) and \( G^\delta/Z(G'') \) are coprime.

It follows from 8.1.6 that \( \delta \) induces dualities from \( G/G'' \) onto \( \overline{G^\delta} \) and from \( G^\delta \) onto \( \overline{G/G''} \), so that these groups have the structure given in 8.2.2. Furthermore \( \delta \) induces a duality between the perfect groups \( G''/Z(G'') \) and \( \overline{G''G^\delta/G^\delta} \simeq \overline{G''/Z(G'')} \). The structure of these groups is not known: every Tarski group is self-dual and, using a theorem of Obraztsov [1990], it is easy to construct many other infinite simple groups with duals.

Consequences of the main theorem

In the remainder of this section we give some corollaries to the Main Theorem and handle some special cases. These corollaries will follow once 8.2.2 has been proved, but of course they will also hold in the inductive situations of this proof for dualities which are not counterexamples and therefore satisfy 8.2.2.

First of all, if we are only interested in the structure of a group with dual, we have the following more elegant version of the statements in 8.2.1 and 8.2.2.

8.2.4 Theorem. The locally finite group \( G \) has a dual if and only if \( G \) is a direct product of finite coprime groups \( G_x \) such that every \( G_x \) is either a \( P \)-group or a non-hamiltonian \( p \)-group with modular subgroup lattice.
By 2.4.5, every finite group with modular subgroup lattice is metabelian. Therefore all the $G_\lambda$ in 8.2.4 are metabelian and then so is $G$. By 2.2.3 and 2.5.9, every $G_\lambda$ is lattice-isomorphic to an abelian $p$-group where $p$ is a prime dividing $|G_\lambda|$. Thus these abelian groups are coprime and, by 1.6.4, their direct product is lattice-isomorphic to $G$. Using 8.1.11, we get the following result.

**8.2.5 Corollary.** Every locally finite group $G$ with dual is metabelian and lattice-isomorphic to an abelian group. Thus $G$ is self-dual and every dual of $G$ is lattice-isomorphic to $G$.

Finally, every $G_\lambda$ is supersoluble and a nonnormal Sylow subgroup of $G_\lambda$ has prime order. So we get the following result.

**8.2.6 Corollary.** Let $G$ be a finite group with dual. Then $G$ is supersoluble and every nonnormal Sylow subgroup of $G$ has prime order.

---

### Special cases

In the remainder of this section let $G$ be a group and $\delta$ a duality from $G$ to a group $\overline{G}$. We start with the proof of the Main Theorem and handle some special cases.

**8.2.7 Lemma.** If $G$ is abelian, $\delta$ satisfies 8.2.2.

*Proof.* By 8.1.11, $G = \bigcup_{\lambda \in \Lambda} G_\lambda$ with finite $p$-groups $G_\lambda$. By 8.1.8, $\overline{G} = \bigcup_{\lambda \in \Lambda} \overline{G_\lambda}$ where $\overline{G_\lambda} = \bigcup_{\mu \in \Lambda} G_\mu$, the images $\overline{G_\lambda}$ are coprime torsion groups, and $\delta$ induces a duality from $G/\overline{G} \simeq G_\lambda$ onto $\overline{G_\lambda}$; again by 8.1.11, $\overline{G_\lambda}$ is lattice-isomorphic to $G_\lambda$. So (a) and (b) of 8.2.2 hold and, by 2.2.6, (1) or (2) is satisfied, or $|\overline{G_\lambda}| = |G_\lambda|$. In this case, $G_\lambda$ and $\overline{G_\lambda}$ clearly are nonhamiltonian $p$-groups with modular subgroup lattices for some prime $p$. Thus $\delta$ satisfies 8.2.2. □

**8.2.8 Lemma.** If $G$ is a $P$-group, then $G$ and $\overline{G}$ lie in $P(n, p)$ for some $n \in \mathbb{N}$, $p \in \mathbb{P}$.

*Proof.* By 2.2.3 there exists a projectivity $\varphi$ from $G$ to an elementary abelian group $G^*$. Then $\varphi^{-1} \delta$ is a duality from $G^*$ to $\overline{G}$ and, by 8.1.9, $G^*$ is finite. Thus $G^* \in P(n, p)$ for some $n \in \mathbb{N}$, $p \in \mathbb{P}$. By 8.1.11, $\overline{G}$ is lattice-isomorphic to $G^*$; by 2.2.5, $G$ and $\overline{G}$ lie in $P(n, p)$. □

**8.2.9 Lemma.** If $G$ is a locally finite $p$-group, $\delta$ satisfies 8.2.2.

*Proof.* By 8.1.10, $G$ is finite and we use induction on $|G|$ to show that $\delta$ has the required properties. By 8.2.7, we may assume that $G$ is not abelian; in particular, $G$ is neither elementary abelian nor cyclic and hence

1. $\Phi(G) \neq 1$, $|G : \Phi(G)| = p^m$, $m \geq 2$.  

(4) $\Phi(G) \neq 1$, $|G : \Phi(G)| = p^m$, $m \geq 2$.  

(4) $\Phi(G) \neq 1$, $|G : \Phi(G)| = p^m$, $m \geq 2$.
By 8.1.6, \( \delta \) induces a duality from \( G/\Phi(G) \) onto \( \Phi(G)^{\delta} \) and 8.2.8 shows that \( \Phi(G)^{\delta} \in P(m, p) \). Suppose, for a contradiction, that \( \Phi(G)^{\delta} \) is not a \( p \)-group. Then \( \Phi(G)^{\delta} \) is a nonabelian \( P \)-group of order \( p^{m-1}q \), \( p > q \in \mathbb{P} \). If \( |\Phi(G)| > p \), there exists a minimal normal subgroup \( N \) of \( G \) such that \( 1 < N < \Phi(G) \). Since \( G/N \) is neither cyclic nor elementary abelian, the induction assumption implies that \( G/N \) and \( N^{\delta} \) are \( p \)-groups; but \( \Phi(G)^{\delta} \leq N^{\delta} \) is not a \( p \)-group, a contradiction. Thus \( |\Phi(G)| = p \) and \( |G| = p^{m+1} \).

By 8.1.7, \( \Phi(G)^{\delta} \leq \overline{G} \). Let \( P \) be the Sylow \( p \)-subgroup of \( \Phi(G)^{\delta} \). Then \( P \) is characteristic in \( \Phi(G)^{\delta} \) and hence normal in \( \overline{G} \); let \( M^{\delta} \) be a minimal normal subgroup of \( \overline{G} \) contained in \( P \). Since \( L(G) \) satisfies the Jordan-Dedekind chain condition, so does \( L(\overline{G}) \) and hence, by 5.3.9, \( \overline{G} \) is supersoluble. Thus \( |M^{\delta}| = p \) and \( |M| = p^{m} \). By 8.1.6, \( \delta \) induces a duality from \( M \) onto \( \overline{G}/M^{\delta} \) which, by induction, satisfies 8.2.2. Since \( \Phi(G)^{\delta}/M^{\delta} \) is a normal subgroup of order \( p^{m-2}q \) of \( \overline{G}/M^{\delta} \), the group \( \overline{G}/M^{\delta} \) is not a \( p \)-group, nor does it lie in \( P(m, p) \). Thus \( M \) and \( \overline{G}/M^{\delta} \) are cyclic of prime power order. This implies that \( m = 2 \) so that \( |G| = p^{3} \) and \( |\overline{G}| = pq^{2} \).

The Sylow \( q \)-subgroups of \( \overline{G} \) are cyclic and intersect trivially since \( \Phi(G)^{\delta} \) contains nonnormal subgroups of order \( q \). Thus \( \Phi(\overline{G}) = 1 \) and hence \( G \) is generated by minimal subgroups. Since \( p > q \geq 2 \), it follows that \( G \) has exponent \( p \); but \( M \) is cyclic of order \( p^{2} \). This contradiction shows that

\[
(5) \quad \Phi(G)^{\delta} \text{ is a } \alpha \text{-group.}
\]

It follows that every minimal subgroup of \( \overline{G} \) has order \( p \), and Sylow's theorem implies that \( \overline{G} \) is a \( p \)-group. By 2.1.8, \( L(\overline{G}) \) is lower semimodular and so its image \( L(G) \) under the duality \( \delta^{-1} \) is upper semimodular. Thus \( L(G) \) is lower and upper semimodular and hence modular, by 2.1.10. If \( G \) were hamiltonian, then by 2.3.12, \( G = Q \times A \) where \( Q \approx Q_{8} \) and \( \delta \) induces a duality from \( G/A \approx Q_{8} \) onto \( A^{\delta} \). Then \( A^{\delta} \) has only one maximal subgroup, hence is cyclic, and \( L(A^{\delta}) \) is a chain; but this is not the case. Thus \( G \) is a nonhamiltonian \( p \)-group with modular subgroup lattice. The same is true for \( \overline{G} \), so (3) holds and \( \delta \) satisfies 8.2.2.

Finally, we have the following rather obvious general remark.

**8.2.10 Lemma.** Let \( G = A \times B \) with coprime groups \( A \) and \( B \). If \( \delta \) induces dualities in \( G/A \) and in \( G/B \) which satisfy 8.2.2, then \( \delta \) satisfies 8.2.2.

**Proof.** By 8.1.8, \( \overline{G} = A^{\delta} \times B^{\delta} \) where \( A^{\delta} \) and \( B^{\delta} \) are coprime. By assumption, \( G/A \approx B \) and \( A^{\delta} \) are direct products of groups satisfying (1), (2), or (3). The same holds for \( G/B \approx A \) and \( B^{\delta} \) and then also for \( G = A \times B \) and \( \overline{G} = A^{\delta} \times B^{\delta} \).

**Exercises**

1. (Suzuki [1951a]) Show that a nilpotent group \( G \) has a dual if and only if \( G \) is a torsion group and every primary component of \( G \) is a finite \( M^{*} \)-group.
8.3 Soluble groups with duals

The aim of this section is to prove the following special case of our Main Theorem.

8.3.1 Theorem (Suzuki [1951a], Zacher [1961a]). Every duality $\delta$ of a soluble group $G$ to a group $\bar{G}$ satisfies 8.2.2.

To prove this we suppose the theorem is false and choose a "minimal counter-example" in the following way: if there exists a finite soluble group with a duality violating 8.2.2, we take a group $G$ of minimal order with this property; and if there is no such finite group, we take a counterexample $G$ with minimal derived length $d(G)$. In both cases, we study a duality $\delta$ from $G$ to a group $\bar{G}$ for which 8.2.2 does not hold. Then $\delta$ has the following properties:

1. $\delta$ does not satisfy 8.2.2,
2. if $G$ is finite, every duality $\vartheta$ of a finite soluble group $X$ such that $|X| < |G|$ satisfies 8.2.2, and
3. if $G$ is infinite, every duality $\vartheta$ of a soluble group $X$ such that $|X|$ is finite or $d(X) < d(G)$ satisfies 8.2.2.

Throughout this section we assume that $\delta: L(G) \to L(\bar{G})$ is such a minimal counter-example; let $d(G) = n$. The special cases settled in § 8.2 yield the following results.

8.3.2 Lemma. $G$ is a nonabelian locally finite group. If $G$ is finite, $L(G)$ is directly indecomposable.

Proof. By 8.1.2, $G$ is a soluble torsion group and hence locally finite (see Robinson [1982], p. 147). By 8.2.7, $G$ is not abelian. Suppose, for a contradiction, that $G$ is finite and $L(G)$ is directly decomposable. Then by 1.6.5, $G = A \times B$ where $A \neq 1 \neq B$ and $(|A|, |B|) = 1$. By (2), the dualities induced by $\delta$ in $G/A$ and $G/B$ satisfy 8.2.2 and hence so does $\delta$, by 8.2.10. But this contradicts (1). Thus $L(G)$ is directly indecomposable.

We prove another general remark.

8.3.3 Lemma. If $G$ is finite, $G$ is supersoluble.

Proof. Suppose, for a contradiction, that $G$ is not supersoluble. If $N$ is a minimal normal subgroup of $G$, then by 8.1.6, $\delta$ induces a duality in $G/N$. By (2), this duality satisfies 8.2.2 and hence, by 8.2.6, $G/N$ is supersoluble. Since $G$ is not supersoluble, it follows that $N$ is the unique minimal normal subgroup of $G$, $N$ is not cyclic and, by Huppert's theorem (see Robinson [1982], p. 268), $N \not\leq \Phi(G)$. Since $N$ is not cyclic, 5.4.4 implies that $N^\sigma$ is a minimal normal subgroup of $G$ for every $\sigma \in P(G)$. Thus $N^\sigma = N$ for every $\sigma \in P(G)$ and, by 8.1.7, $N^\delta \leq \bar{G}$. Since $N \not\leq \Phi(G)$, there exists a maximal subgroup $M$ of $G$ such that $N \not\leq M$. Then $N \cap M \leq NM = G$ and hence $N \cap M = 1$. Therefore $\bar{G} = N^\delta \cup M^\delta = N^\delta M^\delta$ and, since $M^\delta$ is a minimal subgroup
of $\bar{G}$, it follows that $N^\delta$ has prime index in $\bar{G}$. Thus $N$ is cyclic of prime order, a contradiction.

Since $d(G) = n$, we have $G^{(n)} = 1$ and $G^{(n-1)} \neq 1$. Consider first the case that $G^{(n-1)}$ is a $p$-group for some prime $p$.

**8.3.4 Lemma.** If $G^{(n-1)}$ is a $p$-group, every autoprojectivity of $G$ is regular at $p$.

**Proof.** Suppose that this is false. Then there exist $\sigma \in P(G)$ and $a \in G$ such that $|\langle a \rangle| = p$ and $|\langle a \rangle^\sigma| \neq p$. Since $G^{(n-1)} = (G^{(n-2)})'$, there exist $x, y \in G^{(n-2)}$ such that $[x, y] \neq 1$. Let $H$ be a finite subgroup of $G$ containing $a, x, y$. Then $\sigma$ induces a projectivity from $H$ onto $H^\sigma$ which is singular at $p$ since $a \in H$. If $\sigma$ satisfies (b) of 4.2.6, $H$ contains a normal $p$-complement $N$ with abelian factor group. Thus $[x, y] \in H' \leq N$ and so $[x, y] \in N \cap G^{(n-1)} = 1$, since $N$ is a $p'$-group and $G^{(n-1)}$ is a $p$-group. This contradiction shows that (a) of 4.2.6 holds, that is, $H = S \times T$ where $S$ is a $p$-group containing a Sylow $p$-subgroup of $H$ and $|S|, |T| = 1$. Since $1 \neq [x, y] \in H \cap G^{(n)}$, $H \cap G^{(n)}$ is a nontrivial normal $p$-subgroup of $H$ and hence $p$ is the larger prime dividing $|S|$. Thus

$$(4) \quad H = S \times T, \quad |S|, |T| = 1, \quad S \in P(m, p) \text{ for some } m \in \mathbb{N}.$$ 

In particular, since $G$ is locally finite, this holds for $H = \langle a, x, y \rangle$. Let $\langle a, x, y \rangle = S_0 \times T_0$ where $|S_0| = p^k q$, $p > q$, and let $b \in S_0$ such that $o(b) = q$ and $a^b = a^r (r \in \mathbb{Z})$; note that $o(a) = p$ and hence $\langle a \rangle \leq S_0$. Now let $P$ be the set of all $p$-elements and $K$ the set of all $\{p, q\}$-elements of $G$, and let $w$ be an arbitrary $q$-element. For $c, d \in P$ and $u, v \in K$, consider $H = \langle a, x, y, c, d, u, v, w \rangle$. Since $G$ is locally finite, $H$ is a finite subgroup of $G$ and hence $H = S \times T$ as in (4). It follows that $a, c, d \in S$ and $cd^{-1} \in P$, $cd = dc$, and $o(c) \leq p$; thus $P$ is an elementary abelian $p$-group. Furthermore, $a \in S$ implies $b \not\in C_p(S)$; therefore $q$ is the smaller prime dividing $|S|$ and $b \in S$. Thus $c^b = c^r$ and, since $c$ was an arbitrary element of $P$, this shows that $P \langle b \rangle$ is a $P$-group. Also $w \in S \leq P \langle b \rangle$, which implies that $P \langle b \rangle$ is the set of all $\{p, q\}$-elements of $G$. Finally, $u, v \in T$ and so $uw^{-1} \in T \subseteq K$; hence the set $K$ of all $\{p, q\}$-elements is a subgroup of $G$. It follows that $G = P \langle b \rangle \times K$.

By 8.1.6, $\delta$ induces dualities $\delta_1$ in $G/K \simeq P \langle b \rangle$ and $\delta_2$ in $G/P \langle b \rangle$. By 8.2.8, $G/K$ is finite and $\delta_1$ satisfies 8.2.2. Since $G^{(n-1)} \leq P$, we have $d(G/P \langle b \rangle) < n$ and so (2) or (3) implies that $\delta_2$ satisfies 8.2.2. But then by 8.2.10, $\delta$ also satisfies 8.2.2, a contradiction.

**8.3.5 Lemma.** If $G^{(n-1)}$ is a $p$-group and $P \in \text{Syl}_p(G)$, then $P \trianglelefteq G$ and $G$ is finite.

**Proof.** Suppose, for a contradiction, that $P$ is not normal in $G$. By (2) or (3), $G/G^{(n-1)}$ has the structure given in 8.2.2 and, since $P/G^{(n)}$ is a nonnormal Sylow $p$-subgroup of $G/G^{(n-1)}$, it follows that $G/G^{(n-1)} = S/G^{(n-1)} \times T/G^{(n-1)}$ where $S/G^{(n-1)}$ and $T/G^{(n-1)}$ are coprime and $S/G^{(n-1)}$ is a $P$-group of order $r^m p$, $r > p$. Then $G^{(n)}$ is the intersection and $S$ the join of all the Sylow $p$-subgroups of $G$. If $\sigma \in P(G)$, then by 8.3.4, $\sigma$ and $\sigma^{-1}$ are regular at $p$ and hence $\sigma$ maps Sylow $p$-subgroups of $G$ to Sylow $p$-subgroups. Thus $G^{(n-1)}$ and $S$ are invariant under $P(G)$ and therefore, by 8.1.7, $\delta$
induces dualities $\delta_1$ in $G^{(n-1)}$ and $\delta_2$ in $S$. By 8.1.10, $G^{(n-1)}$ is finite and so $S$ is a finite \{p, r\}-group with indecomposable subgroup lattice. If $S < G$, then by (2) or (3), $\delta_2$ satisfies 8.2.2 and hence $S$ is a $P$-group. But $G^{(n-1)}$ is a normal $p$-subgroup of $S$ and since $p < r$, it follows that $G^{(n-1)} = 1$, a contradiction. Thus $G = S$ is a finite \{p, r\}-group. By 8.3.3, $G$ is supersoluble and, since $r > p$, $G \leq G$ if $R \in Syl_r(G)$ (see Robinson [1982], p. 145). By 8.3.2, $n \geq 2$ and therefore $G' \geq G^{(n-1)}$. Since $G/G^{(n-1)}$ is a $P$-group of order $r^mp$, it follows that $G' = R \times G^{(n-1)}$ is abelian and hence $1 = G' < G^{(n-1)} < G'$. This contradiction shows that

(5) $P \leq G$.

Again by 8.3.4, 8.1.7 and 8.1.10, $P$ is invariant under $P(G)$; therefore it has a dual and so is finite. Suppose, for a contradiction, that $G$ is not finite. Then $G/P$ is infinite and $G^{(n-1)} \leq P$. By (3), $G/P$ is an infinite direct product of finite coprime groups satisfying (1)–(3) of 8.2.2. If there exists a prime $q \neq p$ and a $q$-element $x \in C_G(P)$, then let $K$ be the set of all \{p, q\}-elements and $y$ be any $q$-element of $G$: if there is no such prime, let $K$ be the set of $p'$-elements in $G$ and put $x = 1 = y$. In any case, if $u, v \in K$, there exists a finite join $H/P$ of components of the above decomposition of $G/P$ such that $u, v, x, y \in H$. Since $H^p$ is characteristic in $P^p \leq G$, we obtain $H^p \leq G$ and hence $\delta$ induces a duality in the finite subgroup $H$ of $G$. By (3), this duality satisfies 8.2.2 and it follows that $H = Q \times L$ where $Q = \langle P, x \rangle$ and $L$ are coprime, and $Q$ is a $P$-group if $x \neq 1$. Thus $u^{-1} v L \leq K$ and hence $K$ is a subgroup of $G$. Now if $x \neq 1$, then $Q$ contains $y$ and hence is the set of \{p, q\}-elements of $G$; thus $G = Q \times K$. If $x = 1$, then $P = Q$ and $G = P \times K = Q \times K$ in this case too. By (3), the dualities induced by $\delta$ in the finite subgroup $H$ of $G$. By 8.3.6 Lemma. $G^{(n-1)}$ is not a $p$-group.

$G^{(n-1)}$ is not a $p$-group.

\textbf{Proof.} Suppose that $G^{(n-1)}$ is a $p$-group. Then by 8.3.5, $G$ is finite and has a normal Sylow $p$-subgroup $P$. By 8.3.4, $P$ is invariant under $P(G)$ and so by 8.1.7, $P^G \leq G$. Finally, by 8.2.9, $G$ is not a $p$-group. Thus

(6) $P \leq G$, $P^G \leq G$, $P \neq G$.

Since $G$ is soluble, there exists a complement $K$ to $P$ in $G$. Thus $P \cap K = 1$ and hence $G = P^G K$ and $G = P^G K$. So if $X \leq P$, Dedekind's law implies that $X^G = P^G (X^G \cap K)$ and hence $X = P \cap (X \cup K) \leq X \cup K$ since $P \leq G$. By 8.3.2, $L(G)$ is not directly decomposable and hence $K \leq C_G(P)$. Thus

(7) $P$ has a complement $K$ inducing nontrivial power automorphisms in $P$.

We show next that $P$ is elementary abelian. So suppose, for a contradiction, that $\Phi(P) \neq 1$ and let $N$ be a minimal normal subgroup of $P$ contained in $\Phi(P)$. By (7), $N \leq G$ and, by (2), the duality induced by $\delta$ in $G/N$ satisfies 8.2.2. Now $P \leq G$ implies that $\Phi(P) \leq \Phi(G)$ (see Robinson [1982], p. 131). Therefore if $L(G/N)$ were directly decomposable, then so would $L(G/\Phi(G))$ be, and then also $L(G)$, by 1.6.9; but this contradicts Lemma 8.3.2. Thus $L(G/N)$ is directly indecomposable and, since $P/N$ is a nontrivial proper normal Sylow $p$-subgroup of $G/N$, it follows that $G/N$ is
a $P$-group of order $p^m q$, $p > q$, $m \in \mathbb{N}$. Thus $|K| = q$ and $|N_G(K)| = q$ or $pq$. Hence there are $|G : N_G(K)| = p^{m+1}$ or $p^m$ conjugates to $K$, that is, complements to $P$ in $G$. Since $|G : P| = q$, clearly $|P^\delta|$ is a prime $s$. And since $P$ is not elementary abelian and 8.2.2 holds for the duality induced in $P$, the group $\overline{G}/P^\delta$ is a $t$-group for some prime $t$. By 8.2.9, $\overline{G}$ is not a primary group; for, in this case $\delta^{-1}$, and hence also $\delta$, would satisfy 8.2.2. Thus $s \neq t$ and the complements to $P^\delta$ in $\overline{G}$ are the Sylow $t$-subgroups of $\overline{G}$. Their number is $|G : N_G(K^\delta)| = 1$ or $s$. Since $\delta$ maps complements of $P$ to complements of $P^\delta$, it follows that $p^m$ or $p^{m+1}$ is equal to 1 or $s$. This is only possible if $m = 1$ and $s = p = |G : N_G(K)|$. Thus $|\overline{G}| = p^2 q$, $N_G(K) = NK$ and $P$ is cyclic since $\Phi(P) \neq 1$. But then $K$ centralizes $N$ and hence $P$; so $G = P \times K$, a contradiction. Thus $\Phi(P) = 1$, that is

$$\Phi(P) = 1.$$ 

(8) $P$ is elementary abelian.

We show next that $K$ is an abelian $q$-group for some prime $q$. First of all, if there are two different minimal normal subgroups $N_1$ and $N_2$ of $G$, then the dualities induced in $G/N_1$ satisfy 8.2.2 and hence, by 8.2.5, $G' \leq N_1 \cap N_2 = 1$. So $n = 2$ and $G' = G^{g(n-1)} \leq P$; this implies that $K \cong G/P$ is abelian. By (7) and (8), every minimal subgroup of $P$ is normal in $G$. Thus $K$ is abelian if $|P| \geq p^2$. If $|P| = p$ and $C_K(P) \neq 1$, then $C_K(P)$ contains a minimal normal subgroup of $G$ different from $P$ and so $K$ is abelian; and if $C_K(P) = 1$, then $K$ is isomorphic to a subgroup of $Aut P$ and hence is even cyclic. Thus in all cases,

(9) $K$ is abelian.

Now $K = Q_1 \times \cdots \times Q_r$ is the direct product of its Sylow subgroups $Q_i$ and $G/P = S_1/P \times \cdots \times S_r/P$ where $S_i = P Q_i$. Suppose, for a contradiction, that $r \geq 2$. By 8.1.8, $P^\delta = T_1^\delta \times \cdots \times T_r^\delta$ where $T_i = \bigcup S_j$ and the $T_i^\delta$ are coprime. So $P^\delta = S_i^\delta \times T_i^\delta$, where $S_i^\delta$ is a characteristic subgroup of $P^\delta \trianglelefteq \overline{G}$ and hence $S_i^\delta \trianglelefteq \overline{G}$. Thus $\delta$ induces a duality from $S_i$ onto $\overline{G}/S_i^\delta$. By (2), $S_i = P \times Q_i$ or $S_i$ is a $P$-group. In the latter case, $P$ is a normal $p$-subgroup of $S_i$ and hence $S_i \in P(p, k)$ for some $k \in \mathbb{N}$. Also, by 8.2.8, $\overline{G}/S_i^\delta \in P(k, p)$ and, as $P^\delta/S_i^\delta$ is a nontrivial normal subgroup of this $P$-group, $p$ divides $|P^\delta/S_i^\delta| = |T_i^\delta|$. Since these $T_i^\delta$ are coprime, this can happen for at most one $i$. Thus there exists $j \in \{1, \ldots, r\}$ such that $T_j = P \times Q_j$ and, since $K$ is abelian, it follows that $Q_j \leq Z(G)$. But $Q_j$ is a Sylow subgroup of $G$, hence $L(G)$ is directly decomposable and this contradicts 8.3.2. Thus

(10) $K$ is a $q$-group for some prime $q$.

Suppose, for a contradiction, that $|P| \geq p^2$ and let $N \leq P$ such that $|N| = p$. By (7) and 1.5.4, $K$ induces nontrivial universal power automorphisms in $P$. So $K$ does not centralize $P/N$ and, by (2), $G/N$ is a $P$-group. Thus $|K| = q$ and $G = PK$ is a $P$-group. By 8.2.8, $\delta$ satisfies 8.2.2, a contradiction. Thus


Now suppose that $C_K(P) \neq 1$. Since $K$ is abelian, $C_K(P) \leq Z(G)$; let $N \leq C_K(P)$ such that $|N| = q$. Then $G/N$ has a dual and, by (7), $K/N$ is not normal in $G/N$. By (2) and 8.2.8, $G/N$ is a $P$-group of order $pq$ and $N^\delta \in P(2, p)$. Since $P^\delta \cap N^\delta \leq N^\delta$, we have
| \[ P^6 \cap N^6 = p. \] So \( \delta \) induces a duality from the \( q \)-group \( G/P \cong K \) of order \( q^2 \) onto \( P^6 \), a group whose order is divisible by \( p > q \). It follows that \( G/P \) and \( P^6 \) are cyclic of prime power order. By 8.2.9, \( \bar{G} \) is not a \( p \)-group. It follows that \( |K^6| \neq p \), \( N^6 \) is nonabelian and is the unique maximal subgroup of \( G \) containing \( K^6 \). Thus \( N_\bar{G}(K^6) = K^6 \) and \( K^6 \) has \( p^2 \) conjugates in \( \bar{G} \). These are mapped by \( \delta^{-1} \) to complements of \( P \) in \( G \); but \( P \) has only \( p \) complements. This contradiction shows that

\[ (12) \quad C_K(P) = 1. \]

Now \( K \) is isomorphic to a subgroup of \( \text{Aut} \ P \) and hence is cyclic. Then \( G/P \) and \( P^6 \) are also cyclic so that \( M^6 \leq \bar{G} \) if \( M^6 \) is the minimal subgroup of \( P^6 \). By (1) and 8.2.8, \( G \neq P(2, p) \) and hence \( M \) contains \( P \) properly, has a dual and has nonnormal Sylow \( q \)-subgroups, by (12). Thus by (2), \( M \) is a \( P \)-group of order \( pq \) and \( \bar{G}/M^6 \in P(2, p) \).

Since \( P^6 \leq \bar{G} \), we obtain \( |P^6| : M^6| = p \) and hence \( |P^6| = p^2 \). Again by 8.2.9, \( \bar{G} \) is not a \( p \)-group. So \( |K^6| \neq p \) and \( \bar{G}/M^6 \) is nonabelian. Now \( P \) has \( p \) complements, the same holds for \( P^6 \) and this implies that \( M^6 \leq N_\bar{G}(K^6) \). It follows that \( K^6 \) centralizes \( M^6 \) and hence also \( P^6 \); but then \( \bar{G}/M^6 \) is abelian, a final contradiction.

It remains to study the case that \( G^{(n-1)} \) is not a primary group.

8.3.7 Lemma. (a) \( n = 2 \).

(b) For every prime \( r \), let \( S_r \) be the \( r \)-component and \( T_r \) the \( r' \)-component of \( G' \), so that \( G' = S_r \times T_r \). Then either

\[ (13) \quad G/T_r \text{ is a direct product of coprime finite primary groups, or} \]

\[ (14) \quad G/T_r = X_r/T_r \times Y_r/T_r \text{ where } X_r/T_r \in P(m, r) \text{ for some } m \in \mathbb{N}, \ Y_r/T_r \text{ is a direct product of coprime finite primary groups and } X_r/T_r \text{ and } Y_r/T_r \text{ are coprime; in this case, } G/G' \text{ is an } r' \text{-group}. \]

(c) Every primary subgroup of \( G \) is finite.

Proof. Let \( r \) be a prime. Since \( G^{(n-1)} \) is an abelian torsion group, \( G^{(n-1)} = R \times K \) where \( R \) is the \( r \)-component and \( K \) the \( r' \)-component of \( G^{(n-1)} \). Then the duality \( \delta_0 \) induced by \( \delta \) in \( G/K \) satisfies (2) and (3) and \( (G/K)^{(n-1)} = G^{(n-1)} / K \) is an \( r \)-group; by 8.3.6, \( \delta_0 \) cannot satisfy (1), that is, 8.2.2 holds for \( \delta_0 \). Thus \( G/K \) is a direct product of coprime finite \( P \)-groups and \( p \)-groups. In particular, \( G/K \) has finite Sylow \( r \)-subgroups and is metabelian, by 8.2.5. Since \( K \) is an \( r' \)-group, it follows that \( G \) has finite Sylow \( r \)-subgroups and \( G'' \) is an \( r' \)-group. This holds for every prime \( r \) and therefore every primary subgroup of \( G \) is finite and \( G'' = 1 \). Thus (a) and (c) hold.

Now \( G^{(n-1)}/K = G'/K \) is an \( r \)-group and therefore lies in a component \( X/K \) of the above direct decomposition of \( G/K \). The other components are then abelian and hence primary groups. If \( X/K \) also is a primary group, (13) holds. If \( X/K \) is not primary, it is a \( P \)-group with nontrivial normal \( r \)-subgroup \( G'/K \) and hence lies in \( P(m, r) \) for some \( m \in \mathbb{N} \). Then \( (X/K) = G'/K \) is the Sylow \( r \)-subgroup of \( G/K \) so that \( G/G' \) is an \( r' \)-group. Thus (14) holds.

8.3.8 Lemma. Let \( p > q \) be primes, \( P \in \text{Syl}_p(G) \), \( Q \in \text{Syl}_q(G) \) and suppose that \( [P, Q] \neq 1 \). Then \( G = PQ \times \bar{Y} \) where \( PQ \) is a finite \( P \)-group and \( \bar{Y} \) a normal \( \{p, q\} \)-complement of \( G \).
Proof. Let \( r \) be a prime and let \( T_r \) be as in 8.3.7. If \( r \neq p \), then \( PT_r/T_r \) and \( QT_r/T_r \) lie in different components of the decomposition of \( G/T_r \); for, either these components are primary groups or they lie in \( P(m,r) \) and \( r \neq p > q \). It follows that \([P,Q] \leq T_r\).

If also \([P,Q] \leq T_p\), we would obtain \([P,Q] \leq \bigcap_{r \neq p} T_r \geq 1\), a contradiction; thus \([P,Q] \not\leq T_p\). It follows that (14) holds for \( r = p \) and \( PQT_p/T_p = X_p/T_p \in P(m,p) \) for some \( m \in \mathbb{N} \); let \( Y = Y_p \). Then \( G'/T_p = PT_p/T_p \) and hence

\[ \text{(15)} \quad P \leq G' \text{ and } |QG' : G'| = q. \]

Thus \( G/G' \) is not a \( q' \)-group and so 8.3.7 yields that (13) holds for \( r = q \). So \( QT_q/T_q \) is a direct factor in \( G/T_q \) containing the \( q' \)-group \( G'/T_q \). But then by (15), \( G'/T_q = (G/T_q)' = (QT_q/T_q)' = (QG'/T_q)' \) is of index \( q \) in the finite \( q' \)-group \( QG'/T_q \) and this implies that \( QG'/T_q \) is cyclic of order \( q \). It follows that \( T_q = G' \), that is, \( G' \) is a \( q' \)-group, and \( |Q| = q \). Then \( T_p \) is a \( \{p,q\}' \)-group and, since \( P \) is characteristic in \( G' \), \( P \leq G' \) and \( PQ \) is a \( \{p,q\}' \)-group. So \( PQ \cap T_p = 1 \) and \( PQ \simeq PQT_p/T_p = X_p/T_p \). Also \( PQ \cap Y = 1 \) since \( Y \) is a \( \{p,q\}' \)-group and \( PQ \cup Y = PQTPY = XPYP = G \). Thus

\[ \text{(16)} \quad PQ \text{ is a finite } P\text{-group and } Y \text{ is a normal } \{p,q\}'\text{-complement of } G. \]

We have to show that \( PQ \leq G \); then \( G = PQ \times Y \), as desired. So suppose, for a contradiction, that \( PQ \) is not normal in \( G \). Then since \( P \leq G \), there exist a prime \( r \) and a Sylow \( r \)-subgroup \( R \) of \( G \) such that \( p \neq r \neq q \) and \([Q,R] \neq 1\). By (15) and (16), \( R \leq G' \), \( RQ \) is a finite \( P \)-group and there exists a normal \( \{r,q\}' \)-complement \( Z \) in \( G \). Then \( PQR \) is a \( \{p,q,r\}' \)-group and \( Y \cap Z \) a \( \{p,q,r\}' \)-group so that \( PQR \cap (Y \cap Z) = 1 \). Furthermore, \( G/Y \cap Z \) is finite. So by (2) or (3), if \( Y \cap Z \neq 1 \), the duality induced in \( G/Y \cap Z \) would satisfy 8.2.2. But \( PQR \simeq G/Y \cap Z \) is not directly decomposable, a contradiction. Thus \( Y \cap Z = 1 \) and \( G = PQR \) is finite. If \( N \) is a minimal subgroup of \( P \), then \( N \) is centralized by \( PR \leq G' \) and normalized by \( Q \) so that \( N \leq G \). By (2), the duality induced in \( G/N \) satisfies 8.2.2 and it follows that \( N = P \). Thus \( |P| = p \), similarly \( |R| = r \) and so \( |G| = pqr \). Then \( PR \) is the unique cyclic subgroup of composite order of \( G \) and hence is invariant under \( P(G) \). By 8.1.7, \((PR)^\delta = P^\delta \cap R^\delta \leq \overline{G}\). Now \( P^\delta \in P(2,r) \) since \( G/P \in P(2,r) \), and so \( |P^\delta \cap R^\delta| = r \); but \( R^\delta \in P(2,p) \) since \( G/R \in P(2,p) \), and hence \( |P^\delta \cap R^\delta| = p \). This contradiction shows that \( PQ \leq G \) and \( G = PQ \times Y \).

Proof of Theorem 8.3.1. By 8.3.7, every Sylow subgroup of \( G \) is finite. If any two Sylow subgroups of different order centralize each other, \( G \) is the direct product of its Sylow subgroups. And if there exist Sylow subgroups of different order not centralizing each other, then by 8.3.8, the join of any such pair is a finite \( P \)-group and a direct factor of \( G \). In any case, \( G = Dr G_\lambda \) with coprime finite groups \( G_\lambda \) which are \( p \)-groups or \( P \)-groups. By 8.1.8, \( \overline{G} = Dr \overline{G}_\lambda \) where \( \overline{G}_\lambda = \bigcup_{\delta \in \Lambda} G_\mu \) and the \( \overline{G}_\lambda \) are coprime. For every \( \lambda \in \Lambda \), \( \delta \) induces a duality \( \overline{\delta}_\lambda \) from \( G/\overline{G}_\lambda \simeq \overline{G}_\lambda \) onto \( \overline{G}_\lambda \). By 8.2.8 and 8.2.9, these \( \overline{\delta}_\lambda \) satisfy 8.2.2. It follows that \( \delta \) satisfies 8.2.2, a final contradiction.
Exercises

1. Try to prove Theorem 8.3.1 for finite groups in the shortest possible way.

8.4 Finite groups with duals

The aim of this section is to prove that every finite group $G$ with dual is soluble. Together with Theorem 8.3.1 this will imply that every duality $\delta$ of $G$ satisfies 8.2.2. In the crucial case of this proof, $G$ will be simple so that 8.1.6–8.1.8 will not be of much help. However, it is possible to find certain proper sections of $G$ which have duals and to which the induction assumption may therefore be applied. For this purpose, we introduce the following two concepts both of which are generalizations of $P(G)$-invariance.

$P(G)$-connected subgroups

Let $H$ and $X$ be subgroups of an arbitrary group $G$. We say that $X$ is $P(G)$-connected to $H$ if $H^\sigma = H$ implies $X^\sigma = X$ for $\sigma \in P(G)$.

8.4.1 Remark. (a) If $H = G$ (or $H = 1$), every $\sigma \in P(G)$ satisfies $H^\sigma = H$ and therefore $X$ is $P(G)$-connected to $G$ if and only if $X$ is invariant under $P(G)$.

(b) Conversely, if $X \leq H$ and $X$ is invariant under $P(H)$, then $X$ is $P(G)$-connected to $H$; for, every $\sigma \in P(G)$ satisfying $H^\sigma = H$ induces an autopjectivity in $H$ and hence fixes $X$. Thus subgroups like $\Phi(H)$ or $\Omega(H)$ are $P(G)$-connected to $H$.

(c) Finally, note that if $X$ is $P(G)$-connected to $H$, then $N_G(H) \leq N_G(X)$. For, every $g \in N_G(H)$ induces an autopjectivity in $G$ fixing $H$ and therefore also $X$; thus $X^g = X$ and $g \in N_G(X)$. \qed

Since we are studying dualities of groups, we are not only interested in the case that $X \leq H$, but also in the situation that $H \leq X$ or even that $H$ and $X$ are incomparable. This is shown by the following simple result and, in particular, its corollary.

8.4.2 Lemma. Let $\delta$ be a duality from the group $G$ to the group $\widetilde{G}$ and let $H, X \leq G$. If $X$ is $P(G)$-connected to $H$, then $X^\delta$ is $P(\widetilde{G})$-connected to $H^\delta$; in particular, $H^\delta \leq N_{\widetilde{G}}(X^\delta)$.

Proof. Let $\tau \in P(\widetilde{G})$ such that $(H^\delta)^\tau = H^\delta$. By 8.1.5, $\delta \tau \delta^{-1} \in P(G)$ and $H^{\delta \tau \delta^{-1}} = H$. Since $X$ is $P(G)$-connected to $H$, it follows that $X^{\delta \tau \delta^{-1}} = X$ and hence $(X^\delta)^\tau = X^\delta$. Thus $X^\delta$ is $P(\widetilde{G})$-connected to $H^\delta$. By (c) of 8.4.1, $H^\delta \leq N_{\widetilde{G}}(X^\delta)$. \qed

This lemma will mainly be used in the following two situations.
8.4 Finite groups with duals

8.4.3 Corollary. Let $\delta$ be a duality from $G$ to $\bar{G}$, let $H, X \leq G$ and suppose that $X$ is $P(G)$-connected to $H$.

(a) If $H \leq X$, then $X^\delta \leq H^\delta$ and $\delta$ induces a duality from $X/H$ onto $H^\delta/X^\delta$.

(b) If $H \cap X = 1$, then $X^\delta \leq \bar{G}$ and $\delta$ induces a duality from $X$ onto $\bar{G}/X^\delta$.

Proof. If $H \leq X$, then $X^\delta \leq H^\delta$ and hence $X^\delta \leq H^\delta$, by 8.4.2. And if $H \cap X = 1$, then $N_G(X^\delta) \geq H^\delta \cup X^\delta = (H \cap X)^\delta = \bar{G}$, that is, $X^\delta \leq \bar{G}$. By 8.1.6, $\delta$ induces dualities in $X/H$ and $X$, respectively.

$P(G)$-normality

Let $H$ and $K$ be subgroups of a group $G$ such that $H \leq K$. We say that $H$ is $P(G)$-normal in $K$ if $H^\sigma \leq K^\sigma$ for all $\sigma \in P(G)$.

Of course, $H \leq K$ if $H$ is $P(G)$-normal in $K$; but $P(G)$-normality strongly depends on the group $G$ (see Exercise 2). It is important that if $G$ has a dual, then $K/H$ is contained in a factor $L/H$ with dual.

8.4.4 Lemma. Let $G$ be a group, $H \leq K \leq G$ and suppose that $H$ is $P(G)$-normal in $K$. If $\delta$ is a duality from $G$ to a group $\bar{G}$, and $L^\delta$ is the core of $K^\delta$ in $H^\delta$, then $H \leq L = \bigcup_{u \in H^\delta} K^{bud^{-1}}$ and hence $\delta$ induces a duality from $L/H$ onto $H^\delta/L^\delta$.

Proof. Clearly, $H^\delta \geq K^\delta \geq L^\delta$ so that $H \leq K \leq L$. By 8.1.1, $L = \left( \bigcap_{u \in H^\delta} (K^\delta)^u \right)^{d^{-1}} = \bigcup_{u \in H^\delta} K^{bud^{-1}}$. Now 8.1.5 shows that $\delta u d^{-1} \in P(G)$ for every $u \in H^\delta$, and therefore $H = H^{bud^{-1}} \leq K^{bud^{-1}}$ since $H$ is $P(G)$-normal in $K$. Thus $H \leq L$ and, by 8.1.6, $\delta$ induces a duality from $L/H$ onto $H^\delta/L^\delta$. □

The main theorem

In the remainder of this section we prove the result announced above.

8.4.5 Theorem (Zacher [1961b]). Every finite group with dual is soluble.

To prove this, we suppose the theorem is false and choose a counterexample $G$ of minimal order; let $\delta$ be a duality from $G$ to a group $\bar{G}$. Then if $X$ is a group such that $|X| < |G|$ and $X$ has a dual, it follows that $X$ is soluble and, by 8.3.1, that

(1) every duality of $X$ satisfies 8.2.2.

Of course, $G$ is not soluble; indeed we show first that our inductive hypothesis implies that $G$ and $\bar{G}$ are in fact simple.

8.4.6 Lemma. $G$ and $\bar{G}$ are nonabelian simple groups.
Proof. We suppose the lemma is false and show that there exists a subgroup $R$ of $G$ such that $1 < R < G$ and $R^\sigma = R$ for all $\sigma \in P(G)$. By 8.1.7, $\delta$ induces dualities in $R$ and in $G/R$; then by induction, $R$ and $G/R$, and therefore $G$, are soluble, a contradiction.

If $G$ is not simple, there exists $N \leq G$ such that $1 < N < G$. By 8.1.6, $G/N$ has a dual and therefore, by induction, it is soluble. Thus if $R = G_2$ is the soluble residual of $G$, then $R \leq N < G$ and, of course, $R \neq 1$ since $G$ is not soluble. By 5.3.6, $R^\sigma = R$ for all $\sigma \in P(G)$.

Now suppose that $G$ is not simple. Then there exists $N \leq G$ such that $1 < N < G$ and $N^\delta \leq G$. Again by 8.1.6, $\delta$ induces a duality from $N$ onto $G/N^\delta$; by (1), $N$ and $G/N^\delta$ are soluble. Let $R \leq G$ be such that $R^\delta = G_2$. Then $R^\delta \leq N^\delta < G$; if $R^\delta = 1$, the group $G$ is soluble and hence by 8.3.1 applied to $S'$, $G$ is soluble, a contradiction. Thus $1 < R < G$ and, again by 5.3.6, $R^\delta$ is invariant under $P(G)$. By 8.1.7, $R^\sigma = R$ for all $\sigma \in P(G)$.

In the sequel let $q$ be the smallest prime dividing $|G|$ and let $Q \in \text{Syl}_q(G)$. Of course, the Feit-Thompson Theorem implies that $q = 2$; however, we do not need this. In fact, the proof of Theorem 8.4.5 does not use any of the deeper results proved in the course of the classification of finite simple groups. We shall only need some transfer arguments culminating in Grün's Second Theorem. So, for example, the additional assumption in the following lemma, that $Q$ is not a generalized quaternion group, is superfluous by a well-known theorem of Brauer and Suzuki. However, it will be no problem to get rid of this assumption later on.

8.4.7 Lemma. If $Q$ is not a generalized quaternion group, there exists $Q_1 \in \text{Syl}_q(G)$ such that $Q_1 \neq Q$ and $Q \cap Q_1 \neq 1$.

Proof. Suppose, for a contradiction, that $Q \cap Q_1 = 1$ for all $Q_1 \in \text{Syl}_q(G)$ such that $Q_1 \neq Q$. Since $G$ is simple, $1 < Q < G$ and $Q$ is not cyclic (see Robinson [1982], p. 280). By assumption, $Q$ is not a generalized quaternion group and it follows (see Robinson [1982], p. 138) that $Q$ has at least two minimal subgroups. Let $H$ be one of these and let $\sigma \in P(G)$ such that $H^\sigma = H$. By 4.2.8, $\sigma$ is index preserving and hence $Q^\sigma \in \text{Syl}_q(G)$. So if $Q^\sigma \neq Q$, then $1 \neq H \leq Q \cap Q^\sigma$, a contradiction. Thus $Q^\sigma = Q$, that is $Q$ is $P(G)$-connected to $H$. By 8.4.2, $Q^\delta \leq H^\delta$. So if $K$ is another minimal subgroup of $Q$, it follows that $Q^\delta \leq H^\delta \cup K^\delta = (H \cap K)^\delta = 1^\delta = G$. But this contradicts the simplicity of $G$.

In the sequel let $q$ be the smallest prime dividing $|G|$ and let $Q \in \text{Syl}_q(G)$. Of course, the Feit-Thompson Theorem implies that $q = 2$; however, we do not need this. In fact, the proof of Theorem 8.4.5 does not use any of the deeper results proved in the course of the classification of finite simple groups. We shall only need some transfer arguments culminating in Grün's Second Theorem. So, for example, the additional assumption in the following lemma, that $Q$ is not a generalized quaternion group, is superfluous by a well-known theorem of Brauer and Suzuki. However, it will be no problem to get rid of this assumption later on.

8.4.8 Lemma. Suppose that $N \leq K \leq G$, $|N| = q$, $N \unlhd K$ and $K/N$ is a $P$-group of order $p^aq$ where $q < p \in \mathbb{P}$. Then $n = 1$.

Proof. Let $P \in \text{Syl}_q(K)$. Then $P$ operates on the cyclic group $N$ of order $q$ and since $q < p$, we can assert that $P$ centralizes $N$. Thus $PN = P \times N$. Let $H \leq P$ such that $|H| = p$. Then $H$ is characteristic in $H \times N \unlhd K$ and hence $H \unlhd K$. So if $S \in \text{Syl}_q(K)$,
then \( H \) is the unique subgroup of order \( p \) in \( HS \). By 4.2.8, every autoprojectivity \( \sigma \) of \( G \) is index preserving. It follows that \( P^\sigma \) is an elementary abelian \( p \)-group and that \( H^\sigma \) is the unique subgroup of order \( p \) in \((HS)^\sigma\). Thus \( H^\sigma \leq P^\sigma \cup S^\sigma = K^\sigma \), that is, \( H \) is \( P(G) \)-normal in \( K \). By 8.4.4 there exists \( L \leq G \) such that \( K \leq L, H \leq L \) and \( \delta \) induces a duality in \( L/H \); by (1), this duality satisfies 8.2.2. Since \( q^2 \) divides the order of \( L/H \), this group has a normal Sylow \( q \)-subgroup, by 8.2.6. Then \( K/NH \) also has a normal Sylow \( q \)-subgroup and since \( K/N \) is a \( P \)-group of order \( p^\alpha q \), it follows that \( |K : NH| = q \). Thus \( H = P \) and \( n = 1 \), as desired.

We come to the main step in the proof of Theorem 8.4.5. Recall that \( q \) is the smallest prime dividing \( |G| \).

**8.4.9. Lemma.** Let \( D \neq 1 \) be a maximal intersection of two different Sylow \( q \)-subgroups of \( G \). Then \( |D| = q, |N_G(D)| = pq^2 \) where \( q < p \in \mathbb{P} \) and \( N_G(D)/D \) is nonabelian of order \( pq \).

**Proof.** Let \( D = Q_1 \cap Q_2 \) where \( Q_i \in Syl_q(G) \) and \( Q_1 \neq Q_2 \); let \( S_i \in Syl_q(N_G(D)) \) and \( T_i \in Syl_q(G) \) such that \( N_{Q_i}(D) \leq S_i \leq T_i \) (\( i = 1, 2 \)). Then \( Q_i \cap T_i \geq N_{Q_i}(D) > D \) and the choice of \( D \) implies that \( Q_i = T_i \). Thus \( S_i \leq Q_i \) and hence \( S_i = N_{Q_i}(D) \) and \( D = S_1 \cap S_2 \). This shows that \( N_G(D) \) has nonnormal Sylow \( q \)-subgroups and \( D = O_q(N_G(D)) \).

Let \( \sigma \in P(G) \) such that \( D^\sigma = D \). By 8.4.6 and 4.2.8, \( \sigma \) is index preserving. Thus \( D^\sigma = O_q(N_G(D)^\sigma) \leq N_G(D)^\sigma \) and hence \( N_G(D)^\sigma \leq N_G(D) \). Since \( G \) is finite, this implies that \( N_G(D)^\sigma = N_G(D) \), that is, \( N_G(D) \) is \( P(G) \)-connected to \( D \). By 8.4.3, \( \delta \) induces a duality in \( N_G(D)/D \) and since \( N_G(D)/D \) has nonnormal Sylow \( q \)-subgroups, it follows from (1) that

\[
(2) \quad N_G(D)/D = A/D \times B/D \quad \text{where} \quad (|A/D|, |B/D|) = 1 \quad \text{and} \quad A/D \text{ is a } P\text{-group of order } p^\alpha q, p > q, n \in \mathbb{N}.
\]

We have to study \( A \) and show first that \( \Phi(A) = 1 \) or \( \Phi(A) = D \); in fact, we prove a more general result that will be applied several times in the sequel.

(3) Let \( H \leq D \) and \( D \leq K \leq A \) such that \( pq \) divides \( |K : D| \). If \( H \) is \( P(G) \)-normal in \( K \), then \( H = 1 \) or \( H = D \).

To prove this, suppose that \( 1 < H \leq D \). By 8.4.4 there exists a subgroup \( L \) of \( G \) such that \( K \leq L, H \leq L \) and \( L/H \) has a dual. Since \( pq \) divides \( |K : D| \), \( K/D \) has nonnormal Sylow \( q \)-subgroups and then so does \( L/H \). Therefore by (1) and 8.2.6, \( |L/H| \) is not divisible by \( q^2 \). It follows that \( H = D \), as desired. Now \( \Phi(A)^\sigma = \Phi(A^\sigma) \leq A^\sigma \) for all \( \sigma \in P(G) \). Thus \( \Phi(A) \) is \( P(G) \)-normal in \( A \) and, since \( A/D \) is a \( P \)-group, \( \Phi(A) \leq D \). So we may apply (3) with \( H = \Phi(A) \) and \( K = A \) to obtain that

(4) \( \Phi(A) = 1 \) or \( \Phi(A) = D \).

We want to show that \( |D| = q \) and, as a first step, we prove this in a special case.

(5) Let \( P \in Syl_p(A) \). If \( C_p(D) \neq 1 \), then \( |D| = q \).

To see this, put \( C = C_p(D) \) and \( K = CS \) where \( S \in Syl_q(A) \). Since \( CD \leq A \), it follows that \( K = CS = CDS \) is a subgroup of \( A \) containing \( D \); also \( pq \) divides \( |K : D| \) since

\[
\text{Hence } |D| = q.
\]

---

8.4 Finite groups with duals

471
C $\neq 1$. Let $\sigma \in P(G)$. If $H \leq D$, then $HC = H \times C$ and hence $H^\sigma \leq (HC)^\sigma$, by 1.6.7. So if $H^\sigma \leq S^\sigma$, it follows that $H^\sigma \leq C^\sigma \cup S^\sigma = K^\sigma$. We now apply this argument three times. First, $H = \Phi(S) \leq D$ and, clearly, $H^\sigma = \Phi(S^\sigma) \leq S^\sigma$. Thus $H^\sigma \leq K^\sigma$ and so $H$ is $P(G)$-normal in $K$. By (3), $\Phi(S) = 1$ or $\Phi(S) = D$. If $\Phi(S) = D$, then $S$ is cyclic; hence $S^\sigma$ is cyclic and every subgroup $H$ of $D$ satisfies $H^\sigma \leq S^\sigma$. If $\Phi(S) = 1$, then $S$ is elementary abelian, since $\sigma$ is index preserving, $S^\sigma$ too is elementary abelian and again $H^\sigma \leq S^\sigma$ for all $H \leq D$. In both cases, it follows that every subgroup $H$ of $D$ is $P(G)$-normal in $K$. By (3), $H = 1$ or $H = D$, that is, $|D| = q$, as desired.

(6) $|D| = q$.

Suppose that this is false and let $P \in \text{Syl}_p(A)$, as before. The Frattini argument applied to the normal subgroup $PD$ of $A$ yields that $A = DN_A(P)$. So if $\Phi(A) = D$, it would follow that $A = N_A(P)$ and hence $[P, D] \leq P \cap D = 1$. By (5), $|D| = p$, a contradiction. Thus $\Phi(A) \neq D$, and so by (4), $\Phi(A) = 1$. Since $D \leq A$, it follows that $\Phi(D) = 1$ (see Robinson [1982], p. 131) and hence

(6a) $D$ is elementary abelian, $|D| \geq q^2$.

Since $q$ is the smallest prime dividing $|G|$, a minimal subgroup of $D$ which is normal in $A$ is centralized by $A$. Therefore if every minimal subgroup of $D$ were normal in $A$, then $C_p(D) = P$ and, again by (5), $|D| = p$, a contradiction. Thus there exist minimal subgroups of $D$ which are not normal in $A$. Since $G$ is simple, $D^\delta$ can be normal in the image of at most one of these minimal subgroups, that is, there exists

(6b) $H \leq D$ such that $|H| = q$, $H \not\subseteq A$ and $D^\delta \not\subseteq H^\delta$.

Let $L^\delta = \bigcap_{u \in H^\delta} (D^\delta)^u$ be the core of $D^\delta$ in $H^\delta$. Then by 8.1.1, $L = \bigcup_{u \in H^\delta} D^\delta u^{-1}$ and, by (6a) and (6b), $H < D < L$. Since every autoprojectivity $\sigma$ of $G$ is index preserving, $D^\sigma$ is elementary abelian and hence $H^\sigma \leq D^\sigma$ for every $\sigma \in P(G)$. By 8.4.4, $H \leq L$ and $\delta$ induces a duality from $L/H$ onto $H^\delta/L^\delta$; by (1), this duality satisfies 8.2.2. Since every autoprojectivity $\delta u \delta^{-1}$ of $G$ ($u \in H^\delta$) is index preserving, $L$ is a join of $q$-groups; in particular, $L(L/H)$ is directly indecomposable. Furthermore, since $D$ is elementary abelian, $D^\delta/L^\delta$ is the intersection of maximal subgroups of $H^\delta/L^\delta$, and $D^\delta \not\subseteq H^\delta$ im-

---

Figure 23

---
plies that $H^\delta /L^\delta$ is not a primary group. It follows that

\[(6c)\quad H^\delta /L^\delta \text{ is a } P\text{-group of order } r^m s, \quad r > s,\]

and $L/H \in P(m + 1, r)$; since $L$ is generated by $q$-groups,

\[(6d)\quad L/H \text{ is an elementary abelian } q\text{-group (and } q = r) \text{ or a nonabelian } P\text{-group of order } r^m q, \quad r > q.\]

Now $H < D < L$. So if $L/H$ is abelian, $L \leq N_G(D)$ and then $|L : D| = q$, by (2). And if $L/H$ is not abelian, 8.4.8 applied with $N = H$ and $K = L$ yields that $|L : H| = rq$. In both cases,

\[(6e)\quad D \text{ is a maximal subgroup of } L.\]

We finally show that

\[(6f)\quad D^\delta \text{ is a } p\text{-group}\]

where $p$ is the prime appearing in (2). For this we choose $x \in A$ such that $H^x \neq H$, and consider the autoprojectivity $\tau = \delta^{-1} x \delta$ of $G$ induced by $x$. Then $H^\delta$ and $H^{\delta x} = H^\delta$ are different maximal subgroups of $G$ and hence $G = H^\delta \cup H^{\delta x}$. Furthermore, $D^\delta = D^{\delta x} = D^\delta$ since $x \in A \leq N_G(D)$. And finally, by (6e), $L^\delta$ is a maximal subgroup of $D^\delta$; also $|D^\delta /L^\delta| = t \in \mathbb{P}$ since $L^\delta \leq D^\delta$. Because $\tau$ is index preserving, 4.3.5 yields that $L^{\delta x} \leq D^{\delta x} = D^\delta$ and $|D^\delta /L^{\delta x}| = t$. So if $N = O^t(D^\delta)$, then $N = O^t(L^\delta) = O^t(L^{\delta x})$. Thus $N$ is characteristic in $L^\delta \leq H^\delta$ and hence $N \leq H^\delta$. Moreover, since $H^\delta /L^\delta$ is a $P$-group, $H^\delta$ is the join of subgroups in which $L^\delta$ is maximal and so 4.3.5 implies that $L^{\delta x} \leq H^{\delta x}$. Therefore $N \leq H^{\delta x}$ also and hence $N \leq H^\delta \cup H^{\delta x} = G$. But $G$ is simple and it follows that $N = 1$, that is $D^\delta$ is a $t$-group. Since $A/D$ is a $P$-group, $A^\delta$ is the intersection of maximal subgroups of $D^\delta$ and so $A^\delta \leq D^\delta$. By 8.1.6, $\delta$ induces a duality from $A/D$ onto $D^\delta /A^\delta$ and, by 8.2.8, $D^\delta /A^\delta \in P(n + 1, p)$. Thus $t = p$ and (6f) holds.

It follows from (6f) that $p$ divides $|H^\delta /L^\delta|$. Therefore $r \geq p > q$ in (6c) and hence $L/H$ cannot be an elementary abelian $q$-group. By (6d), $L/H$ is a nonabelian $P$-group of order $r^m q$ and so $D$ is not normal in $L$. By (6e), $D$ is a maximal subgroup of $L$ and, by (2), $D$ is also maximal in $S$ if $S \in Syl_q(A)$. Now $S \neq L$ since $D \not\leq S$; let $M = L \cup S$. Then $L^\delta$ and $S^\delta$ are different maximal subgroups of the $p$-group $D^\delta$ and hence $D^\delta / (L^\delta \cap S^\delta) = D^\delta /M^\delta$ is elementary abelian of order $p^2$. So $\mathcal{X} = [M/D] \setminus \{M, D, S\}$ is an antichain on which $S$ operates by conjugation. Since $|\mathcal{X}| = p$, the $q$-group $S$ must fix some $X \in \mathcal{X}$ and then $X \leq S \cup X = M$. It follows that $D = X \cap Y \leq Y$ for every $Y \in \mathcal{X}$ such that $Y \neq X$, and, since these $Y$ generate $M$, we get that $D \leq M$. In particular, $D \leq L$ and this contradiction finally proves (6).

Now we may apply Lemma 8.4.8 with $N = D$ and $K = A$ and obtain that $|A/D| = pq$. Thus

\[(7)\quad |A| = pq^2.\]

It remains to be shown that $N_G(D) = A$; then (6), (7), and (2) contain all the assertions of the lemma. Since $|D| = q$ is the smallest prime dividing $|G|$, we have $D \leq Z(N_G(D))$; in addition, $D$ is a normal Hall subgroup of $B$ and so the Schur-Zassenhaus Theorem implies that $B = D \times H$ where $(|D|, |H|) = 1$. Then $H$ is char-
acteristic in \( B \trianglelefteq N_G(D) \) and hence \( H \trianglelefteq N_G(D) \); thus \( N_G(D) = A \times H \) and \(|A|, |H| = 1\). By 1.6.6, \( N_G(D)^\sigma = A^\sigma \times H^\sigma \) for every \( \sigma \in P(G) \), that is, \( H \) is \( P(G) \)-normal in \( N_G(D) \).

By 8.4.4 there exists \( L \leq G \) such that \( N_G(D) \leq L \), \( H \trianglelefteq L \) and \( L/H \) has a dual. Since \( A \cong N_G(D)/H \leq L/H \), \( q^2 \) divides \(|L/H|\). So if \( H \neq 1 \), (1) and 8.2.6 would imply that \( L/H \) has a normal Sylow \( q \)-subgroup; but (2) shows that \( A \) has nonnormal Sylow \( q \)-subgroups, a contradiction. Thus \( H = 1 \), that is \( N_G(D) = A \), as desired. \( \square \)

Recall that \( q \) is the smallest prime dividing \(|G|\) and \( Q \in \text{Syl}_q(G) \). Lemma 8.4.9 implies that \( Q \) is small and \( q = 2 \); so we can finally work with involutions.

8.4.10 Lemma. \(|Q| \leq q^2\); hence \( q = 2 \), \( Q \) is elementary abelian of order 4 and \(|N_G(Q)/C_G(Q)| = 3\).

Proof. Suppose, for a contradiction, that \(|Q| \geq q^3\). We show first that for every \( g \in G \),

\[(8) \ Z(Q) \leq Q^g \text{ implies } Q^g = Q.\]

For, if \( Z(Q) \leq Q^g \) and \( Q^g \neq Q \), there would exist a maximal intersection \( D \) of two different Sylow \( q \)-subgroups of \( G \) such that \( D \geq Q \cap Q^g \geq Z(Q) \). By 8.4.9, \(|D| = q \) and \(|N_G(D)| = pq^2 \) for some prime \( p \). So it would follow that \( D = Z(Q) \) and hence \( Q \leq N_G(D) \), impossible since \(|Q| \geq q^3\). Thus (8) holds and a similar argument yields that

\[(9) \ Z(Q) < Q.\]

Indeed this is clear if \( Q \) is a generalized quaternion group. If \( Q \) is not of this type, then by 8.4.7 there exists a maximal intersection \( D \neq 1 \) of \( Q \) and another Sylow \( q \)-subgroup \( Q_1 \). Again by 8.4.9, \(|D| = q \) and \(|N_G(D)| = pq^2 \) for some prime \( p \). Since \( Z(Q) \leq N_G(D) \), it follows that \(|Z(Q)| \leq q^2 \) and hence \( Z(Q) < Q \).

Now \( Z(Q) \) is a characteristic subgroup of \( Q \), and hence \( N_G(Q) \leq N_G(Z(Q)) \). If \( g \in N_G(Z(Q)) \), then \( Z(Q) = Z(Q)^g \leq Q^g \) and so by (8), \( Q^g = Q \). Thus \( g \in N_G(Q) \), that is, \( N_G(Q) = N_G(Z(Q)) \). Let \( \sigma \in P(G) \) such that \( Z(Q)^\sigma = Z(Q) \). Since \( \sigma \) is index preserving, \( Q^\sigma \) is a Sylow \( q \)-subgroup of \( G \) containing \( Z(Q) \) and hence by (8), \( Q^\sigma = Q \). It follows that \( Q \) is the unique Sylow \( q \)-subgroup of \( N_G(Q)^\sigma \) and so \( N_G(Q)^\sigma \leq N_G(Q) \). Since \( G \) is finite, this implies that \( N_G(Q)^\sigma = N_G(Q) \). Thus we have shown that

\[(10) \ X = N_G(Q) = N_G(Z(Q)) \text{ is } P(G)\text{-connected to } Z(Q)\].

By 8.4.3, \( \delta \) induces a duality in \( X/Z(Q) \) and by (1), this duality satisfies 8.2.2. Thus \( X/Z(Q) \) is a direct product of coprime \( P \)-groups and \( p \)-groups. By (9), \( Z(Q) < Q \). Since \( q \) is the smallest prime dividing \(|G|\), the direct factor of the decomposition of \( X/Z(Q) \) containing \( Q/Z(Q) \) is either a \( q \)-group or a nonabelian \( P \)-group of order \( p^nq \), \( p > q \), \( n \in \mathbb{N} \). In both cases, \( X = N_G(Z(Q)) \) has a normal subgroup of index \( q \).

Now (8) shows that \( G \) is \( q \)-normal, that is, \( Z(Q)^g \leq Q \) implies \( Z(Q)^g = Z(Q) \); for, \( Z(Q)^g \leq Q \) implies \( Z(Q) \leq Q^{g^{-1}} \), hence \( Q^{g^{-1}} = Q \) and then \( Z(Q)^g = Z(Q^g) = Z(Q) \).

So Grün's Second Theorem (see Robinson [1982], p. 285) yields that \( G \) has a normal subgroup of index \( q \); but by 8.4.6, \( G \) is simple. This contradiction shows that \(|Q| \leq q^2 \). It is a well-known consequence of Burnside's criterion for \( p \)-nilpotence (see
8.4 Finite groups with duals

Robinson [1982], p. 280) that now \( q = 2 \), \( Q \) is elementary abelian of order 4 and \( |N_G(Q)/C_G(Q)| = 3 \).

8.4.11 Lemma. If \( t \in G \) is an involution, \( C_G(t) \leq \bar{G} \).

Proof. By 8.4.7 there exists a nontrivial intersection \( D = Q \cap Q_1 \) of \( Q \) and another Sylow 2-subgroup \( Q_1 \) of \( G \). By 8.4.10, \( |Q| = 4 \) so that \( D \) has order 2 and is a maximal intersection of two different Sylow 2-subgroups; in addition, \( |N_G(Q)/C_G(Q)| = 3 \) implies that all involutions in \( G \) are conjugate. So we may assume that \( D = \langle t \rangle \); put \( C = C_G(t) = N_G(D) \). Then by 8.4.9, \( C/D \) is nonabelian of order 2p for some prime \( p > 2 \); let \( P \in \text{Syl}_p(C) \). Then \( PD = P \times D \leq C \) so that \( P \leq C \), and hence \( P \) is the unique subgroup of order \( p \) of \( C \).

We want to show that \( C \) is \( P(G) \)-connected both to \( D \) and to \( P \); by 8.4.2, this will imply that \( C^P \leq D^P \cap P^P = (D \cap P)^P = \bar{G} \), as desired. Clearly, \( C \) is the join of all the Sylow 2-subgroups of \( G \) containing \( D \). So if \( \sigma \in P(G) \) such that \( D^\sigma = D \) and, as we have just shown, it will follow that \( C^\sigma = C \), as desired. So suppose, for a contradiction, that \( s \in G \) is an involution such that \( t \neq s \in C_G(P) \). Then \( \langle s, t \rangle \) is a dihedral group centralizing \( P \); hence \( \langle s, t \rangle \cap P = 1 \). Furthermore, since \( C/D \) is nonabelian, \( P \not\leq Z(C) \); hence \( s \notin C \) and \( \langle s, t \rangle \) is not a 2-group. Now \( P \) is the unique subgroup of order \( p \) of \( C \) and therefore \( P \) is \( P(G) \)-normal in \( C = C_G(t) \). Then \( P \) is the unique subgroup of order \( p \) of \( C_G(s) \) since \( C_G(s) \) is conjugate to \( C_G(T) \); thus it is \( P(G) \)-normal in \( C_G(s) \). Hence \( P \) is \( P(G) \)-normal in \( C_G(t) \cap C_G(s) \) and by 8.4.4 there exists \( L \leq G \) such that \( C_G(t) \cap C_G(s) \leq L \) and \( L/P \) has a dual. Since \( |C/P| = 4 \) (1) and 8.2.6 imply that \( L/P \) has a normal Sylow 2-subgroup; but \( \langle s, t \rangle P/P \cong \langle s, t \rangle \) does not. This contradiction shows that \( t \) is the unique involution of \( G \) centralizing \( P \). Thus \( D^\sigma = D \) and \( C^\sigma = C \), as desired.

Proof of Theorem 8.4.5. By 8.4.6, a minimal counterexample \( G \) to Theorem 8.4.5 is simple and, by 8.4.10, \( |G| \) is even. If \( t \in G \) is an involution, it follows that \( 1 < C_G(t) < G \). By 8.4.11, \( C_G(t)^P \leq \bar{G} \); but by 8.4.6, \( \bar{G} \) is simple. This contradiction proves the theorem.

Exercises

1. Give examples of subgroups \( H, X \) of a group \( G \) such that \( X \) is \( P(G) \)-connected to \( H \) and
   (a) \( 1 < H < X < G \), or
   (b) \( H \not\leq X \) and \( X \not\leq H \), or
   (c) \( X \leq H \) and \( X \) is not invariant under \( P(H) \).
2. Find groups $H \leq K \leq G \leq G^*$ such that
(a) $H$ is $P(G)$-normal in $K$ but $H$ is not $P(G^*)$-normal in $K$,
(b) $H$ is not $P(G)$-normal in $K$ but $H$ is $P(G^*)$-normal in $K$.

3. (Calcaterra [1987]) Let $A$ be a group acting on a finite group $G$ and suppose that $(A, G)$ satisfies the double centralizer property (or DCP), that is, $C_G C_A(H) = H$ for any subgroup $H$ of $G$ and $C_A C_G(B) = B$ for any subgroup $B$ of $A$.
(a) If $A = A_1 \times \cdots \times A_n$ with coprime groups $A_i$, show that $G = G_1 \times \cdots \times G_n$ with coprime groups $G_i$ such that $(A_i, G_i)$ satisfies the DCP for all $i$.
(b) If $A$ is nontrivial and $L(A)$ is directly indecomposable, show that either
(i) $|A| = q$ and $|G| = p$ where $p$ and $q$ are primes such that $q | p - 1$, or
(ii) $A$ and $G$ lie in $P(n, p)$ for some prime $p$ and integer $n$.

8.5 Locally finite groups with duals

The aim of this section is to show that every locally finite group with dual is soluble; this together with Theorem 8.3.1 will complete the proof of the Main Theorem 8.2.2 of this chapter. For this purpose we first of all have to prove Theorem 8.2.3(a), without using 8.2.2, of course.

Subgroups of finite index

8.5.1 Theorem. If $G$ is a group with dual, then $G'' = G_{\bar{\alpha}} = G_{\bar{\beta}}$ where $G_{\bar{\alpha}}$ is the intersection of all subgroups of finite index in $G$ and $G_{\bar{\beta}}$ is the intersection of all normal subgroups of $G$ with soluble factor group.

Proof. First of all, if $H$ is a subgroup of finite index in $G$, then $G/H_G$ is a finite group; by 8.1.6, $G/H_G$ has a dual and hence is soluble, by 8.4.5. Now if $N$ is an arbitrary normal subgroup of $G$ with soluble factor group, then 8.3.1 and 8.2.5 yield that $G/N$ is metabelian. Thus $G'' \leq N$; in particular, $G'' \leq H_G \leq H$. It follows that $G'' \leq G_{\bar{\beta}}$. Conversely, since $G/G''$ is soluble, obviously $G_{\bar{\beta}} \leq G''$; furthermore, the duality induced in $G/G''$ satisfies 8.2.2 and hence $G'/G''$ is a direct product of finite groups. Therefore $G''$ is the intersection of normal subgroups of finite index in $G$ and so $G_{\bar{\beta}} \leq G''$. Thus $G'' = G_{\bar{\beta}} = G_{\bar{\alpha}}$.

8.5.2 Corollary. If $G$ is a group with dual, $G''$ is a perfect group with dual and has no proper subgroup of finite index.

Proof. By 8.5.1, $G'' = G_{\bar{\alpha}} = G_{\bar{\beta}}$. Since $G'' \leq G$ and $G/G''$ is soluble, we see that $(G'')' = G'' \leq G_{\bar{\beta}} = G''$, thus $G''$ is perfect. The Zacher-Rips Theorem 6.1.7 shows that $G_{\bar{\beta}}$ is invariant under $P(G)$. By 8.1.7, $G'' = G_{\bar{\alpha}}$ has a dual and then 8.5.1 applied to this group yields that $(G'')_{\bar{\alpha}} = (G'')'' = G''$. Thus $G''$ has no proper subgroup of finite index.
The locally soluble radical $S(G)$

For a locally finite group $G$, define $S(G)$ to be the join of all locally soluble normal subgroups of $G$.

Suppose that $N/S(G)$ is a locally soluble normal subgroup of $G/S(G)$ and let $H$ be a finitely generated subgroup of $N$. Since $G$ is locally finite, $H$ is a finite group. Therefore $H/H \cap S(G) \simeq HS(G)/S(G)$ is soluble since $N/S(G)$ is locally soluble. And the finite subgroup $H \cap S(G)$ of $S(G)$ is contained in the join of a finite number of locally soluble normal subgroups $N_1, \ldots, N_k$ of $G$. If $K$ is a finitely generated subgroup of $N_1 N_2$, then again $K$ is finite and therefore $K \cap N_1$ is soluble; and since $N_2 N_1/N_1 \simeq N_2/N_1 \cap N_2$ is locally soluble, $KN_1/N_1 \simeq K/K \cap N_1$ is soluble. Thus $K$ is soluble and so $N_1 N_2$ is locally soluble. An obvious induction yields that $N_1 \ldots N_k$ is locally soluble and hence $H \cap S(G)$ is soluble. So, finally, $H$ is soluble and this shows that $N$ is locally soluble. This holds in particular for $N = S(G)$, that is

1. $S(G)$ is locally soluble;

moreover, we have shown that $N \leq S(G)$, that is

2. $S(G/S(G)) = 1$.

Now suppose that $\sigma \in P(G)$. By 6.6.10 and (2), $S(G)\sigma \leq G$. By 6.6.4 and 1.2.11, the class of locally soluble groups is invariant under projectivities. Thus by (1), $S(G)\sigma$ is a locally soluble normal subgroup of $G$ and hence $S(G)\sigma \leq S(G)$. This result applied to $\sigma^{-1}$ yields the other inclusion. Thus $S(G)\sigma = S(G)$ and hence

3. $S(G)$ is invariant under $P(G)$.

By 8.1.2, a locally soluble group with dual is locally finite. Thus our next result is a partial case of the main theorem of this section.

8.5.3 Theorem (Zacher [1966]). Every locally soluble group with dual is soluble.

Proof. Suppose that the theorem is false and consider a counterexample $G$. Then by 8.5.2, $G'' \neq 1$ is a perfect locally soluble group with dual and we may assume that $G = G''$ is perfect.

Since $G$ is locally soluble, every chief factor $H/K$ of $G$ is abelian (see Robinson [1982], p. 367) and we show that $H/K$ is even central. For this we may assume that $K = 1$ since $G/K$ is also a perfect locally soluble group with dual. Then $H$ is a normal $p$-subgroup of $G$ for some prime $p$ and hence lies in the intersection $O_p(G)$ of all the Sylow $p$-subgroups of $G$. By 6.5.9, every autoprojectivity of $G$ is index preserving and therefore $O_p(G)$ is invariant under $P(G)$. By 8.1.7 and 8.1.10, $O_p(G)$ has a dual and is finite. Thus $H$ is finite and, since $G/C_G(H)$ is isomorphic to a group of automorphisms of $H$, it follows that $G/C_G(H)$ is finite. But by 8.5.2, $G$ has no proper subgroup of finite index; so $C_G(H) = G$, that is, $H/K$ is central.

Thus every chief factor of $G$ is central and this implies that every finitely generated, hence finite, subgroup of $G$ has a central series. Thus $G$ is locally nilpotent and hence it is the direct product of its primary components (see Robinson [1982], p. 342). By 8.1.6 and 8.1.10, these are finite $p$-groups. Since $G$ is perfect, it follows that $G = 1$, a contradiction. \[\square\]
8.5.4 Corollary. If $G$ is a locally finite group and $\delta$ a duality from $G$ to a group $\overline{G}$, then $S(G)$ is a soluble group with dual and $S(G)^\delta$ is perfect.

Proof. By (1), (3), and 8.1.7, $S(G)$ is a locally soluble group with dual, and 8.5.3 implies that $S(G)$ is soluble. Suppose, for a contradiction, that $S(G)^\delta$ is not perfect. Since $\delta$ induces a duality from $G/S(G)$ onto $S(G)^\delta$ and $S(G/S(G)) = 1$, we may assume that $S(G) = 1$. Then $\overline{G}' < \overline{G}$ and hence there exists a subgroup $H$ of prime order of $G$ such that $\overline{G}' \leq H^\delta < \overline{G}$. If $\sigma \in P(G)$, then $\delta^{-1}\sigma\delta \in P(\overline{G})$ and therefore $H^\sigma = (H^\delta)^{\sigma\delta}$ is a projective image of the normal subgroup $H^\delta$ of prime index in $\overline{G}$. By 6.5.3, this projective image contains $\overline{G}'$; thus $H^\sigma \geq \overline{G}'$ for all $\sigma \in P(G)$. Now $L = \bigcup_{\sigma \in P(G)} H^\sigma$ is clearly invariant under $P(G)$ and, by 8.1.1, $L^\delta = \bigcap_{\sigma \in P(G)} H^\sigma \geq \overline{G}'$; by 8.1.7, $\delta$ induces a duality from $L$ onto the soluble group $\overline{G}/L^\delta$. But then 8.3.1 implies that $L$ is soluble, a contradiction since $S(G) = 1$.

The main theorem

We come to the proof of the result announced above.

8.5.5 Theorem (Zacher [1971]). Every locally finite group with dual is soluble.

Again we need several steps to prove this. In contrast to the finite case, however, we shall use the Feit-Thompson Theorem at several points in this proof. First of all, we need the following fact (see Robinson [1982], p. 415):

(4) every infinite locally finite group has an infinite abelian subgroup.

No proof of this is known which avoids using the Feit-Thompson Theorem. Another frequently used result is:

(5) if $G$ is locally finite and $S \leq G$ is such that $o(s) \neq 2$ for all $s \in S$, then $S$ is locally soluble;

indeed, every finitely generated subgroup of $S$ is a finite group of odd order and hence soluble.

In the sequel, let $G$ be a locally finite group and $\delta$ a duality from $G$ to a group $\overline{G}$. We start with the following special case of 8.5.5.

8.5.6 Lemma. If $G$ has a finite Sylow 2-subgroup, $G$ is soluble.

Proof. We suppose that this is false and choose a counterexample $\delta$: $L(G) \to L(\overline{G})$ for which the order of the Sylow 2-subgroups of $G$ is minimal; recall that these Sylow 2-subgroups are conjugate since one of them is finite (see Robinson [1982], p. 413). By 8.4.5, $G$ is infinite. By 8.5.2 and 8.1.6, $\delta$ induces a duality in $G''/S(G'')$ and the Sylow 2-subgroups of this group cannot have larger order than those of $G$. Thus we may assume that $G = G''$ is perfect and, by (2), that $S(G) = 1$; it follows from 8.5.4 that $\overline{G}$ is perfect. Thus

(6) $G$ and $\overline{G}$ are perfect.
For \( c \in G \) of prime order, we define \( X_c = \Omega(C_G(c)) = \langle x \in C_G(c) \mid o(x) \in \mathbb{P} \rangle \). Let \( \sigma \in P(G) \) such that \( \langle c \rangle^\sigma = \langle c \rangle \). By 6.5.9, \( \sigma \) is index preserving. If \( x \in C_G(c) \) such that \( o(x) \in \mathbb{P} \), then \( \langle c, x \rangle \) is either elementary abelian of order \( p \) or \( p^2 \) or cyclic of order \( pq \) for primes \( p \) and \( q \). The same then holds for \( \langle c, x \rangle^\sigma \), and therefore \( \langle c \rangle^\sigma \) centralizes \( \langle c \rangle^\sigma = \langle c \rangle \). Thus \( \langle x \rangle^\sigma \leq X_c \) and, since these elements \( x \) generate \( X_c \), it follows that \( X_c^\sigma \leq X_c \). This result applied to \( \sigma^{-1} \) yields the other inclusion. Thus

\[ (7) \quad X_c \text{ is } P(G)-\text{connected to } \langle c \rangle \text{ and hence } X_c/\langle c \rangle \text{ has a dual,} \]

by 8.4.3. Now suppose, for a contradiction, that every element of \( G \) has prime power order. By (4), \( G \) has an infinite abelian subgroup \( A \) which then has to be a \( p \)-group for some prime \( p \). Moreover, if \( c \in A \) has order \( p \), then \( C_G(c) \) is also a \( p \)-group and hence \( X_c/\langle c \rangle \) is a locally finite \( p \)-group with dual. By 8.1.10, \( X_c \) is finite and, since \( \Omega(A) \leq X_c \), it follows that \( A \) has finite \( p \)-rank. Thus \( A \) is a direct product of finitely many cyclic and quasicyclic groups (see Robinson [1982], p. 107) and, since \( A \) is infinite, there exists a quasicyclic subgroup \( K \) of \( A \); let \( H \leq K \) such that \( |H| = p \). By 1.2.3, every projective image of \( K \) is locally cyclic (in fact, quasicyclic, by Exercises 1.2.1 and 1.2.2). Thus \( H \) is \( P(G) \)-normal in \( K \) and, by 8.4.4, \( L/H \) has a dual where \( L = \bigcup_{u \in H^\delta} K^{\delta u^{-1}} \). Since \( H = H^{\delta u^{-1}} \) is centralized by \( K^{\delta u^{-1}} \) for every \( u \in H^\delta \), we have

\[ L \leq C_G(H) \text{ and hence } L \text{ is a } p \text{-group. Again by 8.1.10, } L/H \text{ is finite, a contradiction since } H \leq K \leq L. \text{ Thus not every element of } G \text{ has prime power order and hence there exists } c \in G \text{ such that} \]

\[ (8) \quad o(c) = q \in \mathbb{P} \text{ and } X_c \text{ is not a } q \text{-group.} \]

Let \( q \) be the smallest prime such that there exists \( c \in G \) satisfying (8). If \( q = 2 \), then \( X_c/\langle c \rangle \) has Sylow 2-subgroups of smaller order than \( G \); the choice of \( G \) implies that \( X_c/\langle c \rangle \) is soluble. If \( q \neq 2 \), then \( X_c \) does not contain elements of order 2; by (5) and (7), \( X_c/\langle c \rangle \) is a locally soluble group with dual and hence is soluble, by 8.5.3. In both cases, by 8.3.1, \( X_c/\langle c \rangle \) is a direct product of finite primary groups and \( P \)-groups. Since \( q \) is the smallest prime involved in \( X_c \), it follows that \( X_c/\langle c \rangle \) has a normal \( q \)-complement \( N/\langle c \rangle \). Let \( Q \) be the set of \( q \)-elements of \( X_c \). If \( x, y \in Q \), then \( \langle c, x, y \rangle \) is a finite subgroup of \( N \) in which \( \langle c \rangle \) is a central Hall subgroup; thus \( \langle c, x, y \rangle = \langle c \rangle \times (Q \cap \langle c, x, y \rangle) \) and hence \( xy^{-1} \in Q \). So \( Q \) is a subgroup of \( N \) and \( N = \langle c \rangle \times Q \). If \( \sigma \in P(G) \) such that \( \langle c \rangle^\sigma = \langle c \rangle \), then by (7), \( X_c^\sigma = X_c \) and hence \( Q^\sigma = Q \), since \( \sigma \) is index preserving. So \( Q \) is \( P(G) \)-connected to \( \langle c \rangle \) and, by 8.4.3, \( Q^\delta \leq \bar{G} \) and \( \delta \) induces a duality from \( Q \) onto \( \bar{Q}^\delta \). The choice of \( q \) implies that the \( q \)-group \( Q \) does not contain elements of order 2 and, by (5), \( Q \) is locally soluble. By 8.5.3 and 8.3.1, \( Q \) and \( \bar{G}/Q^\delta \) are soluble and, since \( \bar{G} \) is perfect, \( Q = 1 \). But then \( X_c \) is a \( q \)-group, contradicting (8).

8.5.7 Lemma. Let \( H \leq G \) such that \( H \) is not locally soluble. Then every primary subgroup of \( C_G(H) \) is finite.

Proof. We suppose the lemma is false and consider a counterexample \( H \leq G \); let \( C = C_G(H) \). Since \( H \) is not locally soluble, there exists a finitely generated subgroup of \( H \) which is not soluble; since \( G \) is locally finite, this subgroup is finite and its
soluble residual $K$ is a nontrivial finite perfect subgroup of $H$. Let $B$ be a maximal normal subgroup of $K$. Then $K/B$ is simple and, by 5.4.9, $B$ is $P(G)$-normal in $K$. By 8.4.4, $A/B$ has a dual where $A = \bigcup_{u \in B^{\delta^{-1}}} K^{u \delta^{-1}}$ is perfect since, by 5.3.4, it is a join of perfect groups. On the other hand, $B$ is a finite normal subgroup of $A$, and so $A/BC_A(B)$ is a finite group with dual and hence is soluble, by 8.4.5. Thus $A = BC_A(B)$ and so $K = B(C_A(B) \cap K) = BC_K(B)$. Then $C_K(B)/(B \cap C_K(B)) \cong K/B$ and $B \cap C_K(B) = Z(C_K(B))$. So if $F$ is the soluble residual of $C_K(B)$, then $F$ is a finite perfect subgroup of $H$ such that $F/Z(F)$ is simple. Since $C_G(H) \leq C_G(F)$, the group $F$ is a counterexample to the lemma and so we may assume that $H$ is a finite perfect group and $H/Z(H)$ is simple.

It follows that $Z(H)$ is $P(G)$-normal in $HC$. For, since $H$ is perfect and the factor group $HC/C \cong H/Z(H)$ is simple, 6.5.4 implies that $H^\sigma \leq (HC)^\sigma$ and $C^\sigma \leq (HC)^\sigma$ for every $\sigma \in P(G)$; hence $Z(H)^\sigma = H^\sigma \cap C^\sigma \leq (HC)^\sigma$. Again by 8.4.4 there exists $W \leq G$ such that $HC \leq W$, $Z(H) \leq W$ and $W/Z(H)$ has a dual. In this group, $H/Z(H)$ is a finite simple subgroup whose centralizer contains $C/Z(H)$; therefore, since $Z(H)$ is finite, this centralizer contains an infinite primary subgroup. Thus $H/Z(H)$ is a counterexample to the lemma and so we finally may assume that

(9) $H$ is a finite simple group.

It follows that $C_G(H)^\sigma = C_G(H^\sigma)$ for every $\sigma \in P(G)$. For, if $X$ is a $p$-subgroup of $C_G(H)$, then, since $H = O_p^*(H)$, 1.6.8 implies that $[H^\sigma, X^\sigma] = 1$. Since $C_G(H)$ is generated by primary subgroups, we obtain that $C_G(H)^\sigma \leq C_G(H^\sigma)$; and if we apply this result to $\sigma^{-1}$ and the simple group $H^\sigma$, we get the other inclusion. This shows, in particular, that $C$ is $P(G)$-connected to $H$ and, since $H \cap C = 1$, 8.4.3 yields that

(10) $C^\delta \leq \overline{G}$.

Let $D = \bigcup_{u \in C^\delta} H^{u \delta^{-1}}$ and put $M = C \cup D$ and $N = C \cap D$. As we have just shown, $H^{u \delta^{-1}}$ is centralized by $C^{u \delta^{-1}} = C$ for all $u \in C^\delta$. Thus $D$ is centralized by $C$; so $N \leq Z(M)$ and $M/N = C/N \times D/N$. Similarly, it is clear that $D^\delta = \bigcap_{u \in C^\delta} (H^\delta)^u$ is invariant under $C^\delta$ and so by (10), $M^\delta = C^\delta \cap D^\delta \leq C^\delta D^\delta = N^\delta$ and the factor group $N^\delta/M^\delta = C^\delta/M^\delta \times D^\delta/M^\delta$. By 8.1.6, $\delta$ induces a duality from $M/N$ onto $N^\delta/M^\delta$ and we claim that

(11) $C^\delta/M^\delta$ and $D^\delta/M^\delta$ are coprime.

To prove this, suppose, for a contradiction, that both groups contain a subgroup of order $p \in \mathbb{P}$. The join of these is elementary abelian of order $p^2$ and therefore contains a subgroup $T^\delta/M^\delta$ of order $p$ which is neither contained in $C^\delta/M^\delta$ nor in $D^\delta/M^\delta$. Thus $T^\delta \cap C^\delta = M^\delta = T^\delta \cap D^\delta$ and hence $T \cup C = M = T \cup D$. Since $[C, D] \leq N$ and $D \leq M$, it follows that $T \cup D$ is normalized by $C$ and by $T$ and hence by $C \cup T = M$. In particular, $T \cap D \leq D$ and $[D/T \cap D]$ is dual isomorphic to $[T^\delta \cup D^\delta/D^\delta] \cong [T^\delta/M^\delta]$. So $D/T \cap D$ is cyclic of order $p$, a contradiction since $D = \bigcup_{u \in C^\delta} H^{u \delta^{-1}}$ is generated by simple groups and hence is perfect. Thus (11) holds.

Now (11) and 8.1.8 imply that $C/N$ and $D/N$ are coprime. Since $H \cap C = 1$, the finite simple group $H$ is isomorphic to a subgroup of $D/N$ and the Feit-Thompson
8.5 Locally finite groups with duals

Theorem implies that $D/N$ has elements of order 2. Thus $C/N$ has none and so, by (5), it is locally soluble; since $N \leq Z(C)$, we conclude that $C$ is locally soluble. Now $\delta$ induces a duality from $C$ onto $G/C^\delta$ and 8.5.3 implies that $C$ is soluble. By 8.3.1, every primary subgroup of $C$ is finite, a final contradiction.

We come to the last step in the proof of Theorems 8.5.5 and 8.2.2.

8.5.8 Lemma. If $G \neq 1$, $G \neq G'$.

Proof. Suppose, for a contradiction, that $G = G'$. By 8.5.4, $S(G)$ is soluble and, since $S(G/S(G)) = 1$, we may assume that $S(G) = 1$. So again by 8.5.4, we have that

(12) $G$ and $\overline{G}$ are perfect.

By 8.5.6, every Sylow 2-subgroup of $G$ is infinite. Let $S \in \text{Syl}_2(G)$ and suppose, for a contradiction, that $S$ has a subgroup of the form $A \times B$ where $A$ and $B$ are infinite elementary abelian or quasicyclic groups; let $H = \bigcup_{x \in A^\delta} B^{\delta x -1}$. By 6.5.9, every automorphism $\sigma$ of $G$ is index preserving. So $(A \times B)^{\sigma}$ is either elementary abelian or a locally finite 2-group with modular subgroup lattice and infinite exponent; by 2.4.15, $(A \times B)^{\sigma}$ is abelian in this case also. It follows that if $x \in A^{\delta}$, then $A = A^{\delta x -1}$ centralizes $B^{\delta x -1}$ and hence $A \leq C_G(H)$. In particular, $A \leq AH$ and, since $H^\delta = \bigcap_{x \in A^\delta} (B^{\delta})^x$ is invariant under $A^\delta$, $(AH)^{\delta} = A^\delta \cap H^\delta \leq A^\delta$. By 8.1.6, $\delta$ induces a duality from $AH/A$ onto $A^\delta/(AH)^{\delta}$. Now $AH/A$ contains the infinite 2-group $AB/A$ and hence, by 8.5.3 and 8.3.1, cannot be locally soluble; it follows that $H$ is not locally soluble. But $C_G(H)$ contains the infinite 2-group $A$, and this contradicts Lemma 8.5.7. The contradiction first of all shows that every abelian subgroup of $S$ has finite
rank and therefore (see Robinson [1982], p. 107) $S$ satisfies the minimal condition for abelian subgroups. So $S$ is a Cernikov group (see Robinson [1982], p. 408), that is, contains a subgroup $E$ of finite index isomorphic to a direct product of quasicyclic groups. Since $S$ is infinite and does not contain subgroups isomorphic to the direct product of two quasicyclic groups, it follows that $E$ is quasicyclic. Thus

(13) $S$ has a quasicyclic subgroup $E$ of finite index.

If $M$ is any group containing a quasicyclic subgroup $E$ of finite index, then for every quasicyclic subgroup $F$ of $M$, the subgroup $E_M \cap F$ has finite index in $F$, and hence $E_M \cap F = F$. Thus $F \leq E$ and then $F = E$; so $E$ is the unique quasicyclic subgroup of $M$. In particular, $E \subseteq S$, and we want to show that $S = N_G(E)$. First of all, if $\sigma \in P(G)$ and $X$ is a cyclic subgroup of $N_G(E)$, then $E$ is of finite index in $M = EX$ and hence is the unique quasicyclic subgroup of $M$. Then $E^{\sigma}$ is the unique quasicyclic subgroup of $M^\sigma$, that is, $X^\sigma \leq N_G(E^\sigma)$. It follows that $N_G(E^\sigma) \leq N_G(E^\sigma)$, and this result for $\sigma^{-1}$ and $E^\sigma$ yields the other inclusion. Thus

(14) $N_G(E^\sigma) = N_G(E^\sigma)$ for all $\sigma \in P(G)$.

In particular, $N_G(E)$ is $P(G)$-connected to $E$. By 8.4.3, $\delta$ induces a duality in $N_G(E)/E$. This group has a finite Sylow 2-subgroup $S/E$ and hence is soluble, by 8.5.6. Then 8.3.1 implies that $N_G(E)/E$ is a direct product of $P$-groups and $p$-groups, and therefore possesses a normal 2-complement $K/E$. Since $\text{Aut} E$ is a 2-group, $K \leq C_G(E)$ and, since $G$ is locally finite, it follows that the set $Q$ of 2'-elements of $K$ is a subgroup of $K$ and $K = E \times Q$. By (14), every $\sigma \in P(G)$ satisfying $E^\sigma = E$ fixes $N_G(E)$; therefore it fixes $Q$ since $\sigma$ is index preserving. Thus $Q$ is $P(G)$-connected to $E$ and, by 8.4.3, $Q \leq G$. By (5), $Q$ is locally soluble; hence $Q$ and $G/Q^\delta$ are soluble, by 8.5.3 and 8.3.1. Since $G$ is perfect, it follows that $Q = 1$. So $K = E$ and

(15) $N_G(E) = S$.

Now let $D$ be the subgroup of order 4 of $E$, and suppose, for a contradiction, that $N_G(D)$ is a 2-group. If $\sigma \in P(G)$ satisfies $D^{\sigma} = D$, then $D$ is a characteristic subgroup of $E^{\sigma} \leq S^{\sigma}$, and hence $D \leq S^{\sigma}$. It follows that $S^{\sigma} \leq N_G(D) = S$ and, similarly, $S^{\sigma^{-1}} \leq S$ so that $S^{\sigma} = S$. Thus $S$ is $P(G)$-connected to $D$ and, by 8.4.3, $S/D$ has a dual; but this contradicts 8.1.10 since $S/D$ is infinite. So we see that $N_G(D)$ is not a 2-group, that is, there exists a subgroup $H$ of prime order $p > 2$ normalizing and hence centralizing $D$. Let $X = H \langle x \in C_G(H)|o(x) = 4 \rangle$ and consider $\sigma \in P(G)$ such that $H^\sigma = H$. By 1.6.7 and since $\sigma$ is index preserving, $\sigma$ maps cyclic subgroups of order 4 of $C_G(H)$ to cyclic subgroups of order 4 of $C_G(H)$, and it follows that $X^{\sigma} = X$. Thus

(16) $X$ is $P(G)$-connected to $H$.

and, by 8.4.3, $\delta$ induces a duality in $X/H$. Clearly, $D \leq X$. Let $T$ be a Sylow 2-subgroup of $X$ containing $D$, and let $S_1 \in \text{Syl}_2(G)$ such that $T \leq S_1$. By (13) and (15) there exists a quasicyclic subgroup $E_1$ of finite index in $S_1$, and $N_G(E_1) = S_1$. So $H \not\leq C_G(E_1)$, but $H \leq C_G(X) \leq C_G(T)$ and hence $E_1 \cap T < E_1$. Since $E_1$ is quasicyclic, it follows that $E_1 \cap T$ is finite. Furthermore, $T/E_1 \cap T$ is isomorphic to a subgroup of $S_1/E_1$ and hence is also finite. Thus $T$ is finite and, by 8.5.6, $X/H$ is soluble. Since $\text{Exp} T \geq 4$, $TH/H$ cannot be contained in a $P$-group. Thus 8.3.1 im-
plies that the Sylow 2-subgroup $TH/H$ is a direct factor of $X/H$. Since $H \leq Z(X)$, we have $TH = T \times H$ and hence $T \unlhd X$. By (16), every $\sigma \in P(G)$ satisfying $H^\sigma = H$ fixes $X$ and hence $T$. So $T$ is $P(G)$-connected to $H$ and, by 8.4.3, $T^\delta \unlhd \bar{G}$. Thus $\delta$ induces a duality from $T$ onto $\bar{G}/T^\delta$ and, by 8.4.5, $\bar{G}/T^\delta$ is soluble. Since $\bar{G}$ is perfect, it follows that $T = 1$; but $D \leq T$, a final contradiction.

Proof of Theorems 8.5.5 and 8.2.2. Let $G$ be a locally finite group with dual. Then by 8.5.2, $G''$ is a perfect locally finite group with dual, and so by 8.5.8, $G'' = 1$. Thus $G$ is soluble and this proves Theorem 8.5.5. The Main Theorem 8.2.2 follows from 8.5.5 and 8.3.1.

Arbitrary groups with duals

In the remainder of this section we give the proof of Theorem 8.2.3. Since Theorem 8.5.1 and Corollary 8.5.2 are just part (a) of this theorem, it remains to prove (b)-(e). Of these, (b)-(d) are immediate consequences of 8.2.2 and (a).

Proof of Theorem 8.2.3. Let $\delta$ be a duality from the group $G$ to the group $\bar{G}$. Then $\delta$ induces a duality from $G/G''$ onto $(G'')^\delta$. Therefore $(G'')^\delta$ has the structure given in 8.2.2 and hence is the join of finite soluble characteristic subgroups. By 8.5.1, $G'' = G_\delta$ and the Zacher-Rips Theorem shows that this group is invariant under $P(G)$. By 8.1.7, $(G'')^\delta \unlhd \bar{G}$ and hence every characteristic subgroup of $(G'')^\delta$ is normal in $\bar{G}$. It follows that $(G'')^\delta \leq \bar{G}^\delta \leq \bar{G}^L=\delta$ and $(G'')^\delta \leq \bar{G}^\delta \leq \bar{G}^L=\delta$. Conversely, by 6.5.17, $\bar{G}^L=\delta$ is invariant under $P(G)$; again by 8.1.7, $N = (\bar{G}^L=\delta)^{-1} \unlhd G$ and $\delta$ induces a duality from $G/N$ onto $\bar{G}^{L-\delta}$. Since $\bar{G}^{L-\delta}$ is locally finite, 8.2.2 implies that $G/N$ is metabelian; thus $N \unlhd G''$ and $\bar{G}^{L-\delta} = N^{\delta} \leq (G'')^{\delta}$. It follows that $(G'')^{\delta} = \bar{G}^{L-\delta} = \bar{G}^\delta = \bar{G}^\delta$. If we apply this result to $\delta^{-1}$, we obtain $(\bar{G}''')^{\delta^{-1}} = \bar{G}^{L-\delta} = \bar{G}^\delta = \bar{G}^\delta$ and so $(G'')^{\delta} = \bar{G}''$. Thus (b) and (c) hold.

By (c), $\delta$ induces a duality from $G'' \cap G^\delta$ onto $\bar{G}^L \cap G^\delta$. Moreover, if $H = G'' N \cap G^\delta$, then $H$ is a locally finite group by a locally finite group (see Robinson [1982], p. 411); hence $H \leq Z(G'')$. Thus $G'' \cap G^\delta \leq Z(G'')$. The reverse inclusion is obvious, so $Z(G'') = G'' \cap G^\delta$ and (d) holds.

Suppose, for a contradiction, that $G''/Z(G'')$ and $G^\delta/Z(G'')$ are not coprime, and let $p$ be a prime such that both groups contain a subgroup of order $p$. Since $G^\delta/Z(G'')$ has the structure given in 8.2.2, there exists a normal subgroup $N$ of $G^\delta$ such that $Z(G'') \leq N \leq G^\delta$ and $G^\delta/N$ is cyclic of order $p$ or nonabelian of order $pq$, $p > q \in \mathbb{P}$. Then $\delta$ induces a duality from $H = G'' G^\delta/N = G'' N \times G^\delta/N$ onto $N^{\delta}/\bar{G}^{L-\delta} \cap \bar{G}^\delta$, and $H'' = G'' N / N$, by (a). Moreover, if $H'' = K/N$, then $K$ is locally finite as an extension of a locally finite group by a locally finite group (see Robinson [1982], p. 411); hence $K \leq (G'' G^\delta)^\delta \leq G^\delta$ and so $H'' = G^\delta/N$. Thus $H$ is a counterexample to (e) and we may assume that $G = H$; that is,

\begin{equation}
G = G'' \times F \text{ where } F = G^\delta \text{ has order } p \text{ or } pq \text{ and } G'' \text{ has a subgroup } A \text{ of order } p.
\end{equation}
Let $B$ be the normal subgroup of order $p$ of $F$ and consider $T = A \times B$. Clearly $T$ is elementary abelian of order $p^2$; therefore it contains a third subgroup $C$ of order $p$. If $B^\delta \leq \overline{G}$, it follows that $T^\delta = A^\delta \cap B^\delta = C^\delta \cap B^\delta \leq A^\delta \cup C^\delta = \overline{G}$. Thus $\delta$ induces a duality from $T$ onto $\overline{G}/T^\delta$ and hence $\overline{G}/T^\delta$ is metabelian. Therefore $\overline{G}^\prime \leq T^\delta$; however, by (c), $F^\delta = \overline{G}^\prime$. It follows that $F^\delta \leq T^\delta$ and hence $T \leq F$, a contradiction since $A \not\leq F$.

Thus $B^\delta$ is not normal in $\overline{G}$. Since $F^\delta = \overline{G}^\prime \leq \overline{G}$, it follows that $B \neq F$ and so $|F| = pq$, $p > q$. Now $\delta$ induces a duality from $F$ onto $\overline{G}/F^\delta$ and so $\overline{G}/F^\delta \in P(2, p)$. Hence there exists a subgroup $Q$ of order $q$ of $F$ such that $Q^\delta \leq \overline{G}$; let $M = A \times F = TQ$. Since $p > 2$, there exist two different subgroups $C$ and $D$ of $T$ which are not normalized by $Q$. It follows that $C \cup Q = D \cup Q = TQ = M$ and hence $M^\delta = C^\delta \cap Q^\delta = D^\delta \cap Q^\delta \leq C^\delta \cup D^\delta = \overline{G}$. Again this implies that $\overline{G}/M^\delta$ is metabelian; hence $F^\delta = \overline{G}^\prime \leq M^\delta$ and so $M \leq F$, a final contradiction.

Exercises

1. (Stonehewer and Zacher [1994]) Let $G$ be a group with dual, $p$ a prime and $P$ the $p$-component of $Z(G^\prime)$.
   (a) If $X$ is a $p$-subgroup of $G^\prime$, show that either $X \leq P$ or $P \leq X$.
   (b) If $G^\prime/Z(G^\prime)$ has a nontrivial $p$-element, show that $P$ is cyclic.

2. Let $G$ be a $p$-group with dual and $p$ a prime.
   (a) Show that $Z(G^\prime) = 1$.
   (b) If $G$ is self-dual, show that either $G$ is finite or $G$ is perfect and has trivial centre.

3. (Foguel [1992]) If $G$ is a locally finite group such that $(Aut G, G)$ satisfies the double centralizer property (see Exercise 8.4.3), show that $G$ is trivial, cyclic of order 3, or the symmetric group on 3 letters.
In this final chapter we study briefly the other four lattices connected with a group which were introduced in §1.1 together with \( L(G) \): the lattice \( \mathfrak{N}(G) \) of normal subgroups, the lattice \( \mathfrak{A}(G) \) of composition subgroups, the centralizer lattice \( \mathfrak{C}(G) \), and the coset lattice \( \mathfrak{R}(G) \). In each case we wish to determine the structure of groups for which the given lattice has special properties and to find out how far a group is determined by this lattice. Since \( \mathfrak{N}(G) \), \( \mathfrak{A}(G) \), and \( \mathfrak{C}(G) \) may be rather small compared with \( L(G) \), the latter problem in these cases can only be tackled under rather strong assumptions on the groups involved, and the results are usually much weaker than those for subgroup lattices.

First we describe the groups \( G \) for which \( \mathfrak{N}(G) \) is directly decomposable, give a criterion for a finite group to have a distributive lattice of normal subgroups, and show that \( \mathfrak{N}(G) \) is complemented if and only if \( G \) is a direct product of simple groups. Then we show that isomorphisms between lattices of normal subgroups map abelian groups to abelian groups, with the obvious exceptions of groups of rank 1. In the remainder of §9.1 we study isomorphisms and dualities between \( \mathfrak{N}(G) \) and \( \mathfrak{N}(\bar{G}) \), where we assume that \( G \) is a finite nilpotent and \( \bar{G} \) a finite soluble group. The main result here is due to Heineken [1965] and states that if in addition \( G \) has only noncyclic Sylow subgroups, and \( c(G) \leq 2 \) or \( \bar{G} \) is nilpotent, then \( G \) is nilpotent and \( |\bar{G}| = |G| \). This theorem has been generalized to many classes of infinite groups.

In the study of \( \mathfrak{A}(G) \) in §9.2 we restrict our attention to finite groups although some of the results hold more generally for groups with a composition series. We determine when \( \mathfrak{A}(G) \) is directly decomposable, show that \( \mathfrak{A}(G) \) is modular if and only if every subnormal section of order \( p^3 \) has modular subgroup lattice, and that \( \mathfrak{A}(G) \) is distributive if and only if every subnormal section of order \( p^2 \) is cyclic. Moreover \( \mathfrak{A}(G) \) is complemented if and only if \( \mathfrak{A}(\bar{G}) \) is complemented. Our main result on isomorphisms \( \varphi: \mathfrak{A}(G) \to \mathfrak{A}(\bar{G}) \) is due to Pazderski [1972] and says that if \( p > 2 \) is a prime and \( O_p(G) \) is not cyclic, then \( O_p(G)\varphi = O_p(\bar{G}) \); similarly \( O^p(G)\varphi = O^p(\bar{G}) \) if \( G/O^p(G) \) is not cyclic. Both assertions also hold for \( p = 2 \) under the additional assumption that \( \bar{G} \), or in the second case \( G \) and \( \bar{G} \), are soluble; these assumptions are needed since \( \mathfrak{A}(\bar{G}) \approx \mathfrak{A}(PTL(2, q^2)) \) for \( 2 < q \in \mathbb{P} \). Finally we study dualities between lattices of subnormal subgroups of finite soluble groups.

In §9.3 we show that every group with distributive centralizer lattice is abelian, and characterize groups \( G \) for which \( \mathfrak{C}(G) \) is directly decomposable. The structure of groups with modular centralizer lattice is not known. However we present the characterization, due to Schmidt [1970c], of finite groups \( G \) for which \( \mathfrak{C}(G) \) is (modular) of length 2 and use it to show that the groups \( SL(2, 2^n) \) are the only nonabelian
finite simple groups with modular centralizer lattice, a result due to Antonov [1987].
Finally we determine those finite groups $G$ for which $\mathcal{C}(G) = L(G)$ or, more generally, in which every subgroup containing the centre is a centralizer.

The study of coset lattices of groups was initiated by Curzio [1953]. Since the atoms of $\mathfrak{R}(G)$ are the sets $\{g\}$ with $g \in G$ and the interval $[G/\{g\}]$ in $\mathfrak{R}(G)$ is isomorphic to $L(G)$, the coset lattice determines rather strongly the structure of $G$.
In particular, every isomorphism $\sigma: \mathfrak{R}(G) \to \mathfrak{R}(\overline{G})$ can be considered as a bijective map from $G$ to $\overline{G}$ preserving cosets; such a map will be called an $R$-isomorphism.
Using our results on projectivities of abelian groups of torsion-free rank $r \geq 2$ and on torsion-free locally nilpotent groups, we prove in §9.4 that every $R$-isomorphism of such a group is an isomorphism or an antiisomorphism. These results are due to Loiko who also showed that the situation is different for mixed abelian groups of torsion-free rank $1$. Gaschütz and Schmidt [1981] introduced the concept of an affinity; this is an $R$-isomorphism $\sigma: G \to \overline{G}$ satisfying $(xH)^\sigma = x^\sigma H^\sigma$ and $(Hx)^\sigma = H^\sigma x^\sigma$ for all $x \in G$, $H \leq G$. In general even such a map need not be an isomorphism, and there exist affinities between nonisomorphic groups. But we show that every affinity of $G$ is an isomorphism if $G$ is generated by elements of infinite order and involutions, or if $Z(G) = 1$, or if $G$ is a finite perfect group.

9.1 Lattices of normal subgroups

We have seen in 2.1.4 that the lattice of normal subgroups is a modular sublattice of the subgroup lattice of the group $G$. Since $\mathfrak{R}(G)$ can be much smaller than $L(G)$, rather different groups may have isomorphic lattices of normal subgroups. We give some examples of this phenomenon.

9.1.1 Examples. Let $G$ be a group.
(a) $\mathfrak{R}(G)$ is a chain of length one if and only if $G$ is simple.
(b) If $G$ is abelian, $\mathfrak{R}(G) = L(G)$. In particular, $\mathfrak{R}(\mathbb{Z}_{pn})$ is a chain of length $n$ for every prime $p$ and $n \in \mathbb{N}$.
(c) For $3 \leq n \neq 4$, $A_n$ is a simple normal subgroup of index 2 in $S_n$ and hence $\mathfrak{R}(S_n)$ is a chain of length 2. Similarly, for every odd prime power $q \geq 5$, $Z(SL(2, q))$ is a normal subgroup of order 2 with simple factor group in $SL(2, q)$ and hence also $\mathfrak{R}(SL(2, q))$ is a chain of length 2. Finally, since $A_4$ and Klein's four group are the only normal subgroups of $S_4$, it follows that $\mathfrak{R}(S_4)$ is a chain of length 3.
(d) For every odd prime $p \geq 5$, $\mathfrak{R}(\text{PG}L(2, p^2)) \simeq \mathfrak{R}(\text{Aut} A_6) \simeq \mathfrak{R}(D_8) \simeq \mathfrak{R}(Q_8) = L(Q_8)$ since all these groups have a unique minimal normal subgroup with factor group elementary abelian of order 4.

We introduce a concept which is quite useful in the study of $\mathfrak{R}(G)$.

$G$-isomorphic normal subgroups

Let $A$ and $B$ be normal subgroups of $G$. A map $\alpha: A \to B$ is a $G$-isomorphism if it is an isomorphism satisfying $(a^g)^\alpha = (a^\alpha)^g$ for all $a \in A$, $g \in G$; $A$ and $B$ are called
9.1 Lattices of normal subgroups

G-isomorphic if there exists a $G$-isomorphism between them. We note some simple properties of this concept.

9.1.2 Lemma. Let $A$ and $B$ be $G$-isomorphic normal subgroups of $G$.
(a) Then $C_G(A) = C_G(B)$.
(b) If $A \trianglelefteq R \trianglelefteq G, B \trianglelefteq S \trianglelefteq G$ and $R \cap S = 1$, then $A \times B \trianglelefteq Z(R \times S)$.
(c) If $A \cap B = 1$, then $A \times B$ is abelian.

Proof. (a) Let $\alpha: A \to B$ be a $G$-isomorphism. If $c \in C_G(A)$ and $b = \alpha'(a) \in B$, then $b' = (\alpha'(a))' = (\alpha'(a)) = a^2 = b$. Thus $c \in C_G(B)$ and hence $C_G(A) \trianglelefteq C_G(B)$. Since $(b^\theta)^{x^{-1}} = ((a^\theta)^x)^{x^{-1}} = a^\theta = ((a^\theta)^x)^y = (b^x)^y$, also $x^{-1}$ is a $G$-isomorphism. It follows that $C_G(B) \trianglelefteq C_G(A)$ and hence that $C_G(A) = C_G(B)$, as desired.
(b) Since $A \cap S = 1$, we have $S \trianglelefteq C_G(A)$; similarly, $R \trianglelefteq C_G(B)$. By (a), $C_G(A) = C_G(B)$ and hence $A \times B$ is centralized by $R \times S$.
(c) Apply (b) with $A = R$ and $B = S$.

We now show that it is possible to decide in $\mathfrak{R}(G)$ whether or not two normal subgroups $A$ and $B$ with trivial intersection are $G$-isomorphic.

9.1.3 Lemma. Let $A, B \trianglelefteq G$ such that $A \cap B = 1$.
(a) If $\alpha: A \to B$ is a $G$-isomorphism, then $C = \{aa^\theta | a \in A\}$ is a normal subgroup of $G$ satisfying $A \times B = A \times C = B \times C$.
(b) Conversely, if there exists a normal subgroup $C$ of $G$ such that $A \times B = A \times C = B \times C$, then $A$ and $B$ are $G$-isomorphic and abelian.

Proof. (a) By 1.6.2, $C$ is a diagonal in $A \times B$ and we only have to show that $C \trianglelefteq G$; then $A \times B = A \times C = B \times C$. So let $g \in G$. Since $\alpha$ is a $G$-isomorphism, $(aa^\theta)^g = a^g(a^\theta)^g \in C$ for all $a \in A$. Thus $C^g \subseteq C$ and hence $C \trianglelefteq G$.
(b) By assumption, $C$ is a diagonal in $A \times B$ and so, by 1.6.2, $C = \{aa^\theta | a \in A\}$ for some isomorphism $\alpha: A \to B$. Let $a \in A, g \in G$. Since $C \trianglelefteq G$, we have $(aa^\theta)^g = a^g(a^\theta)^g \in C$ and hence $(a^\theta)^g = (a^\theta)^g$. Thus $\alpha$ is a $G$-isomorphism. By 9.1.2, $A$ and $B$ are abelian.

If we apply 9.1.3 to minimal normal subgroups, we obtain information about certain intervals in $\mathfrak{R}(G)$. We add an index $N$ to distinguish in our notation between these and intervals in $L(G)$; thus if $S, T \in \mathfrak{R}(G)$ such that $T \trianglelefteq S$, then

$$[S/T]_N = \{X \in \mathfrak{R}(G) | T \leq X \leq S\}.$$ 

Furthermore, recall that $M_n$ is the (modular) lattice of length 2 with $n$ atoms.

9.1.4 Lemma. Let $A$ and $B$ be different minimal normal subgroups of $G$.
(a) If $A$ and $B$ are $G$-isomorphic, they are abelian and $[A \times B/1]_N \cong M_n$ for some cardinal $n \geq 3$.
(b) If $A$ and $B$ are not $G$-isomorphic, then $[A \times B/1]_N \cong M_2$. 

Proof. Since $A$ and $B$ are different minimal normal subgroups, $A \cap B = 1$. As $\mathfrak{N}(G)$ is modular, $[A \times B/1]_N$ has length 2 and therefore is some $M_n$ where $n \geq 2$. By 9.1.3, $A$ and $B$ are $G$-isomorphic if and only if $n \geq 3$. 

Groups with special lattices of normal subgroups

We now study groups whose lattices of normal subgroups have certain special properties. First we use 1.6.1 to characterize those groups $G$ for which $\mathfrak{N}(G)$ is directly decomposable.

9.1.5 Theorem (Curzio ([1964b]). The lattice $\mathfrak{N}(G)$ of normal subgroups of the group $G$ is directly decomposable if and only if $G = H \times K$ where $H \neq 1 \neq K$ and any two nontrivial central factors $X/Y$ of $H$ and $S/T$ of $K$ are coprime (recall that $X/Y$ is a central factor of $H$ if $Y < X < H$ and $[X, H] < Y$).

Proof. Suppose first that $G = H \times K$ has this property. We claim that for every $U \in \mathfrak{N}(G)$,

\[(1) \ U = (U \cap H) \times (U \cap K).\]

Indeed, since $U \trianglelefteq G$ and $[H, K] = 1$, we obtain $[UK \cap H, H] \leq [UK, H] \leq U \cap H$ and $[UH \cap K, K] \leq U \cap K$. Thus if (1) did not hold, then by 1.6.1, $UK \cap H/U \cap H$ and $UH \cap K/U \cap K$ would be isomorphic nontrivial central factors in $H$ and $K$ respectively. But this implies that there exist central factors of the same prime order $p$ in $H$ and $K$, which contradicts our assumption. Thus (1) holds. Now we define maps $\varphi: \mathfrak{N}(G) \rightarrow \mathfrak{N}(H) \times \mathfrak{N}(K)$ and $\psi: \mathfrak{N}(H) \times \mathfrak{N}(K) \rightarrow \mathfrak{N}(G)$ by

\[
\begin{align*}
U^\varphi &= (U \cap H, U \cap K) \\
(V, W)^\psi &= V \times W
\end{align*}
\]

for $U \in \mathfrak{N}(G)$, $V \in \mathfrak{N}(H)$, $W \in \mathfrak{N}(K)$. Then (1) shows that $U^\varphi = U$ and since, trivially, $(V, W)^{\psi \varphi} = ((V \times W) \cap H, (V \times W) \cap K) = (V, W)$, it follows that $\varphi$ and $\psi$ are inverse maps. Thus $\varphi$ is bijective and hence is an isomorphism by 1.1.2. Thus $\mathfrak{N}(G)$ is directly decomposable.

Suppose conversely that $\mathfrak{N}(G) = L_1 \times L_2$ where the $L_i$ are nontrivial lattices. If $O_1, I_1$ and $O_2, I_2$ are least and greatest elements of $L_1$ and $L_2$, respectively, then $H = (I_1, O_2)$ and $K = (O_1, I_2)$ are normal subgroups of $G$ such that $H \cap K = (O_1, O_2) = 1$ and $H \cup K = (I_1, I_2) = G$. Thus $G = H \times K$. Suppose, for a contradiction, that there are nontrivial central factors of $H$ and $K$ which are not coprime. Since an infinite cyclic group has factors of every prime order, this implies that there are central factors $X/Y$ of $H$ and $S/T$ of $K$ of the same prime order $p$. Then $[X \times S, G] = [X, H][S, K] \leq Y \times T$ so that $(X \times S)/(Y \times T)$ is a central elementary abelian subgroup of order $p^2$ in $G/(Y \times T)$. Thus $[(X \times S)/(Y \times T)]_N \simeq M_{p+1}$; but $[(X \times S)/(Y \times T)]_N \simeq [X/Y]_N \times [S/T]_N \simeq M_2$, a contradiction. 

Note that 1.6.5 and 9.1.5 imply that if $L(G)$ is directly decomposable for a group $G$, then so is $\mathfrak{N}(G)$. However, there are groups with $\mathfrak{N}(G)$ decomposable and $L(G)$ indecomposable; see Exercise 1 or simply take $G = S_3 \times C_3$. 

488 Further lattices
The structure of groups with distributive lattice of normal subgroups is not known. For finite groups, we have the following characterization.

9.1.6 Theorem (Pazderski [1987]). The following properties of a finite group $G$ are equivalent.

(a) $\mathcal{N}(G)$ is distributive.

(b) In every factor group $G/N$, any two $G/N$-isomorphic minimal normal subgroups coincide.

(c) In every factor group $G/N$, any two $G/N$-isomorphic normal subgroups coincide.

(d) The socle of every factor group $G/N$ is a direct product of pairwise non-$G/N$-isomorphic minimal normal subgroups.

Proof. Suppose first that $\mathcal{N}(G)$ is distributive. If $A/N$ and $B/N$ were different $G/N$-isomorphic minimal normal subgroups of $G/N$, then by 9.1.4, $[AB/N]_N \cong M_n$ for some $n \geq 3$, impossible in a distributive lattice. Thus (a) implies (b).

Now suppose that (b) holds and that $L_1/N$ and $L_2/N$ are two $G/N$-isomorphic normal subgroups of $G/N$; let $\alpha: L_1/N \to L_2/N$ be a $G/N$-isomorphism. If $L_1 = N$, then $L_2 = N$ and $L_1 = L_2$. So suppose that $L_1 > N$ and let $M_1/N < L_1/N$ be a minimal normal subgroup of $G/N$. Since $\alpha$ is a $G/N$-isomorphism, $(M_1/N)^\alpha = M_2/N$ is a minimal normal subgroup of $G/N$ which is $G/N$-isomorphic to $M_1/N$. By (b), $M_1 = M_2 = M$. Now $\alpha$ induces a $G/M$-isomorphism $\alpha': L_1/M \to L_2/M$ and an obvious induction yields that $L_1 = L_2$. Thus (b) implies (c).

Now suppose that (c) holds. It is well-known that a modular lattice is distributive if and only if it does not contain a sublattice isomorphic to $M_3$ (see Grätzer [1978], p. 59). Thus if $\mathcal{N}(G)$ were not distributive, there would exist distinct normal subgroups $A, B, C$ of $G$ such that $A \cap B = A \cap C = B \cap C = N$ and $A \cup B = A \cup C = B \cup C$. By 9.1.3, $A/N$ and $B/N$ would be $G/N$-isomorphic, which contradicts our assumption (c). Thus (c) implies (a).

Finally, it is well-known that the socle of a group is a direct product of minimal normal subgroups and that any two such decompositions are $G$-isomorphic (see Robinson [1982], pp. 80–84). So (b) and (d) are equivalent.

9.1.7 Remark. There are a number of recent results on groups with distributive lattice of normal subgroups; we can only mention the most interesting of these. For the proofs and for further results we refer the reader to the literature cited.

(a) Let $G$ be a finite group. Pazderski [1987] proves that if $\mathcal{N}(G)$ is distributive, then every factor group of $G$ has a faithful irreducible character. Longobardi and Maj [1986a] show that the converse is true for groups with nilpotent commutator subgroup, but does not hold in general. Their example has supersoluble commutator subgroup.

(b) Again Longobardi and Maj [1986a] show that there are finite soluble groups of arbitrarily large derived length with distributive lattice of normal subgroups.

(c) (Pazderski [1987]) If $G$ is a finite soluble group with $\mathcal{N}(G)$ distributive, then $\text{Aut } G$ is soluble of derived length at most $2k$ where $k$ is the socle length of $G$.

(d) (Maj [1984]) The following properties of an infinite supersoluble group $G$ are equivalent.
(i) $\mathcal{R}(G)$ is distributive.
(ii) Every finite factor group of $G$ has distributive lattice of normal subgroups.
(iii) $G = G' \langle x \rangle$ where $G'$ is finite of odd order, $\mathcal{R}(G/Z(G))$ is distributive, and $Z(G/N)$ is cyclic for every $N \trianglelefteq G$.

Longobardi and Maj [1986b] determine the neutral elements in the lattice of normal subgroups of a finite supersoluble group and prove that if $G$ is an infinite supersoluble group, then $N$ is neutral in $\mathcal{R}(G)$ if and only if $NT/T$ is neutral in $\mathcal{R}(G/T)$ for every finite factor group $G/T$ of $G$.

We mention a result of a different character: every finite distributive lattice is isomorphic to the lattice of normal subgroups of a wreath product of finite non-abelian simple groups (Silcock [1977]) and of a finite soluble group (Pálfy [1986]).

Straightforward applications of Zorn’s Lemma yield the following result.

9.1.8 Theorem. Let $G$ be a group. Then $\mathcal{R}(G)$ is complemented if and only if $G$ is a direct product of simple groups.

Proof. If $G = \text{Dr} \ G\lambda$ with simple groups $G\lambda$ and $N \trianglelefteq G$, Zorn’s Lemma implies that there exists $K \in \mathcal{R}(G)$ maximal with the property that $N \cap K = 1$. If $NK \neq G$, there would exist $\lambda \in \Lambda$ such that $G\lambda \nsubseteq NK$. Since $G\lambda$ is simple, it would follow that $NK \cap G\lambda = 1$ and hence $NKG\lambda = N \times K \times G\lambda$. So $KG\lambda \nsubseteq G$ and $N \cap KG\lambda = 1$, contradicting the maximality of $K$. Thus $NK = G$ and $K$ is a complement to $N$ in $\mathcal{R}(G)$.

Conversely, suppose that $\mathcal{R}(G)$ is complemented and $G \neq 1$. Then we claim that $G$ contains a simple normal subgroup. Indeed, if $1 \neq g \in G$, Zorn’s Lemma implies that there exists $M \in \mathcal{R}(G)$ maximal with the property that $g \notin M$. Thus $M \neq G$; let $N$ be a complement to $M$ in $\mathcal{R}(G)$. Then $G = N \times M$ and if $N$ were not simple, there would exist $N_1 \in \mathcal{R}(G)$ such that $1 < N_1 < N$. Let $K$ be a complement to $N_1$ in $\mathcal{R}(G)$ and let $N_2 = N \cap K$. Then $N = N \cap N_1 K = N_1 (N \cap K) = N_1 N_2$ so that $N_2$ is a complement to $N_1$ in $N$. Thus $G = N_1 \times N_2 \times M$ and the maximality of $M$ implies that $g \in N_1 M \cap N_2 M = M$, a contradiction. Thus $N$ is simple. Now Zorn’s Lemma implies that there exists a maximal direct product $S$ of simple normal subgroups of $G$. If $S \neq G$, then $G = S \times T$ for some $T \neq 1$ and, since $\mathcal{R}(T)$ must be complemented, there exists a simple normal subgroup $N$ of $T$, as we have shown. But this contradicts the maximality of $S$. Thus $S = G$, as desired.

Isomorphisms between lattices of normal subgroups

In the remainder of this section we study isomorphisms and dualities between the lattices of normal subgroups of two groups $G$ and $\overline{G}$. As usual, we want to show that $G$ and $\overline{G}$ must be to some extent similar. The examples in 9.1.1 show that this can only be done under rather restrictive assumptions on $G$ and $\overline{G}$. We shall study the situation where one of the two groups is abelian or nilpotent. First of all we present some simple general properties.
9.1.9 Lemma. Let \( \varphi : \mathfrak{N}(G) \to \mathfrak{N}(\tilde{G}) \) be an isomorphism.
(a) If \( A \leq G \), then \( \mathfrak{N}(G/A) \cong \mathfrak{N}(\tilde{G}/A^\varphi) \).
(b) If \( A \) and \( B \) are \( G \)-isomorphic normal subgroups of \( G \) such that \( A \cap B = 1 \), then \( A^\varphi \) and \( B^\varphi \) are \( \tilde{G} \)-isomorphic and abelian.
(c) If \( N_\lambda \leq G (\lambda \in \Lambda) \) such that \( N = \langle N_\lambda | \lambda \in \Lambda \rangle = \text{Dr } N_\lambda \), then \( N^\varphi = \text{Dr } N_\lambda^\varphi \). If, in addition, all the \( N_\lambda \) are \( G \)-isomorphic and \( |\Lambda| \geq 2 \), then \( N^\varphi \) is abelian.

Proof. (a) This is obvious since \( \mathfrak{N}(G/A) \cong [G/A]_N \).
(b) By (a) of 9.1.3 there exists a normal subgroup \( C \) of \( G \) which is a diagonal in \( A \times B \). Then \( C^\varphi \) has the same property in \( A^\varphi \times B^\varphi \) and now (b) of 9.1.3 yields that \( A^\varphi \) and \( B^\varphi \) are \( \tilde{G} \)-isomorphic and abelian.
(c) Since \( N = \text{Dr } N_\lambda \), we have that \( 1^\varphi = (N_\lambda \cap \langle N_\mu | \lambda \neq \mu \in \Lambda \rangle)^\varphi = N_\lambda^\varphi \cap \langle N_\mu^\varphi | \lambda \neq \mu \in \Lambda \rangle \) and hence \( N^\varphi = \text{Dr } N_\lambda^\varphi \). If \( N_\lambda \) and \( N_\mu \) are \( G \)-isomorphic and \( \lambda \neq \mu \), then by (b), \( N_\lambda^\varphi \) and \( N_\mu^\varphi \) are abelian. Thus \( N^\varphi \) is abelian if \( |\Lambda| \geq 2 \).

It follows immediately from 9.1.9 that if \( G \) is a torsion-free abelian group of rank \( r_0(G) \geq 2 \), then \( \tilde{G} \) is abelian. So \( \varphi \) is a projectivity from \( G \) to \( \tilde{G} \) and by 2.6.10, \( \tilde{G} \cong G \).

We want to show that this result holds for a larger class of abelian groups.

Images of abelian groups

We start with torsion groups; clearly, by 9.1.5, we may restrict our attention to \( p \)-groups. By 9.1.1, we have to assume that \( G \) is not cyclic and the crucial case is handled in the following lemma.

9.1.10 Lemma. Let \( G = R \times S \) be abelian, \( R \cong C_{p^n} (1 \leq n \leq \infty) \) and \( B \leq S \) such that \( |B| = p \). If \( \varphi : \mathfrak{N}(G) \to \mathfrak{N}(\tilde{G}) \) is an isomorphism, then \( \tilde{G} = R^\varphi \times S^\varphi \) and \( R^\varphi \cong R \).

Proof. Clearly \( \tilde{G} = R^\varphi \times S^\varphi \); so we have to show that \( R^\varphi \cong R \). Let \( A \) be the subgroup of order \( p \) of \( R \). Then \( A \) and \( B \) are \( G \)-isomorphic; hence by 9.1.9, \( A^\varphi \) and \( B^\varphi \) are \( \tilde{G} \)-isomorphic and 9.1.2 (b) shows that \( A^\varphi \times B^\varphi \leq Z(\tilde{G}) \). It follows that

\[
L(A^\varphi \times B^\varphi) = [A^\varphi \times B^\varphi/1]_N \simeq [A \times B/1]_N = L(A \times B)
\]

and hence \( A^\varphi \times B^\varphi \) is elementary abelian of order \( p^2 \). Thus

\[
(2) \ |A^\varphi| = p \text{ and } A^\varphi \leq Z(\tilde{G}).
\]

It suffices to show that \( R^\varphi \) is abelian. Indeed, since \( \tilde{G} = R^\varphi \times S^\varphi \), it will then follow that \( L(R^\varphi) = [R^\varphi/1]_N \simeq [R/1]_N = L(R) \) is a chain of length \( n \). And since \( |A^\varphi| = p \), Exercise 1.2.2 (or Theorem 1.2.3) will imply that \( R^\varphi \simeq C_{p^n} \simeq R \), as desired.

For \( n \in \mathbb{N} \), we prove the lemma by induction on \( n \). The induction assumption applied to \( G/A = R/A \times S/A \) yields that \( R^\varphi/A^\varphi \) is cyclic of order \( p^{n-1} \). Since \( A^\varphi \leq Z(R^\varphi) \), it follows that \( R^\varphi \) is abelian.
Further lattices

So let \( n = \infty \) and \( A_i \) be the subgroup of order \( p^i \) of \( R \). Then (2) applied to the isomorphism from \( \mathfrak{I}(G/A_i) \) to \( \mathfrak{I}(\overline{G}/A_i^p) \) induced by \( \varphi \) yields that \( A_{i+1}^p / A_i^p \leq Z(\overline{G}/A_i^p) \) and \( |A_{i+1}^p / A_i^p| = p \). Thus

\[
(3) \ |A_i^p| = p^k \text{ for all } k \in \mathbb{N}.
\]

Now suppose, for a contradiction, that \( Z(R^p) < R^p \). Since \( Z(R^p) \leq \overline{G} \), it follows that \( Z(R^p) = A_j^p \) for some \( j \in \mathbb{N} \). Choose \( a \in A_{j+1}^p \setminus A_j^p \) and define the map \( \sigma: R^p \to R^p \) by \( x^p = [x, a] \) where \( x \in R^p \). Since \( A_{j+1}^p / A_j^p \leq Z(\overline{G}/A_j^p) \), we have \( x^p = [x, a] \in A_j^p = Z(R^p) \) and hence by (1) of \( \S\ 1.5 \), \( (xy)^p = [x, a][y, a] = x^py^p \) for all \( x, y \in R^p \). Thus \( \sigma \) is a homomorphism from \( R^p \) into \( Z(R^p) \); let \( K \) be its kernel. Then the homomorphism theorem implies that \( R^p / K \cong (R^p)^p \) is finite. Since \( a \notin Z(R^p) \), we have \( (R^p)^p \neq 1 \) and hence \( K < R^p \). Every proper normal subgroup of \( R^p \) is normal in \( G \) and therefore of the form \( A_k^p \) for some \( k \in \mathbb{N} \). By (3), \( K \) is finite and hence \( R^p \) is finite. But this is impossible since \( R^p \) has an infinite chain of subgroups \( A_i^p \). Thus \( R^p \) is abelian, as desired.

9.1.11 Theorem (Curzio [1965]). Let \( G \) be an abelian \( p \)-group which is not locally cyclic. If \( \varphi: \mathfrak{I}(G) \to \mathfrak{I}(\overline{G}) \) is an isomorphism, then \( \overline{G} \) is abelian (and isomorphic to \( G \)).

Proof. We use induction on \( n \) to show that the groups \( \Omega_n(G)^p \) are abelian for all \( n \in \mathbb{N} \). Since \( G = \bigcup_{n \in \mathbb{N}} \Omega_n(G) \), it follows that \( \overline{G} = \bigcup_{n \in \mathbb{N}} \Omega_n(G)^p \) is abelian. So \( \varphi \) is a projectivity from \( G \) to \( \overline{G} \) and by 2.6.8, \( \overline{G} \simeq G \).

By assumption, \( \Omega_1(G) \) is not cyclic and hence 9.1.9(c) yields that \( \Omega_1(G)^p \) is abelian. Now suppose that \( n \geq 2 \) and that \( \Omega_{n-1}(G)^p \) is abelian. It is well-known (see Robinson [1982], p. 105) that \( \Omega_n(G) \) is a direct product of cyclic groups and hence \( \Omega_n(G) = R_n \times S_n \) where \( R_n \) is a direct product of \( k \) cyclic groups of order \( p^r \) (\( 0 \leq k \leq \infty \)) and \( S_n \leq \Omega_{n-1}(G) \). Then \( S_n^p \leq \Omega_{n-1}(G)^p \) is abelian and \( \Omega_n(G)^p = R_n^p \times S_n^p \).

If \( k \geq 2 \), then 9.1.9(c) implies that \( R_n^p \) is abelian; therefore so is \( \Omega_n(G)^p \). If \( k = 0 \), we are done. So suppose that \( k = 1 \). Then \( G / \Omega_{n-1}(G) \) has a unique subgroup of order \( p \) and hence is isomorphic to \( C_{p^m} \) (\( 1 \leq m \leq \infty \)). If \( p < \infty \), then \( G = \Omega_{n-1}(G) = R \times S \) where \( R \approx C_{p^m-m} \) and \( S \leq \Omega_{n-1}(G) \). Again \( S^p \leq \Omega_{n-1}(G)^p \) is abelian and by 9.1.10, \( R^p \approx R \); thus \( \overline{G} = R^p \times S^p \) is abelian. So, finally, assume that \( m = \infty \). Then \( G / \Omega_{n-1}(G) \simeq C_p \) and the map \( \tau: G \to G \) defined by \( x^p = x^{p-1} \) is an endomorphism satisfying \( \text{Ker} \tau = \Omega_{n-1}(G) \), and hence \( G^\tau \simeq G / \text{Ker} \tau \simeq C_p \).

Since a divisible subgroup of an abelian group is a direct factor (see Robinson [1982], p. 93), it follows that \( G = G^\tau \times T \) where \( 1 \neq T \leq \Omega_{n-1}(G) \). Again \( T^p \leq \Omega_{n-1}(G)^p \) is abelian and by 9.1.10, \( (G^\tau)^p \) and \( \overline{G} = (G^\tau)^p \times T^p \) are abelian.

We can now also prove the desired result for abelian groups of torsion-free rank at least 2.

9.1.12 Theorem (Brandl [1986]). Let \( G \) be an abelian group which contains two elements \( a \) and \( b \) of infinite order such that \( \langle a \rangle \cap \langle b \rangle = 1 \). If \( \varphi: \mathfrak{I}(G) \to \mathfrak{I}(\overline{G}) \) is an isomorphism, then \( \overline{G} \) is abelian (and isomorphic to \( G \)).
Proof. Let \( r_0(G) \) be the torsion-free rank of \( G \). By assumption, \( r_0(G) \geq 2 \) and the definition of \( r_0(G) \) (or Zorn's Lemma) implies that there exists a free abelian group \( F \) of rank \( r_0(F) = r_0(G) \) such that \( G/F \) is a torsion group. For \( p \in \mathbb{P} \), let \( S_p/F \) be the \( p' \)-component of \( G/F \). If \( F^p = \{ x^p | x \in F \} \), then \( G/F^p \) is also a torsion group; let \( T^p/F^p \) be the \( p' \)-component of \( G/F^p \). Since \( F/F^p \) is a \( p' \)-group and \( T^p/F^p \) a \( p' \)-group, \( F \cap T^p = F^p \). So \( T^p/F \cong T^p/F^p \) is a \( p' \)-group and hence \( T^p \leq S_p \). Since \( FT_p/T_p \cong F/F^p \) and \( r_0(F) \geq 2 \), we see that \( G/T_p \) is a \( p' \)-group which is not locally cyclic. By 9.1.11, \( \overline{G}/T_p^\circ \) is abelian and hence \( \overline{G}/T_p^\circ \leq S_p^\circ \). Now \( F = \bigcap_{p \in \mathbb{P}} S_p^\circ \) and it follows that \( \overline{G}/T_p^\circ \leq \bigcap_{p \in \mathbb{P}} S_p^\circ = (\bigcap_{p \in \mathbb{P}} S_p^\circ)^\circ = F^\circ \).

With \( F \), every \( F^n = \{ x^n | x \in F \} \) (\( n \in \mathbb{N} \)) is free abelian of rank \( r_0(G) \) and \( G/F^n \) is a torsion group. So we may apply the above result with \( F^n \) in place of \( F \) and obtain that \( G' \leq (F^n)^\circ \). Thus \( \overline{G} \leq \bigcap_{n \in \mathbb{N}} (F^n)^\circ = (\bigcap_{n \in \mathbb{N}} F^n)^\circ = 1 \) and \( \overline{G} \) is abelian. Now \( \varphi \) is a projectivity from \( G \) to \( \overline{G} \) and by 2.6.10, \( \overline{G} \cong G \).

As an application of 9.1.12, we get the following result for arbitrary groups \( G \) and \( \overline{G} \).

9.1.13 Corollary. Let \( \varphi : \mathfrak{N}(G) \to \mathfrak{N}(\overline{G}) \) be an isomorphism. If \( r_0(G/G') \geq 2 \), then \( G/G' \cong \overline{G}/\overline{G}' \) and \( (G')^\varphi = \overline{G}' \).

Proof. Since \( \varphi \) induces an isomorphism from \( \mathfrak{N}(G/G') \) onto \( \mathfrak{N}(\overline{G}/(G')^\varphi) \), 9.1.12 implies that \( G/G' \cong \overline{G}/(G')^\varphi \). In particular, \( \overline{G} \leq (G')^\varphi \) and \( r_0(\overline{G}/G') \geq 2 \). So we may apply 9.1.12 to the isomorphism induced by \( \varphi^{-1} \) in \( \mathfrak{N}(\overline{G}/G') \) and obtain that \( G/(G')^\varphi \) is abelian. Thus \( G' \leq (G')^\varphi \) and hence \( (G')^\varphi \leq \overline{G} \). It follows that \( (G')^\varphi = \overline{G}' \), as desired.

The case \( r_0(G) = 1 \) has not been settled yet. For example, it is not known whether a group whose lattice of normal subgroups is isomorphic to that of an infinite cyclic group is abelian (and hence infinite cyclic). Under the additional assumption that \( \overline{G} \) is soluble, however, we get the desired result.

9.1.14 Theorem (Curzio [1965]). Let \( G \) be abelian of torsion-free rank \( r_0(G) = 1 \). If \( \varphi : \mathfrak{N}(G) \to \mathfrak{N}(\overline{G}) \) is an isomorphism and \( \overline{G} \) is soluble, then \( \overline{G} \) is abelian and \( r_0(\overline{G}) = 1 \).

Proof. Assume first that \( G \) is torsion-free. Then it is well-known (see Robinson [1982], p. 112) that \( G \) is isomorphic to a subgroup of \((\mathbb{Q}, +)\) and hence is countable; it follows that there exist infinite cyclic groups \( N_i \) such that \( N_1 \leq N_2 \leq \cdots \) and \( G = \bigcup_{i=1}^{\infty} N_i \). Let \( N_i = \langle x \rangle \). Since \( N_i^\varphi \) is soluble, there exists a characteristic abelian subgroup \( A \) of \( N_i^\varphi \) such that \( A \neq 1 \). Then \( A \leq \overline{G} \) and \( A^\varphi = \langle x^n \rangle \) for some \( n \in \mathbb{N} \). For every prime \( p \) not dividing \( n \), \( N_i^\varphi = \langle x^n \rangle \cup \langle x^p \rangle \); hence \( N_i^\varphi = A \cup \langle x^p \rangle \) and \( N_i^\varphi/\langle x^p \rangle \cong A/A \cap \langle x^p \rangle \) is abelian. Thus \( (N_i^\varphi)^\varphi \leq \bigcap_{p \mid n} \langle x^p \rangle^\varphi = (\bigcap_{p \mid n} \langle x^p \rangle)^\varphi = 1 \) and hence \( N_i^\varphi \) is abelian. Since \( \overline{G} = \bigcup_{i=1}^{\infty} N_i^\varphi \) and \( N_1^\varphi \leq N_2^\varphi \leq \cdots \), it follows that \( \overline{G} \) is abelian. Then \( \varphi \) is a projectivity from \( G \) to \( \overline{G} \) and therefore \( r_0(\overline{G}) = r_0(G) = 1 \).
Now suppose that $G$ is an arbitrary abelian group with $r_0(G) = 1$ and let $T = T(G)$ be the torsion subgroup of $G$. If $x \in G \setminus T$, then $o(x) = \infty$ and hence $\langle x \rangle \cap T = 1$. It follows that $(T \times \langle x \rangle)^o = T^o \times \langle x \rangle^o$, that is, $T^o$ is centralized by $\langle x \rangle^o$. Since $G = \bigcup_{x \in T} \langle x \rangle$, the group $G$ is generated by these $\langle x \rangle^o$ and hence $T^o \leq Z(G)$. By the case already settled, $\overline{G}/T^o$ is torsion-free abelian of rank 1. Therefore if $x, y \in \overline{G}$, $\langle x, y \rangle/\langle x, y \rangle \cap T \simeq \langle x, y \rangle T/T$ is cyclic and, since $\langle x, y \rangle \cap T \leq Z(\overline{G})$, it follows that $\langle x, y \rangle$ is abelian. Thus $\overline{G}$ is abelian, $\varphi$ is a projectivity from $G$ to $\overline{G}$, and $r_0(\overline{G}) = r_0(G) = 1$.

**Images of nilpotent groups**

We now study the situation when $G$ is a finite nilpotent group. Example 9.1.1(d) shows that here we must assume not only that the Sylow subgroups of $G$ are not cyclic but also that the image group $\overline{G}$ is soluble. Then, of course, we can only hope to prove that $\overline{G}$ is nilpotent and not that $\overline{G} \simeq G$. However, the following example shows that even this is not possible.

**9.1.15 Example.** Let $N = \langle x, y \rangle$ be elementary abelian of order 9, and $D$ the subgroup of $\text{Aut } N$ generated by the automorphisms $\alpha$ and $\beta$ of $N$ defined by $x^\alpha = y$, $y^\alpha = x$ and $x^\beta = x^{-1}$, $y^\beta = y$. Then $o(\alpha) = o(\beta) = 2$ and $o(\alpha \beta) = 4$ since $x^{\alpha \beta} = y$ and $y^{\alpha \beta} = x^{-1}$. Thus $D$ is a dihedral group of order 8 and we consider the semidirect product $G = ND$. Then $N$ is the unique minimal normal subgroup of $G$ and $G/N \simeq D$. The dihedral group $G$ of order 16 has a unique minimal normal subgroup $Z(G)$ of order 2 with factor group $G/Z(G) \simeq D$. It follows that $\vartheta(G) \simeq \vartheta(\overline{G})$, but $\overline{G}$ is not nilpotent.

In the above example, $G' = NZ(D)$ is supersoluble and $c(G) = 3$. However, under slightly stronger assumptions, we can prove the desired result. For this we need a simple lemma.

**9.1.16 Lemma.** Let $G$ be a finite $p$-group of class 2. If $G$ has only one minimal normal subgroup $N$, then $G/N$ has at least 2 minimal normal subgroups.

**Proof.** Since $G$ is not abelian, $G/Z(G)$ is not cyclic; so there exist two different minimal subgroups $X/Z(G)$ and $Y/Z(G)$ of $G/Z(G)$. Let $X/Z(G) = \langle xZ(G) \rangle$ and $g \in G$. Then $x^g \in Z(G)$ and $1 = [x^g, g] = [x, g]^g$ since $G' \leq Z(G)$. Therefore $[x, g] \in N$, the unique minimal subgroup of $Z(G)$, and, since this holds for all $g \in G$, we see that $xN \in Z(G/N)$. Thus $X/N = \langle x, Z(G) \rangle/N \leq Z(G/N)$ and, similarly, $Y/N \leq Z(G/N)$. So $Z(G/N)$ is not cyclic since it contains two different subgroups of the same order. It follows that $G/N$ has at least 2 minimal normal subgroups.

**9.1.17 Theorem** (Heineken [1965]). Let $G$ and $\overline{G}$ be finite groups such that $\vartheta(G) \simeq \vartheta(\overline{G})$ and assume that $G$ is nilpotent with all its nontrivial Sylow subgroups noncyclic. If
9.1 Lattices of normal subgroups

(a) \( \bar{G} \) is nilpotent or
(b) \( c(G) \leq 2 \) and \( \bar{G} \) is soluble,
then \( \bar{G} \) is nilpotent and \( |\bar{G}| = |G| \).

Proof. We use induction on \( |G| \). Let \( \varphi: \mathfrak{R}(G) \to \mathfrak{R}(\bar{G}) \) be an isomorphism. Since \( G \) is nilpotent, \( G = G_1 \times \cdots \times G_r \) with nontrivial Sylow subgroups \( G_i \) and by 9.1.9, \( \bar{G} = G_i^p \times \cdots \times G_r^p \). Clearly, all the \( G_i \) and \( G_i^p \) satisfy the assumptions of the theorem and therefore we may assume that \( G \) is a \( p \)-group.

If \( G \) is abelian, then by 9.1.11, \( \bar{G} \) is isomorphic to \( G \) and we are done. So let \( G' \neq 1 \) and \( N \) be a minimal normal subgroup of \( G \). Then \( N \leq Z(G) \) and, since \( G \) is not abelian, \( G/N \) is not cyclic. By induction,

\[ \frac{\bar{G}}{N^p} \] is a \( p \)-group which is not cyclic

since \( G/N \) is not cyclic. Suppose, for a contradiction, that \( \bar{G} \) is not a \( p \)-group. Then since \( \bar{G} \) is soluble, 

(5) \( N^p \) is an elementary abelian \( q \)-group for some prime \( q \neq p \).

If \( M \) were a minimal normal subgroup of \( G \) such that \( M \neq N \), then by (4) \( \bar{G}/M^p \), and hence also \( N^pM^p/M^p \cong N^p \), would be a \( p \)-group, a contradiction. Thus

(6) \( N \) is the unique minimal normal subgroup of \( G \).

By Schur’s Lemma, every irreducible subgroup of \( GL(m, q) \) has cyclic centre and hence

(7) \( Z(\bar{G}/C_{\bar{G}}(N^p)) \) is cyclic.

We show that this implies that \( N^p < C_{\bar{G}}(N^p) \). Indeed, if (b) holds, then by 9.1.16, \( G/N \) has two different minimal normal subgroups. Then \( \bar{G}/N^p \) has the same property and, since it is a \( p \)-group, this implies that its centre is not cyclic. By (7), \( N^p \neq C_{\bar{G}}(N^p) \). Now suppose that (a) holds. Then we claim that \( \bar{G}' \leq C_{\bar{G}}(N^p) \). Indeed, this is clear if \( N^p \cap \bar{G}' = 1 \); and if \( N^p \cap \bar{G}' \neq 1 \), then \( N^p \cap Z(\bar{G}') \neq 1 \) by a well-known property of the nilpotent group \( \bar{G}' \). Since \( N^p \) is a minimal normal subgroup of \( \bar{G} \), it follows that \( N^p \leq Z(\bar{G}') \). Thus \( \bar{G}' \leq C_{\bar{G}}(N^p) \); hence \( \bar{G}/C_{\bar{G}}(N^p) \) is abelian and therefore cyclic, by (7). Since \( \bar{G}/N^p \) is not cyclic, \( N^p \neq C_{\bar{G}}(N^p) \).

Thus in both cases, \( N^p < C_{\bar{G}}(N^p) \) and hence by (4) and (5), \( C_{\bar{G}}(N^p) = N^p \times P \) for some nontrivial \( p \)-group \( P \). Since \( P \) is a characteristic subgroup of \( C_{\bar{G}}(N^p) \leq \bar{G} \), it follows that \( P \subseteq \bar{G} \) and hence \( P^{p^{-1}} \leq G \), contrary to (6). This contradiction shows that \( \bar{G} \) is a \( p \)-group and then \( |\bar{G}| = p^n = |G| \) where \( n \) is the length of \( \mathfrak{R}(G) \).

Theorem 9.1.17(a) had been proved by Curzio [1962] under the stronger assumption that \( \bar{G} \) is supersoluble. If \( c(G) = 2 \) in 9.1.17, however, even the assumption that \( \bar{G} \) is soluble is rather strong. Using 9.1.16, it is not difficult to show that Example 9.1.1(d) is "worst possible" in this situation; that is, if \( G \) is a \( p \)-group of class 2 and \( \bar{G} \) is not a \( p \)-group, then \( \bar{G} \) has a unique minimal normal subgroup \( N^p \) and \( |\bar{G}/N^p| = |G/N| \) (see Exercise 11). Much deeper is the result of Longobardi and Maj [1987] that if \( G \) and \( \bar{G} \) are finite \( p \)-groups with \( \mathfrak{R}(G) \simeq \mathfrak{R}(\bar{G}) \) and \( c(G) = 2 \), then \( c(\bar{G}) \leq 3 \). An example in which \( c(\bar{G}) = 3 \) is given in Exercise 12.
Remark. Heineken's theorem has been generalized to many classes of infinite groups. We mention some of these results; for the proofs and for further results in this direction we refer the reader to the literature cited. So let $G$ and $\overline{G}$ be groups such that $\mathcal{N}(G) \cong \mathcal{N}(\overline{G})$ and assume that $G$ is not locally cyclic.

(a) (Franchetta and Tuccillo [1976]) Let $G$ be a hypercentral $p$-group with the following property.

8) If $G' \neq 1$, there exists $N \leq G$ such that $N \leq G'$ and $|G'|/N| = p$.

If $\overline{G}$ is hypercentral, then $\overline{G}$ is a hypercentral $p$-group such that $|\overline{G}| = |G|$.

The additional assumption (8), in fact, is needed; indeed, if $G = N\langle u \rangle$ and $\overline{G} = M\langle v \rangle$ with $N \cong C_{2^k}$, $M \cong C_p$ $(p > 2)$, $u$ and $v$ involutions inverting $N$ and $M$ respectively, then $G$ and $\overline{G}$ have isomorphic lattices of normal subgroups. Here $G$ is a hypercentral 2-group and $G' = N$ has no subgroup of index 2.

(b) (de Giovanni and Franciosi [1985]) If $G$ is a nilpotent $p$-group and $G'$ is hypercentral, then $\overline{G}$ is a hypercentral $p$-group such that $|\overline{G}| = |G|$.

(c) (Longobardi and Maj [1987]) If $G$ is a nilpotent $p$-group of class 2 and $\overline{G}$ is soluble, then $\overline{G}$ is a nilpotent $p$-group of class at most 3.

(d) (de Giovanni and Franciosi [1985]) Let $G$ be a torsion-free nilpotent group. If $G$ is hypercyclic or if $G$ is finitely generated and $\overline{G}$ hypercentral, then $\overline{G}$ is torsion-free nilpotent and $c(\overline{G}) = c(G)$.

(e) (Brandl [1986]) If $G$ is a finitely generated torsion-free nilpotent group of class 2, then so is $\overline{G}$.

Dualities

Results similar to those for isomorphisms hold for dualities between lattices of normal subgroups. Again we consider only finite nilpotent groups $G$, but now we assume that $\overline{G}$ is supersoluble; recall that then (see Robinson [1982], pp. 145–146)

9) $\overline{G}$ has nilpotent commutator subgroup and normal subgroups of order $r$ and of index $s$ where $r$ is the largest and $s$ the smallest prime dividing $|\overline{G}|$.

9.1.19 Lemma. Let $G$ be a noncyclic finite $p$-group, $\overline{G}$ a finite supersoluble group and $\delta: \mathcal{N}(G) \to \mathcal{N}(\overline{G})$ a duality.

(a) If $Z(G)$ is not cyclic, $|\overline{G}| = |G|$.

(b) If $Z(G)$ is cyclic, then $\overline{G}$ is a $p$-group and $\overline{G}/\overline{G}'$ a cyclic $q$-group, $p > q \in \mathbb{P}$.

Proof. Since $G$ is not cyclic, $G/\Phi(G)$ is elementary abelian of order $p^n$ where $n \geq 2$. So if $M = \Phi(G)^k$, then $[M/1]_N$ is dual and hence also isomorphic to $[G/\Phi(G)]_N \cong L(G/\Phi(G))$. By 9.1.4, $M = M_1 \times \cdots \times M_n$ with $\overline{G}$-isomorphic minimal normal subgroups $M_i$ of $G$. Since $\overline{G}$ is supersoluble, $|M_i| = r$ for some prime $r$ and an element $g \in \overline{G}$ induces the same power in every $M_i$. Thus every subgroup of $M$ is normal in $\overline{G}$ and so $[M/1]_N = L(M)$. It follows that $r = p$ and $|M| = p^n$.

(a) Now if $Z(G)$ is not cyclic, then the product $S$ of all the minimal normal subgroups of $G$ is an elementary abelian central subgroup of order $p^m$ of $G$ where $m \geq 2$. 


Therefore \([\overline{G}/S^k] \cong [S/1] = L(S)\) and by 9.1.4, as above, \(\overline{G}/S^k\) is elementary abelian of order \(p^k\). Every maximal normal subgroup of \(\overline{G}\) contains \(S^k\) and therefore has index \(p\) in \(\overline{G}\), every minimal normal subgroup of \(\overline{G}\) is contained in \(M\) and therefore has order \(p\). By (9), \(\overline{G}\) is a \(p\)-group and then \(|\overline{G}| = p^k = |G|\) where \(k\) is the length of \(\mathfrak{N}(G)\).

(b) Since \(Z(G)\) is cyclic, \(G\) has a unique minimal normal subgroup \(N\) and \(N^p\) is the unique maximal normal subgroup of \(\overline{G}\). Thus \(\overline{G}/G'\) is an abelian group with only one maximal subgroup and hence is a cyclic \(q\)-group for some prime \(q\). By (9), \(G'\) is nilpotent and hence is a \(p\)-group since every minimal normal subgroup of \(\overline{G}\) has order \(p\). If \(p = q\), then \(\overline{G}\) is cyclic since it has only one maximal normal subgroup. But \(M\) is elementary abelian of order \(p^n\), \(n \geq 2\), a contradiction. Thus \(p \neq q\) and then by (9), \(p > q\).

Note that if \(G\) is a nonabelian group of order \(p^3\) and \(\overline{G}\) a \(P\)-group of order \(p^2q\), then \(\mathfrak{N}(\overline{G})\) is dual to \(\mathfrak{N}(G)\). Thus case (b) in Lemma 9.1.19 actually occurs.

9.1.20 Theorem (Curzio [1962]). Let \(G\) be a finite nilpotent group all of whose nontrivial Sylow subgroups have noncyclic centre. If \(\overline{G}\) is a finite supersoluble group and \(\delta: \mathfrak{N}(G) \to \mathfrak{N}(\overline{G})\) is a duality, then \(\overline{G}\) is nilpotent and \(|\overline{G}| = |G|\).

**Proof.** Since \(G\) is nilpotent, \(G = G_1 \times \cdots \times G_r\) with nontrivial Sylow subgroups \(G_i\). Then, as in 8.1.8, \(\overline{G} = \overline{G}_1 \times \cdots \times \overline{G}_r\) where \(\overline{G}_i = \bigcup_{j \neq i} G_j\). So \(\delta\) induces a duality from \(\mathfrak{N}(G_i/\overline{G}_i) \cong \mathfrak{N}(G_i)\) onto \(\mathfrak{N}(\overline{G}_i)\) and by (a) of 9.1.19, \(|\overline{G}_i| = |G_i|\). Thus \(\overline{G}\) is nilpotent and \(|\overline{G}| = |G|\).

Theorem 9.1.20 has also been generalized to infinite groups; see Franciosi [1981] and de Giovanni and Franciosi [1986].

**Exercises**

1. (Curzio [1964b]) (a) Let \(G\) be an infinite supersoluble group. If \(\mathfrak{N}(G)\) is directly decomposable, show that \(G = H \times K\) where \(H\) is infinite and \(K\) is a finite group of odd order.

(b) Construct an infinite supersoluble group for which \(\mathfrak{N}(G)\) is directly decomposable. (Note that by 1.6.5 and (a), \(L(G)\) cannot be directly decomposable.)

2. Let \(G\) be a finite group.

(a) (Curzio [1957b]) If any two normal subgroups of \(G\) have different order, show that \(\mathfrak{N}(G)\) is distributive.

(b) Give an example of a group \(G\) with \(\mathfrak{N}(G)\) distributive having two normal subgroups of the same order.

3. (Curzio [1964b]) Let \(G\) be a supersoluble group. Show that \(\mathfrak{N}(G)\) is a chain if and only if \(G\) is either a cyclic \(p\)-group or a group of order \(p^nq^m\) with cyclic Sylow subgroups and trivial centre (\(p\) and \(q\) primes, \(p \neq q\)).

4. (Longobardi and Maj [1986a]) Let \(G\) be a finite group and \(A, B \leq G\) such that \((|A|, |B|) = 1\). If \(\mathfrak{N}(G/A)\) and \(\mathfrak{N}(G/B)\) are distributive, show that \(\mathfrak{N}(G)\) is distributive.
5. (Longobardi and Maj [1986a]) Let $G = P\langle x \rangle$ be a finite supersoluble group, $P$ a normal Sylow $p$-subgroup and $P \cap \langle x \rangle = 1$. Show that $\mathcal{R}(G)$ is distributive if and only if $\langle a \rangle^p = \langle b \rangle^p$ for all $a, b \in P$ for which there exists $r \in \mathbb{Z}$ such that $a^x = a^r$ and $b^x = b^r$.

6. (Maj [1984]) If $G$ is an infinite supersoluble group, show that $\mathcal{R}(G)$ is distributive if and only if $\mathcal{R}(G/N)$ is distributive for every finite factor group $G/N$ of $G$. (Hint: First show that this condition implies that $G = G' \langle x \rangle$ where $G'$ is finite of odd order.)

7. Show that $\mathcal{R}(G)$ is a Boolean algebra (that is, it is distributive and complemented) if and only if $G$ is a direct product of simple groups such that no two abelian factors are isomorphic.

8. (Zitarosa [1952]) If $G$ is a finite nilpotent group, show that $N$ is a neutral element in $\mathcal{R}(G)$ if and only if $N$ is the unique normal subgroup of its order in $G$.

9. (Longobardi and Maj [1986b]) Let $G$ be a finite group with normal Sylow $p$-subgroup $P$. Show that $P$ is a neutral element of $\mathcal{R}(G)$ and that $N \in \mathcal{R}(G)$ is neutral in $\mathcal{R}(G)$ if and only if $N \cap P$ and $NP/P$ are neutral elements in $\mathcal{R}(G)$ and $\mathcal{R}(G/P)$, respectively.

10. (Longobardi and Maj [1986b]) If $G$ is an infinite supersoluble group and $N$ a neutral element in $\mathcal{R}(G)$, show that either $N$ or $G/N$ is finite.

11. (Brandi [1986]) Let $G$ and $\bar{G}$ be finite groups, $G$ a $p$-group of class 2 and suppose that $\mathcal{R}(\bar{G}) \simeq \mathcal{R}(G)$.
   (a) If $Z(G)$ is not cyclic, show that $|\bar{G}| = |G|$.
   (b) If $Z(G)$ is cyclic and $N$ is the (unique) minimal normal subgroup of $G$, show that $|\bar{G}/N^p| = |G/N|$.

12. (Heineken [1965]) Let $p > 2$, $G = \langle x, y, z | x^{p^2} = y^{p^2} = z^{p^2} = [x, z] = [y, z] = 1, [x, y] = z \rangle$ and let $\bar{G}$ be the group with the same defining relations except that $[x,z] = 1$ is replaced by $[x,z] = z^p$. Show that $\mathcal{R}(G) \simeq \mathcal{R}(\bar{G})$, $c(G) = 2$ and $c(\bar{G}) = 3$.

### 9.2 Lattices of subnormal subgroups

We have seen in § 1.1 that the set $\mathcal{R}(G)$ of all composition subgroups of a group $G$ is a sublattice of $L(G)$ and that if $G$ has a composition series, the composition subgroups coincide with the subnormal subgroups of $G$. In this section we are going to study the lattice $\mathcal{R}(G)$, but mainly for finite groups. Since in this case the term "subnormal subgroup" is more common, we shall usually speak of the lattice of subnormal subgroups of $G$. Some of the results also hold in the more general situation where $G$ has a composition series, but in most cases it is not known what happens for arbitrary groups.

### General properties of subnormal subgroups

Recall that $S \trianglelefteq G$ if and only if there exist subgroups $S_i$ of $G$ ($i = 0, \ldots, n$) such that

1. $S = S_0 \trianglelefteq S_1 \trianglelefteq \cdots \trianglelefteq S_n = G$;
the smallest integer \( n \) for which there exists such a chain (1) is called the defect of \( S \) in \( G \). If \( H \leq G \) and (1) holds, then \( S \cap H = S_0 \cap H \leq S_1 \cap H \leq \cdots \leq S_n \cap H = H \), that is \( S \cap H \trianglelefteq H \). In particular, \( S \trianglelefteq H \) if \( S \trianglelefteq G \) and \( S \leq H \leq G \). It follows that

(2) \( S \trianglelefteq H \) if \( S, H \in \mathcal{R}(G) \) and \( H \) covers \( S \) in \( \mathcal{R}(G) \).

It is obvious that \( S \trianglelefteq H \trianglelefteq G \) implies \( S \trianglelefteq G \) and that if \( N \trianglelefteq G \) and \( N \leq S \leq G \), then \( S \trianglelefteq G \) if and only if \( S/N \trianglelefteq G/N \). So we have the following basic property of the lattice of subnormal subgroups of a group \( G \) with a composition series.

(3) If \( N \leq H \leq G \), \( H \trianglelefteq G \) and \( N \trianglelefteq H \), then \([H/N]_\mathcal{R} \cong \mathcal{R}(H/N) \).

Here, for arbitrary \( S, T \in \mathcal{R}(G) \) such that \( T \leq S \), we write

\[
[S/T]_\mathcal{R} = \{X \trianglelefteq G | T \leq X \leq S\}
\]

for the interval in \( \mathcal{R}(G) \).

Now let \( G \) be finite, \( \pi \) a set of primes and \( S \) satisfy (1). Then \( O_\pi(S_i) \) is a characteristic subgroup of \( S_i \trianglelefteq S_{i+1} \) and hence a normal \( \pi \)-subgroup of \( S_{i+1} \). Thus \( O_\pi(S_i) \leq O_\pi(S_{i+1}) \) and so, by induction,

(4) \( O_\pi(S) \leq O_\pi(G) \).

In particular, \( S \leq O_\pi(G) \) if \( S \) is a \( \pi \)-subgroup of \( G \). In just the same way we see that if \( S \) is soluble, then \( S \leq G^G \), the soluble radical of \( G \). It follows that \( S^G \leq G^G \) and so we have:

(5) If \( S \) is a soluble subnormal subgroup of \( G \), then \( S^G \) is soluble.

Dually, suppose that \( N \trianglelefteq G \) and \( G/N \) is a \( \pi \)-group. Then \( O^\pi(G) \leq N \) and \( N/O^\pi(G) \) is a \( \pi \)-group; so \( O^\pi(N) \leq O^\pi(G) \). On the other hand, \( O^\pi(N) \) is a characteristic subgroup of \( N \trianglelefteq G \) and hence a normal subgroup of \( G \) with factor group a \( \pi \)-group. Thus \( O^\pi(G) \leq O^\pi(N) \) and then \( O^\pi(N) = O^\pi(G) \). This generalizes to a subnormal subgroup \( S \) whose index in \( G \) is a \( \pi \)-number, that is, is divisible only by primes in \( \pi \).

(6) If \( S \trianglelefteq G \) and \( |G:S| \) is a \( \pi \)-number, then \( O^\pi(S) = O^\pi(G) \).

Indeed, for the \( S_i \) in (1), \( O^\pi(S) = O^\pi(S_i) = \cdots = O^\pi(S_n) = O^\pi(G) \). Clearly, (4) implies the following property which we, in fact, proved in 6.2.15 for arbitrary groups \( G \).

(7) If \( S \) is a subnormal \( \pi \)-subgroup of \( G \), then \( S^G \) is a \( \pi \)-group.

It follows that

(8) \([S, T] = 1 \) if \( S \) and \( T \) are coprime subnormal subgroups of \( G \).

Indeed, \([S, T] \leq S^G \cap T^G = 1 \) since \( S^G \) is a \( \pi \)-group and \( T^G \) a \( \pi' \)-group for a suitable set \( \pi \) of primes. Less trivial is the following result of Wielandt.

(9) Let \( S, T \trianglelefteq G \) such that \( S \cap T = 1 \). If \( S \) is a nonabelian simple group, then \([S, T] = 1 \).
Proof. Suppose that (9) is wrong and choose a counterexample $S$, $T$ for which the defect $d$ of $S$ in $J = \langle S, T \rangle$ is minimal; let $S = S_0 \leq \cdots \leq S_d = J$. If $d \leq 1$, then $S \leq J$ and $[S, T] \leq S$. Since $[S, T] \neq 1$ and $S$ is simple, it follows that $S = [S, T]$, so that $S \leq T^J$ and $T^J = J$. Therefore $T = J$ by subnormality of $T$, and this implies $S = S \cap T = 1$, a contradiction. Thus $d \geq 2$ so that $S \neq S'$ for some $t \in T$. Since $S \cap S' \leq S$ and $S$ is simple, $S \cap S' = 1$. Now $S' \leq S_{d-1}$ and the minimality of $d$ yields $[S, S'] = 1$. So for any $x, y \in S$, by (1) of § 1.5,

$$1 = [x, y'] = [x, y[y, t]] = [x, [y, t]][x, y]^{[y, t]};$$

since $[S, T] \leq J$, it follows that $[x, y] \in [S, T]$. Thus $S' \leq [S, T]$; but $S = S'$ since $S$ is nonabelian simple and so $S \leq [S, T]$. As before this leads to $T^J = J$ and the contradiction $S = 1$.

Again let $S$ be a nonabelian simple subnormal subgroup of $G$. By (9), any two different conjugates of $S$ centralize each other and hence $S^s \leq S^g = \langle S^g | g \in G \rangle$ for all $x \in G$. By Zorn's Lemma, $S^G$ is the direct product of some of these $S^s$. Thus we have shown:

(10) If $S \leq G$ and $S$ is a nonabelian simple group, then $S^G$ is a direct product of conjugates of $S$.

It is easy to see that $S^G$ is also a minimal normal subgroup of $G$. Note that neither this nor any of properties (9) and (10) in general holds if $|S|$ is a prime; this is shown by any nonnormal subgroup $S$ of order $p$ of a finite $p$-group $G$. We discuss some further examples.

9.2.1 Examples. Let $G$ be a finite group.

(a) $\mathcal{R}(G)$ is a chain of length one if and only if $G$ is simple. (Note that for $p \in \mathbb{P}$, $\mathcal{R}(C_p \times C_p)$ is also a chain of length 1.)

(b) If $G$ is nilpotent, every subgroup of $G$ is subnormal and hence $\mathcal{R}(G) = L(G)$. In particular, $\mathcal{R}(C_{p^n})$ is a chain of length $n$ for every prime $p$ and $n \in \mathbb{N}$.

(c) The unique maximal normal subgroup of $S_4$ is $A_4$ and that of $A_4$ is $V_4$. So we get the lattices $\mathcal{R}(G)$ in Figure 25 for $G = Q_8$, $A_4$, and $S_4$. Now let $G = Q_8C_3$ be the semidirect product of $Q_8$ by a subgroup of order 3 of its automorphism group.
9.2 Lattices of subnormal subgroups

C₃ permutes transitively the subgroups of order 4 of Q₈ and hence G has no normal subgroup of index 2. Thus Q₈ is the unique maximal normal subgroup of G and R(G) consists of G and the subgroups of Q₈.

(d) Finally, as in 9.1.1 we see that for 3 ≤ n ≠ 4 and every odd prime power q ≥ 5, R(Sₙ) ≅ R(SL(2, q)) is a chain of length 2; furthermore, for every odd prime p ≥ 5, R(ΠL(2, p²)) ≅ R(Aut A₆) ≅ R(Q₈) = L(Q₈).

Groups with special lattices of subnormal subgroups

We now study groups whose lattices of composition subgroups have certain special properties. First we use 1.6.1 to characterize those groups G with composition series for which R(G) is directly decomposable; note the similarity to Theorem 9.1.5.

9.2.2 Theorem (Tamaschke [1961]). Let G be a group with a composition series. Then R(G) is directly decomposable if and only if G = H × K where H ∩ K and no abelian composition factor of H is isomorphic to a composition factor of K.

Proof. Suppose first that G = H × K has this property. We claim that for every U ∈ R(G),

(11) U = (U ∩ H) × (U ∩ K).

Indeed, let U = Uₙ ≤ Uₙ₋₁ ≤ ⋯ ≤ U₀ = G and suppose, for a contradiction, that (11) does not hold for U. Since (11) is trivially satisfied for U₀ = G, there exists a smallest integer k such that (11) does not hold for Uₖ. We may suppose that U = Uₖ so that U ≤ Uₖ₋₁ = S × T where S = Uₖ₋₁ ∩ H and T = Uₖ₋₁ ∩ K. By 1.6.1, UT ∩ S/U ∩ S and US ∩ T/U ∩ T are nontrivial isomorphic factors in S ≤ H and T ≤ K, respectively. Since U ≤ S × T, we have [UT ∩ S, S] ≤ [UT, S] ≤ U ∩ S, so UT ∩ S/U ∩ S is abelian, as a central factor in S. Since U and S × T are subnormal subgroups of G, it follows that UT ∩ S ≤ H and US ∩ T ≤ K. Thus a composition factor of UT ∩ S/U ∩ S is an abelian composition factor of H which is isomorphic to a composition factor of K, a contradiction. This proves (11).

Suppose conversely that R(G) = L₁ × L₂ where the Lᵢ are nontrivial lattices. If O₁, I₁ and O₂, I₂ are least and greatest elements of L₁ and L₂, respectively, then H = (I₁, O₂) and K = (O₁, I₂) are subnormal subgroups of G such that H ∩ K = (O₁, O₂) = 1 and H ∪ K = (I₁, I₂) = G. Since H is the unique complement of K in R(G), every (inner) automorphism of G fixing K also fixes H. It follows that K ≤ N_G(H) and so H ≤ G. Similarly, K ≤ G and hence G = H × K. If X/Y and S/T were composition factors of the same prime order p in H and K, respectively, then as in the proof of Theorem 9.1.5, (X × S)/(Y × T) would be an elementary abelian factor of order p² in G and, by (3), [(X × S)/(Y × T)]ₖ ≅ Mₚ₊₁, a contradiction. Thus H and K have no isomorphic abelian composition factors.

Next we study finite groups with modular and distributive lattices of subnormal subgroups. Here we have two similar results.
9.2.3 Theorem (Zappa [1956b]). The following properties of the finite group $G$ are equivalent.

(a) $\mathcal{R}(G)$ is modular.
(b) If $T \leq S \leq G$ and $S/T$ is a $p$-group, $p$ a prime, then $L(S/T)$ is modular.
(c) If $T \leq S \leq G$ and $|S/T| = p^3$, $p$ a prime, then $L(S/T)$ is modular.

Proof. If $\mathcal{R}(G)$ is modular and $T \leq S \leq G$ such that $S/T$ is a $p$-group, then by (3), $L(S/T) = \mathcal{R}(S/T) \simeq [S/T]_K$ is modular. Thus (a) implies (b), while it is trivial that (b) implies (c).

Now suppose that $G$ satisfies (c). By 2.1.8, $\mathcal{R}(G)$ is lower semimodular. We show that $\mathcal{R}(G)$ is also upper semimodular; then by 2.1.10, $\mathcal{R}(G)$ is modular and (c) implies (a). For this, since $\mathcal{R}(G)$ is finite, it suffices to show that if $H, K \in \mathcal{R}(G)$ such that $H$ and $K$ cover $H \cap K$, then $H \cup K$ covers $H$ (see Grätzer [1978], p. 173). By (2), $H \cap K \leq H \cup K$ and by (3), we may assume that $G = H \cup K$ and $H \cap K = 1$. Then $H$ and $K$ are minimal subnormal subgroups of $G$, hence simple groups, and we claim that $HK = KH$. Indeed, this follows from (9) if $H$ or $K$ is nonabelian, and from (8) if $|H|$ and $|K|$ are different primes. And if $|H| = |K| = p \in \mathbb{P}$, then by (4), $H \cup K$ is a $p$-group. Our assumption implies that every section of order $p^3$ of $H \cup K$ has modular subgroup lattice. By 2.3.3, $H \cup K$ is an $M$-group and by 2.3.2, $HK = KH$, as desired. Now if $X \in \mathcal{R}(G)$ such that $H \leq X \leq HK$, then $X = H(X \cap K)$ and, since $K$ is simple, $X \cap K = 1$ or $X \cap K = K$. Thus $X = H$ or $X = HK$ and so $HK$ covers $H$ in $\mathcal{R}(G)$.

9.2.4 Theorem (Zacher [1957]). The following properties of the finite group $G$ are equivalent.

(a) $\mathcal{R}(G)$ is distributive.
(b) If $T \leq S \leq G$ and $S/T$ is a $p$-group, $p$ a prime, then $S/T$ is cyclic.
(c) If $T \leq S \leq G$ and $|S/T| = p^2$, $p$ a prime, then $S/T$ is cyclic.

Proof. If $\mathcal{R}(G)$ is distributive and $T \leq S \leq G$ such that $S/T$ is a $p$-group, then by (3), $L(S/T) = \mathcal{R}(S/T) \simeq [S/T]_K$ is distributive and hence $S/T$ is cyclic by 1.2.4. Thus (a) implies (b) and again (b) clearly implies (c).

Now suppose that $G$ satisfies (c). If $K \leq H \leq G$ such that $|H/K| = p^3$, then every subgroup of order $p^2$ of $H/K$ is cyclic and hence, by 2.3.3, $L(H/K)$ is modular; by 9.2.3, $\mathcal{R}(G)$ is modular. Suppose, for a contradiction, that $\mathcal{R}(G)$ is not distributive. Then since $\mathcal{R}(G)$ is finite, there exists a 5-element sublattice $\{A, B, C, N, M\}$ of $\mathcal{R}(G)$ such that $A \cap B = A \cap C = B \cap C = N$, $A \cup B = A \cup C = B \cup C = M$ and $A, B, C$ all cover $N$ (see Birkhoff [1948], p. 134). Then $M$ covers $A, B, C$ and hence by (2), $A, B, C$, and $N$ are normal subgroups of $M$. Thus $M/N = A/N \times B/N = A/N \times C/N = B/N \times C/N$ with simple groups $A/N, B/N, C/N$. By 9.1.3 applied to $M/N$, $A/N \simeq B/N$ is abelian and hence $M/N$ is elementary abelian of order $p^2$, contradicting our assumption. Thus $\mathcal{R}(G)$ is distributive and (c) implies (a).

9.2.5 Corollary (Zappa [1956a]). Let $G$ be a finite soluble group. Then $\mathcal{R}(G)$ is distributive if and only if every Sylow subgroup of $G$ is cyclic.
Proof. If $\mathfrak{R}(G)$ is distributive, then by 9.2.4, every chief factor of $G$ is cyclic, that is, $G$ is supersoluble. So $G$ has a Sylow tower (see Robinson [1982], p. 145) and again 9.2.4 implies that every Sylow subgroup of $G$ is cyclic. Conversely, any group with cyclic Sylow subgroups clearly satisfies (b) of 9.2.4.

Another characterization of finite groups with distributive lattice of subnormal subgroups is given in Exercise 2. Using some deeper properties of the permutizer $P_H(K) = \langle X | X \leq H, XK = KX \rangle$ of two subnormal subgroups $H$ and $K$, it is possible to generalize 9.2.3 and 9.2.4 to infinite groups. We give this result without proof.

9.2.6 Theorem (Napolitani [1970]). Let $G$ be a group and $\mathbb{SN}(G)$ the partially ordered set of all subnormal subgroups of $G$.

(a) $\mathbb{SN}(G)$ is a modular sublattice of $L(G)$ if and only if for all $S, T \leq G$ such that $T \leq S \leq G$ and $|S/T| = p^3$, $p$ a prime, $L(S/T)$ is modular.

(b) $\mathbb{SN}(G)$ is a distributive sublattice of $L(G)$ if and only if for all $S, T \leq G$ such that $T \leq S \leq G$ and $|S/T| = p^2$, $p$ a prime, $S/T$ is cyclic.

Our next result together with Theorem 9.1.8 shows that for a finite group, $\mathfrak{R}(G)$ is complemented if and only if $\mathfrak{R}(G)$ is complemented; and in this case, $\mathfrak{R}(G) = \mathfrak{R}(G)$.

9.2.7 Theorem (Curzio [1958]). The following properties of the finite group $G$ are equivalent.

(a) $\mathfrak{R}(G)$ is complemented.

(b) Every minimal normal subgroup of $G$ is a direct factor of $G$.

(c) $G$ is a direct product of simple groups.

(d) $\mathfrak{R}(G)$ is relatively complemented.

Proof. Suppose first that $\mathfrak{R}(G)$ is complemented and let $N$ be a minimal normal subgroup of $G$. Then $N \in \mathfrak{R}(G)$ and hence there exists $M \in \mathfrak{R}(G)$ such that $G = N \cup M = NM$ and $N \cap M = 1$. Since $M$ is a proper subnormal subgroup of $G$, there exists $L \leq G$ such that $M \leq L < G$. By Dedekind's law, $L = (N \cap L)M$. Since $N$ is a minimal normal subgroup of $G$, $N \cap L = N$ or $N \cap L = 1$. In the first case, $L = NM = G$, a contradiction. Hence $N \cap L = 1$ and so $M = L \leq G$ and $G = N \times M$. Thus (a) implies (b).

We use induction on $|G|$ to show that (b) implies (c). Let $N$ be a minimal normal subgroup of $G$ and let $M \leq G$ such that $G = N \times M$. If $R$ is a minimal normal subgroup of $M$, then since $M$ is a direct factor, $R$ is a minimal normal subgroup of $G$. By assumption there exists $S \leq G$ such that $G = R \times S$; it follows that $M = R \times (M \cap S)$. Thus $M$ satisfies (b) and therefore, by induction, it is a direct product of simple groups. Then $G = N \times M$ is also such a direct product and (c) holds.

Now if $G$ satisfies (c), then by 9.1.8, $\mathfrak{R}(G)$ is complemented. Thus every normal subgroup $N$ of $G$ is a direct factor and hence every normal subgroup of $N$ is normal in $G$. It follows that every subnormal subgroup is normal, that is, $\mathfrak{R}(G) = \mathfrak{R}(G)$. Then $\mathfrak{R}(G)$ is modular and complemented and hence relatively complemented. Thus (c) implies (d), while it is clear that (d) implies (a).
We finally mention that Pazderski [1972] determined the finite soluble groups having a unique minimal subnormal subgroup (see Exercise 4) and that Tamaschke [1961] characterized the neutral elements of $\mathcal{R}(G)$ for a group $G$ with a composition series. He shows that $N \in \mathcal{R}(G)$ is neutral in $\mathcal{R}(G)$ if and only if for every $S \in \mathcal{R}(G)$, no abelian composition factor between $N$ and $N \cap S$ is isomorphic to a composition factor between $S$ and $N \cap S$.

**Isomorphisms between lattices of subnormal subgroups**

We are now going to study isomorphisms between lattices of subnormal subgroups of two groups $G$ and $\bar{G}$. Here we restrict our attention to finite groups and, in fact, most often even to finite soluble groups. First we want to show that under suitable assumptions, suggested by the examples in 9.2.1, such an isomorphism maps $p$-groups to $p$-groups and, more generally, $O_p(G)$ to $O_p(\bar{G})$ and $O^p(G)$ to $O^p(\bar{G})$. For this we need the following simple lemma.

**9.2.8 Lemma.** Let $G$ and $\bar{G}$ be finite groups and $\varphi: \mathcal{R}(G) \to \mathcal{R}(\bar{G})$ an isomorphism. If $N, H \in \mathcal{R}(G)$ such that $N \leq H$ and $H/N$ is a noncyclic elementary abelian $p$-group, then $N^\varphi \leq H^\varphi$ and $H^\varphi/N^\varphi \cong H/N$.

**Proof.** Since $H/N$ is not cyclic, there exists $D \in \mathcal{R}(G)$ such that $N \leq D \leq H$ and $|H/D| = p^2$; let $M_i \in \mathcal{R}(G)$ such that $D < M_i < H$ ($i = 1, 2, 3$) and $M_1 \neq M_2 \neq M_3 \neq M_1$.

By (2), $M_i^\varphi \leq H^\varphi$; hence $D^\varphi = M_i^\varphi \cap M_j^\varphi \leq H^\varphi$ and $H^\varphi/D^\varphi = M_i^\varphi/D^\varphi \times M_j^\varphi/D^\varphi$ for all $i \neq j$. By 9.1.3, $H^\varphi/D^\varphi$ is abelian and then $L(H^\varphi/D^\varphi) = [H^\varphi/D^\varphi]_K \cong [H/D]_K \cong L(H/D)$.

By 2.2.5, $H^\varphi/D^\varphi$ is elementary abelian of order $p^2$. Since $N^\varphi$ is the intersection of all subgroups $D^\varphi$ such that $N \leq D \leq H$ and $|H/D| = p^2$, it follows that $N^\varphi \leq H^\varphi$ and $H^\varphi/N^\varphi$ is an elementary abelian $p$-group. But then $|H^\varphi/N^\varphi| = p^n = |H/N|$ where $n$ is the length of $[H^\varphi/N^\varphi]_K \cong [H/N]_K$ and hence $H^\varphi/N^\varphi \cong H/N$.

**9.2.9 Theorem** (Curzio [1957a], Zacher [1962]). Let $G$ be a finite $p$-group and $\varphi: \mathcal{R}(G) \to \mathcal{R}(\bar{G})$ an isomorphism.

(a) If $G$ has at least 2 maximal subgroups, then $|\bar{G}| = |G|$.

(b) If $G$ is generalized quaternion and $\bar{G}$ is a finite soluble group, then $\bar{G} \cong G$.

**Proof.** (a) We use induction on $|G|$. Since $G$ has 2 maximal subgroups, $G$ is not cyclic and hence $G/\Phi(G)$ is an elementary abelian $p$-group of order $p^n$ for some $n \geq 2$. By 9.2.8, $|\bar{G} : \Phi(G)^\varphi| = p^n$. So if $\Phi(G) = 1$, we are done. And if $\Phi(G) \neq 1$, we choose $A, B \leq G$ of order $p$ such that $A \leq Z(G)$ and $A \neq B$. Then $AB$ is elementary abelian of order $p^2$, hence $AB \neq G$ and so there exists a maximal subgroup $M$ of $G$ containing $AB$. By induction, $|M^\varphi| = |M|$ and, since $|\bar{G} : M^\varphi| = p$, it follows that $|\bar{G}| = |G|$.

(b) Let $|G| = 2^n$ and $N = Z(G)$. Then $N^\varphi$ is the unique minimal subnormal subgroup of $\bar{G}$. Hence $N^\varphi \leq \bar{G}$ and $|N^\varphi| = p,$ a prime, since $\bar{G}$ is a finite soluble group. Now $G/N$ is a dihedral group and so by (a), $|\bar{G}/N^\varphi| = |G/N| = 2^{n-1}$. Since $|N^\varphi| = p,$ the group $\bar{G}/C_{\bar{G}}(N^\varphi)$ is cyclic; on the other hand, $\mathcal{R}(\bar{G}/N^\varphi)$ is not a chain and hence $\bar{G}/N^\varphi$ is not cyclic. Thus $N^\varphi < C_{\bar{G}}(N^\varphi)$. So if $p > 2$, then $C_{\bar{G}}(N^\varphi) = N^\varphi \times S$ for some
9.2 Lattices of subnormal subgroups

nontrivial 2-group $S$; but then $S$ would contain a minimal subnormal subgroup of $\overline{G}$, a contradiction. It follows that $p = 2$ and $|\overline{G}| = |G|$. Then $L(\overline{G}) = \mathfrak{N}(\overline{G})$, so $\overline{G}$ has only one minimal subgroup and hence is generalized quaternion of order $2^n$. Thus $\overline{G} \simeq G$.

We want to generalize Theorem 9.2.9 to an assertion on the images of $O_p(G)$ and $O^p(G)$. For this we need the following lemma.

9.2.10 Lemma. Let $G$ and $\overline{G}$ be finite groups, $\varphi: \mathfrak{N}(G) \to \mathfrak{N}(\overline{G})$ an isomorphism and $\pi$ a set of primes. If $\overline{G}$ is soluble, then $O_{\pi}(G)^\varphi$ and $O^\varphi(G)^\pi$ are characteristic subgroups of $\overline{G}$.

Proof. (a) Let $N = O_{\pi}(G)$. We use induction on $|G|$ to show that $N^\varphi$ is characteristic in $\overline{G}$. We may assume that $N \neq 1$ and claim that there exists

$$L \leq G \text{ such that } 1 \neq L \leq N \text{ and } L^\varphi \text{ is characteristic in } \overline{G}.$$ 

By induction, it will follow that $N^\varphi/L^\varphi$ is characteristic in $\overline{G}/L^\varphi$ and then $N^\varphi$ is characteristic in $\overline{G}$, as desired. To prove (12), consider a minimal normal subgroup $M$ of $G$ contained in $N$. If $M^\varphi$ is characteristic in $\overline{G}$, we are done. So assume that $M^\varphi$ is not characteristic in $\overline{G}$. Since $M$ is the join of minimal subnormal subgroups, the same holds for $M^\varphi$ and hence there exist a minimal subnormal subgroup $R^\varphi \leq M^\varphi$ and $\pi \in \text{Aut } G$ such that $(R^\varphi)^\pi \neq R^\varphi$. Since $\overline{G}$ is soluble, $|R^\varphi| = |(R^\varphi)^\pi| = p$, a prime. Let $L \leq G$ such that $L^\varphi = O_p(\overline{G})$. By (4), $R^\varphi$ and $(R^\varphi)^\pi$ are different minimal subgroups of $L^\varphi$ and hence by 9.2.9, $L$ is a $p$-group. Therefore $|R| = p$ and $p \in \pi$ since $R \leq M \leq N$. Again by (4), $L \leq O_p(G) \leq N$. Hence $O_p(G)$ has more than one minimal subgroup; so 9.2.9 and (4) imply that $O_p(G)^\varphi$ is a $p$-group and $O_p(G)^\varphi \leq O_p(\overline{G}) = L^\varphi$.

It follows that $L = O_p(G) \leq G \leq L$ satisfies (12).

(b) Now let $N = O^\varphi(G)$. There are subgroups $L$ of $G$ such that

$$L \leq L \leq G \text{ and } L^\varphi \text{ is characteristic in } \overline{G};$$

for example, $L = G$ satisfies (13). Let $L$ be minimal with this property and suppose, for a contradiction, that $N < L$. Since $N^\varphi \leq L^\varphi$, there exists a maximal subnormal subgroup $K^\varphi$ of $L^\varphi$ containing $N^\varphi$. By (2), $K^\varphi \leq L^\varphi$ and, since $\overline{G}$ is soluble, $|L^\varphi: K^\varphi| = p$, a prime. The minimality of $L$ implies that $K^\varphi$ is not characteristic in $\overline{G}$; thus there exists $\pi \in \text{Aut } \overline{G}$ such that $(K^\varphi)^\pi \neq K^\varphi$. For every such $\pi$, $(K^\varphi)^\pi$ is a normal subgroup of index $p$ in $(L^\varphi)^\pi = L^\varphi$; hence $M^\varphi = \bigcap_{\pi \in \text{Aut } \overline{G}} (K^\varphi)^\pi$ is characteristic in $\overline{G}$ and $L^\varphi/M^\varphi$ is a noncyclic elementary abelian $p$-group. By 9.2.8, $M \leq L$ and $L/M$ is an elementary abelian $p$-group. Thus $|L: K| = p$ and $p \in \pi$ since $N \leq K$. It follows that $|G: M| = |G: L||L: M|$ is a $\pi$-number and hence by (6), $N = O^\varphi(G) = O^\varphi(M) \leq M$; but this contradicts the minimality of $L$. Thus $N = L$ and $N^\varphi$ is a characteristic subgroup of $\overline{G}$.

We can now prove the desired result on $O_p(G)^\varphi$ and $O^\varphi(G)^\pi$. We clearly have to assume that $O_p(G)$ and $G/O^p(G)$ are not cyclic; but the examples in (d) of 9.2.1 show that for $p = 2$, an additional assumption is needed.
9.2.11 Theorem (Pazderski [1972]). Let $G$ and $\bar{G}$ be finite groups, $\varphi: \mathcal{R}(G) \to \mathcal{R}(\bar{G})$ an isomorphism and $p$ a prime.

(a) Assume that $O_p(G)$ is not cyclic and if $p = 2$, in addition, that $\bar{G}$ is soluble. Then $O_p(G)^o = O_p(\bar{G})$.

(b) Assume that $G/O^p(G)$ is not cyclic and if $p = 2$, in addition, that $G$ and $\bar{G}$ are soluble. Then $O^p(G)^o = O^p(\bar{G})$.

Proof. (a) Let $N = O^p(G)$. By 9.2.9, $N^o$ is a $p$-group and so $N^o \leq O^p(\bar{G})$, by (4). If $N^o < O^p(\bar{G})$, take $H$ such that $N^o < H \leq O^p(\bar{G})$ and $|H : N^o| = p$. Since $N^o$ is not cyclic, neither is $H$ and hence $\Phi(H) < N^o < H$. By 9.2.8, $H^o = \Phi(H)^o - 1$ is an elementary abelian $p$-group. So $H^{o - 1}$ is a subnormal $p$-subgroup of $G$ and by (4), $H^{o - 1} \leq O_p(G) = N$, a contradiction. Thus $N^o = O_p(\bar{G})$, as desired.

(b) We use induction on $|G|$ to show that $O_p(G)^o \geq O^p(\bar{G})$. Then $\bar{G}/O^p(G)$ is not cyclic and the above assertion for $\varphi^{-1}$ yields the other inclusion. So let $N = O^p(G)$, $D/N = \Phi(G/N)$ and assume that the assertion is true for groups of smaller order. Since $G/N$ is not cyclic, neither is $G/D$ and so by 9.2.8, $D^o \leq \bar{G}$ and $\bar{G}/D^o$ is an elementary abelian $p$-group. Thus $D^o \geq O^p(\bar{G})$ and we are done if $D = N$. So we may assume that $G/N$ is not elementary abelian.

If $M$ is a maximal subgroup of $G$ containing $N$, then $|\bar{G} : M^o| = p$ and by (6), $O^p(M) = O^p(G) = N$ and $O^p(M^o) = O^p(\bar{G})$. If $M/N$ is not cyclic, the induction assumption yields that $N^o = O^p(M)^o \geq O^p(M^o) = O^p(\bar{G})$, as desired. So we may assume that $G/N$ has only cyclic maximal subgroups. Since it is not elementary abelian of order $p^2$, it then has only one minimal subgroup and is isomorphic to $Q_8$. Thus $p = 2$, hence $\bar{G}$ is soluble, by assumption, and so $N^o \leq \bar{G}$, by 9.2.10. Now 9.2.9 yields that $\bar{G}/N^o \cong Q_8$ and hence $N^o \geq O^2(\bar{G})$, as desired.

Our second main result on isomorphisms between lattices of subnormal subgroups is that under suitable assumptions they are "index preserving".

9.2.12 Theorem (Heineken [1965]). Let $G$ and $\bar{G}$ be finite soluble groups, $\varphi: \mathcal{R}(G) \to \mathcal{R}(\bar{G})$ an isomorphism and $p$ a prime. If $O^p(G)/O^{p, p}(G)$ is not cyclic, then $|H^o : K^o| = p$ for every composition factor $H/K$ of order $p$ of $G$.

Proof. We use induction on $|G|$ and first note that for any normal subgroup $N$ and subgroups $Y \leq X$ of a group,

$$|X : Y| = |XN : YN|/|X \cap N : Y \cap N|.$$

Indeed, if we write $T = X \cap YN = Y(X \cap N)$, then $|X : T| = |X : X \cap YN| = |XN : YN|$ and $|T : Y| = |Y(X \cap N) : Y| = |X \cap N : Y \cap N|$, and (14) follows.

Now let $K \leq H \leq G$ such that $|H : K| = p$. Since $\bar{G}$ is soluble and $K^o$ is a maximal subnormal subgroup of $H^o$,

$$|H^o : K^o| = p.$$
normal subgroups of \( \bar{G} \). By (14), \(|HR:KR|\) \(|H \cap R : K \cap R| = |H : K| = p\) and, since \( G/R \) is a \( p' \)-group, it follows that \(|H \cap R : K \cap R| = p\). If \( R \neq G \), the induction assumption applies to \( R \) and so \( p = |(H \cap R)^\phi : (K \cap R)^\phi| = |H^\phi \cap R^\phi : K^\phi \cap R^\phi| \); then (14) shows that \( p \) divides \(|H^\phi : K^\phi|\) and (15) implies that \(|H^\phi : K^\phi| = p\), as desired. So we may assume that

\[
(16) \quad G = R = O^{p'}(G).
\]

Suppose that there exists \( T \leq S \) such that \( 1 < T \leq G, T^\phi \leq \bar{G}, \) and \( HT \neq KT \). Then by (14), \(|HT : KT| = p\) and we may apply the induction assumption to \( G/T \). We obtain that \(|H^\phi T^\phi : K^\phi T^\phi| = p\) and then again \(|H^\phi : K^\phi| = p\), by (14) and (15). So we may assume that

\[
(17) \quad HT = KT \ 	ext{for all} \ T \leq S \ 	ext{such that} \ 1 < T \leq G \ 	ext{and} \ T^\phi \leq \bar{G}.
\]

Since \( G/S \) is a \( p \)-group and \( Q \) a \( p' \)-group, \( Q \leq S \) and \(|H \cap Q : K \cap Q| \) is prime to \( p\). So (14) implies that \( HQ \neq KQ \) and, since \( Q^\phi \leq \bar{G} \), it follows from (17) that

\[
(18) \quad Q = 1.
\]

This implies that \( P \) is the Fitting subgroup of \( G \) and so \( C_G(P) \leq P \), by a well-known property of soluble groups (see Robinson [1982], p. 144). If \( P \) were cyclic, then \( G/C_G(P), \) as a subgroup of \( \text{Aut} \ P \), would be abelian. Thus \( G/P \) is abelian and (16) implies that \( G/P \) is a \( p \)-group. But then \( G \) is a \( p \)-group, contrary to our assumption. Thus \( P \) is not cyclic and by 9.2.9,

\[
(19) \quad P^\phi \text{ is a } p \text{-group}.
\]

Since \( G \) is not a \( p \)-group, \( S \neq 1 \) and by (18), every minimal normal subgroup of \( G \) is a \( p \)-group; thus \( T = P \cap S \neq 1 \). Of course, \( T \leq G \) and \( T^\phi = P^\phi \cap S^\phi \leq \bar{G} \). By (17), \( HT = KT \) and then (14) shows that \(|H \cap T : K \cap T| = p\). Since \( T^\phi \leq P^\phi \) is a \( p \)-group, \(|H^\phi \cap T^\phi : K^\phi \cap T^\phi| = p\) and again (14) and (15) yield that \(|H^\phi : K^\phi| = p\).

9.2.13 Corollary. Let \( G \) and \( \bar{G} \) be finite soluble groups, \( \varphi: \mathfrak{S}(G) \to \mathfrak{S}(\bar{G}) \) an isomorphism and assume that for every prime \( p \) dividing \(|G|\), the group \( O^{p'}(G)/O^{p'}p(G) \) is not cyclic. Then \(|H^\phi| = |H|\) for every \( H \in \mathfrak{S}(G)\).

Proof. By 9.2.12, \( \varphi \) maps every composition factor of \( G \) onto a composition factor of the same order in \( \bar{G} \). It follows that \(|H^\phi| = |H|\) for every \( H \in \mathfrak{S}(G)\).

Exercise 6 shows that it is not possible to replace the assumption on the factor group \( O^{p'}(G)/O^{p'}p(G) \) in Theorem 9.2.12 by the assumption that the Sylow \( p \)-subgroups of \( G \) are not cyclic.

### Dualities

We have seen in Chapter 8 that for a group \( G \) to have a duality of \( L(G) \) is a rather restrictive property. The same holds for \( \mathfrak{S}(G) \), at least if \( G \) has sufficient subnormal subgroups. We want to show that if \( G \) is a finite soluble group of odd order with a
Further lattices

9.2.14 Lemma. If \( \mathcal{R}(G) \) has finite length and \( \delta: \mathcal{R}(G) \rightarrow \mathcal{R}(\overline{G}) \) is a duality, then \( \mathcal{R}(G) \) is modular.

Proof. By 2.1.8, \( \mathcal{R}(G) \) and \( \mathcal{R}(\overline{G}) \) are lower semimodular. It follows that \( \mathcal{R}(G) \) is upper semimodular and hence modular, by 2.1.10.

By (3), we have the following inheritance properties (compare with 8.1.6).

9.2.15 Lemma. Let \( G \) and \( \overline{G} \) be finite groups and \( \delta: \mathcal{R}(G) \rightarrow \mathcal{R}(\overline{G}) \) a duality.

(a) If \( N \trianglelefteq G \), then \( \delta \) induces a duality from \( \mathcal{R}(G/N) \) to \( \mathcal{R}(\overline{G}/\overline{N}) \).

(b) If \( N^\delta \trianglelefteq \overline{G} \), then \( \delta \) induces a duality from \( \mathcal{R}(N) \) to \( \mathcal{R}(\overline{G}/N^\delta) \).

More interesting are the following two results on maximal elementary abelian sections.

9.2.16 Lemma. Let \( G \) and \( \overline{G} \) be finite soluble groups and \( \delta: \mathcal{R}(G) \rightarrow \mathcal{R}(\overline{G}) \) a duality. Suppose that \( p \) is a prime and \( N \) is the join of all subnormal subgroups of order \( p \) of \( G \). Then \( N \) is an elementary abelian normal \( p \)-subgroup of \( G \) and \( N^\delta \) is a characteristic subgroup of \( \overline{G} \). If \( N \) is not cyclic, \( \overline{G}/N^\delta \simeq N \).

Proof. This is clear if there are no subnormal subgroups of order \( p \) in \( G \), that is if \( N = 1 \); so let \( N \neq 1 \). Then \( N^\delta \) is the intersection of maximal subnormal subgroups of \( \overline{G} \) and hence \( N^\delta \trianglelefteq \overline{G} \), by (2). Thus \( \delta \) induces a duality from \( \mathcal{R}(N) \) onto \( \mathcal{R}(\overline{G}/N^\delta) \). By (4), every subnormal subgroup of order \( p \) of \( G \) is contained in \( O_p(G) \) and therefore \( N \) is a normal \( p \)-subgroup of \( G \). So \( \mathcal{R}(N) = L(N) \) and by 9.2.14, \( L(N) \) is modular. Since \( N \) is generated by subgroups of order \( p \), it follows from 2.3.5 that \( N \) is elementary abelian. Thus \( \mathcal{R}(N) \) is self-dual and so \( \mathcal{R}(\overline{G}/N^\delta) \simeq \mathcal{R}(N) \). By 9.2.8, \( \overline{G}/N^\delta \simeq N \) if \( N \) is not cyclic; in any case, since \( \overline{G} \) is soluble, \( \overline{G}/N^\delta \) is an elementary abelian \( q \)-group of order \( q^n \) for some prime \( q \) (with \( q = p \) if \( n > 1 \)). Suppose, for a contradiction, that there exists a normal subgroup \( M^\delta \) of index \( q \) in \( \overline{G} \) such that \( N^\delta \not\leq M^\delta \). Then \( \overline{G}/N^\delta \cap M^\delta \) is elementary abelian of order \( q^{n+1} \), \( \delta \) induces a duality from \( \mathcal{R}(NM) \) onto \( \mathcal{R}(\overline{G}/N^\delta \cap M^\delta) \), and hence \( NM \) is elementary abelian of order \( q^{n+1} \). Since \( |N| = p \), it follows that \( q = p \) and then \( M \leq N \), by definition of \( N \). Thus \( N^\delta \leq M^\delta \), a contradiction. So we see that there is no such \( M^\delta \), that is, \( N^\delta \) is the intersection of all normal subgroups of index \( q \) in \( \overline{G} \). In particular, \( N^\delta \) is a characteristic subgroup of \( \overline{G} \) and all assertions of the lemma hold.

9.2.17 Lemma. Suppose that \( N \trianglelefteq G \) such that \( N \) is elementary abelian of order \( p^n \), \( G/N \) is elementary abelian of order \( q^n \), \( p \) and \( q \) primes, \( C_G(N) = N \) and \( Z(G) = 1 \). If \( \overline{G} \) is a finite soluble group and \( \delta: \mathcal{R}(G) \rightarrow \mathcal{R}(\overline{G}) \) a duality, then either \( |G| = pq \) or \( G \simeq A_4 \) and \( \overline{G} \simeq Q_8 \).

Proof. In the first place \( p \neq q \) since \( Z(G) = 1 \). If \( |N| = p \), then \( G/C_G(N) \) is cyclic and hence \( |G| = pq \). So suppose that \( n \geq 2 \). By 9.2.16, \( N^\delta \trianglelefteq \overline{G} \) and \( \overline{G}/N^\delta \) is elementary.
abelian of order $p^n$. Let $Q \in \text{Syl}_q(G)$. Then by 4.1.3, $N = [N, Q]C_N(Q) = [N, Q]$ since $C_N(Q) \leq Z(G) = 1$. Thus $N \leq G'$ and so every maximal normal subgroup of $G$ contains $N$. It follows that

\[(20)\) every minimal subnormal subgroup of $\bar{G}$ is contained in $N^\delta$.

Now 9.2.16 applied to the duality induced in $\mathcal{R}(G/N)$ yields that $N^\delta$ is elementary abelian of order $q^m$ if $m \geq 2$; and if $m = 1$, $|N^\delta|$ is a prime since $\bar{G}$ is soluble. Suppose, for a contradiction, that $G$ is not a $p$-group. Then $(|N^\delta|, |\bar{G}/N^\delta|) = 1$ and so $C_{\bar{G}}(N^\delta) = N^\delta \times P$ for some $p$-group $P$; by (20), $P = 1$, that is, $C_{\bar{G}}(N^\delta) = N^\delta$. Since $\bar{G}/N^\delta$ is not cyclic, it follows that $|N^\delta|$ is not a prime; so $m \geq 2$ and $|N^\delta| = q^m$. As in 4.1.7, by Maschke's Theorem, $N$ is a completely reducible $GF(p)Q$-module, that is, $N = N_1 \times \cdots \times N_r$ with irreducible $Q$-modules $N_i$. By Schur's Lemma, $Q/CQ(N_i)$ is cyclic and, since $Q$ is elementary abelian, $|Q : CQ(N_i)| \leq q$ for all $i$. Now $C_G(N) = N$ and it follows that

$$q^m = |Q| = |Q : CQ(N)| = |Q : \bigcap_{i=1}^{r} CQ(N_i)| \leq q \leq q^n$$

since $|N| = p^n$ and so $r \leq n$. Thus $m \leq n$ and equality implies that $|N_i| = p$ and $|Q : CQ(N_i)| = q$ for all $i$, so that $q/p - 1$. Since $C_G(N^\delta) = N^\delta$, the same argument applies to $\bar{G} = N^\delta S$ for $S \in \text{Syl}_p(\bar{G})$ and yields that $n \leq m$ and equality implies that $p/q - 1$. But since $m \leq n$ and $n \leq m$, we have equality and so get the contradiction that $q/p - 1$ and $p/q - 1$. Thus $\bar{G}$ is a $p$-group. It follows that $m = 1$ and by (20), $N^\delta$ is the unique minimal (subnormal) subgroup of $\bar{G}$. Since $\bar{G}/N^\delta$ is elementary abelian, $\bar{G} \simeq Q_8$ and so $|N| = 4$; then $|G : N| = 3$ since $C_G(N) = N$, and $G \simeq A_4$, as desired.

We can now prove the result announced above.

9.2.18 Theorem (Zacher [1962]). Let $G$ and $\bar{G}$ be finite soluble groups and let $\delta : \mathcal{R}(G) \to \mathcal{R}(\bar{G})$ be a duality. If $|G|$ is odd, then $G$ is supersoluble.

**Proof.** We use induction on $|G|$. By 9.2.15, $\delta$ induces a duality in $\mathcal{R}(G/\Phi(G))$. If $\Phi(G) \neq 1$, then by induction, $G/\Phi(G)$ is supersoluble and then so is $G$ (see Robinson [1982], p. 268). So let $\Phi(G) = 1$. Then $F(G)$ is a direct product of minimal normal subgroups of $G$ (see Robinson [1982], p. 131). If $N_1$ and $N_2$ are two of these, then again by induction, $G/N_i$ is supersoluble ($i = 1, 2$) and then so is $G/N_1 \cap N_2 = G$. Thus we may assume that $N = F(G)$ is the unique minimal normal subgroup of $G$; let $|N| = p^n$. By 9.2.16, $N$ is the join of all subnormal subgroups of order $p$ of $G$ and $N^\delta$ is a characteristic subgroup of $\bar{G}$. If $N = G$, we are done. So let $N \neq G$. Then for some prime $q$, the join $M/N$ of all subnormal subgroups of order $q$ of $G/N$ is non-trivial; 9.2.16 applied to the duality induced by $\delta$ in $\mathcal{R}(G/N)$ yields that $M/N$ is elementary abelian of order $q^m$ for some $m \in \mathbb{N}$ and $M^\delta$ is a characteristic subgroup of $N^\delta$. So $M^\delta \subseteq \bar{G}$ and $\delta$ induces a duality from $\mathcal{R}(M)$ onto $\mathcal{R}(\bar{G}/M^\delta)$ which satisfies the assumptions of 9.2.17. Indeed, $N = F(G)$ and a well-known property of soluble groups (see Robinson [1982], p. 144) yields that $N = C_G(N) = C_M(N)$. It follows that
Further lattices

$Z(M) < N$; since $Z(M) \trianglelefteq G$ and $N$ is a minimal normal subgroup of $G$, we have $Z(M) = 1$. Now $|G|$ is odd and so 9.2.17 implies that $|N| = p$. By induction, $G/N$ is supersoluble and so, finally, $G$ is supersoluble.

The assumption that $|G|$ is odd is needed in Theorem 9.2.18. In fact, in (c) of 9.2.1, we saw that $A_4$ and $Q_8$ have dual lattices of subnormal subgroups and that $R(Q_8C_3)$ is self-dual; clearly, $A_4$ and $Q_8C_3$ are not supersoluble. On the other hand, these are the only bad examples.

9.2.19 Theorem (Zacher [1962]). Let $G$ and $\bar{G}$ be finite soluble groups and let $\varnothing: R(G) \rightarrow R(\bar{G})$ be a duality. Then $G = H \times K$ where $(|H|, |K|) = 1$, $H$ is supersoluble and $K$ is isomorphic to $A_4$, $Q_8C_3$, or 1.

We sketch a proof of this theorem in Exercise 8 and mention that it has been extended to infinite groups by Franchetta [1978].

$\mathcal{X}$-subnormal subgroups

We finally report on an interesting generalization of the lattice of subnormal subgroups. Let $\mathcal{X}$ be a class of finite groups which is closed under extensions, epimorphic images, and subgroups. A subgroup $H$ of $G$ is called $\mathcal{X}$-normal in $G$ if $H \trianglelefteq G$ or $G/H \in \mathcal{X}$; then, of course, $H$ is called $\mathcal{X}$-subnormal in $G$ if there exist $H_i \leq G$ such that $H = H_0 \leq H_1 \leq \cdots \leq H_n = G$ and $H_i$ is $\mathcal{X}$-normal in $H_{i+1}$ for $i = 0, \ldots, n - 1$.

9.2.20 Theorem (Kegel [1978]). For every finite group $G$, the set $R_{\mathcal{X}}(G)$ of all $\mathcal{X}$-subnormal subgroups of $G$ is a sublattice of $L(G)$.

Clearly, $R_{\mathcal{X}}(G)$ contains $R(G)$ for every class $\mathcal{X}$; furthermore $R_{\mathcal{X}}(G) = R(G)$ if $\mathcal{X} = \{1\}$ and $R_{\mathcal{X}}(G) = L(G)$ if $\mathcal{X}$ is the class of all groups. For every set $\pi$ of primes, we may choose the class $\mathcal{X}$ of $\pi$-groups. In this way we obtain infinitely many functors $R_{\mathcal{X}}$ assigning to every finite group $G$ a sublattice $R_{\mathcal{X}}(G)$ of $L(G)$ containing $R(G)$.

Exercises

1. If $S$ is a nonabelian simple subnormal subgroup of $G$, show that $S^G$ is a minimal normal subgroup of $G$.

2. (Zacher [1957]) If $G$ is a finite group, show that $R(G)$ is distributive if and only if for all $S$, $T \trianglelefteq G$ such that $T \leq S$ and $S/T$ is a $p$-group for some prime $p$, $S/T$ is cyclic. (Hint: First show that if $G$ has this property and $H \in R(G)$ is soluble, then every Sylow subgroup of $H$ is cyclic and $H \trianglelefteq G$.)

3. Let $G$ be a finite soluble group. Show that $R(G)$ is a chain if and only if either $G$ is a cyclic $p$-group or $G = PQ$ where $P \trianglelefteq G$ is a cyclic $p$-group, $Q$ a cyclic $q$-group, $p$ and $q$ different primes, and $C_G(P) = P$. 

4. (Pazderski [1972]) Let \( G \) be a finite soluble group. Show that \( G \) has only one minimal subnormal subgroup if and only if it has one of the following properties.
(a) \( G = PQ \) where \( P \leq G \) is a cyclic \( p \)-group, \( p \) a prime, \(|Q| \) divides \( p - 1 \), and \( C_G(P) = P \).
(b) \( G \) is a generalized quaternion group.
(c) \( G = Q_8C_3 \) as defined in Example 9.2.1.
(d) \( G \) has a normal subgroup \( N \simeq Q_8 \) such that \( G/N \simeq S_3 \) and \( C_G(N) = Z(N) \).

5. Determine \( \mathfrak{R}(G) \) for the groups \( G \) in Exercise 4(d). Note that there are two different such groups, a semidirect product and a non-splitting extension of \( Q_8 \) by \( S_3 \).

6. (Heineken [1965]) Show that there are groups \( G \) and \( \bar{G} \) with \( \mathfrak{R}(G) \simeq \mathfrak{R}(\bar{G}) \) satisfying \(|G/G'| = 2\), \(|\bar{G}/\bar{G}'| = 3\), and \( G' \simeq \bar{G}' \simeq A \times B \) where \(|A| = 2^{18}19\), \(|B| = 3^{18}19\); here a cyclic group of order 19 operates irreducibly on elementary abelian groups of order 2^{18} and 3^{18}, respectively.

7. (Curzio [1957d]) Let \( G \) be a finite supersoluble group without nontrivial cyclic Sylow subgroups. If \( \mathfrak{R}(G) \) is self-dual, show that \( G \) is nilpotent.

8. (Zacher [1962]) Let \( G \) and \( \bar{G} \) be finite soluble groups and let \( \delta: \mathfrak{R}(G) \rightarrow \mathfrak{R}(\bar{G}) \) be a duality.
(a) If \( O_2(G) \) is cyclic, show that \( G \) is supersoluble.
(b) If \( G \) is not supersoluble and \(|G| = p^{a}2^{b} \) for some prime \( p \), show that \( G \simeq A_4 \) or \( G \simeq Q_8C_3 \).
(c) Prove Theorem 9.2.19. (Hint: Study \( O_2(G)H \) where \( H \) is a Hall \( \{2,3\}' \)-subgroup of \( G \).)

### 9.3 Centralizer lattices

In this section we study the centralizer lattice \( \mathfrak{C}(G) \) which we defined in \( \S \) 1.1. Again our main aim will be to determine the structure of groups whose centralizer lattices have special properties and to find out which groups are determined by their centralizer lattices (modulo abelian direct factors). But since \( \mathfrak{C}(G) \) is only a meet-sublattice of \( L(G) \), there is the additional question: under which conditions is \( \mathfrak{C}(G) \) a sublattice of \( L(G) \) or even \( \mathfrak{C}(G) = L(G) \)?

Throughout this section we shall write \( C(X) \) for \( C_G(X) \) if \( X \leq G \) and there is no ambiguity. We also write \( Z \) for the centre \( Z(G) \) of \( G \) and \( CC(X) \) for \( C(C(X)) \) and use an index \( C \) to denote intervals in \( \mathfrak{C}(G) \). Thus if \( H, K \in \mathfrak{C}(G) \) and \( K \leq H \), then

\[
[H/K]_C = \{X \in \mathfrak{C}(G)| K \leq X \leq H\}.
\]

**Basic properties of centralizers**

It is well-known and easy to prove that for every set \( \mathcal{X} \) of subgroups of \( G \),

\[
(1) \bigcap_{X \in \mathcal{X}} C(X) = C\left(\bigcup_{X \in \mathcal{X}} X \right) \quad \text{and} \quad \bigcup_{X \in \mathcal{X}} C(X) \leq C\left(\bigcap_{X \in \mathcal{X}} X \right).
\]
By 1.1.6, it follows from (1) that $\mathfrak{C}(G) = \{C(X) \mid X \in L(G)\}$ is a complete meet-sublattice of $L(G)$. We write $\wedge$ and $\vee$ for the operations of this lattice and have that for $H, K \in \mathfrak{C}(G)$,

\[ (2) \quad H \wedge K = H \cap K \text{ and } H \vee K = \bigcap \{X \in \mathfrak{C}(G) \mid H \leq X \text{ and } K \leq X\}. \]

The least element of $\mathfrak{C}(G)$ is $Z(G) = C_0(G)$ and the largest element is $G = C_G(1)$. For all subgroups $X, Y$ of $G$, we clearly have that $X \leq Y$ implies $C(Y) \leq C(X)$ and that $X \leq C(C(X))$. This yields the following important property of $\mathfrak{C}(G)$.

**9.3.1 Theorem.** The map $\mathfrak{C}|_{\mathfrak{C}(G)} : \mathfrak{C}(G) \to \mathfrak{C}(G)$ is an involutory duality, that is, for all $H, K \in \mathfrak{C}(G)$,

\[ (3) \quad H \leq K \text{ if and only if } C(K) \leq C(H) \quad \text{and} \quad (4) \quad C(C(H)) = H. \]

It follows that

\[ (5) \quad C(H \wedge K) = C(H) \vee C(K) \quad \text{and} \quad C(H \vee K) = C(H) \wedge C(K). \]

**Proof.** Let $H, K \in \mathfrak{C}(G)$ and take $X \leq G$ such that $H = C_G(X)$. Then $X \leq C(C(X))$ and $H \leq C(C(H))$; and the first inclusion implies that $C(C(C(X))) \leq C(X)$, that is, $C(C(H)) \leq H$. Thus $H = C(C(H))$ and (4) holds. It follows that the map $\mathfrak{C}|_{\mathfrak{C}(G)}$ is bijective; indeed, it is surjective since $H = C(C(H))$, and it is injective since $C(H) = C(K)$ implies that $H = C(C(H)) = C(C(K)) = K$. Now if $H \leq K$, then clearly $C(K) \leq C(H)$, and $C(K) \leq C(H)$ yields $H = C(C(H)) \leq C(C(K)) = K$. Thus (3) holds and $\mathfrak{C}|_{\mathfrak{C}(G)}$ is a duality of $\mathfrak{C}(G)$. Finally, (5) follows from 8.1.1; in fact, since $\mathfrak{C}(G)$ is a complete lattice, 8.1.1 even yields the infinite analogue of (5).

We give some simple examples of centralizer lattices.

**9.3.2 Examples.** Let $G$ be a group, $Z = Z(G)$, $p$ and $q$ primes such that $q \mid p - 1$, and $k, n \in \mathbb{N}$.

(a) $G$ is abelian if and only if $G = Z$, that is, if and only if $\mathfrak{C}(G)$ is the trivial lattice containing only one element.

(b) On the other hand, if $G$ is nonabelian of order $pq$, then every subgroup of $G$ is a centralizer so that $\mathfrak{C}(G) = L(G)$. Similarly, if $G$ is a $p$-group and $|G : Z| = p^2$, then every subgroup of $G$ lying properly between $G$ and $Z$ is abelian and hence is its own centralizer; thus $\mathfrak{C}(G) = [G/Z]$.

(c) We write $G \in \mathfrak{M}(k)$ if $\mathfrak{C}(G)$ is (modular) of length 2 and has $k$ atoms. Thus all the groups considered in (b) lie in $\mathfrak{M}(p + 1)$. More generally, we claim that if $G$ is a finite nonabelian group with an abelian normal subgroup $N$ of prime index, then $G \in \mathfrak{M}(|N : Z| + 1)$. Indeed, since $G$ is nonabelian and $G/N$ is cyclic, $N \not\leq Z$ and hence $N = C_G(N) \in \mathfrak{C}(G)$. Let $|G : N| = p$ and $\Lambda = \mathfrak{C}(G) \setminus \{Z, N, G\}$. If $H \in \Lambda$, then $H = C_G(X)$ for some $X \leq G$ such that $X \not\leq N$. Therefore $C_G(N \cap H) \geq NX = G$ and $N \cap H \leq Z$. On the other hand, every centralizer contains $Z$ and so $N \cap H = Z$. It follows that $H \not\leq N$, hence $NH = G$ and $|H : Z| = |G : N| = p$. Thus all the $H \in \Lambda$ have the same order and $\Lambda \cup \{N\}$ is an antichain, that is, $\mathfrak{C}(G)$ is of length 2. If
x ∈ G \ N, then ⟨x⟩Z ≤ C_G(⟨x⟩) ∈ Λ and hence |⟨x⟩Z : Z| = p. It follows that every element in \( G/Z \) not contained in \( N/Z \) has order \( p \) and, since there are \((p - 1)|N/Z|\) such elements, |Λ| = |N : Z|. Thus \( G ∈ \mathcal{M}(|N : Z| + 1) \) and this proves our assertion.

As special cases we obtain that \( A_4 ∈ \mathcal{M}(5) \) and that \( G ∈ \mathcal{M}(p^n + 1) \) if \( G \) is a non-abelian \( P \)-group of order \( p^nq \). Here, if \( n ≥ 2 \), there are subgroups of order \( q \) in \( G \) generating a subgroup of order \( pq \) and hence \( \mathcal{E}(G) \) is not a sublattice of \( L(G) \).

Another special case is the dihedral group \( D_{2n} \) of order \( 2n \) whose centre is nontrivial (and of order 2) if and only if \( n \) is even. Thus \( D_{4k} ∈ \mathcal{M}(k + 1) \) for all \( k ≥ 2 \) and \( D_{2k} ∈ \mathcal{M}(k + 1) \) if \( k \) is odd, \( k ≥ 3 \).

(d) Let \( G = SL(2, 2^n) \), \( n ≥ 2 \). Then \( G \) has a partition \( Σ \) consisting of the Sylow 2-subgroups of order \( 2^n \) and the maximal cyclic subgroups of order \( 2^n + 1 \) and \( 2^n - 1 \) (see 3.5.1). We claim that \( \mathcal{E}(G) \) consists of \( Z = 1 \), \( G \), and the groups in \( Σ \). Indeed, every component \( X \) of \( Σ \) is abelian and so \( X ≤ C_G(x) \) for every \( 1 ≠ x ∈ X \). If \( X ≤ C_G(x) \) and \( y ∈ C_G(x) \setminus X \), then by 3.5.2, \( x \) and \( y \) have the same prime order \( p \). Then \( ⟨x, y⟩ \) is elementary abelian of order \( p^2 \) and contained in a Sylow \( p \)-subgroup \( P \). Since the Sylow subgroups for odd primes are cyclic (they are contained in components of \( Σ \), \( p = 2 \) and \( P ∈ Σ \). But then \( x ∈ P ∧ X \) implies \( P = X \) and so \( y ∈ X \), a contradiction. Thus \( X = C_G(x) \) for every \( 1 ≠ x ∈ X \). By (1), every centralizer is an intersection of element centralizers and since \( Σ \) is a partition, the assertion follows. Now it is well-known (see Huppert [1967], pp. 191–194) that the normalizers of the components of \( Σ \) have orders \( 2^n(2^n - 1), 2(2^n + 1), 2(2^n - 1) \), respectively, and, since every component contains a Sylow subgroup of \( G \), all components of the same order are conjugate. Since \( |G| = 2^n(2^n - 1)2^n \), it follows that

\[
|Σ| = (2^n + 1) + \frac{1}{2}(2^n - 1)2^n + \frac{1}{2}(2^n + 1)2^n = 2^{2n} + 2^n + 1.
\]

Thus \( SL(2, 2^n) ∈ \mathcal{M}(2^{2n} + 2^n + 1) \). So we see that \( SL(2, 2^n) \) and the dihedral group of order \( 4(2^n + 2^n) \), that is, a nonabelian simple and a metacyclic group, have isomorphic centralizer lattices.

(e) Let \( G = S_4 \). Then \( G \) has no element of order 6 and hence every proper centralizer in \( G \) is either a 2-group or a 3-group. It follows easily that \( \mathcal{E}(G) \) consists of 1, \( G \), and the centralizer lattices of the Sylow subgroups of \( G \). Since \( G \) has 4 Sylow 3-

![Figure 26](image-url)
Further lattices

subgroups of order 3 and 3 Sylow 2-subgroups isomorphic to $D_3$ intersecting in the
Klein four-group, we obtain the lattice $\mathcal{E}(G)$ displayed in Figure 26.

If $H$ is a subgroup of $G$, the only connection between $\mathcal{E}(H)$ and $\mathcal{E}(G)$ in general is
that every element $K$ in $\mathcal{E}(H)$ is of the form $K = C_H(X) = C_G(X) \cap H$ for some
$X \leq H$ and hence is the intersection of $H$ with an element of $\mathcal{E}(G)$. Since the intersection
of two centralizers is a centralizer, it follows that $K \in \mathcal{E}(G)$ if $H \in \mathcal{E}(G)$. Thus

(6) $\mathcal{E}(H) \subseteq [H/Z(H)]_c$ if $H \in \mathcal{E}(G)$.

The following two simple remarks are used quite often. First, if $x \in G$, then

(7) $C_G(x) = C_G(\langle x \rangle) \in \mathcal{E}(G)$,

that is, every element centralizer belongs to $\mathcal{E}(G)$. The other is that every abelian
subgroup of $G$ is contained in a maximal abelian subgroup of $G$ and these also
belong to $\mathcal{E}(G)$.

(8) If $A$ is a maximal abelian subgroup of $G$, then $A = C(A) \in \mathcal{E}(G)$.

Indeed, $A \leq C(A)$ since $A$ is abelian. And if $x \in C(A)$, then $B = \langle A, x \rangle$ is an abelian
subgroup of $G$ containing $A$ and hence equal to $A$ by maximality of $A$. Thus $x \in A$
and $A = C(A) \in \mathcal{E}(G)$. Conversely, if $H \in \mathcal{E}(G)$ satisfies $H = C(H)$, then $H$ is clearly a
maximal abelian subgroup of $G$. Thus the maximal abelian subgroups are precisely
the fixed points of the duality $C$ in Theorem 9.3.1.

We come to another important general property of $\mathcal{E}(G)$.

9.3.3 Lemma. Let $H \in \mathcal{E}(G)$. Then $\mathcal{E}(H \vee C(H)) = [H \vee C(H)/H \wedge C(H)]_c$.

Proof. For short, let $F = H \vee C(H)$ and $D = H \wedge C(H)$. Then by 9.3.1,

$C(F) = C(H \vee C(H)) = C(H) \wedge CC(H) = C(H) \wedge H = D$

and hence $C(D) = CC(F) = F$. Since $D \leq F$, it follows that $D = Z(F)$. Now if
$X \in C(F)$, then $X \geq Z(F) = D$ and, by (6), $X \in \mathcal{E}(G)$; thus $X \in [F/D]_c$. Conversely,
if $X \in [F/D]_c$, then $D \leq X \leq F$ and hence by (3), $D = C(F) \leq C(X) \leq C(D) = F$.
Thus $C(X) = C_F(X)$, and if we apply this to $C(X)$ in place of $X$, we obtain that
$X = CC(X) = C_F(C(X)) \in \mathcal{E}(F)$.

Let us call an atom of $\mathcal{E}(G)$ a minimal centralizer and an antiautom a maximal
centralizer of $G$. If $N$ is a minimal centralizer of $G$ and $x \in N \setminus Z(G)$, then
$x \in C_G(x) \cap N \in \mathcal{E}(G)$ so that $Z(G) < C_G(x) \cap N \leq N$. The minimality of $N$ implies
that $C_G(x) \cap N = N$ and hence $N \leq C_G(x)$. Since this clearly also holds for $x \in Z(G)$,
we have shown that

(9) every minimal centralizer is abelian.

If $M$ is a maximal centralizer, then by (4), $Z(G) \neq C(M)$ and hence there exists an
element $x$ (of prime power order if $G$ is finite) in $C(M) \setminus Z(G)$. Then $M \leq C_G(x) < G$
and so $M = C_G(x)$. Thus
(10) every maximal centralizer is of the form $M = C_G(x)$ where $x$ can be chosen of prime power order if $G$ is finite.

But the main property of a maximal centralizer is the following consequence of 9.3.3 and (9).

**9.3.4 Lemma.** If $M$ is a maximal centralizer of $G$, then $C(M) \leq M$ and $\mathcal{C}(M) = \left[ M/C(M) \right]_C$.

**Proof.** Since $C|_{\mathbb{S}(G)}$ is a duality, $C(M)$ is a minimal centralizer of $G$ and hence is abelian, by (9). It follows that $C(M) \leq CC(M) = M$. Now 9.3.3 yields that $\mathcal{C}(M) = \left[ M/C(M) \right]_C$.

Finally, suppose that $G$ is nonabelian and $\mathcal{C}(G)$ satisfies the maximal condition. Then maximal centralizers exist and, by (8), every maximal abelian and hence

(11) every abelian subgroup of $G$ is contained in a maximal centralizer.

In particular, every element of $G$ is contained in a maximal centralizer and since $G$ cannot be the set-theoretic union of two proper subgroups, it follows that

(12) $G$ has at least 3 maximal centralizers.

**Distributive centralizer lattices**

There are no distributive centralizer lattices except the trivial one, a fact that can be proved quite simply.

**9.3.5 Theorem.** Let $G$ be a group. Then $\mathcal{C}(G)$ is distributive if and only if $G$ is abelian.

**Proof.** If $G$ is abelian, then $|\mathcal{C}(G)| = 1$ and therefore $\mathcal{C}(G)$ is distributive. Suppose conversely that $\mathcal{C}(G)$ is distributive and let $a, b \in G$. Then $C_G(b) \wedge C_G(ab) = C_G(b) \cap C_G(ab) \leq C_G(a)$ and hence the distributive law implies that

$$C_G(a) = C_G(a) \vee (C_G(b) \wedge C_G(ab)) = (C_G(a) \vee C_G(b)) \wedge (C_G(a) \vee C_G(ab)).$$

Now $b \in C_G(b) \leq C_G(a) \vee C_G(b)$ and $b = a^{-1}ab \in C_G(a) \cup C_G(ab) \leq C_G(a) \vee C_G(ab)$, by (2). Therefore $b$ is contained in the right hand side of the above equation and so $b \in C_G(a)$. Thus $ab = ba$ and $G$ is abelian.

**Direct products**

It is easy to see that, in contrast to subgroup lattices, the centralizer lattice of an arbitrary direct product of groups is the direct product of the centralizer lattices of the direct factors. We restrict ourselves to a finite number of direct factors and prove a more general result. For this we need a name for the set of all commutators of
elements of a group, which, as is well-known, in general is different from the commutator subgroup. So let us write \( \text{Com} G = \{ [x, y] | x, y \in G \} \).

9.3.6 Theorem. If \( G = HK \) such that \( [H, K] = 1 \) and \( \text{Com} H \cap \text{Com} K = 1 \), then \( \mathfrak{C}(G) \cong \mathfrak{C}(H) \times \mathfrak{C}(K) \). In particular, if \( G = H \times K \), then \( \mathfrak{C}(G) \cong \mathfrak{C}(H) \times \mathfrak{C}(K) \).

Proof. We show first that for every subset \( M \) of \( G \),

\[
(13) \quad C_G(M) = C_H(M)C_K(M).
\]

For this let \( c \in C_G(M) \) and \( x \in M \). Since \( G = HK \), there exist elements \( c_1, x_1 \in H \) and \( c_2, x_2 \in K \) such that \( c = c_1c_2 \) and \( x = x_1x_2 \). Since \( [H, K] = 1 \), we have \( 1 = [c, x] = [c_1, x_1][c_2, x_2] \) and hence \( [c_1, x_1] = [x_2, c_2] \in \text{Com} H \cap \text{Com} K = 1 \). So \( c_1 \) centralizes \( x_1 \) and hence also \( x \); this holds for all \( x \in M \) so that \( c_1 \in C_H(M) \). Similarly, \( c_2 \in C_K(M) \) and we see that \( C_G(M) \leq C_H(M)C_K(M) \). Since the other inclusion is trivial, (13) follows.

Now let \( X = C_H(R) \in \mathfrak{C}(H) \) and \( Y = C_K(S) \in \mathfrak{C}(K) \) where \( R \leq H \) and \( S \leq K \). Then \( RS \) is a subgroup of \( G \) since \( [H, K] = 1 \), and, by (13), \( C_G(RS) = C_H(RS)C_K(RS) = C_H(R)C_K(S) = XY \). This shows that there is a well-defined map \( \psi : \mathfrak{C}(H) \times \mathfrak{C}(K) \to \mathfrak{C}(G) \) satisfying \((X, Y) \psi = XY \). Since \( K \cap H \leq Z(H) \leq X \),

\[
(14) \quad XK \cap H = X(K \cap H) = X.
\]

So if \( A \in \mathfrak{C}(H) \), \( B \in \mathfrak{C}(K) \), and \((A, B) \psi = (X, Y) \psi \), then \( X = XK \cap H = XYK \cap H = ABK \cap H = AK \cap H = A \); similarly, \( Y = B \) and \( \psi \) is injective. For \( T \leq G = HK \), Dedekind's law implies that \( TK = (TK \cap H)K \) and \( TH = H(TH \cap K) \). So by (13),

\[
C_G(T) = C_H(T)C_K(T) = C_H(TK)C_K(TH) = C_H(TK \cap H)C_K(TH \cap K)
\]

and this shows that \( \psi \) is surjective. Finally, \((A, B) \leq (X, Y) \) clearly implies \((A, B) \psi = AB \leq XY = (X, Y) \psi \); conversely, if \((A, B) \psi \leq (X, Y) \psi \), then \( AB \leq XY \leq XK \) and by (14), \( A \leq XK \cap H = X \). Similarly, \( B \leq Y \) and so \((A, B) \leq (X, Y) \). By 1.1.2, \( \psi \) is an isomorphism.

Exercise 3 shows that the assumption \( \text{Com} H \cap \text{Com} K = 1 \) is needed in the above theorem. In fact, we are now going to show that for groups whose centralizer lattice has finite length, the converse of 9.3.6 almost holds. For this we need the following auxiliary result.

9.3.7 Lemma. Assume that \( G = HK \) where \( H = C_G(K) \) and \( K = C_G(H) \). If \( A \in \mathfrak{C}(H) \) and \( B \in \mathfrak{C}(K) \), then \( AB \in \mathfrak{C}(G) \).

Proof. By (6), \( A, B \in \mathfrak{C}(G) \) and, by (2), \( AB \leq A \lor B \). Let \( x \in A \lor B \) and write \( x = x_1x_2 \) where \( x_1 \in H, x_2 \in K \). Then by 9.3.1, \( x \in A \lor B \leq A \lor K = CC(A) \lor C(H) = C(C(A) \land H) = C(C_H(A)) \). Therefore every \( c \in C_H(A) \) satisfies \( 1 = [c, x] = [c, x_1x_2] = [c, x_1] \) since \([c, x_2] \in [H, K] = 1 \). Thus \( x_1 \in C_H(C_H(A)) = A \). Similarly, \( x_2 \in B \) and so \( x = x_1x_2 \in AB \). It follows that \( AB = A \lor B \in \mathfrak{C}(G) \).
9.3 Centralizer lattices

9.3.8 Theorem. Let $G$ be a group such that $\mathcal{C}(G)$ has finite length. Assume that $\mathcal{C}(G)$ is the direct product of two lattices $L_1$ and $L_2$, write $O_1, I_1$ and $O_2, I_2$ for the least and greatest elements of $L_1$ and $L_2$, respectively, and let $H = (I_1, O_2)$ and $K = (O_1, I_2)$. Then

(a) $C_G(H) = K$ and $C_G(K) = H$,

(b) $\text{Com } H \cap \text{Com } K = 1$, and

(c) $\mathcal{C}(H) = [H/Z(G)]_c \cong L_1$, $\mathcal{C}(K) = [K/Z(G)]_c \cong L_2$, and hence $\mathcal{C}(HK) \cong \mathcal{C}(G)$.

Proof. (a) If $|L_1| = 1$, then $H = Z(G)$, $K = G$, and (a)–(c) hold trivially. So we may assume that $|L_1| \neq 1 \neq |L_2|$ and show first by induction on the length of $\mathcal{C}(G)$ that

$$[H, K] = 1.$$ 

By (12), $G$ contains at least 3 maximal centralizers. These have the form $(I_1, x) \text{ or } (y, I_2)$ with antiatoms $x$ of $L_2$ and $y$ of $L_1$; hence at least one of the two lattices has more than one antiatom. So let $x_1, x_2$ be two different antiatoms of $L_2$, say, and let $M = (I_1, x)$ where $x = x_1$ or $x = x_2$. Then by 9.3.4, $C(M) \leq M$ and $\mathcal{C}(M) = [M/C(M)]_c$. So $C(M) = (w, z)$ where $w \in L_1$, $z \in L_2$ and $z \leq x$; it follows that

$$[M/C(M)]_c = [(I_1, x)/(w, z)] = \{(s, t) \mid w \leq s \leq I_1, z \leq t \leq x\} = [I_1/w] \times [x/z].$$

Since $[M/C(M)]_c$ is a proper interval in $\mathcal{C}(G)$, by induction, (15) holds for $M$. So if $H_0 = (I_1, x)$ and $K_0 = (w, x)$, then $[H_0, K_0] = 1$. Now $H \leq H_0$ and $(O_1, x) \leq K_0$; thus $(O_1, x) \leq C(H)$. If we apply this with $x = x_1$ and $x = x_2$, it follows that $K = (O_1, I_2) = (O_1, x_1) \vee (O_1, x_2) \leq C(H)$ and (15) holds.

By (15), $C(H) \geq K = (O_1, I_2)$ and hence $C(H) = (u, I_2)$ for some $u \in L_1$; similarly $C(K) = (I_1, v)$ with $v \in L_2$. Since $G = (I_1, I_2) = H \lor K$, Theorem 9.3.1 yields that $Z(G) = C(H) \land C(K) = (u, v)$. It follows that $u = O_1$ and $v = O_2$; thus $C(H) = (O_1, I_2) = K$ and $C(K) = H$.

(b) Let $a \in H$ and $b \in K$. Every $X \in \mathcal{C}(G) = L_1 \times L_2$ satisfies $X = (X \land H) \lor (X \land K)$ and so $C_G(ab) = C_H(ab) \lor C_K(ab) = C_H(a) \lor C_K(b)$ since $[H, K] = 1$. By 9.3.7 applied to the group $HK$ there exists $T \leq HK$ such that $C_H(a)C_K(b) = C_{HK}(T)$. Then $C_H(a)$ and $C_K(b)$ are contained in $C_G(T)$; it follows that

$$C_{HK}(ab) = C_G(ab) \cap HK = (C_H(a) \lor C_K(b)) \cap HK \leq C_G(T) \cap HK$$

and hence $C_{HK}(ab) \leq C_{HK}(T) = C_H(a)C_K(b)$. Since the other inclusion is trivial, we have shown that

$$C_{HK}(ab) = C_H(a)C_K(b) \text{ for all } a \in H, b \in K.$$ 

Now suppose, for a contradiction, that $\text{Com } H \cap \text{Com } K \neq 1$. Then there exist $a, c \in H$ and $b, d \in K$ such that $1 \neq [a, c] = [d, b]$. Since $[H, K] = 1$, this implies that $1 = [a, c][b, d] = [ab, cd]$ and hence $cd \in C_{HK}(ab) = C_H(a)C_K(b)$, by (16). Since $d \in K$, it follows that $c \in C_H(a)K \cap H = C_H(a)(K \cap H) = C_H(a)$, contradicting $[a, c] \neq 1$. Thus $\text{Com } H \cap \text{Com } K = 1$.

(c) Of course, $[H/Z]_c = \{(x, O_2) \mid x \in L_1\} \cong L_1$ and we show that $\mathcal{C}(H) = [H/Z]_c$. 

Further lattices

Indeed, if \( X \in \mathcal{C}(H) \), then by (6), \( X \in \mathcal{C}(G) \) and so \( Z \leq X \leq H \); thus \( \mathcal{C}(H) \subseteq [H/Z]_c \). Conversely, if \( X \in [H/Z]_c \), then \( C_G(X) \geq C_G(H) = K \) and hence \( C_G(X) = (y, 1) = Y \cup K \) for some \( y \in L_1 \) and \( Y = (y, O_2) \leq H \). By 9.3.1,

\[
X = C_G(C_G(X)) = C_G(Y \cup K) = C_G(Y) \cap H = C_H(Y) \in \mathcal{C}(H).
\]

Thus \( \mathcal{C}(H) = [H/Z]_c \simeq L_1 \), similarly \( \mathcal{C}(K) \simeq L_2 \) and, by 9.3.6, \( \mathcal{C}(HK) \simeq L_1 \times L_2 = \mathcal{C}(G) \).

If we combine Theorems 9.3.6 and 9.3.8, we obtain a result that was proved by Antonov [1987] for finite groups with modular centralizer lattices.

9.3.9 Corollary. Let \( G \) be a group such that \( \mathcal{C}(G) \) has finite length. Then \( \mathcal{C}(G) \) is a direct product of two lattices \( L_1 \) and \( L_2 \) if and only if \( G \) contains subgroups \( H \) and \( K \) such that \( \mathcal{C}(HK) \simeq \mathcal{C}(G) \), \( [H, K] = 1 \), \( \text{Com} H \cap \text{Com} K = 1 \), \( \mathcal{C}(H) \simeq L_1 \) and \( \mathcal{C}(K) \simeq L_2 \).

It is not known whether 9.3.8 and 9.3.9 are true without the assumption that \( \mathcal{C}(G) \) has finite length. Exercise 4 shows that \( HK \) may be a proper subgroup of \( G \) in Theorem 9.3.8, although, of course, \( G \) is the join of \( H \) and \( K \) in the centralizer lattice.

Modular centralizer lattices

There are many groups with modular centralizer lattice and so there are only a few general results about these groups and lattices. One of them is the simple fact that their length is even if it is finite. After proving this we shall study finite groups with centralizer lattice of length 2 and, as an application, determine all finite simple groups with modular centralizer lattice.

9.3.10 Lemma. If \( \mathcal{C}(G) \) is modular and of finite length \( l \), then \( l \) is even.

Proof. Recall from 2.1.10 that \( \mathcal{C}(G) \) satisfies the Jordan-Dedekind chain condition, and consider a maximal abelian subgroup \( A \) of \( G \). By (8), \( A = C(A) \in \mathcal{C}(G) \) and hence there exists a maximal chain \( Z(G) = A_0 < A_1 < \cdots < A_n = A < A_{n+1} < \cdots < A_l = G \) in \( \mathcal{C}(G) \) containing \( A \). Then \( Z = A_0 < \cdots < A_n = A \) and \( Z = C(A_1) < \cdots < C(A_n) = A \) are two maximal chains from \( Z \) to \( A \) and therefore have the same length. Thus \( n = l - n \), that is, \( l = 2n \) is even.

Let us write \( G \in \mathcal{M} \) if \( \mathcal{C}(G) \) is (modular) of length 2. So \( \mathcal{M} \) is the union of the classes \( \mathcal{M}(k) \), \( k \in \mathbb{N} \cup \{\infty\} \), defined in 9.3.2(c). We shall also say that \( G \) is an \( \mathcal{M} \)-group if \( G \in \mathcal{M} \), trusting that the reader will not confuse these with the \( M \)-groups studied in Chapter 2. If \( G \) is an \( \mathcal{M} \)-group, then every \( H \in \mathcal{C}(G) \setminus \{G, Z\} \) is a minimal centralizer and hence is abelian, by (9). Conversely, if \( G \) is nonabelian and every proper centralizer of \( G \) is abelian, then every \( H \in \mathcal{C}(G) \setminus \{G, Z\} \) is contained in a maximal abelian subgroup \( A \) of \( G \). If \( H < A \), it would follow that \( A = C(A) < C(H) \) and so \( C(H) \)
would not be abelian, a contradiction. Therefore \( H = A \) and since two different maximal abelian subgroups cannot be contained in each other, it follows that \( G \in \mathcal{M} \).

Thus

\[(17) \ G \in \mathcal{M} \text{ if and only if } G \text{ is nonabelian and every proper centralizer of } G \text{ is abelian.}\]

Now if \( H \leq G \in \mathcal{M} \), then every proper centralizer of \( H \) is contained in a proper centralizer of \( G \) and hence is abelian. So (17) implies that

\[(18) \text{ every subgroup of an } \mathcal{M}\text{-group is an } \mathcal{M}\text{-group or abelian.}\]

The main property of \( \mathcal{M}\)-groups, however, is the following. Recall from § 3.5 that a partition of a group \( G \) is a set \( \Sigma \) of nontrivial subgroups of \( G \) such that every nonidentity element of \( G \) is contained in a unique subgroup \( X \in \Sigma \).

**9.3.11 Lemma.** If \( G \) is an \( \mathcal{M}\)-group, then the set \( \Sigma \) of all \( M/Z(G) \) where \( M \) is a maximal abelian subgroup of \( G \) is a normal partition of \( G/Z(G) \); we call \( \Sigma \) the centralizer partition of \( G/Z(G) \).

**Proof.** Let \( Z = Z(G) \). If \( x \in G \), then \( x \in \langle x \rangle \leq M \) for some maximal abelian subgroup \( M \) of \( G \); thus \( xZ \in M/Z \). And if \( xZ \in M_1/Z \cap M_2/Z \) for two different maximal abelian subgroups \( M_1 \) and \( M_2 \) of \( G \), then \( x \in M_1 \cap M_2 = M_1 \land M_2 = Z \) and hence \( xZ = 1 \) in \( G/Z \). This shows that \( \Sigma \) is a partition. If \( M \) is a maximal abelian subgroup of \( G \) and \( g \in G \), then \( M^g \) is a maximal abelian subgroup of \( G \) and so \( \Sigma \) is normal.

Using the results of § 3.5 on partitions of finite groups, we obtain the following characterization of finite \( \mathcal{M}\)-groups.

**9.3.12 Theorem (Schmidt [1970c]).** A finite group \( G \) is an \( \mathcal{M}\)-group (and lies in \( \mathcal{M}(k) \)) if and only if it is a group of one of the following types:

(i) \( G = A \times P \) where \( A \) is abelian and \( P \) is a \( p\)-group in \( \mathcal{M}(k), \ p \) a prime; here \( k \equiv 1 \pmod{p} \).

(ii) \( G \) is nonabelian and has an abelian normal subgroup \( N \) of prime index; here \( k = |N : Z(G)| + 1 \).

(iii) \( G/Z(G) \) is a Frobenius group with Frobenius kernel \( F/Z(G) \) and Frobenius complement \( K/Z(G) \) where \( F \) and \( K \) are abelian; here \( k = |F : Z(G)| + 1 \).

(iv) \( G/Z(G) \) is a Frobenius group with Frobenius kernel \( F/Z(G) \) and Frobenius complement \( K/Z(G) \) where \( K \) is abelian, \( Z(F) = Z(G), F/Z(G) \) is a \( p\)-group, \( p \) a prime, and \( F \) is an \( \mathcal{M}\)-group; here \( k = |F : Z(G)| + m \) if \( F \in \mathcal{M}(m) \).

(v) \( G/Z(G) \cong S_4 \) and \( V \) is not abelian if \( V/Z(G) \) is the Klein four-group; here \( k = 13 \).

(vi) \( G/Z(G) \cong PSL(2, p^n) \) or \( PGL(2, p^n) \), \( G' \cong SL(2, p^n), \ p \) a prime, \( p^n > 3 \); here \( k = p^{2n} + p^n + 1 \).

(vii) \( G/Z(G) \cong PSL(2, 9) \) or \( PGL(2, 9) \), \( G' \) is isomorphic to the representation group of \( PSL(2, 9) \) in the sense of Schur; here \( k = 121 \).
Proof. We show first that every $\mathfrak{M}$-group has one of the properties (i)–(vii); then we prove that, conversely, every such group indeed lies in $\mathfrak{M}(k)$ where $k$ is as stated. So assume that $G$ is an $\mathfrak{M}$-group, let $Z = Z(G)$ and let $\Sigma$ be the centralizer partition of $G/Z$. By 3.5.10 and 3.5.11, we know the possible structure of $G/Z$ and, since the partition $\Sigma$ is normal, 3.5.7 and 3.5.9 show in addition that if $G/Z$ is a Frobenius group, then the Frobenius complements are components of $\Sigma$. Also, if $G/Z \simeq S_4$, then $\Sigma$ consists of the maximal cyclic subgroups of $G/Z$. So we have to consider the following six possibilities for $G/Z$.

(a) $G/Z$ is a $p$-group for some prime $p$. Let $A$ be the $p'$-component of $Z$ and $P \in \text{Syl}_p(G)$. Then $G = A \times P$, $A$ is abelian and, by 9.3.6, $\mathfrak{C}(P) \simeq \mathfrak{C}(G)$. Thus $G$ is of type (i).

(b) $G/Z$ has a normal subgroup $N/Z \in \Sigma$ of prime index. Since $N/Z \in \Sigma$, the group $N$ is abelian and so (ii) holds.

(c) $G/Z$ is a Frobenius group and the Frobenius complements are components of $\Sigma$. Let $F/Z$ be the Frobenius kernel and $K/Z$ a Frobenius complement of $G/Z$. Then $K$ is abelian since $K/Z \in \Sigma$. If $F$ too is abelian, then (iii) holds. Thus we assume that $F$ is not abelian. By (18), $F$ is an $\mathfrak{M}$-group and hence $Z(F) = A_1 \cap A_2$ for some maximal abelian subgroup $A_i$ of $F$. If $M_1$ is a maximal abelian subgroup of $G$ containing $A_i$ ($i = 1, 2$), it follows that $M_1 \neq M_2$ and $Z(F) = A_1 \cap A_2 \leq M_1 \cap M_2 = Z$. Since $Z \leq F$, the other inclusion is trivial and so $Z(F) = Z$. As a Frobenius kernel, $F/Z$ is nilpotent (see 3.5.1) and hence is a $p$-group for some prime $p$, by 3.5.3. Thus (iv) holds.

(d) $G/Z \simeq S_4$ and $\Sigma$ consists of the maximal cyclic subgroups of $S_4$. Since $V/Z$ is not cyclic, it is not contained in a component of $\Sigma$ and so $V$ is not contained in a maximal cyclic subgroup of $G$. Thus $V$ is not abelian and (v) holds.

(e) $G/Z \simeq \text{PSL}(2, p^n)$ or $\text{PGL}(2, p^n)$, $p$ a prime, $p^n \geq 4$. Let $H = G'Z$. Since $H/Z \simeq \text{PSL}(2, p^n)$ is simple, $H'/Z = H$ and hence $H/H'$ is central in $G/H'$ of index at most 2. Thus $G/H'$ is abelian, that is, $G' = H' = (G'Z)' = G''$. Therefore $G' \cap Z \leq (G')' \cap Z(G')$ and, by a well-known theorem of Schur's (see Huppert [1967], p. 629), $G' \cap Z$ is isomorphic to a subgroup of the Schur multiplier $M$ of $G'/G' \cap Z \simeq H/Z \simeq \text{PSL}(2, p^n)$. Now this Schur multiplier and the representation group of $\text{PSL}(2, p^n)$ are well-known (see Huppert [1967], p. 646). If $p = 2$ and $p^n \neq 4$, then $M = 1$ and so $G' \simeq \text{PSL}(2, 2^n) = \text{SL}(2, 2^n)$, as desired. If $p > 2$ and $p^n \neq 9$, then $|M| = 2$ and so $G' \simeq \text{PSL}(2, p^n)$ or $\text{SL}(2, p^n)$. Let $p^n \neq 5$ and suppose, for a contradiction, that $G' \simeq \text{SL}(2, p^n)$. Then $p^n + 1$ or $p^n - 1$ has 4 as a proper factor and $G'$ contains a dihedral group $D$ of this order (see Huppert [1967], p. 213). Then $Z(D) \neq 1$ and $C_G(Z(D))$ is a nonabelian proper centralizer in $G$, a contradiction. Thus $G' \simeq \text{SL}(2, p^n)$, as desired. We are left with the exceptional cases $p^n = 4$, 5, 9. Here $\text{PGL}(2, 4) = \text{PSL}(2, 4) \simeq \text{PSL}(2, 5)$ has representation group $\text{SL}(2, 5)$, so that if $G/Z \simeq \text{PSL}(2, 5)$, then (vi) holds with $p^n = 4$ or $p^n = 5$. Now let $G/Z \simeq \text{PGL}(2, 5)$ and suppose, for a contradiction, that $G' \simeq \text{PSL}(2, 5)$. Then $G' \cap Z = 1$ and if $A \in \text{Syl}_2(G')$, $S \in \text{Syl}_2(G)$ and $A \leq S$, then $A = G' \cap S \leq S$ and so $A \cap Z(S) \neq 1$. Thus $S \leq C_G(A \cap Z(S)) \leq G$ and, since $S$ is nonabelian, this is impossible. Thus $G' \simeq \text{SL}(2, 5)$ and (vi) holds. Finally, if $p^n = 9$, then $|M| = 6$ and, as shown above, $G' \neq \text{PSL}(2, 9)$. So $G' \cap Z \neq 1$ and we claim that $|G' \cap Z| \neq 3$. Indeed, if $|G' \cap Z| = 3$, a Sylow 2-subgroup $S$ of $G'$ would be dihedral of order 8 and, since $Z(S) \leq Z$, there would exist a nonabelian centralizer in $G$. Thus $|G' \cap Z| = 2$ or 6 and so (vi) or (vii) holds.
(f) $G/Z \cong S_2(q)$, $q$ a power of 2. The group $S_2(q)$ has nonabelian Sylow 2-subgroups which, by 3.5.3, have to be contained in components of $\Sigma$. Since all components of $\Sigma$ are abelian, this case cannot occur.

Now assume that, conversely, $G$ has one of the properties (i)–(vii). If $G$ satisfies (i), then by 9.3.6, $C(G) \cong C(P)$; so $G \in \mathfrak{M}(k)$ where $k \equiv 1 \pmod{p}$, by 3.5.10. If $G$ is of type (ii), then $G \in \mathfrak{M}([N : Z] + 1)$, by (c) of 9.3.2. If $G$ satisfies (iii) or (iv), then, since $K/Z$ operates fixed-point-freely on $F/Z$, every proper centralizer of $G$ is contained in $F$ or in a conjugate of $K$. So if $F$ and $K$ are abelian, $C(G) = \{Z, F, G\} \cup \{K^g | g \in C\}$ and therefore $G \in \mathfrak{M}(k)$ where $k = |G : N_0(K)| + 1 = |G : K| + 1 = |F : Z| + 1$. And if $F \in \mathfrak{M}(m)$ and $Z(F) = Z$, then $C(G)$ consists of $Z$, $G$, the maximal abelian subgroups of $F$, and the conjugates of $K$; thus $G \in \mathfrak{M}(k)$ where $k = |F : Z| + m$.

Now let $G$ be of type (v) and $M$ a maximal centralizer of $G$. We claim that $M/Z$ is a maximal cyclic subgroup of $G/Z$; since $S_4$ has 13 of these, it will follow that $G \in \mathfrak{M}(13)$. By (10), $M = C_G(x)$ for some $p$-element $x \in G \setminus Z$ and, since $M/Z$ centralizes $x$, we have that $M/Z$ is a $p$-group. Therefore we are done if $p = 3$. So let $p = 2$, $S/Z$ be a Sylow 2-subgroup of $G/Z$ containing $M/Z$, and $D/Z$ be the cyclic subgroup of order 4 of $S/Z$. As a cyclic extension of a central subgroup, $D$ is abelian. Since $V$ is nonabelian, $Z(V) = Z$ and hence $Z(S) = Z$. So $|M : Z| \leq 4$ and $Z < Z(M)$ implies that $M$ is abelian. If $D = M$, we are done. And if $D \neq M$, then $D \cap M \leq Z(S) = Z$ and hence $M/Z$ is a maximal cyclic subgroup of order 2 of $G/Z$, as desired.

We leave it as an exercise for the reader to show that every group of type (vi) and (vii) is an $\mathfrak{M}$-group. In the first case, the centralizer partition $\Sigma$ of $G/Z$ is described in 3.5.1(e); it has the Sylow $p$-subgroups of $G/Z$ as components. As in Example 9.3.2(c) for $SL(2, 2^n)$ one shows that $|\Sigma| = p^{2n} + p^n + 1$. In the second case, the centralizer partition of $G/Z$ consists of the maximal cyclic subgroups of $G/Z$, of which there are $3^4 + 4(3^2 + 1) = 121$.

As particular cases of the above theorem we obtain that $GL(2, p^n)$ and $SL(2, p^n)$ lie in $\mathfrak{M}(p^{2n} + p^n + 1)$ for $p^n > 3$. Also note that the two representation groups of $S_4$ satisfy (v); one of them is $GL(2, 3)$ (see Huppert [1967], p. 653).

Our theorem does not say much in the case where $G$ is a $p$-group in $\mathfrak{M}$. Here if $x \in Z_2(G) \setminus Z$, then $G' \leq C_G(Z_2(G)) \leq C_G(x) < G$ and so $N = C_G(x)$ is a normal maximal abelian subgroup of $G$ with abelian factor group; by 3.5.3, every element in $G/Z \setminus N/Z$ has order $p$. If $|G : N| = p$, then $G$ is a $p$-group with an abelian subgroup of index $p$ and so its structure is well-known. If $|G : N| \geq p^2$, Rocke [1975] shows that $c(G) \leq p$ and that $G'$ and $G/Z$ are of exponent $p$. In addition, for every $n \geq 2$ and $r \geq 0$, he constructs a $p$-group $G \in \mathfrak{M}$ of class $p$ having a normal maximal abelian subgroup $N$ of index $p^r$ such that $|N : G'Z| = p^r$.

Since $SL(2, p^n)$ is not simple for $p > 2$, Theorem 9.3.12 yields that the only finite nonabelian simple $\mathfrak{M}$-groups are the groups $SL(2, 2^n)$. We shall now show that these groups are the only finite nonabelian simple groups with modular centralizer lattice. For this we need the following two results which are perhaps of independent interest. The first one implies that every finite group in $\mathfrak{M}(p^n + 1)$ is soluble. We mention in passing another strange result of this kind: If $k$ is even, every finite group in $\mathfrak{M}(k)$ is soluble. This follows immediately from Theorem 9.3.12 and the simple fact that $p^{2n} + p^n + 1$ is odd for every prime $p$ and $n \in \mathbb{N}$.
9.3.13 Lemma. Let $p$ be a prime, $n \in \mathbb{N}$, and $G$ a finite group.

(a) If $G \in \mathcal{M}(p^n + 1)$, then either $G/Z(G)$ is a $p$-group or $G$ has a maximal abelian subgroup $A$ such that $A/Z(G)$ is a $p$-group and $B/Z(G)$ is a $p'$-group for every other maximal abelian subgroup $B$ of $G$.

(b) If $\mathcal{C}(G)$ is isomorphic to the lattice of subspaces of a vector space over $GF(p^n)$, then $G \in \mathcal{M}(p^n + 1)$ or $G/Z(G)$ is a $p$-group.

Proof. (a) Let $G \in \mathcal{M}(p^n + 1)$. Since $12$, $q^{2m} + q^m = q^m(q^{m} + 1)$, and $120$ are not prime powers, $G$ is not of type (v), (vi), or (vii). Suppose, for a contradiction, that $G$ is of type (iv). Then $F/Z$ is a $q$-group in $\mathcal{M}(m)$ for some $q \in \mathbb{P}$, $m \in \mathbb{N}$ and so $p^n + 1 = |F : Z| + m \equiv 1 \pmod{q}$, by (i) of 9.3.12. Thus $p = q$, let $|F : Z| = p^t$. Since $m$ is the number of components of a partition of $F/Z$, clearly $m < p^t$ and so $m = p^t + 1$ where $s < r$ and $(t, p) = 1$. It follows that $p^n = p^t + p^t = p^t(p^{r-t} + t)$; but $p^{r-t} + t$ is not a power of $p$. This contradiction shows that $G$ is of type (i), (ii), or (iii). Now if $G$ is of type (i), then $G/Z$ is a $q$-group and $p^n + 1 \equiv 1 \pmod{q}$ implies that $p = q$. If $G$ is of type (ii), then $|N : Z| = p^{r}$ and $|G : N| = q \in \mathbb{P}$. So if $q = p$, $G/Z$ is a $p$-group; and if $q \neq p$, every maximal abelian subgroup $B \neq N$ of $G$ satisfies $|B/Z| = |G/N| = q$ so that $B/Z$ is a $p'$-group. Similarly, if $G$ is of type (iii), $|F : Z| = p^n$ and the Frobenius complements have order prime to $|F/Z|$. This proves (a).

(b) If $H \in \mathcal{C}(G)$, then by (6), $\mathcal{C}(H) \subseteq [H/Z(H)]_c$. Suppose that this interval has length 2. Then $\mathcal{C}(H)$ has length 2, that is, $H$ is an $\mathcal{M}$-group. Further $[H/Z(H)]_c$ is isomorphic to the lattice of subspaces of a 2-dimensional vector space over $GF(p^n)$ and therefore has $p^n + 1$ atoms. If $X$ is such an atom and $x \in X \setminus Z(H)$, there exists a maximal abelian subgroup $A$ of $H$ such that $x \in A$. Then $x \in X \cap A$ and, since $X$ and $A$ are atoms in $[H/Z(H)]_c$ and $x \notin Z(H)$, it follows that $X = A \in \mathcal{C}(H)$. Thus we have shown:

(19) If $H \in \mathcal{C}(G)$ such that $[H/Z(H)]_c$ has length 2, then $\mathcal{C}(H) = [H/Z(H)]_c$ and $H \in \mathcal{M}(p^n + 1)$.

By 9.3.10, $\mathcal{C}(G)$ has even length $l$. If $l = 2$, then (19) shows that $G \in \mathcal{M}(p^n + 1)$, as desired. So we may assume that $l \geq 4$ and we have to show first that $A/Z$ is a $p$-group for every minimal centralizer $A$ of $G$. For this we need the following assertion.

(20) Let $A, B$ be atoms of $\mathcal{C}(G)$ such that $[A, B] = 1$. If $A/Z$ is a $p$-group, then so is $B/Z$.

To show this we may, of course, assume that $A \neq B$. Since $A$ and $B$ are atoms, $C(A)$ and $C(B)$ are antiatoms of $\mathcal{C}(G)$. And since any two maximal subspaces of a vector space have a common complement, there is an atom $D$ of $\mathcal{C}(G)$ such that $D \leq C(A)$ and $D \leq C(B)$. It follows that $H = A \lor B \lor D$ is not abelian. However, since $[A, B] = 1$, (9) yields that $AB$ is abelian and hence is contained in a maximal abelian subgroup $X$ of $H$. By (8) and (6), $X \in \mathcal{C}(G)$ and so $A \lor B \leq X$; since $[H/Z(G)]_c$ has length at most 3, it follows that $A \lor B = X$. Now $H = X \lor D$ implies that $Z(H) = H \cap C(H) = H \cap C(X) \cap C(D) = C_H(X) \cap C(D) = X \cap C(D)$. Since $C(D)$ is an antiatom of $\mathcal{C}(G)$ and $\mathcal{C}(G)$ is modular, $X \cap C(D)$ is maximal in $X$ and so $Z(H)$ is an atom of $\mathcal{C}(G)$. Thus $[H/Z(H)]_c$ has length 2 and, by (19), $H \in \mathcal{M}(p^n + 1)$. \\[25x606]
By (a), $H/Z(H)$ is a $p$-group or has a maximal abelian subgroup $N$ such that $N/Z(H)$ is a $p$-group and $Y/Z(H)$ is a $p'$-group for any other maximal abelian subgroup $Y$ of $H$. In the latter case, since $AZ(H)/Z(H) \simeq A/A \cap Z(H) = A/Z$ is a nontrivial $p$-group contained in $X/Z(H)$, it follows that $X = N$. Thus in both cases $X/Z(H)$ is a $p$-group; hence $B/Z$ is a $p$-group since $B/Z \simeq BZ(H)/Z(H) \leq X/Z(H)$. This proves (20).

(21) If $A$ is an atom of $\mathfrak{C}(G)$, then $A/Z$ is a $p$-group.

Indeed, let $B$ be an atom of $\mathfrak{C}(G)$ such that $B \not\leq C(A)$ and let $H = A \lor B$. Since $\mathfrak{C}(H) \subseteq [H/Z]_C$ and this interval has length 2, we must have $Z(H) = Z$ and so $H \in \mathfrak{M}(p^n + 1)$, by (19). Now (a) implies that $H$ contains an atom $X$ of $\mathfrak{C}(G)$ such that $X/Z$ is a $p$-group. Since $l \geq 4$, we have $H \neq G$ and so $C(H)$ contains an atom $Y$ of $\mathfrak{C}(G)$. Then $[X, Y] = 1 = [Y, A]$ and, applying (20) twice, we obtain that $Y/Z$ and $A/Z$ are $p$-groups. This proves (21).

Finally we use induction on the length $l$ of $\mathfrak{C}(G)$ to show that $G/Z$ is a $p$-group (if $l \geq 4$); this will complete the proof of the lemma. Since every element $x \in G$ lies in a maximal abelian subgroup of $G$, it suffices to show that $A/Z$ is a $p$-group for every maximal abelian subgroup $A$ of $G$. For this let $M$ be a maximal centralizer containing $A$. Then $Z < C(M) = Z(M) < A < M < G$. So if $l = 4$, $[M/Z(M)]_C$ has length 2 and by (19), $M \in \mathfrak{M}(p^n + 1)$. Since $[A/Z]_C$ is isomorphic to the lattice of subspaces of a 2-dimensional vector space, there exists an atom $X \not\leq Z(M)$ of $\mathfrak{C}(G)$ such that $X \leq A$. By (21), $X/Z$ and $Z(M)/Z$ are $p$-groups and $X/Z \simeq XZ(M)/Z(M) \leq A/Z(M)$; it follows from (a) that $A/Z(M)$ is a $p$-group. Thus $A/Z$ is a $p$-group, as desired. If $l > 4$, then by 9.3.10, $l \geq 6$ and so $\mathfrak{C}(M) = [M/Z(M)]_C$ has length at least 4. By induction and (21), $M/Z(M)$ and $Z(M)/Z$ are $p$-groups and then so is $A/Z$.

9.3.14 Theorem. (Antonov [1987]). If $G$ is a finite nonabelian simple group with modular centralizer lattice, then $G \simeq SL(2, 2^n)$ for some $n \geq 2$.

Proof. Suppose, for a contradiction, that the length $l$ of $\mathfrak{C}(G)$ is at least 4. Since the join of all atoms of $\mathfrak{C}(G)$ is clearly a normal subgroup of $G$ and $G$ is simple, this join—in $L(G)$ and in $\mathfrak{C}(G)$—equals $G$. By a well-known property of modular lattices (see Crawley and Dilworth [1973], p. 30), $\mathfrak{C}(G)$ is complemented.

Now suppose, for a contradiction, that $\mathfrak{C}(G)$ is directly decomposable. Then there exist nontrivial lattices $L_i$ ($i = 1, 2$) with least elements $O_i$ and greatest elements $I_i$ such that $\mathfrak{C}(G) = L_1 \times L_2$ and $L_1$ is directly indecomposable. If $H = (O_1, O_2)$ and $K = (O_1, I_2)$, then by 9.3.8, $[H, K] = 1$ and $\mathfrak{C}(H) = [H/Z(G)]_C \simeq L_1$. For $g \in G$, $H^g \in \mathfrak{C}(G)$; hence $H^g = (x, y)$ with $x \in L_1$, $y \in L_2$ and

$$\mathfrak{C}(H^g) = ([H/Z(G)]_C)^g = [H^g/Z(G)]_C \simeq [x/O_1] \times [y/O_2].$$

On the other hand, $\mathfrak{C}(H^g) \simeq \mathfrak{C}(H)$ is directly indecomposable and it follows that $x = O_1$ or $y = O_2$, that is, $H^g \leq K$ or $H^g = H$. In any case, $H^g \leq HK$ for all $g \in G$ and, since $G$ is simple, it follows that $HK = G$. But $K$ centralizes $H$, a contradiction.

Thus $\mathfrak{C}(G)$ is a finite, directly indecomposable, complemented, modular lattice of length at least 4 and it is well-known (see Crawley and Dilworth [1973], Chapter 13) that such a lattice is isomorphic to the lattice of subspaces of a vector space over
some finite field $GF(p^n)$. But now 9.3.13(b) yields that $G$ is a $p$-group, a contradiction. It follows that $l \leq 3$ and so $l = 2$, by 9.3.10. Thus $G$ is an $\mathfrak{M}$-group and, by 9.3.12, $G \simeq SL(2, 2^n)$ for some $n \geq 2$.

The structure of arbitrary finite groups with modular centralizer lattices is not known; only very special classes of such groups have been investigated. By 9.3.13, every finite group whose centralizer lattice is isomorphic to the lattice of subspaces of a vector space of dimension at least 3 over $GF(p^n)$ is a $p$-group. Antonov [1987] shows that $|A : Z| \leq p^n$ for every minimal centralizer $A$ of such a group and determines the group if $|A : Z| = p^n$ for all such $A$.

Jürgensen [1976] studies finite groups with modular centralizer lattices of length 4. She shows that such a group is soluble if it has trivial centre and the intersection $N$ of all the maximal centralizers of $G$ is different from $Z$; Exercise 9 gives an example of such a group. If $N = Z$, then either $G/Z$ is a $p$-group or $C(G)$ is decomposable into a direct product of two lattices of length 2; in this case 9.3.8 and 9.3.12 give the structure of $G$.

Finally, Vasileva [1977] studies $\mathfrak{M}_2$-groups, that is, non-$\mathfrak{M}$-groups whose maximal centralizers are either abelian or in $\mathfrak{M}$. These centralizer lattices, of course, need not be modular, an example is $C(S_4)$. Her main result is that the finite simple $\mathfrak{M}_2$-groups are precisely the groups $PSL(2, q)$ ($q$ odd, $q \geq 5$), $Sz(2^{2n+1})$ ($n \geq 1$), $PSL(3, q)$ ($q > 2$), $PSU(3, q)$ ($q > 2$), the Janko group $J_1$, the alternating group $A_7$, and the Mathieu group $M_{11}$.

Characterization by centralizer lattices

By 9.3.6, $C(G) \simeq C(G \times A)$ for every abelian group $A$. So at best it is possible to characterize a group modulo abelian direct factors or in a certain class of groups, for example, among the groups with trivial centre. Vasileva's theorem and Theorem 9.3.12 (or 9.3.14) yield such characterizations. We give three other results of this type without proof; all these proofs are quite technical and use rather special properties of the groups studied.

9.3.15 Theorem. Let $G$ be a finite group, $p$ a prime, $n \in \mathbb{N}$.

(a) (Schmidt [1970d]) If $C(G) \simeq C(J_1)$, then $G = A \times J_1$, where $A$ is abelian.

(b) (Schmidt [1972a]) If $C(G) \simeq C(PSL(2, p^n))$ and $Z(G) = 1$, then $G \simeq PSL(2, p^n)$.

(c) (Vasileva [1976]) If $C(G) \simeq C(PSL(3, p^n))$ and $Z(G) = 1$, then $G \simeq PSL(3, p^n)$.

$C(G)$ as a sublattice of $L(G)$

Finally we turn to the question of when $C(G)$ is a sublattice of $L(G)$. This is certainly the case if $C(G) = L(G)$, that is, if every subgroup of $G$ is a centralizer. The finite groups with this property were determined by Gaschütz in 1955. More generally, we study finite groups $G$ for which $C(G) = [G/Z(G)]$, that is, in which every subgroup containing the centre is a centralizer. This property is inherited by subgroups.
9.3.16 Lemma. If $\mathcal{C}(G) = [G/Z(G)]$ and $H \leq G$, then $\mathcal{C}(H) = [H/Z(H)]$.

Proof. By 9.3.1, the centralizer map is a duality of $[G/Z]$. In particular, for all $X, Y \geq Z$, we have $C(X \cap Y) = C(X) \cup C(Y)$. Using this, 9.3.1, and Dedekind's law, we get for $Z(H) \leq A \leq H$,

$$C_H(C_H(A)) = C(C(A) \cap H) \cap H = C((C(A) \cap H)Z) \cap H = C(C(A) \cap HZ) \cap H = (CC(A) \cup C(H)) \cap H = AC(H) \cap H = A(C(H) \cap H) = AZ(H) = A.$$ 

Thus $A \in \mathcal{C}(H)$, as desired.

9.3.17 Theorem. The finite group $G$ satisfies $\mathcal{C}(G) = [G/Z(G)]$ if and only if $G = G_1 \times \cdots \times G_r \times A$ where $(|G_1|, |G_i|) = 1 = (|G_i|, |A|)$ for $i \neq j$, $A$ is abelian, and every $G_i$ is either a $\{p, q\}$-group with $|G_i/Z(G_i)| = pq$ or a $p$-group satisfying $\mathcal{C}(G_i) = [G_i/Z(G_i)]$, $p$ and $q$ primes.

Proof. Suppose that $G$ has this structure. Then $G/Z \simeq G_1/Z(G_1) \times \cdots \times G_r/Z(G_r)$. If $|G_i/Z(G_i)| = pq$ and $Z(G_i) < X < G_i$, then $X$ is a maximal abelian subgroup of $G_i$ and hence $X \in \mathcal{C}(G_i)$. Thus $\mathcal{C}(G_i) = [G_i/Z(G_i)]$ for all $i$; by 9.3.6 and 1.6.4,

$$\mathcal{C}(G) \simeq \mathcal{C}(G_1) \times \cdots \times \mathcal{C}(G_r) = [G_1/Z(G_1)] \times \cdots \times [G_r/Z(G_r)] \simeq [G/Z].$$

Since $\mathcal{C}(G)$ is a subset of $[G/Z]$, it follows that $\mathcal{C}(G) = [G/Z]$.

Suppose conversely that $\mathcal{C}(G) = [G/Z]$. Then by 9.3.1, $G/Z$ has a dual and hence, by 8.2.3, is a direct product of coprime $p$-groups and $P$-groups. Now, in general, if $G/Z = X/Z \times Y/Z$ where $X/Z$ is a $\pi$-group and $Y/Z$ is a $\pi'$-group, then $G = H \times K$ with $\pi$-group $H$ and $\pi'$-group $K$ satisfying $H/Z(H) \simeq X/Z$. Indeed, $O_\pi(Z)$ is a normal Hall subgroup in $X$ and hence has a complement $H$ in $X$, by the Schur-Zassenhaus Theorem. Then $X = H \times O_\pi(Z)$ and $H \leq G$ since $H$ is characteristic in $X \leq G$. Similarly, $Y = O_{\pi'}(Z) \times K$ where $K$ is a normal $\pi'$-subgroup of $G$. Since $O_\pi(Z) \leq H$ and $O_{\pi'}(Z) \leq K$, it follows that $G = H \times K$. Now $Z(H) = H \cap Z$ and so $H/Z(H) \simeq X/Z$.

If we apply this to the given direct decomposition of $G/Z$, we see that $G = G_1 \times \cdots \times G_r \times A$ where $A$ is abelian, $(|G_i|, |G_j|) = 1 = (|G_i|, |A|)$ for $i \neq j$, and $G_i/Z(G_i)$ is a $p$-group or a $P$-group. By 9.3.16, $\mathcal{C}(G_i) = [G_i/Z(G_i)]$ for all $i$. If $G_i/Z(G_i)$ is a $P$-group of order $p^aq$, $p > q$, then $G_i/Z(G_i)$ has a unique maximal normal subgroup (of order $p^a$). Since the centralizer duality maps normal subgroups to normal subgroups, it follows that $G_i/Z(G_i)$ has only one minimal normal subgroup. But every subgroup of order $p$ of $G_i/Z(G_i)$ is normal, so $n = 1$.

If we add the condition $Z(G) = 1$ in the above theorem, we get the structure of finite groups in which every subgroup is a centralizer.
9.3.18 Corollary (Gaschütz [1955]). Let \( G \) be a finite group. Then \( \mathfrak{C}(G) = L(G) \) if and only if \( G = G_1 \times \cdots \times G_r \) where \( (|G_i|, |G_j|) = 1 \) for all \( i \neq j \) and every \( G_i \) is non-abelian of order \( pq \), \( p \) and \( q \) primes.

Theorem 9.3.17 characterizes the finite groups \( G \) with \( \mathfrak{C}(G) = [G/Z(G)] \) modulo the \( p \)-groups with this property. The structure of these groups is also known; we give it without proof.

9.3.19 Theorem (Reuther [1977], Cheng [1982]). The following properties of the finite \( p \)-group \( G \) are equivalent:

(a) \( \mathfrak{C}(G) = [G/Z(G)] \),
(b) \( [G/Z(G)] \) is modular and \( G' \) is cyclic,
(c) \( G' = \langle a \rangle \) is cyclic and \( \langle \langle a \rangle, G \rangle \rangle \leq \langle a^d \rangle \).

Independently, and more generally, Antonov [1980] determined all groups \( G \) for which \( G/Z(G) \) is locally finite and \( \mathfrak{C}(G) = [G/Z(G)] \).

We return to the more general question of when \( \mathfrak{C}(G) \) is a sublattice of \( L(G) \). By (1), this is clearly the case if

\[
(22) \quad C(X \cap Y) = C(X) \cup C(Y) \quad \text{for all} \quad X, Y \leq G.
\]

However, this condition is much stronger. Reuther [1975] shows that a finite group \( G \) satisfies (22) if and only if \( G = G_1 \times \cdots \times G_r \) where \( (|G_i|, |G_j|) = 1 \) for all \( i \neq j \) and the \( G_i \) are abelian, isomorphic to \( Q_8 \), or have order \( pq^a \), \( p > q \), and cyclic Sylow subgroups. Clearly (22) implies that the map \( C^2 : L(G) \to L(G) \) sending every \( X \leq G \) to \( CC(X) \) is a homomorphism. Antonov [1980] studies the much weaker property that \( C^2 \) is a homomorphism from \( L(G) \) to \( \mathfrak{C}(G) \); since

\[
C^2(X \cup Y) = C(C(X) \cap C(Y)) = C^2(X) \vee C^2(Y)
\]

holds in general, this amounts to the condition that

\[
(23) \quad C^2(X \cap Y) = C^2(X) \wedge C^2(Y) \quad \text{for all} \quad X, Y \leq G.
\]

Nevertheless he is able to determine all groups \( G \) satisfying (23) for which \( G/Z(G) \) is locally finite. For finite groups, he obtains the same structure theorem as Reuther so that (22) and (23) are equivalent for these groups. Both Reuther and Antonov also study groups for which the equations in (22) and (23) only hold for all \( X, Y \in [G/Z(G)] \).

We finish this section by mentioning a result of quite a different nature.

9.3.20 Theorem (Antonov [1991]). If \( \mathfrak{C}(G) \) is a sublattice of \( L(G) \) for a finite group \( G \), then \( \mathfrak{C}(G) \) is modular.

Exercises

1. Show that every abelian centralizer is the intersection of maximal abelian subgroups.
2. If \((G_\alpha)_{\alpha \in \Lambda}\) is a family of groups, show that \(\bigoplus_{\alpha \in \Lambda} G_\alpha \cong G_\Lambda\bigoplus_{\alpha \in \Lambda} C(G_\alpha)\).

3. (Schmidt [1970c]) Let \(G_1 = H_1 \times K_1\) with \(H_1 \cong \mathbb{Z}_8 \cong K_1\) and let \(G = G_1/D\) where \(D\) is the diagonal in the direct product \(Z(H_1) \times Z(K_1)\); let \(H = H_1/D\) and \(K = K_1/D\). Show that \(H \cong \mathbb{Z}_8 \cong K\), \(G = HK\) and \([H, K] = 1\), but \(L(G) \not\cong L(H) \times L(K)\).

4. (J"urgensen [1976]) Let \(P = \langle a \rangle \times \langle b \rangle\) be elementary abelian of order 25 and let \(c, d \in \text{Aut } P\) be defined by \(a^c = a^{-1}, b^c = b,\) and \(x^d = x^2\) for all \(x \in P\). Let \(Q = \langle c, d \rangle \leq \text{Aut } P\) and \(G = PQ\) be the semidirect product of \(P\) and \(Q\). Finally, let \(e = cd^2, H = \langle a, c \rangle\) and \(K = \langle b, e \rangle\). Show that \(H \cong K \cong D_10, H = C_G(K), K = C_G(H), |G : HK| = 2,\) and \(L(G) \cong L(H) \times L(K)\).

5. (Antonov [1987]) If \(G\) is a finite group and \(H \leq G\) such that \(|C(G)| = |C(H)|\), show that \(C(H) \cong C(G)\).

6. (Vasileva [1976]) If \(G\) is a finite group, \(H \leq K \leq G\) and \(C(H) \cong C(G)\), show that \(C(K) \cong C(G)\).

7. (Antonov [1987]) Let \(G\) be a finite \(p\)-group such that \(C(G)\) is isomorphic to the lattice of subspaces of a vector space over \(GF(p^n)\). If \(|A : Z(G)| = p^n\) for every minimal centralizer \(A\) of \(G\), show that \(C(G)\) is a sublattice of \(L(G)\).

8. (J"urgensen [1976]) Suppose that \(G\) is a finite group such that \(C(G)\) is modular of length 4 and the intersection \(N\) of all the maximal centralizers of \(G\) is different from \(Z(G)\).
   (a) Show that \([G/N]_C\) has length 2 and \(G/N\) has a normal partition.
   (b) If \(Z(G) = 1\), show that \(G\) is soluble.

9. (J"urgensen [1976]) Let \(M = \langle a, b, c | a^3 = b^3 = c^3 = 1, [a, b] = c, [a, c] = [b, c] = 1 \rangle\)
   be the nonabelian group of order 27 and exponent 3 and let \(x \in \text{Aut } M\) such that \(a^x = a^2, b^x = b, c^x = c^2\). Show that the semidirect product \(G = M \langle x \rangle\) has centralizer lattice modular of length 4.

10. If \(G\) is a finite group such that \(C(G) \cong C(S_4)\), show that \(G/Z(G) \cong S_4\).

11. (Reuther [1975]) If \(G\) is a finite nonabelian \(p\)-group satisfying (22), show that \(G \cong \mathbb{Z}_8\).

### 9.4 Coset lattices

In this final section we study the coset lattice \(\mathcal{R}(G)\) which was defined in §1.1. Our first main problem, to determine the groups whose coset lattices have special properties, is not a very fruitful one: almost any interesting lattice property is satisfied by nearly all or by very few coset lattices, or else it holds in \(\mathcal{R}(G)\) if and only if it holds in \(L(G)\). More interesting is the study of isomorphisms between coset lattices. Since the atoms of \(\mathcal{R}(G)\) are the one-element subsets of \(G\) and for any such atom \(\{g\}\), the interval \([G/\{g\}]\) in \(\mathcal{R}(G)\) is isomorphic to \(L(G)\), two groups with isomorphic coset lattices have the same order and isomorphic subgroup lattices.
Nevertheless there are nonisomorphic groups with isomorphic coset lattices. An isomorphism \( \sigma : \mathcal{R}(G) \to \mathcal{R}(\bar{G}) \) can be regarded as a bijective map from \( G \) to \( \bar{G} \) preserving cosets. We consider under which conditions \( \sigma \) is an isomorphism from \( G \) to \( \bar{G} \).

### Basic properties of \( \mathcal{R}(G) \)

Recall that \( \mathcal{R}(G) \) is the set of all right cosets of subgroups of \( G \) together with the empty set \( \emptyset \). With the set-theoretic inclusion as relation, \( \mathcal{R}(G) \) is a complete meet-sublattice of the lattice of all subsets of \( G \); we write \( \wedge \) and \( \vee \) for the intersection and join in \( \mathcal{R}(G) \). If \( H, K \leq G \) and \( a, b \in G \), then \( Ha \cap Kb = \emptyset \) or

\[
(1) \quad Ha \wedge Kb = Ha \cap Kb = Hx \cap Kx = (H \cap K)x \text{ for every } x \in Ha \cap Kb.
\]

Clearly, \( Ha \) and \( Kb \) are contained in \( \langle H, K, ba^{-1} \rangle a \). Conversely, if \( Mx \) is a coset containing \( Ha \) and \( Kb \), then \( a \in Mx \) implies \( Ha \subseteq Mx = Ma \) and hence \( H \leq M \); similarly \( K \leq M \) and \( ba^{-1} \in M \) since \( a, b \in Mx \). Thus \( \langle H, K, ba^{-1} \rangle a \) is the smallest coset containing \( Ha \) and \( Kb \), that is,

\[
(2) \quad Ha \vee Kb = \langle H, K, ba^{-1} \rangle a.
\]

Since \( aH = (aHa^{-1})a \), every left coset is a right coset and conversely; thus \( \mathcal{R}(G) \) is the set of all (right or left) cosets of \( G \). We shall need the following characterization of cosets.

\[
(3) \quad \text{A subset } X \text{ of } G \text{ is an element of } \mathcal{R}(G) \text{ if and only if } xy^{-1}z \in X \text{ for all } x, y, z \in X.
\]

Indeed, for \( h \in H \), we have \( h_1a(h_2a)^{-1}h_3a = h_1h_2^{-1}h_3a \in Ha \). Conversely, suppose that \( X \neq \emptyset \) satisfies the condition, let \( S = \{xy^{-1}|x, y \in X\} \) and \( x, y, u, v \in X \). Then \( (xy^{-1})(uv^{-1})^{-1} = xy^{-1}vu^{-1} \in S \) since \( xy^{-1}v \in X \), and so \( S \) is a subgroup of \( G \). Furthermore \( xy^{-1}v \in X \) implies \( Sv \subseteq X \) and \( x = xv^{-1}v \in Sv \) yields \( X \subseteq Sv \); thus \( X = Sv \) is a coset.

The least element of \( \mathcal{R}(G) \) is the empty set \( \emptyset \) and the greatest element is the coset \( G \). The atoms in the lattice of all subsets of \( G \) are the one-element subsets of \( G \) and these are cosets of the trivial subgroup 1. Therefore

\[
(4) \quad \text{the atoms of } \mathcal{R}(G) \text{ are the sets } \{g\} \text{ where } g \in G.
\]

Since the subgroups of \( G \) are precisely the cosets containing 1, we have that

\[
(5) \quad [G/1] = L(G).
\]

Here, and throughout this section, intervals are taken in \( \mathcal{R}(G) \). Note that if \( T \) is a subgroup of \( G \), an interval \([S/T]\) in \( \mathcal{R}(G) \) only contains subgroups of \( G \) so that we do not need to distinguish between intervals in \( \mathcal{R}(G) \) and \( L(G) \).

For \( g \in G \) and \( X, Y \subseteq G \), it is obvious that \( X \subseteq Y \) if and only if \( Xg \subseteq Yg \); and if \( X = Ha \) is a right coset, so is \( Xg = Hag \). Therefore the map

\[
(6) \quad \rho_g : \mathcal{R}(G) \to \mathcal{R}(G) \text{ given by } X^{\rho_g} = Xg \text{ for } \emptyset \neq X \in \mathcal{R}(G) \text{ is an isomorphism.}
\]
9.4 Coset lattices

Since $\mathfrak{R}(G)$ is the set of all left cosets in $G$, the map 

$$(7) \gamma_g: \mathfrak{R}(G) \to \mathfrak{R}(G) \text{ given by } X \mapsto g^{-1}X \text{ for } \emptyset \neq X \in \mathfrak{R}(G) \text{ is an isomorphism.}$$

Now $1^\mathfrak{R} = \{g\}$ yields $[G/\{g\}] \cong [G/1]$ and hence

$$(8) [G/\{g\}] \cong L(G) \text{ for every atom } \{g\} \text{ of } \mathfrak{R}(G).$$

Finally, note that for every subgroup $H$ of $G$, clearly,

$$(9) [H/\emptyset] = \mathfrak{R}(H).$$

**Groups with special coset lattices**

As mentioned above, coset lattices do not usually have nice lattice properties. For example, if $1 < H < G$ and $a \in G \setminus H$, then $\{\emptyset, \{a\}, Ha, \langle H, a \rangle, H\}$ is a nonmodular sublattice of $\mathfrak{R}(G)$. Thus a group with modular coset lattice is cyclic of at most prime order. With a little more effort, we can prove the following.

**9.4.1 Theorem** (Curzio [1957c], Loiko [1962]). The following properties of a group $G$ are equivalent.

1. $\mathfrak{R}(G)$ is modular.
2. $\mathfrak{R}(G)$ is lower semimodular.
3. $|G|$ is a prime or 1.

**Proof.** By 2.1.5, every modular lattice is lower semimodular and so (a) implies (b). Now let $\mathfrak{R}(G)$ be lower semimodular and suppose, for a contradiction, that $1 < H < G$; let $a \in G \setminus H$. By Zorn's Lemma there exists a subgroup $M$ maximal with respect to the properties $H \leq M \leq \langle H, a \rangle$ and $a \notin M$ (see the proof of Lemma 3.1.1). Clearly, $M$ is a maximal subgroup of $\langle H, a \rangle$ and, by (2), $\langle H, a \rangle = M \cup Ma$. So $M \cup Ma$ covers $M$ in $\mathfrak{R}(G)$, but $M \cap Ma = \emptyset \subset \{a\} \subset Ma$. As $\mathfrak{R}(G)$ is lower semimodular, this is a contradiction. It follows that $G$ is cyclic of at most prime order. Finally, if $|G|$ is a prime $p$, then $\mathfrak{R}(G)$ is of length 2 and has $p$ atoms. So $\mathfrak{R}(G)$ is modular.

Since a lattice of length 2 is distributive if and only if it has at most 2 atoms, we obtain from 9.4.1 the following.

**9.4.2 Corollary.** $\mathfrak{R}(G)$ is distributive if and only if $|G| \leq 2$.

**9.4.3 Theorem** (Curzio [1957c]). $\mathfrak{R}(G)$ is directly decomposable if and only if $|G| = 2$.

**Proof.** If $G = \{1, g\}$, then $\mathfrak{R}(G) = \{\emptyset, \{1\}, \{g\}, G\}$ is the direct product of two chains of length 1. Assume conversely that $\mathfrak{R}(G) = L_1 \times L_2$ with nontrivial lattices $L_i$. Let $O_i$ and $I_i$ be the least and greatest elements of $L_i$, respectively, and let $(I_1, O_2) = Hu$ and $(O_1, I_2) = Kv$ where $H, K \leq G$ and $u, v \in G$. Every atom $\{g\}$ of $\mathfrak{R}(G)$ is of the
Further lattices

form \((x, O_2)\) or \((O_1, y)\) with \(x \in L_1, y \in L_2\) and hence is contained in \(Hu\) or \(Kv\). So if \(1 \in Hu\), say, we see that \(G\) is the set-theoretic union of \(H\) and \(Kv\). It follows that \(K \subseteq H\) and \(Hv \subseteq Kv\), that is, \(H = K\) is a subgroup of index 2 in \(G\). But then \(H = (l_1, O_2)\) is maximal in \(G = (l_1, l_2)\) and hence \((O_1, O_2) = \emptyset\) is also maximal in \((O_1, l_2) = Hv\). Thus \(Hv\) is an atom of \(\mathcal{R}(G)\) and this yields \(H = 1\) and \(|G| = 2\).

Exceptions to the statement made at the beginning of this subsection are the following two results.

**9.4.4 Theorem** (Curzio [1957c]). If every proper subgroup of \(G\) is contained in a maximal subgroup, then \(\mathcal{R}(G)\) is complemented. In particular, if \(G\) is finite or cyclic, \(\mathcal{R}(G)\) is complemented.

*Proof.* Let \(X \in \mathcal{R}(G)\) such that \(\emptyset < X < G\). Then there exist \(H < G\) and \(a \in G\) such that \(X = Ha\). By assumption there exists a maximal subgroup \(M\) of \(G\) containing \(H\). For every \(b \in G \setminus Ma\), we have \(ba^{-1} \notin M\) and hence by (2), \(Ha \lor Mb = G\). Clearly, \(Ha \land Mb \leq Ma \cap Mb = \emptyset\) and so \(Mb\) is a complement to \(X = Ha\) in \(\mathcal{R}(G)\).

**9.4.5 Theorem** (Curzio [1957c]). If \(G\) is a finite group, then \(\mathcal{R}(G)\) is relatively complemented if and only if \(L(G)\) is relatively complemented.

*Proof.* If \(\mathcal{R}(G)\) is relatively complemented, then so is its interval \(L(G)\). Suppose conversely that \(L(G)\) is relatively complemented and let \([X/Y]\) be a nontrivial interval in \(\mathcal{R}(G)\). If \(Y \neq \emptyset\), then \(Y = bK\) for some \(b \in G\), \(K \leq G\) and the automorphism \(\lambda_b\) of \(\mathcal{R}(G)\) maps \([X/Y]\) to \([b^{-1}X/K]\). This is an interval in \(L(G)\) and hence is complemented. Now let \(Y = \emptyset\). Then \(X = aH\) for some \(a \in G\), \(H \leq G\) and \(\lambda_a\) maps \([X/Y]\) to \([H/\emptyset]\) = \(\mathcal{R}(H)\). Since \(H\) is finite, \(\mathcal{R}(H)\) is complemented, by 9.4.4. Thus every interval of \(\mathcal{R}(G)\) is complemented and so \(\mathcal{R}(G)\) is relatively complemented.

Groups whose coset lattices are self-dual, or upper semimodular, or satisfy the Jordan-Dedekind chain condition are treated in Exercises 1–3. Similar results as for \(\mathcal{R}(G)\) were proved by d’Andrea [1969] for the lattice \(\mathcal{R}_N(G)\) of all cosets of \(G\) with respect to normal subgroups of \(G\) (see Exercise 4).

**\(\mathcal{R}\)-isomorphisms**

A bijective map \(\sigma: G \to \tilde{G}\) is called an \(\mathcal{R}\)-isomorphism if for every subset \(X\) of \(G\), we have \(X \in \mathcal{R}(G)\) if and only if \(X^\sigma \in \mathcal{R}(\tilde{G})\); \(\sigma\) is called normed if \(1^\sigma = 1\). Clearly, every \(\mathcal{R}\)-isomorphism induces an isomorphism from \(\mathcal{R}(G)\) onto \(\mathcal{R}(\tilde{G})\). Conversely, an isomorphism \(\psi: \mathcal{R}(G) \to \mathcal{R}(\tilde{G})\) maps every atom \(\{g\}\) of \(\mathcal{R}(G)\) to an atom \(\{\tilde{g}\}\) of \(\mathcal{R}(\tilde{G})\) and the map \(g \to \tilde{g}\) is an \(\mathcal{R}\)-isomorphism from \(G\) to \(\tilde{G}\) inducing \(\psi\). Therefore it is an equivalent problem to study isomorphisms between coset lattices or \(\mathcal{R}\)-isomorphisms between groups; we prefer to do the latter. So in the sequel we consider the maps \(\rho_g\) and \(\lambda_g\) defined in (6) and (7) as element maps; these are \(\mathcal{R}\)-
isomorphisms. The product of two $R$-isomorphisms clearly is an $R$-isomorphism. The maps $\rho$ and $\lambda$ sending every $g \in G$ to $\rho g$ and $\lambda g$, respectively, are isomorphisms from $G$ to subgroups $R_t G$ and $L_t G$ of the group $RP(G)$ of all $R$-automorphisms of $G$; to obtain this, we have to multiply by $g^{-1}$ in (7). We call $R_t G$ (and $L_t G$) the group of right (and left) translations of $G$ and have that

$$RP(G) = RP(G)_1 \cdot R_t G = RP(G)_1 \cdot L_t G$$

if $RP(G)_1$ is the group of all normed $R$-automorphisms of $G$.

More generally, if $\sigma: G \rightarrow \overline{G}$ is any $R$-isomorphism, then $\tau = \sigma \lambda \sigma^{-1}: G \rightarrow \overline{G}$ satisfies $\tau^1 = (\sigma^1)^{-1} \cdot \sigma^1 = 1$ and hence is a normed $R$-isomorphism. So we have shown that

$$(10) \ R(G) \text{ and } R(\overline{G}) \text{ are isomorphic if and only if there exists a normed } R\text{-isomorphism from } G \text{ to } \overline{G}.$$ 

Therefore it suffices to study normed $R$-isomorphisms. Every isomorphism or anti-isomorphism $\alpha$ is a normed $R$-isomorphism since in this case $(Hx)^\alpha = H^x x^\alpha$ or $x^\alpha H^x$ is a coset if $H \leq G$ and $x \in G$. Conversely, we wish to find criteria for a normed $R$-isomorphism $\alpha: G \rightarrow \overline{G}$ to be an isomorphism or an antiisomorphism. We start by giving some basic properties of $\alpha$. A subset $X$ of $G$ is a subgroup of $G$ if and only if $X \in R(G)$ and $1 \in X$. Since $\alpha$ is a normed $R$-isomorphism, this holds if and only if $X^\alpha \in R(G)$ and $1 = 1^\alpha \in X^\alpha$, that is, if and only if $X^\alpha \leq \overline{G}$. Thus

$$(11) \ R(G) \text{ and } R(\overline{G}) \text{ are isomorphic if and only if there exists a normed } R\text{-isomorphism from } G \text{ to } \overline{G}.$$ 

In particular, $\alpha$ maps cyclic subgroups to cyclic subgroups and hence satisfies

$$\langle g \rangle^\alpha = \langle g^\alpha \rangle \text{ for every } g \in G;$$

this also follows from the fact that $\langle g \rangle$ is the smallest coset containing 1 and $g$. Clearly, (13) implies that $\alpha(g) = \alpha(g^\alpha)$ and so $\langle g \rangle \simeq \langle g^\alpha \rangle$. We have shown:

$$(14) \text{ Every cyclic group is determined by its coset lattice.}$$

This is one of the few cases in which (12) and $|G| = |\overline{G}|$ yield that $G$ and $\overline{G}$ are isomorphic. If $\alpha(g)$ is infinite, we can even show that $\alpha$ induces an isomorphism in $\langle g \rangle$.

$9.4.6 \text{ Lemma (Loiko [1961]). If } \sigma: G \rightarrow \overline{G} \text{ is a normed } R\text{-isomorphism and } u \in G \text{ is an element of infinite order, then } (u^\sigma)^k = (u^k)^\sigma \text{ for all } k \in \mathbb{Z}.\]

Proof. Put $u^\sigma = v$. Then by (13), $\langle u^\sigma \rangle = \langle v \rangle$ and we show by induction on $k$ that $(u^k)^\sigma = v^k$ for $k \in \mathbb{N}$; since $u^k$ and $u^{-k}$ are the only generators of $\langle u^k \rangle$, it will follow that $(u^{-k})^\sigma = v^{-k}$. For $k = 0$ and $k = 1$, the assertion is clear. So let $k \geq 1$ and assume that $(u^i)^\sigma = v^i$ for $i = 0, \ldots, k$. By (6) and (7), $\tau = \rho_{u^k} \cdot \sigma \cdot \rho_{u^k}^{-1}$ is an $R$-isomorphism satisfying $\tau^1 = v^{-k}(u^k)^\sigma = 1$, by our induction assumption. By (12), $\tau$ induces a projectivity and, since $\langle u^\tau \rangle = v^{-k}(u^\tau)^\sigma = \langle v \rangle$, it follows that $u^\tau = v$ or $u^\tau = v^{-1}$. On the other hand, the definition of $\tau$ yields $u^\tau = v^{-k}(u^{k+1})^\sigma$ and hence $(u^{k+1})^\sigma = v^{k+1}$ or $v^{-k+1}$. Since $\sigma$ is bijective and $v^{-k+1} = (u^{-k+1})^\sigma$, we obtain that $(u^{k+1})^\sigma = v^{k+1}$, as desired. \[\square\]
Further lattices

The above lemma is fundamental in the study of $\mathcal{R}$-isomorphisms. As a first consequence, we note the following.

**9.4.7 Lemma.** If $\sigma: G \to \overline{G}$ is a normed $\mathcal{R}$-isomorphism and $a, b \in G$ such that $o(b) = o(ab) = \infty$, then $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$.

*Proof.* Let $\tau = \rho_{b^{-1}} \cdot \sigma \cdot \rho_b$. Then $\tau$ is a normed $\mathcal{R}$-isomorphism since $1^\tau = (b^{-1})^\sigma = 1$, by 9.4.6. Furthermore $(ab)^\tau = (aba^{-1}b^\sigma = a^\sigma b^\sigma$ and, since $o(ab) = \infty$, again 9.4.6 yields $(aba)^\sigma b^\sigma = (abab)^\tau = ((ab)^\tau)^2 = a^\sigma b^\sigma a^\sigma b^\sigma$. Thus $(aba)^\sigma = a^\sigma b^\sigma a^\sigma$.

It is to be expected that if the projectivity $\delta$ in (12) is induced by an isomorphism, then $\sigma$ has some interesting properties. We show that if $G$ has enough elements of infinite order, then $\sigma$ is in fact an isomorphism or an antiisomorphism in this situation. For this we need the following result.

**9.4.8 Lemma.** Let $G$ be a group which is torsion-free or has an element of infinite order in its centre. If $\omega: G \to G$ is a normed $\mathcal{R}$-automorphism such that $H^\omega = H$ for all subgroups $H$ of $G$, then either $x^\omega = x$ for all $x \in G$ or $x^\omega = x^{-1}$ for all $x \in G$.

*Proof.* Suppose first that $G$ is torsion-free and let $1 \neq x \in G$. Then $x$ and $x^{-1}$ are the only generators of $\langle x \rangle$ and, since $\langle x \rangle^\omega = \langle x \rangle$, it follows that $x^\omega = x$ or $x^\omega = x^{-1}$. Suppose, for a contradiction, that $a, b \in G$ such that $a \neq 1 \neq b$, $a^\omega = a$ and $b^\omega = b^{-1}$. Then by 9.4.7, $(aba)^\omega = a^\omega b^\omega a^\omega = ab^{-1}a$; on the other hand, $(aba)^\omega = ab\omega$ or $(aba)^{-1}$. In the first case, we obtain $b = b^{-1}$, a contradiction since $o(b) = \infty$. So $ab^{-1}a = a^{-1}b^{-1}a^{-1}$ and hence $b^{-1}a^2b = a^{-2}$. This holds for every nontrivial element $b \in G$ which is inverted by $\omega$. By 9.4.6, $(b^2)^\omega = b^{-2}$ and so $b^{-2}a^2b^2 = a^{-2}$; but $b^{-1}a^2b = a^{-2}$ implies $b^{-2}a^2b^2 = a^2$. This contradiction shows that $\omega$ maps every element of $G$ to the same power.

Now suppose that $Z(G)$ contains an element $z$ of infinite order. Again $x^\omega = x$ or $x^{-1}$ for all $x \in G$ of infinite order; let $z^\omega = z^\epsilon$ where $\epsilon \in \{+1, -1\}$. We claim that $x^\omega = x^\epsilon$ for all $x \in G$. If $\langle x \rangle \cap \langle z \rangle \neq 1$, then $1 \neq x^i \in \langle z \rangle$ for some $i \in \mathbb{Z}$; by 9.4.6, $(x^i)^\omega = (x^i)^\epsilon$ and then $x^\omega = x^\epsilon$. If $\langle x \rangle \cap \langle z \rangle = 1$ and $o(x) = \infty$, then $\langle x, z \rangle \cong \langle x \rangle \times \langle z \rangle$ is torsion-free and hence $x^\omega = x^\epsilon$, as we have just shown. Thus $x^\omega = x^\epsilon$ for all $x \in G$ of infinite order. Now suppose that $o(x)$ is finite. Since $z \in Z(G), x \langle z \rangle$ is a coset containing a unique element of finite order, namely $x$. By (13), $\omega$ preserves the order of an element and hence $(x \langle z \rangle)^\omega$ is a coset in which $x^\omega$ is the unique element of finite order. Now $(x \langle z \rangle)^\omega$ contains $(xz)^\epsilon = x^\epsilon z^\epsilon$ and $(xz^2)^\epsilon = x^\epsilon(z^\epsilon)^2$ and therefore, by (3), it contains $x^\epsilon z^\epsilon(x^\epsilon(z^\epsilon)^2)^{-1}x^\epsilon z^\epsilon = x^\epsilon$. Thus $x^\omega = x^\epsilon$, as desired. \hfill $\square$

**9.4.9 Theorem.** Let $G$ be a group which is torsion-free or has an element of infinite order in its centre. If $\sigma: G \to \overline{G}$ is a normed $\mathcal{R}$-isomorphism such that the projectivity $\delta$ induced by $\sigma$ is induced by an isomorphism, then $\sigma$ is an isomorphism or an antiisomorphism.
9.4 Coset lattices

Proof. Let \( \delta \) be an isomorphism inducing \( \delta \). Then \( \omega = \sigma \delta^{-1} \) is a normed \( \mathcal{R} \)-automorphism of \( G \) satisfying \( H^{\omega} = H \) for all \( H \leq G \). By 9.4.8, \( \omega \) is an isomorphism or an antiisomorphism and then so is \( \sigma = \omega \delta \).

We have shown in a number of cases that every projectivity of a given group is induced by an isomorphism. So Theorem 9.4.9 covers some classes of groups which were handled directly, without using the results on projectivities, by Loiko.

9.4.10 Corollary. Let \( \sigma: G \to \bar{G} \) be a normed \( \mathcal{R} \)-isomorphism.

(a) (Loiko [1961], [1963]) If \( G \) is torsion-free abelian or mixed abelian of torsion-free rank \( r \geq 2 \), then \( \sigma \) is an isomorphism.

(b) If \( G \) is a locally free group, then \( \sigma \) is an isomorphism or an antiisomorphism.

(c) (Loiko [1965c], Bruno [1970]) If \( G \) is a locally nilpotent torsion-free group or a free polynilpotent group, then \( \sigma \) is an isomorphism or an antiisomorphism.

Proof. In all cases, \( G \) is torsion-free or has an element of infinite order in its centre. To apply Theorem 9.4.9, we have to show that \( \delta \) is induced by an isomorphism. By 2.6.10, 7.1.19, 7.2.11, and 7.2.13, this holds in all cases except possibly when \( G \) is torsion-free abelian of rank 1. In this case, if \( a, b \in G \), then \( \langle a, b \rangle \) is cyclic and hence \( (ab)^\sigma = a^\sigma b^\sigma \) by 9.4.6; thus \( \sigma \) is an isomorphism.

Mixed abelian groups of torsion-free rank 1 do not fall under Theorem 9.4.9 since in general they are not even determined by their subgroup lattices: we have shown in 2.5.15 that every \( M \)-group with elements of infinite order is lattice-isomorphic to such an abelian group. For coset lattices, the situation is not so simple; it was clarified by Loiko in a special case. We give his result without proof.

9.4.11 Theorem (Loiko [1965a]). Let \( G \) be a mixed abelian group of torsion-free rank 1 which splits over its torsion subgroup \( T(G) \). There exists an \( \mathcal{R} \)-isomorphism from \( G \) to the group \( \bar{G} \) if and only if \( T(G) \simeq T(\bar{G}) \), \( G/T(G) \simeq \bar{G}/T(\bar{G}) \), \( \bar{G} = T(\bar{G})H \) for some torsion-free subgroup \( H \), and for every element \( z \in \bar{G} \) of infinite order and every Sylow \( p \)-subgroup \( T_p \) of \( T(G) \) there exists an integer \( i(z, p) \) with the following properties:

(i) \( z^{-1}az = a^{3-2i(z, p)} \) for all \( a \in T_p \),
(ii) \( i(z, p) = 1 \) if \( \text{Exp } T_p = \infty \),
(iii) \( 2i(z, p) - 1 \equiv 0 \pmod{p^n} \) and \( i(z^k, p) \equiv 1 + (i(z, p) - 1)k \pmod{p^n} \) for all \( k \in \mathbb{N} \) if \( \text{Exp } T_p = p^n \).

It follows from this theorem that there are mixed abelian groups \( G \) of torsion-free rank 1 and nonabelian groups \( \bar{G} \) such that (i) \( \mathcal{R}(G) \simeq \mathcal{R}(\bar{G}) \), and, on the other hand, (ii) \( L(G) \simeq L(\bar{G}) \) and \( \mathcal{R}(G) \neq \mathcal{R}(\bar{G}) \) (see Exercises 6 and 7). For finite abelian groups, the situation is different. Here Theorem 2.5.9 shows that every locally finite non-hamiltonian \( p \)-group \( \bar{G} \) with modular subgroup lattice is \( \mathcal{R} \)-isomorphic to a suitable abelian group \( G \) (see the proof of 9.4.12). Since Baer proved this theorem in 1944, these were the first examples of nonisomorphic groups with isomorphic coset lattices that were discovered. The \( \mathcal{R} \)-isomorphisms \( \sigma: G \to \bar{G} \) constructed in 2.5.9 satisfy
Further lattices

\((Hx)^{\sigma} = H^{\sigma}x^{\sigma}\) for all \(H \leq G\) and \(x \in G\); so every right coset of \(H\) is mapped to a right coset of \(H^{\sigma}\). However, this is not true for left cosets. Indeed, since \(x^{\sigma} \in (xH)^{\sigma}\) and \(G\) is abelian, it would follow that \(x^{\sigma}H^{\sigma} = (xH)^{\sigma} = (Hx)^{\sigma} = H^{\sigma}x^{\sigma}\); so \(H^{\sigma} \leq \bar{G}\) for all \(H \leq G\), a contradiction if \(\bar{G}\) is not abelian. Similar phenomena occur in all the other examples mentioned above and we use the remainder of this section to study \(\mathcal{R}\)-isomorphisms for which this does not happen. Since they preserve the affin structure of \(G\), they will be called affinities.

**Affinities**

An \(\mathcal{R}\)-isomorphism \(\sigma: G \to \bar{G}\) is called an **affinity** if

\[
(15) \quad (Hx)^{\sigma} = H^{\sigma}x^{\sigma} \quad \text{and} \quad (xH)^{\sigma} = x^{\sigma}H^{\sigma} \quad \text{for all} \quad H \leq G \quad \text{and} \quad x \in G.
\]

Note that a bijective map \(\sigma\) satisfying (15) in general is not an \(\mathcal{R}\)-isomorphism. It is rather obvious that \(\sigma\) satisfies \(1^{\sigma} = 1\) and maps subgroups of \(G\) to subgroups of \(\bar{G}\), but \(\bar{G}\) may have more subgroups. For example, any normed bijective map from a cyclic to an elementary abelian group of order 4 satisfies (15), and this is by no means the only example (see Exercise 9). So the extra condition in the following criterion is needed.

**9.4.12 Lemma.** A bijective map \(\sigma: G \to \bar{G}\) is an affinity if and only if \(\sigma\) induces a projectivity from \(G\) to \(\bar{G}\) and satisfies (15).

**Proof.** If \(\sigma\) is an affinity, then \(\{1^{\sigma}\} = (\langle 1 \rangle)^{\sigma} = \langle 1 \rangle^{\sigma}1^{\sigma} = \{(1^{\sigma})^{2}\}\) and hence \(1^{\sigma} = 1\). By (12), \(\sigma\) induces a projectivity. Conversely, suppose that \(\sigma\) induces a projectivity and satisfies (15); let \(\emptyset \neq X \subseteq G\). If \(X \in \mathcal{R}(G)\), then \(X = Hx\) for some \(H \leq G\), \(x \in G\) and our assumptions on \(\sigma\) imply that \(H^{\sigma} \leq \bar{G}\) and \(X^{\sigma} = H^{\sigma}x^{\sigma} \in \mathcal{R}(\bar{G})\). If \(X^{\sigma} \in \mathcal{R}(\bar{G})\), there exist \(K \leq \bar{G}\) and \(y \in \bar{G}\) such that \(X^{\sigma} = Ky = H^{\sigma}x^{\sigma} = (Hx)^{\sigma}\) for some \(H \leq G\), \(x \in G\); so \(X = Hx \in \mathcal{R}(G)\). Thus \(\sigma\) is an \(\mathcal{R}\)-isomorphism satisfying (15).

Recall from (4) of §1.3 the associativity identities for the amorphity \(a\) of a map \(\sigma: G \to \bar{G}\). We defined \(a(x, y) = (y^{\sigma})^{-1}(x^{\sigma})^{-1}(xy)^{\sigma}\) and obtained that

\[
(16) \quad a(x, y)^{\sigma}a(xy, z) = a(y, z)a(x, yz) \quad \text{for all} \quad x, y, z \in G.
\]

We show next that affinities are characterized by the behaviour of their amorphies.

**9.4.13 Theorem.** The bijective map \(\sigma: G \to \bar{G}\) with amorphity \(a\) is an affinity if and only if

(a) \(\sigma\) induces a projectivity from \(G\) to \(\bar{G}\) and

(b) \(a(x, y) \in \langle x \rangle^{\sigma} \cap \langle y \rangle^{\sigma}\) for all \(x, y \in G\).

If \(\sigma\) is an affinity, then \((xy)^{\sigma} = x^{\sigma}y^{\sigma}\) for all \(x, y \in G\) such that \(o(x)\) or \(o(y)\) is infinite.

**Proof.** If \(\sigma\) is an affinity, then 9.4.12 shows that (a) holds and that for \(x, y \in G\), we have \((xy)^{\sigma} \in (\langle x \rangle \cap \langle y \rangle)^{\sigma}\); hence \(a(x, y) \in \langle y \rangle^{\sigma}\) since \(\langle y \rangle^{\sigma}\) is a subgroup of \(\bar{G}\). Similarly, \((xy)^{\sigma} \in \langle x \rangle^{\sigma}y^{\sigma}\) and so \(a(x, y)^{\sigma} = a(x, y)^{\sigma} = a(x, y)^{(xy)^{\sigma}} = a(x, y)\) and (b) holds.
Now assume that \( \sigma \) satisfies (a) and (b) and let \( x \in G, H \leq G \). For \( h \in H \), we have
\[
(xh)^\sigma = x^\sigma h^\sigma a(x, h) \in x^\sigma H^\sigma \text{ since } a(x, h) \in \langle h \rangle^\sigma \leq H^\sigma \leq G.
\] Hence

(17) \( (xH)^\sigma \subseteq x^\sigma H^\sigma \) for all \( x \in G, H \leq G \).

If \( u \in G \) is of infinite order and \( U = \langle u \rangle \), then \( U^\sigma \) is infinite cyclic. Using induction on \( |U : H| \), we show that \( (xH)^\sigma = x^\sigma H^\sigma \) for all \( x \in U, H \leq U \). This is true for \( |U : H| = 1 \); so assume it to be true for subgroups of smaller index than \( |U : H| = n \) and let \( U = x_1 H \cup \cdots \cup x_n H \) with \( x = x_1 \) be the coset decomposition of \( U \) with respect to \( H \). Then

\[
U^\sigma = (x_1 H)^\sigma \cup \cdots \cup (x_n H)^\sigma \subseteq x_1^\sigma H^\sigma \cup \cdots \cup x_n^\sigma H^\sigma
\]

and therefore \( |U^\sigma : H^\sigma| \leq n \). The induction assumption implies that every subgroup of index \( <n \) of \( U^\sigma \) has a preimage different from \( H \) and so \( |U^\sigma : H^\sigma| = n \). It follows that the \( x_i^\sigma H^\sigma \) are distinct and that \( (x_i H)^\sigma = x_i^\sigma H^\sigma \) for all \( i \). In particular, \( (xH)^\sigma = x^\sigma H^\sigma \), as desired. By 9.4.12, \( \sigma \) induces an affinity in \( U \) and so by 9.4.6,

(18) \( (u^\sigma)^k = (u^k)^\sigma \) for all \( k \in \mathbb{Z} \).

Now assume that \( a(x, y) \neq 1 \) for some elements \( x, y \in G \) such that \( o(x) \) or \( o(y) \) is infinite. Since \( a(x, y) \in \langle x \rangle^\sigma \cap \langle y \rangle^\sigma \), it follows that \( o(x) = (o(y) = \infty \) and \( a(x, y) = (x^s)^r = (y^s)^r \) for \( r, s \in \mathbb{Z} \). By (18), \( x^r = y^s \) and, applying the associativity identities (16) to \( x, x^{-r}, x^r y \), we get

\[
a(x, x^{-r})^{(xsy)}a(x^{-r}, x^ry) = a(x^{-r}, x^ry)a(x, y).
\]

Again by (18), \( a(x, x^{-r}) = 1 \) and so \( (y^s)^r = a(x, y) = \langle x^r y \rangle^\sigma = \langle y^{s+1} \rangle^\sigma = \langle (y^s)^{r+1} \rangle^\sigma \).

This contradiction shows that \( a(x, y) = 1 \) and proves that

(19) \( (xy)^\sigma = x^\sigma y^\sigma \) for all \( x, y \in G \) such that \( o(x) \) or \( o(y) \) is infinite.

By 9.4.12, it remains to be shown that \( \sigma \) satisfies (15). So let \( x \in G, H \leq G \) and \( h \in H \). If \( o(h) \) is infinite, then by (19), \( x^s h^\sigma = (xh)^\sigma \in (xH)^\sigma \); if \( o(h) \) is finite, then \( |(x \langle h \rangle)^\sigma| = o(h) = |x^\sigma \langle h \rangle^\sigma| \) and so \( x^s h^\sigma \in x^\sigma \langle h \rangle^\sigma = \langle x \langle h \rangle \rangle^\sigma \), by (17). Thus \( x^\sigma H^\sigma \subseteq (xH)^\sigma \) and so \( (xH)^\sigma = x^\sigma H^\sigma \). Since \( (hx)^\sigma = h^\sigma x^\sigma a(h, x) = h^\sigma a(h, x) x^\sigma \in H^\sigma x^\sigma \), we obtain in the same way \( (Hx)^\sigma = H^\sigma x^\sigma \).

The above theorem enables us to construct affinities which are not isomorphisms and even affinities between nonisomorphic groups.

9.4.14 Examples. (a) Let \( G \) be a group and let \( N \) and \( M \) be subgroups of \( G \) such that \( 1 < N < M < G \) and \( N \leq \langle x \rangle \) for all \( x \in G \setminus M \). For \( 1 \neq d \in N \), the map \( \sigma = \sigma_d : G \to G \) defined by \( x^\sigma = x \) for \( x \in M \) and \( x^\sigma = xd \) for \( x \in G \setminus M \) is an affinity; it is an automorphism if and only if \( |G : M| = 2 \) and \( d^2 = 1 \).

Note that if \( G = \langle u \rangle \times V \) is a \( p \)-group such that \( o(u) = p^n > p^m = \text{Exp } V \) and \( m \geq 1 \), then \( N = \langle u^{p^{n-1}} \rangle = \bigcup_{n-1}(G) \) and \( M = \langle a^{p^{m-1}} \rangle \times B = \Omega_m(G) \) satisfy the above assumptions.

(b) Let \( 2 < p \in \mathbb{P} \), and let \( H = \langle u, v, w \rangle | u^p = v^p = w^p = 1, [v, u] = w = w^r = w^u \rangle \) be the nonabelian group of order \( p^3 \) and exponent \( p \). Denote by \( \tau \) the automorphism...
Further lattices

of order $p$ of $H$ given by $u^s = wv^{-1}$, $v^s = v$. Let $s$ be a quadratic nonresidue modulo $p$ and $G = H \langle g \rangle$, $\bar{G} = H \langle \bar{g} \rangle$ where $g^p = w$, $\bar{g}^p = w^s$, and $h^s = h^s = h^s$ for all $h \in H$. Then $G$ and $\bar{G}$ are nonisomorphic groups of order $p^s$ (see Huppert [1967], p. 347) and the map $\sigma: G \to \bar{G}$ defined by $(g^i x)^s = \bar{g}^i x$ for $x \in H$, $i \in \{0, \ldots, p - 1\}$ is an affinity.

**Proof.** (a) Of course, $\sigma$ is bijective. For $H \leq G$, we have $H^s = H$ if $H \leq M$ and $H^s \leq HN = H$ if $H \not\leq M$. Thus $H^s = H$ in any case. Now $N \leq Z(G)$ since $G$ is generated by the elements in $G \setminus M$ and these elements centralize $N$. It follows that $a(x, y) = 1$ if one of $x$ and $y$ is contained in $M$. If $x, y \in G \setminus M$, then $a(x, y) = d^{-1} y^{-1} x^{-1} (xy)^s = d^{-2}$ if $xy \in M$ and $a(x, y) = d^{-1}$ if $xy \not\in M$. In any case, $a(x, y) \in N \leq \langle x \rangle \cap \langle y \rangle = \langle x^s \rangle \cap \langle y^s \rangle$. By 9.4.13, $\sigma$ is an affinity. And $\sigma$ is an automorphism if and only if $a(x, y) = 1$ for all $x, y \in G \setminus M$, and this is the case if and only if $d^2 = 1$ and $xy \in M$ for all $x, y \in G \setminus M$.

(b) Clearly, $\sigma$ is bijective and an easy computation shows that for $x = g^i h$, $y = g^j k$ ($h, k \in H$, $i, j \in \{0, \ldots, p - 1\}$), $(xy)^s = x^s y^s$ if $i + j < p$ and $(xy)^s = x^s y^s w^1 - s$ if $i + j \geq p$. Now $H = \Omega(G) = \Omega(\bar{G})$ and $\langle w \rangle = \mathcal{U}(G) = \mathcal{U}(\bar{G})$ and hence we see that $(xy)^s \in \langle x^s, y^s \rangle$ and $a(x, y) \in \langle x^s \rangle \cap \langle y^s \rangle$. Since $\sigma^{-1}$ has the corresponding properties, it follows from 1.3.1 that $\sigma$ induces a projectivity, and then from 9.4.13 that $\sigma$ is an affinity.

It is another immediate consequence of Theorem 9.4.13 that affinities map abelian groups onto abelian groups.

9.4.15 Theorem. If $\sigma: G \to \bar{G}$ is an affinity and $H \leq G$ is abelian, then $H^s$ is abelian and $Z(G)^s = Z(\bar{G})$.

**Proof.** Let $x, y \in G$ such that $xy = yx$. If $o(x)$ or $o(y)$ is infinite, then by 9.4.13, $x^s y^s = (xy)^s = (yx)^s = y^s x^s$. So assume that $o(x)$ and $o(y)$ are finite. Then $W = \langle x, y \rangle$ is a finite abelian group, hence $W = \langle w_1, \ldots, w_r \rangle$ with $\langle w_i \rangle \cap \langle w_j \rangle = 1$ and so, by (b) of 9.4.13, $a(w_i, w_j) = 1$ for $i \neq j$ if $a$ is the automorphism of $\sigma$. Since $\sigma$ induces a projectivity, $W^s = \langle w_1^s, \ldots, w_r^s \rangle$ and $w_i^s w_j^s = (w_i w_j)^s = (w_j w_i)^s = w_j^s w_i^s$ for $i \neq j$. Thus $W^s$ is abelian and $xy = yx$. This shows that every abelian subgroup $H$ of $G$ is mapped to an abelian subgroup of $\bar{G}$ and that $Z(G)^s \leq Z(\bar{G})$. Since $\sigma^{-1}$ is also an affinity, we get the other inclusion.

If $\sigma: G \to \bar{G}$ is any map, an element $x \in G$ is called right regular for $\sigma$ if $(xg)^s = x^s g^s$ or, equivalently, $a(x, g) = 1$ for all $g \in G$; $\text{Reg}'(\sigma)$ is the set of right regular elements for $\sigma$. Left regular elements and $\text{Reg}'(\sigma)$ are defined correspondingly.

9.4.16 Lemma. If $\sigma: G \to \bar{G}$ is an affinity, then $\text{Reg}'(\sigma)$ and $\text{Reg}'(\sigma)$ are subgroups of $G$.

**Proof.** Since $1^s = 1$, $1 \in \text{Reg}'(\sigma)$. If $x, y \in \text{Reg}'(\sigma)$, then $(xyg)^s = x^s (yg)^s = x^s y^s g^s = (xy)^s g^s$ for all $g \in G$ and hence $xy \in \text{Reg}'(\sigma)$. If $o(x)$ is finite, this also implies that $x^{-1} \in \text{Reg}'(\sigma)$, and if $o(x)$ is infinite, $x^{-1} \in \text{Reg}'(\sigma)$ by 9.4.13. Thus $\text{Reg}'(\sigma)$ is a subgroup of $G$ and the proof for $\text{Reg}'(\sigma)$ is similar.
We come to our first main result on regular elements. For this we need the following lemma.

9.4.17 **Lemma.** If \( \sigma: G \to \tilde{G} \) is an affinity, then \( \tau: G \to \tilde{G} \) defined by \( g^\tau = ((g^{-1})^\sigma)^{-1} \) for \( g \in G \) is also an affinity.

**Proof.** Of course, \( \tau \) induces the same projectivity as \( \sigma \). For \( H \leq G \) and \( x \in G \), we have

\[
(Hx)^\tau = ((x^{-1}H)^\sigma)^{-1} = ((x^{-1})^\sigma H^\sigma)^{-1} = H^\sigma((x^{-1})^\sigma)^{-1} = H^\tau x^\tau.
\]

Similarly, \( (xH)^\tau = x^\tau H^\tau \) and by 9.4.12, \( \tau \) is an affinity. \( \square \)

9.4.18 **Theorem** (Schmidt [1984a]). Let \( G \) be a group, let \( \text{Reg}^G \) be the set of all elements of \( G \) which are right regular for every affinity from \( G \) to any group \( \tilde{G} \) and define \( \text{Reg}^l G \) similarly. Then \( \text{Reg}^G = \text{Reg}^l G =: \text{Reg} G \) is a characteristic subgroup of \( G \) containing all elements of infinite order and all involutions of \( G \).

**Proof.** Let \( \sigma: G \to \tilde{G} \) be an affinity. By 9.4.16, \( \text{Reg}^G \) and \( \text{Reg}^l G \) are subgroups of \( G \). Let \( x \in \text{Reg}^G \). If \( \tau \) is defined as in 9.4.17, then \( x^{-1} \in \text{Reg}^G(\tau) \) and so for \( g \in G \),

\[
((gx)^\sigma)^{-1} = (x^{-1}g^{-1})^\tau = (x^{-1})^\sigma (g^{-1})^\tau = (x^\sigma)^{-1} (g^\sigma)^{-1} = (g^\sigma x^\sigma)^{-1},
\]

that is, \( (gx)^\sigma = g^\sigma x^\sigma \). Thus \( x \in \text{Reg}^l(\sigma) \) and, since \( \sigma \) was arbitrary, \( x \in \text{Reg}^l G \). So \( \text{Reg}^G \leq \text{Reg}^l G \) and the other inclusion is proved similarly.

Now let \( x \in \text{Reg} G \) and \( \sigma \in \text{Aut} G \). For every \( g \in G \) there exists \( y \in G \) such that \( g = y^\sigma \) and, since \( \sigma \) is an affinity, \( (x^\sigma g)^\sigma = (x^\sigma y^\sigma)^\sigma = (xy)^\sigma = x^\sigma y^\sigma = (x^\sigma)^\sigma = (x^\sigma g)^\sigma \). Thus \( x^\sigma \in \text{Reg}^G(\sigma) \) and, since \( \sigma \) was arbitrary, it follows that \( x^\sigma \in \text{Reg}^G = \text{Reg} G \). So \( (\text{Reg} G)^\sigma \leq \text{Reg} G \) and \( \text{Reg} G \) is a characteristic subgroup of \( G \).

By 9.4.13, \( \text{Reg} G \) contains every element of infinite order. So, finally, let \( x \in G \) be an involution and \( H = \{1, x\} \). Then for \( g \in G \), \( Hg = \{g, xg\} \) and by (15),

\[
\{g^\sigma, (xg)^\sigma\} = (Hg)^\sigma = H^\sigma g^\sigma = \{g^\sigma, x^\sigma g^\sigma\}.
\]

It follows that \( (xg)^\sigma = x^\sigma g^\sigma \) and so \( x \in \text{Reg}^G \). \( \square \)

9.4.19 **Corollary.** If \( G \) is generated by involutions and elements of infinite order, every affinity of \( G \) is an isomorphism.

**Semiaffinities**

We call an \( \mathcal{R} \)-isomorphism \( \sigma: G \to \tilde{G} \) a **left affinity** if it satisfies \( (xH)^\sigma = x^\sigma H^\sigma \) and a **right affinity** if it satisfies \( (Hx)^\sigma = H^\sigma x^\sigma \) for all \( H \leq G \) and \( x \in G \). It is interesting to note that these semiaffinities have similar properties to those just established for affinities. Schmidt [1983] shows that for a left affinity, every element of infinite order
and every involution is left regular, but also gives examples in which certain such elements are not right regular. Nevertheless we obtain as a corollary that for groups generated by elements of infinite order, every left affinity is an isomorphism, a result due to Loiko [1972]. Similar assertions hold for right affinities since for every right affinity \( \sigma \), the map \( \tau \) defined in 9.4.17 is a left affinity and conversely.

### The structure of Am \( G \) and \( G/\text{Reg} \ G \)

We come to our main result on the amorphiness of an affinity.

**9.4.20 Theorem** (Gaschütz and Schmidt [1981], Schmidt [1984a]). If \( \sigma : G \to \overline{G} \) is an affinity and \( a \) the amorphiness of \( \sigma \), then \( a(x, y) \in Z(\overline{G}) \) for all \( x, y \in G \).

**Proof.** Suppose, for a contradiction, that there exist \( x, y \in G \) such that \( a(x, y) \notin Z(\overline{G}) \); by 9.4.13, \( x \) and \( y \) have finite order, and we can choose them so that \( o(x) \) is as small as possible. If \( x = x_1x_2 \) with \( o(x_1) \) and \( o(x_2) \) less than \( o(x) \), then the associativity identities (16) with \( x_1, x_2, y \) would imply

\[
a(x, y) = (a(x_1, x_2)^{(r^1)})^{-1} a(x_2, y) a(x_1, x_2 y) \in Z(\overline{G}),
\]

a contradiction. Thus \( o(x) = p^n \), \( p \) a prime, \( n \in \mathbb{N} \).

Let \( z \in G \) such that \( a(x, y) \) does not commute with \( z^\sigma \). Then \( a(x, y) \notin \langle z^\sigma \rangle \). Since \( o(x^\sigma) = o(x) = p^n \), the subgroups of \( \langle x^\sigma \rangle \) form a chain and by 9.4.13,

\[
\langle a(z, x) \rangle \leq \langle x^\sigma \rangle \cap \langle z^\sigma \rangle < \langle a(x, y) \rangle \leq \langle x^\sigma \rangle \cap \langle y^\sigma \rangle.
\]

Hence \( a(z, x)^{p^k} = a(x, y) = a(x, y)^{p^k} \) with \( k \in \mathbb{Z} \) and the associativity identities for \( z, x, y \) yield

\[
(20) \quad 1 = a(x, y)^{1-kp} a(x, y)^{p^k} a(z, y), \quad a(x, y)^{1-kp} a(z, y) a(x, y)^{p^k}.
\]

Since \( a(x, y) \) and \( a(z, y) \) are elements of \( \langle y^\sigma \rangle \), they commute with \( y^\sigma \) and (20) implies that \( [a(z, x), y^\sigma] = 1 \). In addition, \( a(z, x) \) commutes with \( (xy)^\sigma = x^\sigma y^\sigma a(x, y) = x^\sigma (y^\sigma)^t \), \( (s \in \mathbb{Z}) \), and hence also with \( x^\sigma \). Since \( a(x, y) \in \langle x^\sigma \rangle \), equation (20) yields \( [a(x, y), x^\sigma] = 1 \). Now \( a(z, y) \) also commutes with \( (zx)^\sigma = z^\sigma (x^\sigma)^t \) \((t \in \mathbb{Z})\) and hence with \( z^\sigma \). As \( a(z, x) \in \langle z^\sigma \rangle \), again (20) implies that \( a(x, y)^{1-kp} \) commutes with \( z^\sigma \). Since \( a(x, y) \in \langle x^\sigma \rangle \) is a \( p \)-element, \( \langle a(x, y)^{1-kp} \rangle = \langle a(x, y) \rangle \) and so \( a(x, y) \) commutes with \( z^\sigma \), the desired contradiction. \( \square \)

The above theorem is fundamental in the study of affinities. If \( \sigma : G \to \overline{G} \) is an affinity and \( N \leq G \), then \( x^\sigma N^\sigma = (xN)^\sigma = (Nx)^\sigma = N^\sigma x^\sigma \) for all \( x \in G \). So \( N^\sigma \leq \overline{G} \) and 9.4.13 shows that the map

\[
(21) \quad \overline{\sigma} : G/N \to \overline{G}/N^\sigma, \quad Nx \mapsto N^\sigma x^\sigma
\]

And if \( N = Z(G) \), Theorems 9.4.15 and 9.4.20 show that this map is an isomorphism.
9.4.21 Corollary. Every affinity \( \sigma : G \rightarrow \bar{G} \) induces an isomorphism from \( G/Z(G) \) onto \( \bar{G}/Z(\bar{G}) \).

Another immediate consequence of 9.4.20 is that the associativity identities become

(22) \( a(x, y)a(xy, z) = a(y, z)a(x, yz) \) for all \( x, y, z \in G \)

if \( a \) is the amorph of an affinity \( \sigma : G \rightarrow \bar{G} \). To study the situation inside \( G \), we introduce \( \text{Am} (\sigma) = \langle a(x, y)^{\sigma^{-1}} | x, y \in G \rangle \) and define the amorph \( \text{Am} G \) of \( G \) to be the subgroup generated by all the \( \text{Am}(\sigma) \) where \( \sigma \) ranges over the affinities from \( G \) to groups \( \bar{G} \).

9.4.22 Theorem. If \( G \) is a group, then \( \text{Am} G \) is a characteristic subgroup of \( G \) contained in \( Z(G) \).

Proof. By 9.4.20 and 9.4.15, \( \text{Am} G \leq Z(G) \). Let \( \alpha \in \text{Aut} G \) and let \( \sigma : G \rightarrow \bar{G} \) be an affinity with amorph \( a \). Then \( \tau = \alpha^{-1}\sigma \) is an affinity and its amorph \( b \) satisfies

\[
x^\alpha y^\alpha a(x, y) = (xy)^\alpha = (x^\alpha y^\alpha)^{\sigma^{-1}} = x^\alpha y^\alpha b(x^\alpha, y^\alpha)
\]

for all \( x, y \in G \). So \( (a(x, y)^{\sigma^{-1}})^\alpha = (b(x^\alpha, y^\alpha))^{\tau^{-1}} \in \text{Am} G \). \( \Box \)

In the remainder of this section we want to show that \( G/\text{Reg} G \) is \( \pi \)-closed for every set \( \pi \) of primes; this will yield another criterion for a group to have the property that every affinity is an isomorphism.

9.4.23 Lemma. Let \( \sigma : G \rightarrow \bar{G} \) be an affinity, \( a \) the amorph of \( \sigma \), and let \( u, v \in G \) such that \( uv = vu \) and \( \langle u \rangle \cap \langle v \rangle = 1 \). Then \( a(uv, x) = a(u, x)a(v, x) \) and \( a(x, uv) = a(x, u)a(x, v) \) for all \( x \in G \).

Proof. By (22), \( a(u, v)a(uv, x) = a(v, x)a(u, vx) \) and by 9.4.13, \( a(u, v) \in \langle u \rangle^\sigma \cap \langle v \rangle^\sigma = 1 \). Hence

(23) \( a(uv, x) = a(u, x)a(v, xv) \).

Interchanging \( u \) and \( v \), we get \( a(uv, x) = a(u, x)a(v, ux) \). Since

\[
a(v, x), a(v, ux) \in \langle v \rangle^\sigma \cap Z(\bar{G}) \quad \text{and} \quad a(u, vx), a(u, x) \in \langle u \rangle^\sigma \cap Z(\bar{G})
\]

and the product of these two groups is direct, it follows that \( a(u, vx) = a(u, x) \). By (23), \( a(uv, x) = a(u, x)a(v, x) \), as desired. The other equation is proved in just the same way applying (22) to \( x, u, v \) in place of \( u, v, x \). \( \Box \)

By a trivial induction, 9.4.23 yields that if \( x, y \in G \) are elements of finite order and \( x = \prod_{p \in P} x_p, y = \prod_{p \in P} y_p \) are their primary decompositions, then

(24) \( a(x, y) = \prod_{p \in P} a(x_p, y) = \prod_{p \in P} a(x, y_p) = \prod_{p \in P} a(x_p, y_p) \)
Further lattices

and \( a(x_p, y_p) \) is the \( p \)-primary component of \( a(x, y) \); for the proof of the last equation note that \( a(x, y_p) = \prod_{q \neq p} a(x_q, y_p) = a(x_p, y_p) \) since \( \langle x_q \rangle^\sigma \cap \langle y_p \rangle^\sigma = 1 \) for \( q \neq p \).

Recall that a group \( G \) is \( \pi \)-closed for a set \( \pi \) of primes if the product of any two \( \pi \)-elements of \( G \) is a \( \pi \)-element.

9.4.24 Theorem (Schmidt [1984a]). If \( G \) is a group, then \( G/\text{Reg} G \) is \( \pi \)-closed for every set \( \pi \) of primes. In particular, if \( G/\text{Reg} G \) is finite, it is nilpotent.

Proof. Suppose that \( x(\text{Reg} G) \) and \( y(\text{Reg} G) \) are nontrivial \( \pi \)-elements in \( G/\text{Reg} G \). Then by 9.4.18, \( o(x) \) and \( o(y) \) are finite and so we may choose \( x \) and \( y \) as \( \pi \)-elements. If \( o(xy) \) is infinite, then \( xy \in \text{Reg} G \). So we may assume that \( o(xy) \) is finite; let \( xy = uv = vu \) where \( u \) is a \( \pi \)-element and \( v \) is a \( \pi' \)-element. We have to show that for every affinity \( \sigma: G \to \hat{G} \) with amorphy \( a \) and every \( z \in G \), we have \( a(u, z) = 1 \); then \( v \in \text{Reg'} G = \text{Reg} G \) and \( x(\text{Reg} G)y(\text{Reg} G) = u(\text{Reg} G) \) is a \( \pi \)-element. By 9.4.18 and (24), it suffices to do this for \( z \in G \) of prime power order \( p^s \).

If \( p \in \pi \), then 9.4.13 implies that \( a(v, z) \in \langle u \rangle^\sigma \cap \langle z \rangle^\sigma = 1 \). So let \( p \notin \pi \). Then \( a(x, y), a(y, z), a(x, yz) \) all are \( \pi \)-elements in \( Z(\hat{G}) \), whereas \( a(xy, z) \) is a \( \pi' \)-element; hence (22) implies that \( a(xy, z) = 1 \). Since \( a(u, z) \in \langle u \rangle^\sigma \cap \langle z \rangle^\sigma = 1 \), it follows from 9.4.23 that \( a(v, z) = a(uv, z) = a(xy, z) = 1 \), as desired. Thus \( G/\text{Reg} G \) is \( \pi \)-closed for every set \( \pi \) of primes and a finite group with this property is nilpotent.

\[ \Box \]

9.4.25 Corollary. If \( G \) is a finite perfect group, then every affinity of \( G \) is an isomorphism.

Much more can be said about \( \text{Am} G \) and \( G/\text{Reg} G \). First of all, \( \text{Am} G \) is locally cyclic. Furthermore it is possible to describe \( \text{Am} G \) and \( \text{Reg} G \) within \( G \); note that for the definition of these subgroups one has to consider every affinity from \( G \) to any group \( \hat{G} \). Call a subgroup \( S \) of \( G \) a \( p \)-collecting subgroup of \( G \) if it contains every element of infinite order and every \( p' \)-element of \( G \) and satisfies \( K = \bigcap_{x \in G} \langle x \rangle \neq 1 \); call \( K \) the \( p \)-collector of \( S \). It is easy to see that the intersection \( T_p(G) \) of all \( p \)-collecting subgroups of \( G \) is a \( p \)-collecting subgroup of \( G \), and it is possible to show that for \( p \geq 5 \), \( \text{Reg} G \leq T_p(G) \) and \( T_p(G)/\text{Reg} G \) is the \( p' \)-component of \( G/\text{Reg} G \). Dually, the join of all \( p \)-collectors in \( G \) is not in general a \( p \)-collector, but it is the \( p \)-component of \( \text{Am} G \). If \( p = 2 \) or \( 3 \), the same results hold modulo a few exceptional cases. For details and proofs see Schmidt [1984a].

Exercises

1. (Curzio [1957c]) If \( \mathcal{R}(G) \) is a self-dual lattice, show that \( |G| \) is a prime or 1.
2. (Loiko [1962]) Let \( G \) be a finite group. Show that \( \mathcal{R}(G) \) is upper semimodular if and only if \( G \) is a \( p \)-group.
3. (Loiko [1962]) Show that \( \mathcal{R}(G) \) satisfies the Jordan-Dedekind chain condition if and only if \( L(G) \) does.
4. (d'Andrea [1969]) Let $\mathcal{R}_N(G)$ be the lattice consisting of all cosets of $G$ with respect to normal subgroups and the empty set.

(a) Show that $\mathcal{R}_N(G)$ is modular if and only if $G$ is simple or $G = 1$; show that $\mathcal{R}_N(G)$ is distributive if and only if $|G| \leq 2$.

(b) Show that $\mathcal{R}_N(G)$ is directly decomposable if and only if $|G| = 2$.

(c) Show that $\mathcal{R}_N(G)$ is complemented if and only if every proper normal subgroup of $G$ is contained in a maximal normal subgroup of $G$.

5. (Loiko [1972]) If $\sigma: G \rightarrow \overline{G}$ is an $\mathcal{R}$-isomorphism, show that $(a \langle a^{-1}b \rangle)^\sigma = a^\sigma \langle (a^\sigma)^{-1}b^\sigma \rangle$ and $(\langle ba^{-1} \rangle a)^\sigma = \langle b^\sigma(a^\sigma)^{-1} \rangle a^\sigma$.

6. (Loiko [1965a]) Let $p > 2$, $G = \langle a \rangle \times \langle w \rangle$ and $\overline{G} = \langle b \rangle \langle z \rangle$ where $o(a) = o(b) = p^2$, $o(w) = o(z) = \infty$ and $z^{-1}bz = b^{1-2p}$. Show that the map $\sigma: G \rightarrow \overline{G}$ defined by $(a^\sigma w^\sigma) = b^{q(1+sp)}z^\sigma$ is an $\mathcal{R}$-isomorphism. Find $H \leq G$ and $x \in G$ such that $(Hx)^\sigma \neq H^\sigma x^\sigma$.

7. (Loiko [1965a]) Let $p > 2$, $G = \langle a \rangle \times \langle w \rangle$ and $\overline{G} = \langle b \rangle \langle z \rangle$ where $o(a) = o(b) = p^3$, $o(w) = o(z) = \infty$ and $z^{-1}bz = b^{1+2p}$. Show that $\mathcal{R}(G) \not\cong \mathcal{R}(\overline{G})$; note that by 2.5.15, $L(G) \cong L(\overline{G})$.

8. (Loiko [1965a]) Let $G = \langle a \rangle \times \langle w \rangle$ where $o(a) = 2^n$, $n \geq 2$, and $o(w) = \infty$. Define $\sigma: G \rightarrow G$ by $(a^i w^k)^\sigma = c(i, k)a^i w^k$ where $c(i, k) = a^{2n-1}$ if $i$ and $k$ are odd and $c(i, k) = 1$ in all other cases. Show that $\sigma$ is a normed $\mathcal{R}$-automorphism but no automorphism of $G$.

9. If $G$ is a cyclic and $\overline{G}$ an arbitrary group of order $p^n$, show that there exists a bijective map $\sigma: G \rightarrow \overline{G}$ satisfying (15).

10. (Schmidt [1983]) Let $a: G \rightarrow G$ be bijective, a the amorphy of $a$ and assume that $\sigma$ induces a projectivity from $G$ to $\overline{G}$. Show that

\[ (i) \quad (xH)^\sigma = x^\sigma H^\sigma \text{ for all } H \leq G \text{ and } x \in G \]

implies

\[ (ii) \quad a(x, y) \in \langle y \rangle^\sigma \text{ for all } x, y \in G, \]

and this implies

\[ (iii) \quad (xy)^\sigma = x^\sigma y^\sigma \text{ for all } x, y \in G \text{ such that } o(x) = o(y) = \infty. \]

11. Use Exercise 10 to prove Loiko’s theorem saying that for a group generated by elements of infinite order, every left affinity is an isomorphism.

12. Let $p > 2$ be a prime, $G = \langle g \rangle$ a cyclic group of order $p^n$, $n \geq 1$, and let $H = \langle g^n \rangle$. Show that the map $\sigma: G \rightarrow G$ defined by $(gx)^\sigma = g^2x$ and $(g^2x)^\sigma = gx$ for all $x \in H$ and $y^\sigma = y$ for all $y \in G \setminus (gH \cup g^2H)$ is an affinity of $G$.

13. (Gashütz and Schmidt [1981]) Let $G$ be a group.

(a) If $x, y \in G$ such that $\langle x \rangle \cap \langle y \rangle = 1 = \langle xy \rangle \cap \langle y \rangle$, show that $y \in \Reg G$.

(b) If $x$ and $y$ are $p$-elements of $G$ such that $x \notin \Reg G$ and $y \notin \Reg G$, show that $\langle x \rangle \cap \langle y \rangle \neq 1$.

14. (Schmidt [1984a]) Show that $\Am G$ is locally cyclic.
I.N. Abramovskii

A.B. d'Andrea

V.A. Antonov

M.N. Arshinov

M.N. Arshinov and L.E. Sadovskii

R. Baer

D.W. Barnes

D.W. Barnes and G.E. Wall
P.P. Barysovec

G. Baumslag

H. Bechtell

T.R. Berger and F. Gross

Ja.G. Berkovic

M. Bianchi and M.C. Tamburini Bellani

G. Birkhoff

N. Bourbaki

R.H. Bradway, F. Gross and W.R. Scott

R. Brandl

B. Bruno

G. Busetto
G. Busetto and F. Menegazzo

G. Busetto and F. Napolitani

G. Busetto and S.E. Stonehewer

R.A. Calcaterra

A. Caranti

M. Cardin

S.N. Cernikov

N.V. Cernikova

Y. Cheng

C. Christensen

C.D.H. Cooper

M. Costantini

P. Crawley and R.P. Dilworth

M. Curzio
1957d. Sui gruppi supersolubili per cui il reticolo dei sottogruppi di composizione è autoduale. *Matematiche (Catania)* 12, 74–79.
M. Curzio and S. Rao
G. Daves and H. Heineken
F. De Giovanni and S. Franciosi

W.E. Deskins
R.P. Dilworth
(See P. Crawley and R.P. Dilworth)
L. Di Martino and M.C. Tamburini Bellani
N.T. Dinerstein
M. Emaldi


M. Emaldi and G. Zacher

W. Feit

T. Foguel

A. Fort


A. Franchetta

A. Franchetta and F. Tuccillo

S. Franciosi

(See also F. De Giovanni and S. Franciosi)

L. Fuchs

W. Gaschütz

W. Gaschütz and R. Schmidt

E. Gasparini and C. Metelli

L. Gerhards

Yu.M. Gorčakov

D. Gorenstein

G. Grätzer

F. Gross


(See also T.R. Berger and F. Gross; R.H. Bradway, F. Gross and W.R. Scott)

P. Hall


M. Hall


P. Hauck and H. Kurzweil


H. Heineken


(See also G. Daues and H. Heineken)

K.K. Hickin and R.E. Phillips


D.G. Higman


1988. Automorphisms of the lattice of subgroups of \( Z_{p^m} \times Z_{p^n} \). *Archiv Math.* 51, 491–495.


K. Honda


D.R. Hughes and J.G. Thompson


B. Huppert


B. Huppert and N. Blackburn


N. Ito

N. Ito and J. Szép  

S.G. Ivanov  


K. Iwasawa  


A.W. Jones  

R. Jürgensen  

O.H. Kegel  


E.I. Khukhro  

W. Kimmerle, R. Lyons, R. Sandling, and D.N. Teague  

R. Kochendörfer  

P. Köhler  
1983. $M_1$ as an interval in a subgroup lattice. *Algebra Universalis* 17, 263–266.

P.G. Kontorović and B.I. Plotkin  

A.G. Kurosh  


H. Kurzweil  


(See also P. Hauck and H. Kurzweil)

J.C. Lennox  

J.C. Lennox and S.E. Stonehewer  

S. Li  
Bibliography

W. Lindenberg

N.V. Loiko

P. Longobardi

P. Longobardi and M. Maj

A. Lucchini

E. Lukács and P.P. Pálfy

R. Lyons
(See W. Kimmerle, R. Lyons, R. Sandling, and D.N. Teague)

K. Mahdavi and J. Poland

R. Maier and P. Schmid

M. Mainardis
Bibliography

M. Maj
(See also P. Longobardi and M. Maj)

A. Mann

C. Marchionna Tibiletti

E. Martino

F. Menegazzo
(See also G. Busetto and F. Menegazzo)

C. Metelli
(See also E. Gasparini and C. Metelli)

M.D. Miller

L.S. Mozarovskaja

K. Nakamura

F. Napolitani


F. Napolitani and G. Zacher


(See also G. Busetto and F. Napolitani)

B.H. Neumann


W. Niegel


V.N. Obraztsov


A. Yu. Olshanskii


O. Ore


U. Ostendorf


P.P. Pálfy


P.P. Pálfy and P. Pudlák


(See also E. Lukács and P.P. Pálfy)

K.-J. Paulsen


G. Pazderski


A.S. Pekelis
Univ. Mat. Zap. 3, 72–76.
1963. Lattice isomorphisms of locally nilpotent torsion-free groups (Russian). Uspehi
630.
243.
Vyp. 18, 128–142.

A.S. Pekelis and L.E. Sadovskii

R.E. Phillips
(See K.K. Hickin and R.E. Phillips)

P. Plaumann, K. Strambach and G. Zacher

B.I. Plotkin
(N.S.) 95, 1141–1144.
336.
(See also P.G. Kontorović and B.I. Plotkin)

J. Poland
(See also K. Mahdavi and J. Poland)

S. Pontier
1966a. Sur les groupes (demi-groupes) dont le treillis des sous-groupes (sous-demi-
1966b. Demi-groupes dont le treillis des sous-demi-groupes est géométrique. Groupes
Math. (Lyon) 3, fasc. 4, 1–66.

E. Previato
Ital. B (6) 1, 1003–1014.

P. Pudlák and J. Tuma
1980. Every finite lattice can be embedded in a finite partition lattice. Algebra Universalis
10, 74–95.
(See also P.P. Pálfy and P. Pudlák)
Bibliography

S. Rao
(See M. Curzio and S. Rao)

M. Reuther

D.J.S. Robinson

D. M. Rocke

J.S. Rose

A. Rottländer

R. Rudolph

L.E. Sadovskii
1957a. The lattice of subgroups of a nilpotent torsion-free group (Russian). Uspehi Mat. Nauk (N.S.) 12, 201–204.
(See also M.N. Arshinov and L.E. Sadovskii; A.S. Pekelis and L.E. Sadovskii)

R. Sandling
(See W. Kimmerle, R. Lyons, R. Sandling, and D.N. Teague)
Bibliography

S. Sato

M. Schenke
1987a. Analoga des Fundamentalsatzes der projektiven Geometrie in der Gruppen-
1987b. Analoga des Fundamentalsatzes der projektiven Geometrie in der Gruppen-

E. Schenkman

P. Schmid
(See R. Maier and P. Schmid)

R. Schmidt
1968. Eine verbandstheoretische Charakterisierung der auflösbaren und der überauflös-
Hamburg 34, 115–125.
1970d. Charakterisierung der einfachen Gruppe der Ordnung 175 560 durch ihren Zen-
1974. Lattice isomorphisms and saturated formations of finite soluble groups. Proceed-
Soc. (3) 30, 287–300.
1977b. Untergruppenverbände endlicher einfacher Gruppen. Geometriae Dedicata 6, 275–
290.
Padova 63, 95–126.
J. Algebra 73, 264–272.
1982. Untergruppenverbände endlicher Gruppen mit elementarabelschen Hallschen
Bibliography


C.M. Scoppola


W.R. Scott


(See also R.H. Bradway, F. Gross and W.R. Scott)

G.M. Seitz and C.R.B. Wright
1969. On finite groups whose Sylow subgroups are modular or quaternion-free. J. Algebra 13, 374–381.

M.I. Sergeev

H.L. Silcock

A.L. Smelkin

A.E. Spencer

R.F. Spring

S.E. Stonehewer


S.E. Stonehewer and G. Zacher


(See also G. Busetto and S.E. Stonehewer; J.C. Lennox and S.E. Stonehewer)

K. Strambach

(See P. Plaumann, K. Strambach and G. Zacher)

M. Suzuki


Ja. P. Sysak


J. Szép

(See N. Ito and J. Szép)

O. Tamaschke


M.C. Tamburini Bellani

(See M. Bianchi and M.C. Tamburini Bellani; L.Di Martino and M.C. Tamburini Bellani)

D.N. Teague

(See W. Kimmerle, R. Lyons, R. Sandling, and D.N. Teague)

J.G. Thompson


(See also D.R. Hughes and J.G. Thompson)

J. Tits


M.V. Tsybanev


F. Tuccillo

(See A. Franchetta and F. Tuccillo)

J. Tuma


(See also P. Pudlák and J. Tuma)

T. Uzawa


A.V. Vasileva


Ph. Vassiliou

Bibliography

P. Venzke

H. Völklein

R.W.v.d. Waall

G.E. Wall
(See also D.W. Barnes and G.E. Wall)

P.M. Whitman

G.M. Whitson
1978. Finite groups whose subgroup, composition subgroup, or normal subgroup lattice is an ortholattice. *Algebra Universalis* 8, 123–127.

H. Wielandt

C.R.B. Wright
(See G.M. Seitz and C.R.B. Wright)

B.V. Yakovlev
1974. Conditions under which a lattice is isomorphic to the lattice of subgroups of a group. *Algebra and Logic* 13, 400–412.
1975. An example of solvable torsion-free groups which are lattice isomorphic but not isomorphic. *Algebra and Logic* 14, 282–301.

P. Yff

G. Zacher
Bibliography


(See also M. Emaldi and G. Zacher; F. Napolitani and G. Zacher; P. Plaumann, K. Strambach and G. Zacher; S.E. Stonehewer and G. Zacher)

G. Zappa


H. Zassenhaus

I. Zimmermann

A. Zitarosa
<table>
<thead>
<tr>
<th>Name</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abramovskii, I.N.</td>
<td>129</td>
</tr>
<tr>
<td>d'Andrea, A.B.</td>
<td>530, 541</td>
</tr>
<tr>
<td>Antonov, V.A.</td>
<td>518, 523, 524, 526, 527</td>
</tr>
<tr>
<td>Arshinov, M.N.</td>
<td>344, 359, 377, 384, 417</td>
</tr>
<tr>
<td>Barnes, D.W.</td>
<td>272, 274, 275, 279, 344, 382, 383, 385</td>
</tr>
<tr>
<td>Barysovec, P.P.</td>
<td>125</td>
</tr>
<tr>
<td>Barysovec, P.P.</td>
<td>125</td>
</tr>
<tr>
<td>Beck, H.</td>
<td>125, 126, 134</td>
</tr>
<tr>
<td>Berger, T.R.</td>
<td>220</td>
</tr>
<tr>
<td>Berovic, J. G.</td>
<td>232, 234</td>
</tr>
<tr>
<td>Bianchi, M.</td>
<td>131</td>
</tr>
<tr>
<td>Bradway, R.H.</td>
<td>220</td>
</tr>
<tr>
<td>Bruno, B.</td>
<td>16, 533</td>
</tr>
<tr>
<td>Calcaterra, R.A.</td>
<td>476</td>
</tr>
<tr>
<td>Caranti, A.</td>
<td>277, 344, 392, 393, 394, 395</td>
</tr>
<tr>
<td>Cardin, M.</td>
<td>310, 311</td>
</tr>
<tr>
<td>Cernikov, S.N.</td>
<td>125</td>
</tr>
<tr>
<td>Cernikova, N.V.</td>
<td>123, 124, 126</td>
</tr>
<tr>
<td>Cheng, Y.</td>
<td>526</td>
</tr>
<tr>
<td>Christensen, C.</td>
<td>121</td>
</tr>
<tr>
<td>Cooper, C.D.H.</td>
<td>1, 29, 30, 34</td>
</tr>
<tr>
<td>Costantini, M.</td>
<td>449</td>
</tr>
<tr>
<td>Curzio, M.</td>
<td>10, 121, 134, 137, 486, 488, 492, 493, 495, 497, 503, 504, 511, 512, 529, 530, 540</td>
</tr>
<tr>
<td>Dauess, G.</td>
<td>277</td>
</tr>
<tr>
<td>De Giovanni, F.</td>
<td>125, 133, 135, 319, 320, 321, 496, 497</td>
</tr>
<tr>
<td>Deskins, W.E.</td>
<td>222</td>
</tr>
<tr>
<td>Di Martino, L.</td>
<td>131, 134</td>
</tr>
<tr>
<td>Dinerstein, N.T.</td>
<td>121</td>
</tr>
<tr>
<td>Emaldi, M.</td>
<td>118, 120, 121, 123, 126, 129, 130, 134</td>
</tr>
<tr>
<td>Feit, W.</td>
<td>10</td>
</tr>
<tr>
<td>Foguel, T.</td>
<td>484</td>
</tr>
<tr>
<td>Fort, A.</td>
<td>87, 232, 234</td>
</tr>
<tr>
<td>Franchetti, A.</td>
<td>496, 510</td>
</tr>
<tr>
<td>Franciosi, S.</td>
<td>125, 133, 135, 319, 320, 321, 496, 497</td>
</tr>
<tr>
<td>Fuchs, L.</td>
<td>110</td>
</tr>
<tr>
<td>Gaschütz, W.</td>
<td>23, 397, 486, 524, 526, 538, 541</td>
</tr>
<tr>
<td>Gasparini, E.</td>
<td>108, 113</td>
</tr>
<tr>
<td>Gorčakov, Yu.M.</td>
<td>125</td>
</tr>
<tr>
<td>Goursat, E.</td>
<td>34</td>
</tr>
<tr>
<td>Gross, F.</td>
<td>220, 222, 227, 304, 310, 311</td>
</tr>
<tr>
<td>Hall, P.</td>
<td>114, 122, 126</td>
</tr>
<tr>
<td>Hauck, P.</td>
<td>401</td>
</tr>
<tr>
<td>Heineken, H.</td>
<td>277, 401, 485, 494, 498, 506, 511</td>
</tr>
<tr>
<td>Hickin, K.K.</td>
<td>319</td>
</tr>
<tr>
<td>Higman, D.G.</td>
<td>142</td>
</tr>
<tr>
<td>Holmes, C.S.</td>
<td>104, 200, 276, 277, 359, 430, 438</td>
</tr>
<tr>
<td>Honda, K.</td>
<td>200, 276, 277</td>
</tr>
<tr>
<td>Hughes, D.R.</td>
<td>147</td>
</tr>
<tr>
<td>Huppert, B.</td>
<td>34, 187</td>
</tr>
<tr>
<td>Ito, N.</td>
<td>222, 233, 243</td>
</tr>
<tr>
<td>Ivanov, S.G.</td>
<td>136, 144</td>
</tr>
<tr>
<td>Iwasawa, K.</td>
<td>41, 55, 65, 71, 75, 79, 86, 199, 228, 231</td>
</tr>
<tr>
<td>Jones, A.W.</td>
<td>65, 87</td>
</tr>
<tr>
<td>Jürgensen, R.</td>
<td>524, 527</td>
</tr>
<tr>
<td>Kegel, O.H.</td>
<td>148, 510</td>
</tr>
<tr>
<td>Khukhro, E.I.</td>
<td>148</td>
</tr>
<tr>
<td>Kimmerle, W.</td>
<td>439</td>
</tr>
<tr>
<td>Kochendörfer, R.</td>
<td>125</td>
</tr>
<tr>
<td>Kontorovič, P.G.</td>
<td>343, 361, 385</td>
</tr>
<tr>
<td>Kurosh, A.G.</td>
<td>43</td>
</tr>
<tr>
<td>Kurzweil, H.</td>
<td>401</td>
</tr>
<tr>
<td>Lennox, J.C.</td>
<td>304</td>
</tr>
<tr>
<td>Li, S.</td>
<td>440</td>
</tr>
<tr>
<td>Loiko, N.V.</td>
<td>529, 531, 533, 538, 540, 541</td>
</tr>
</tbody>
</table>
Index of Names

Longobardi, P. 87, 489, 490, 496, 497, 498
Lukács, E. 420
Lyons, R. 439

Mahdavi, K. 112
Maier, R. 218
Mainardis, M. 77, 96, 97, 98, 100
Maj, M. 87, 489, 490, 496, 497, 498
Martino, E. 30


Metelli, C. 108, 113, 441, 449
Mozarovskaja, L.S. 126

Nakamura, K. 222, 227

Neumann, B.H. 283
Niegel, W. 277

Obraztsov, V.N. 459
Olschanskii, A.Yu. 82, 311
Ore, O. 1, 12, 16, 43, 222
Ostendorf, U. 111

Pálfy, P.P. 10, 420, 490
Paulsen, K.-J. 160, 164, 176, 186, 187, 197, 198
Pazderski, G. 485, 489, 504, 506, 511
Pekelis, A.S. 344, 363, 376, 377, 401, 405
Phillips, R.E. 319
Plaumann, P. 401
Plotkin, B.I. 343, 361, 385, 401
Poland, J. 19, 112
Previato, E. 116, 120, 204, 209, 215, 317
Pudlák, P. 9

Rao, S. 134
Reuther, M. 526, 527
Rips, E. 281, 286, 325
Robinson, D.J.S. 33
Rocke, D.M. 521
Rose, J.S. 40
Rottländner, A. 200, 275, 276
Rudolph, R. 83

Sadovskii, L.E. 1, 21, 22, 343, 344, 359, 360, 363, 373, 374, 417
Sandling, R. 439
Sato, S. 41, 65, 96, 99, 142, 233
Schenke, M. 48, 344, 415, 416, 421

Schenkman, E. 30
Schmid, P. 218
Scoppola, C.M. 358
Scott, W.R. 220, 374
Seitz, G.M. 67, 187, 197
Sergeev, M.I. 126
Silcock, H.L. 490
Smelkin, A.L. 374, 418
Spring, R.F. 273
Stonehewer, S.E. 43, 144, 145, 209, 220, 253, 254, 293, 297, 302, 311, 312, 316, 328, 329, 330, 341, 401, 459, 484
Strambach, K. 401
Sysak, J. 125
Szép, J. 222, 243

Tamaschke, O. 501, 504
Tamburini Bellani, M.C. 131, 134
Teague, D.N. 439
Thompson, J.G. 147, 227
Tits, J. 440
Tsybanov, M.V. 126
Tuccillo, F. 496
Tuma, J. 9, 10

Uzawa, T. 437

Vasileva, A.V. 524, 527
Venzke, P. 133, 234, 235
Völklein, H. 449

v.d.Waall, R.W. 67
Wall, G.E. 148, 272, 274, 275, 279, 343, 344, 360, 382, 383, 385
Whitman, P.M. 9
Whitson, G.M. 216
Wielandt, H. 6, 499
Wright, C.R.B. 67, 187, 197

Yff, P. 200, 276, 277

Zappa, G.  115, 141, 142, 143, 144, 157, 181, 502

Zitarosa, A.  498
A
abelian group(s) 43, 86, 94–113, 491–494, 536
character group of 453
elementary 25, 49–52, 131
of torsion-free rank 1 107–113, 493, 533
of torsion-free rank ≥ 2 106, 358, 492, 533
periodic 94, 96, 103–105, 397, 492
power automorphisms of 32
projectivities between 103, 104, 110–113
projectivities of 94, 96, 99, 106
R-isomorphisms of 533
with duals 452–458
abelian Sylow subgroup 185–187, 197
abelian variety 382
absorption identities 2
admissible subgroup of a partition 147
affinity 534–541
algebraic lattice 9
almost free group of a variety 382
alternating group 10, 26, 115–116, 432, 441–449
amorphy of a group 539–541
amorphy of a map 17, 534, 538–541
antiatom 3
antichain 3
antiisomorphism 90, 363, 374, 532
ascendant subgroup 293, 328
ascending chain condition 4, 46
associativity identities 17, 534, 539
atom 3
automorphism
of group 24
of lattice 4
power 24, 29–34
autoproporjectivity 23–29

B
Baer map 416
basic system 352
bound
greatest lower 2
least upper 2
lower/upper 2

C
centre 273, 536
of a finite perfect group 229
of a p-group 243
of a Sylow subgroup 195–197
of a torsion-free group 360
Z_n(G) 183
centralizer
duality 512
lattice 8, 511–527
maximal 514
minimal 514
partition 519
preserving projectivity 272–273
C-group 121–126
chain 3, 16
modular 360, 375
permodular 385–391
supersoluble 319
chain condition 4
ascending 4, 46
descending 4
Jordan-Dedekind 47, 231–234, 540
character group 453
characterization
lattice-theoretic 14
of subgroup lattices 357
classical group 436, 439
class of groups invariant under projectivities 14
classical groups 436, 439
class with lattice-theoretic characterization 14
finite nilpotent-by-abelian groups 399
finite soluble groups of Fitting length k 180, 399
finite soluble groups of rank r 396
formation 398
groups of Lie type 440
hypoabelian groups 315
locally r-groups 15
P-groups 51
radical groups 405
soluble groups 332
Sylow tower groups 396
class of groups with lattice-theoretic
<table>
<thead>
<tr>
<th>Index of Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>characterization 14</td>
</tr>
<tr>
<td>cyclic groups 13</td>
</tr>
<tr>
<td>finite groups 15</td>
</tr>
<tr>
<td>finitely generated nonperiodic nilpotent groups 375</td>
</tr>
<tr>
<td>finitely generated soluble groups 317</td>
</tr>
<tr>
<td>finite soluble groups 229, 230</td>
</tr>
<tr>
<td>finite soluble groups with chief factors of dimension at most k 405</td>
</tr>
<tr>
<td>free groups 356</td>
</tr>
<tr>
<td>hyperabelian groups 316</td>
</tr>
<tr>
<td>hypercyclic groups 319</td>
</tr>
<tr>
<td>locally cyclic groups 12</td>
</tr>
<tr>
<td>locally finite groups 15–16</td>
</tr>
<tr>
<td>nilpotent p-group or P-group 391</td>
</tr>
<tr>
<td>nonperiodic locally nilpotent groups 376</td>
</tr>
<tr>
<td>perfect groups 229, 313</td>
</tr>
<tr>
<td>P-groups 70, 394</td>
</tr>
<tr>
<td>polycyclic groups 317</td>
</tr>
<tr>
<td>residually finite groups 287</td>
</tr>
<tr>
<td>residually finitely generated soluble groups 321</td>
</tr>
<tr>
<td>residually polycyclic groups 320</td>
</tr>
<tr>
<td>residuously supersoluble groups 319</td>
</tr>
<tr>
<td>simple groups 228, 312</td>
</tr>
<tr>
<td>SN-groups 319</td>
</tr>
<tr>
<td>supersoluble groups 230, 231, 318</td>
</tr>
<tr>
<td>torsion-free nilpotent groups 361</td>
</tr>
<tr>
<td>commutators 29</td>
</tr>
<tr>
<td>set of 516</td>
</tr>
<tr>
<td>commutator subgroup 29, 272</td>
</tr>
<tr>
<td>second 174, 326, 476</td>
</tr>
<tr>
<td>compact element 9</td>
</tr>
<tr>
<td>comparable elements 3</td>
</tr>
<tr>
<td>compatible projectivity 380</td>
</tr>
<tr>
<td>complement 115</td>
</tr>
<tr>
<td>permutable 121</td>
</tr>
<tr>
<td>relative 127</td>
</tr>
<tr>
<td>sectional (or S-) 122</td>
</tr>
<tr>
<td>complemented lattice 115</td>
</tr>
<tr>
<td>of cosets 530</td>
</tr>
<tr>
<td>of normal subgroups 490</td>
</tr>
<tr>
<td>of subgroups 115–135</td>
</tr>
<tr>
<td>of composition subgroups 503</td>
</tr>
<tr>
<td>complete</td>
</tr>
<tr>
<td>lattice 2</td>
</tr>
<tr>
<td>meet-sublattice 7</td>
</tr>
<tr>
<td>complex 346</td>
</tr>
<tr>
<td>component of a partition 145</td>
</tr>
<tr>
<td>composition series 6</td>
</tr>
<tr>
<td>composition subgroup 6, 498–511</td>
</tr>
<tr>
<td>conjugacy class 278–280, 425</td>
</tr>
<tr>
<td>conjugacy preserving projectivity 272</td>
</tr>
<tr>
<td>coprime groups 36</td>
</tr>
<tr>
<td>core 199</td>
</tr>
<tr>
<td>coset lattice 8, 527–541</td>
</tr>
<tr>
<td>cover</td>
</tr>
<tr>
<td>elements of a lattice 3</td>
</tr>
<tr>
<td>irreducibly a group 283</td>
</tr>
<tr>
<td>Coxeter group 437</td>
</tr>
<tr>
<td>crossed isomorphism 90–96</td>
</tr>
<tr>
<td>cyclic</td>
</tr>
<tr>
<td>element 345</td>
</tr>
<tr>
<td>group 12–16, 28</td>
</tr>
<tr>
<td>$L_1(G)$ 18</td>
</tr>
<tr>
<td>modular chain 375</td>
</tr>
<tr>
<td>permutable subgroup 223–225, 307–311, 318</td>
</tr>
<tr>
<td>D</td>
</tr>
<tr>
<td>decomposable subgroup lattice 36–39</td>
</tr>
<tr>
<td>Dedekind element 43</td>
</tr>
<tr>
<td>Dedekind subgroup 289</td>
</tr>
<tr>
<td>defect of a subnormal subgroup 125, 499</td>
</tr>
<tr>
<td>$D$-embedded subgroup 289</td>
</tr>
<tr>
<td>derived length 332</td>
</tr>
<tr>
<td>descending chain condition 4</td>
</tr>
<tr>
<td>determined by subgroup lattice vii, 343</td>
</tr>
<tr>
<td>alternating group 432</td>
</tr>
<tr>
<td>classical group 436, 439</td>
</tr>
<tr>
<td>dihedral group 422, 437</td>
</tr>
<tr>
<td>direct product of two isomorphic groups 412, 429</td>
</tr>
<tr>
<td>finite Coxeter group 437</td>
</tr>
<tr>
<td>finite simple group 432, 434, 439</td>
</tr>
<tr>
<td>infinite cyclic group 13</td>
</tr>
<tr>
<td>nilpotent group of class 2 and exponent $p$ 384</td>
</tr>
<tr>
<td>projective general/special linear group 156, 432, 434, 436</td>
</tr>
<tr>
<td>quaternion group 28</td>
</tr>
<tr>
<td>strongly 343</td>
</tr>
<tr>
<td>Suzuki group 156, 434</td>
</tr>
<tr>
<td>symmetric group 432, 438</td>
</tr>
<tr>
<td>diagonal 35, 408–411</td>
</tr>
<tr>
<td>dihedral group 27, 422, 426, 437</td>
</tr>
<tr>
<td>generalized 149</td>
</tr>
<tr>
<td>directly decomposable</td>
</tr>
<tr>
<td>centralizer lattice 515–518, 527</td>
</tr>
<tr>
<td>coset lattice 529</td>
</tr>
<tr>
<td>lattice 8</td>
</tr>
<tr>
<td>lattice of composition subgroups 501</td>
</tr>
<tr>
<td>lattice of normal subgroups 488</td>
</tr>
<tr>
<td>subgroup lattice 36–39</td>
</tr>
<tr>
<td>direct product of groups 34–40</td>
</tr>
<tr>
<td>isomorphic groups 408–416, 426, 429</td>
</tr>
<tr>
<td>lattice-isomorphic groups 418–420</td>
</tr>
<tr>
<td>lattices 8</td>
</tr>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>distributive</td>
</tr>
<tr>
<td>centralizer lattice</td>
</tr>
<tr>
<td>coset lattice</td>
</tr>
<tr>
<td>element</td>
</tr>
<tr>
<td>lattice</td>
</tr>
<tr>
<td>lattice of composition</td>
</tr>
<tr>
<td>subgroups</td>
</tr>
<tr>
<td>lattice of normal subgroups</td>
</tr>
<tr>
<td>pair of elements</td>
</tr>
<tr>
<td>subgroup lattice</td>
</tr>
<tr>
<td>double centralizer property</td>
</tr>
<tr>
<td>doubly transitive permutation group</td>
</tr>
<tr>
<td>duality</td>
</tr>
<tr>
<td>abelian groups with dual</td>
</tr>
<tr>
<td>between lattices of composition</td>
</tr>
<tr>
<td>between lattices of normal</td>
</tr>
<tr>
<td>subgroups</td>
</tr>
<tr>
<td>centralizer</td>
</tr>
<tr>
<td>groups with dual</td>
</tr>
<tr>
<td>dually modular element</td>
</tr>
<tr>
<td>E</td>
</tr>
<tr>
<td>elementary abelian group</td>
</tr>
<tr>
<td>element map</td>
</tr>
<tr>
<td>Baer map</td>
</tr>
<tr>
<td>derived from a projectivity</td>
</tr>
<tr>
<td>inducing a projectivity</td>
</tr>
<tr>
<td>(\varphi)-mapping</td>
</tr>
<tr>
<td>element of a group</td>
</tr>
<tr>
<td>height of</td>
</tr>
<tr>
<td>inducing the power (k) in a subgroup</td>
</tr>
<tr>
<td>left regular</td>
</tr>
<tr>
<td>order modulo a subgroup</td>
</tr>
<tr>
<td>right regular</td>
</tr>
<tr>
<td>type of</td>
</tr>
<tr>
<td>element(s) of a lattice</td>
</tr>
<tr>
<td>compact</td>
</tr>
<tr>
<td>comparable</td>
</tr>
<tr>
<td>cyclic</td>
</tr>
<tr>
<td>Dedekind</td>
</tr>
<tr>
<td>dually modular element</td>
</tr>
<tr>
<td>greatest</td>
</tr>
<tr>
<td>isolated</td>
</tr>
<tr>
<td>join-distributive</td>
</tr>
<tr>
<td>join-quasi-distributive</td>
</tr>
<tr>
<td>least</td>
</tr>
<tr>
<td>maximal</td>
</tr>
<tr>
<td>meet-distributive</td>
</tr>
<tr>
<td>meet-quasi-distributive</td>
</tr>
<tr>
<td>minimal</td>
</tr>
<tr>
<td>modular</td>
</tr>
<tr>
<td>modularly embedded</td>
</tr>
<tr>
<td>neutral</td>
</tr>
<tr>
<td>permodularly embedded</td>
</tr>
<tr>
<td>polymodular</td>
</tr>
<tr>
<td>semimodular</td>
</tr>
<tr>
<td>standard</td>
</tr>
<tr>
<td>uniquely complemented</td>
</tr>
<tr>
<td>embedding</td>
</tr>
<tr>
<td>hypercentral</td>
</tr>
<tr>
<td>hypercyclic</td>
</tr>
<tr>
<td>modular</td>
</tr>
<tr>
<td>of lattices in subgroup lattices</td>
</tr>
<tr>
<td>permodular</td>
</tr>
<tr>
<td>exponent of a group</td>
</tr>
<tr>
<td>extended Tarski group</td>
</tr>
<tr>
<td>F</td>
</tr>
<tr>
<td>finite group</td>
</tr>
<tr>
<td>Fitting</td>
</tr>
<tr>
<td>length</td>
</tr>
<tr>
<td>series</td>
</tr>
<tr>
<td>subgroup</td>
</tr>
<tr>
<td>formation of finite soluble groups</td>
</tr>
<tr>
<td>(\mathcal{F})-projector</td>
</tr>
<tr>
<td>Frattini subgroup</td>
</tr>
<tr>
<td>free group</td>
</tr>
<tr>
<td>of a variety</td>
</tr>
<tr>
<td>2-free group</td>
</tr>
<tr>
<td>free polynilpotent group</td>
</tr>
<tr>
<td>free product of groups</td>
</tr>
<tr>
<td>(\mathcal{F})-residual</td>
</tr>
<tr>
<td>Frobenius group</td>
</tr>
<tr>
<td>G</td>
</tr>
<tr>
<td>(\mathcal{G})-isomorphism</td>
</tr>
<tr>
<td>greatest element</td>
</tr>
<tr>
<td>greatest lower bound</td>
</tr>
<tr>
<td>group(s)</td>
</tr>
<tr>
<td>abelian</td>
</tr>
<tr>
<td>alternating</td>
</tr>
<tr>
<td>amorphism of</td>
</tr>
<tr>
<td>(C)-</td>
</tr>
<tr>
<td>classical</td>
</tr>
<tr>
<td>coprime</td>
</tr>
<tr>
<td>covered irreducibly by cosets (subgroups)</td>
</tr>
<tr>
<td>Coxeter</td>
</tr>
<tr>
<td>cyclic</td>
</tr>
<tr>
<td>determined by its subgroup lattice</td>
</tr>
<tr>
<td>dihedral</td>
</tr>
<tr>
<td>elementary abelian</td>
</tr>
</tbody>
</table>
finite 15
finitely generated modulo subgroup 292
free 345–359, 374, 533
free polynilpotent 374, 533
Frobenius 145, 519
generalized dihedral 149
generated by involutions 421–451, 537
hamiltonian 55, 60, 68, 89
hyperabelian 315, 316
hypercyclic 123, 315, 319
hypoabelian 315
IM- 130–135
K- 115–124
lattice-isomorphic 4
lattice-simple 449
locally cyclic 12
locally finite 15–16
locally free 359, 533
locally nilpotent 373, 376, 533
locally \mathcal{F}- 15
M- 54–100; 55, 71, 75, 79, 82
\mathfrak{M}- 518–523
M* 55, 58–69
metacyclic 225
nilpotent 47, 54, 360–395, 494–498, 533
nilpotent-by-abelian 397
of all autopredictions 23–29
of all power automorphisms 24, 29–34
of Lie type 440, 449
\Omega- 394
P- 49–54
P* 69, 89
P-decomposable 170
perfect 186, 219, 229, 243, 313, 330, 540
permutation 115, 430–449
polycyclic 317
projective general/special linear 116, 120, 146, 152, 156, 177, 432–436, 519, 523–524
Prüfer 16
p-soluble 183, 196
quaternion 28
radical 402–405
RC- 129–130
residually finite 287
residually finitely generated soluble 321
residually polycyclic 320
residually supersoluble 319
RK- 127–135
Rottländer 162, 276, 413, 430
SC- 122–124
simple 116, 156, 228, 312, 432, 434, 439–441, 449, 523
SK- 126
SN- 319
strongly determined by its subgroup lattice 343
supersoluble 122, 230–234, 318
Suzuki 116, 146, 152, 156, 434
Sylow tower 396, 405
symmetric 115, 149, 177, 432, 438, 441–445, 447, 451, 513, 527
T-, T*- 127
Tarski 82, 88
2-free 348–359
with dual 452–484; 458, 459
with identical subgroup structures 275–277
with normal Hall subgroup 158–166
with partition 145–156; 152
Grüenberg radical 329

H
Hall subgroup 158–166
hamiltonian group 55, 60, 68, 89
Hasse diagram 5
height of element in abelian group 107
Hirsch-Plotkin hyppradical 404, 405
radical 402
series 403, 404
homomorphism of lattice 4
Hughes subgroup 147
hyperabelian group 315, 316
hypercentral embedding 217
hypercentre 183, 243
hypercyclic embedding 217
group 315, 319
K-group 123
hypoabelian group 315

I
identical subgroup structures 275–277
IM-group 130–135
index preserving projectivity 166–178, 325–329, 408
induce a power in a subgroup 257
inner automorphism 24
interval 5, 10, 401
invariant under projectivities 14
(see class of groups invariant under projectivities)
involution 421–451, 537
isolated element 360
isomorphism
between lattices of composition subgroups 504–507
between lattices of normal subgroups 490–496
crossed 90–96
of lattice 4
$R$- 530
Iwasawa triple 60–69

J
join-distributive element 136–137, 141–142
join-distributive pair 16
join-quasi-distributive element 136–137
Jordan-Dedekind chain condition 47, 231–234, 540

K
$K$-group 115–124

L
lattice 2
algebraic 9
centralizer 8, 511–527
complemented 115
complete 2
coset 8, 527–541
directly decomposable 8
distributive 11
lower semimodular 47–48
modular 41–48
of composition subgroups 6, 47, 498–511
of cosets with respect to normal subgroups 541
of divisors of $n$ 11
of normal subgroups 5, 43, 486–498
of subnormal subgroups 7, 47, 498–511
partition 10
permodular 312
poly-$k$-modular 405
polymodular 234
relatively complemented 127
sectionally complemented 126
semimodular 46–48, 233
subgroup 3
upper semimodular 46–48
weakly join-complemented 133
weakly meet-complemented 135
weakly modular 87
lattice-isomorphic groups 4
lattice-simple group 449
lattice-theoretic characterization 14
(see class of groups with lattice-theoretic characterization)
least element 3
least upper bound 2
left affinity 537
length of a poset 3, 39
locally cyclic group 12
locally finite group 15–16
$M$-group 78–82
of finite exponent 178
$p$-group 53, 79, 94, 273
$RK$-group 130
$SC$-group 123
with dual 458, 478
locally finite radical 329, 459
locally free group 359, 533
locally nilpotent group 373, 376, 533
locally $P$-embedded subgroup 302
locally soluble radical 477
locally $\mathcal{X}$-group 15
local system of subgroups 21
lower semimodular lattice 47–48, 233, 394, 399, 529

M
map
amorph of 17, 534, 538–541
Baer 416
element 17, 20, 101–107
normed 530
$\varphi$- 361
maximal centralizer 514
maximal condition 4, 46
maximal element 3
maximal sensitive subgroup 133, 234
meet-distributive element 136, 138, 143–145
meet-distributive pair 16, 40
meet-quasi-distributive element 136, 138, 143–145
meet-sublattice 7
metacyclic $p$-group 225
$M$-group 54–100; 55, 71, 75, 79, 82
$\mathfrak{M}$-group 518–523
$M^*$-group 55, 58–69
minimal centralizer 514
minimal condition 4
minimal element 3
minimal normal subgroup 235–238
modular
centralizer lattice 518–524, 527
coset lattice 529
dually 87
element 43–46, 144
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>lattice</td>
<td>41–48</td>
</tr>
<tr>
<td>lattice of composition subgroups</td>
<td>502–503</td>
</tr>
<tr>
<td>subgroup</td>
<td>43, 200–220, 232</td>
</tr>
<tr>
<td>subgroup lattice</td>
<td>54–88</td>
</tr>
<tr>
<td>weakly</td>
<td>87</td>
</tr>
<tr>
<td>modular chain</td>
<td>360</td>
</tr>
<tr>
<td>cyclic</td>
<td>375</td>
</tr>
<tr>
<td>modularly embedded element</td>
<td>360</td>
</tr>
<tr>
<td>N</td>
<td></td>
</tr>
<tr>
<td>neutral element</td>
<td>135, 142–145, 498</td>
</tr>
<tr>
<td>nilpotent-by-abelian group</td>
<td>397</td>
</tr>
<tr>
<td>nilpotent group</td>
<td>360–395</td>
</tr>
<tr>
<td>finite</td>
<td>47, 54, 494–498</td>
</tr>
<tr>
<td>of class 2 and exponent p</td>
<td>384</td>
</tr>
<tr>
<td>periodic</td>
<td>387, 391</td>
</tr>
<tr>
<td>torsion-free</td>
<td>361, 373, 533</td>
</tr>
<tr>
<td>nilpotent residual</td>
<td>181</td>
</tr>
<tr>
<td>nilpotent variety</td>
<td>382–385</td>
</tr>
<tr>
<td>normal closure</td>
<td>199, 207</td>
</tr>
<tr>
<td>of a permutable subgroup</td>
<td>304</td>
</tr>
<tr>
<td>normal Hall subgroup</td>
<td>158–166</td>
</tr>
<tr>
<td>normality relation</td>
<td>302</td>
</tr>
<tr>
<td>normalizer preserving projectivity</td>
<td>272–275, 377–385, 408</td>
</tr>
<tr>
<td>normal partition</td>
<td>146</td>
</tr>
<tr>
<td>normal subgroup</td>
<td>5, 43, 486–498</td>
</tr>
<tr>
<td>minimal</td>
<td>235–238</td>
</tr>
<tr>
<td>projective image</td>
<td>239, 321–323, 334, 340</td>
</tr>
<tr>
<td>( \mathcal{X} )-normal</td>
<td>510</td>
</tr>
<tr>
<td>normed map</td>
<td>530</td>
</tr>
<tr>
<td>norm of a group</td>
<td>24, 30</td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>( \Omega )-group</td>
<td>394</td>
</tr>
<tr>
<td>( \mathcal{O}_p(G) )</td>
<td>181, 506</td>
</tr>
<tr>
<td>( \mathcal{O}_s(G) )</td>
<td>178, 506</td>
</tr>
<tr>
<td>( o(x, H) )</td>
<td>206</td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>( p )-adic unit</td>
<td>32–33</td>
</tr>
<tr>
<td>pair</td>
<td></td>
</tr>
<tr>
<td>join-distributive</td>
<td>16</td>
</tr>
<tr>
<td>meet-distributive</td>
<td>16, 40</td>
</tr>
<tr>
<td>partially ordered set</td>
<td>1</td>
</tr>
<tr>
<td>partition lattice</td>
<td>10</td>
</tr>
<tr>
<td>partition of a group</td>
<td>145–156, 519</td>
</tr>
<tr>
<td>( p )-collecting subgroup</td>
<td>540</td>
</tr>
<tr>
<td>( p )-collector</td>
<td>540</td>
</tr>
<tr>
<td>( P )-decomposition</td>
<td>170</td>
</tr>
<tr>
<td>( P )-embedded subgroup</td>
<td>297</td>
</tr>
<tr>
<td>perfect group</td>
<td>186, 219, 229, 243, 313, 330, 540</td>
</tr>
<tr>
<td>permodular chain</td>
<td>385–391</td>
</tr>
<tr>
<td>permodular lattice</td>
<td>312</td>
</tr>
<tr>
<td>permodularly embedded element</td>
<td>385</td>
</tr>
<tr>
<td>permutable subgroup</td>
<td>288–303</td>
</tr>
<tr>
<td>permutable complement</td>
<td>121</td>
</tr>
<tr>
<td>permutable subgroup</td>
<td>43, 201, 202, 216–227, 293, 296, 303–311, 318</td>
</tr>
<tr>
<td>permutably complemented subgroup</td>
<td>121</td>
</tr>
<tr>
<td>permutation group</td>
<td>430–449</td>
</tr>
<tr>
<td>doubly transitive</td>
<td>434, 435, 438</td>
</tr>
<tr>
<td>primitive</td>
<td>115, 439</td>
</tr>
<tr>
<td>triply transitive</td>
<td>432</td>
</tr>
<tr>
<td>( P(G) )-connected subgroups</td>
<td>468</td>
</tr>
<tr>
<td>( P(G) )-normal subgroup</td>
<td>469</td>
</tr>
<tr>
<td>( P )-group</td>
<td></td>
</tr>
<tr>
<td>finite</td>
<td>52–69, 220–223, 243–272, 274, 279, 391–395, 504</td>
</tr>
<tr>
<td>locally finite</td>
<td>53, 79, 94, 273, 460</td>
</tr>
<tr>
<td>metacyclic</td>
<td>225</td>
</tr>
<tr>
<td>nilpotent</td>
<td>387, 391</td>
</tr>
<tr>
<td>of maximal class</td>
<td>392–395</td>
</tr>
<tr>
<td>regular</td>
<td>392</td>
</tr>
<tr>
<td>with modular subgroup lattice</td>
<td>54–69, 79, 94</td>
</tr>
<tr>
<td>( P )-group</td>
<td>49–54</td>
</tr>
<tr>
<td>( P^* )-group</td>
<td>69, 89</td>
</tr>
<tr>
<td>( \phi )-mapping</td>
<td>361</td>
</tr>
<tr>
<td>( P )-hypercentrally closed formation</td>
<td>400</td>
</tr>
<tr>
<td>( P )-hypercentral triple</td>
<td>399</td>
</tr>
<tr>
<td>( p )-length</td>
<td>183</td>
</tr>
<tr>
<td>( p )-normal</td>
<td>195</td>
</tr>
<tr>
<td>polycyclic group</td>
<td>317</td>
</tr>
<tr>
<td>poly-( k )-modular lattice</td>
<td>405</td>
</tr>
<tr>
<td>polymodular element</td>
<td>234</td>
</tr>
<tr>
<td>polymodular lattice</td>
<td>234</td>
</tr>
<tr>
<td>poset</td>
<td></td>
</tr>
<tr>
<td>length</td>
<td>3, 39</td>
</tr>
<tr>
<td>width</td>
<td>3, 39–40</td>
</tr>
<tr>
<td>power automorphism</td>
<td>24, 29–34</td>
</tr>
<tr>
<td>of abelian group</td>
<td>32</td>
</tr>
<tr>
<td>of ( M^* )-group</td>
<td>68</td>
</tr>
<tr>
<td>of nonperiodic group</td>
<td>33</td>
</tr>
<tr>
<td>universal</td>
<td>32</td>
</tr>
<tr>
<td>prefrratti subgroup</td>
<td>401</td>
</tr>
<tr>
<td>( p )-regular projectivity</td>
<td>167–178, 422–424</td>
</tr>
<tr>
<td>primitive permutation group</td>
<td>115, 439</td>
</tr>
<tr>
<td>product</td>
<td></td>
</tr>
<tr>
<td>direct</td>
<td>8, 34–40, 406–421, 426, 429</td>
</tr>
<tr>
<td>free</td>
<td>359</td>
</tr>
<tr>
<td>wreath</td>
<td>416–418</td>
</tr>
<tr>
<td>projective general/special linear group</td>
<td>116, 120, 146, 152, 156, 177, 432–436, 519, 523–524</td>
</tr>
</tbody>
</table>
projectivity 4
  between abelian groups 103, 104, 110-113
  between finite groups with normal Hall subgroups 160
  centralizer preserving 272-273
  compatible with a pair of epimorphisms 380
  conjugacy preserving 272
  index preserving 166-178, 325-329, 408
  induced by a crossed isomorphism 93
  induced by a group-isomorphism 20-24
  induced by an element map 17, 20
  induced in a factor group 22
  induced in a subgroup 15
  invariant under 14
  normalizer preserving 272-275, 377-385, 408
  of abelian groups 94, 96, 99, 106
  of M-groups 89, 94, 99
  p-regular (or regular at p) 167-178, 422-424
  p-singular (or singular at p) 167-178, 422-424
  singular 166-178
  projector of a formation 397, 401
  Prüfer group 16
  p-singular projectivity 167-178, 422-424
  p-soluble group 183, 196

Q
  quasinormal subgroup 43
  quaternion group 28

R
  radical
    Grunenberg 329
    Hirsch-Plotkin 402
    locally finite 329, 459
    locally solvable 477
    soluble 230, 234
  radical group 402-405
  rank of soluble group 396
  RC-group 129-130
  regular at p 167-178, 422-424
  regular element 536
  regular p-group 392
  relative complement 127
  relatively complemented lattice 127
  residual
    nilpotent 181
    $9K^*$ 240
    of a formation 397, 400
  soluble 230, 234
  supersoluble 234
  residually finite group 287
  residually finitely generated soluble group 321
  residually polycyclic group 320
  residually supersoluble group 319
  right affinity 537
  R-isomorphism 530
  RK-group 127-135
  Rottländer group 162, 276, 413, 430

S
  saturated formation 397
  SC-group 122-124
  Schmidt structure 297
  sectional complement (or S-complement) 122
  sectionally complemented lattice 126
  semiaffinity 537
  semimodular element 49, 216
  semimodular lattice 46-48, 233, 394, 399, 529, 540
  serial subgroup 293
  simple group 116, 156, 228, 312, 432, 434, 439-441, 449, 523
  singular at p 167-178, 422-424
  singular projectivity 166-178
  SK-group 126
  SN-group 319
  soluble group(s) 181, 229, 317, 332, 395-406, 506-511
  derived length of 332
  Fitting length of 180, 399
  formation of 397-401, 405-406
  generalized 315-321
  IM-group 132
  K-group 118-121
  rank of 396
  RK-group 130
  with dual 462-468
  soluble radical 230, 234
  soluble residual 230, 234
  standard element 136-137, 141
  strongly determined by subgroup lattice 343
  abelian group of torsion-free rank $\geq 2$ 106
  alternating group $A_n$, $n \neq 3^r$ or $3^r + 1$, $r$ odd 447
  direct product of isomorphic dihedral groups 426
  free group of rank $\geq 2$ 358
  free polynilpotent group 374
  hamiltonian 2-group 89
nonabelian locally free group 359
nonabelian torsion-free locally nilpotent group 373
simple group of Lie type \( \neq A_3 \) 449
symmetric group 444, 447, 451
2-free group 358
wreath product of torsion-free groups 417
strongly embedded subgroup 153
subgroup(s)
admissible (of a partition) 147
ascendant 293, 328
commutator 29, 272
composition 6, 498–511
cyclic 15, 18
Dedekind 289
\( D \)-embedded 289
diagonal 35, 408–411
Fitting 116, 178–181
Frattini 38, 115
G-isomorphic 487
Hall 158–166
Hughes 147
locally \( P \)-embedded 302
local system of 21
maximal sensitive 133, 234
modular 43, 200–220, 232
of finite index 282–288, 325, 476
\( p \)-collecting 540
\( P \)-embedded 297
permutually complemented 121
\( P(G) \)-connected 468
\( P(G) \)-normal 469
prefrattini 401
quasinormal 43
serial 293
strongly embedded 153
subnormal 6, 240–243, 498–511
Sylow 166, 185–187, 195–198
verbal 382
subgroup lattice(s) 3
chain 16
characterization of 357
complemented 115–126
determined by vii, 343
directly decomposable 36–39
distributive 12–13
\( IM \)- 130–135
Jordan-Dedekind chain condition 231–234
lower semimodular 47, 233, 394, 399
modular 54–88; 55, 71, 75, 79, 82
permutually complemented 121
relatively complemented 127–135
sectionally complemented 126
strongly determined by 343
upper semimodular 233
weakly join-complemented 133
weakly meet-complemented 135
weakly modular 87
sublattice 5
meet-7
subnormal subgroup 6, 240–243, 498–511
defect of 125, 499
projective image of 240–243
\( \mathbb{F} \)- 510
supersoluble
chain 319
group 230–234, 318
\( K \)-group 122
residual 234
Suzuki group 116, 146, 152, 156, 434
Sylow subgroup 166
abelian 185–187, 197–198
centre of 195–197
Sylow tower group 396, 405
symmetric group 115, 149, 177, 432, 438,
\( 441–445, 447, 451, 513, 527 
\( S_4 \) 149, 513, 527

T
Tarski group 82, 88
\( T \)-group 127
\( T^* \)-group 127
triple
Iwasawa 60–69
\( P \)-hypercentral 399
triply transitive permutation group 432
type of abelian group 104, 108
type of element in abelian group 108

U
uniquely complemented element 136, 138–141
unit (\( p \)-adic) 32–33
universal power automorphism 32
upper Hirsch-Plotkin series 403, 404
upper semimodular lattice 46–48, 233, 540

V
variety 382–385
verbal subgroup 382

W
weakly join-complemented lattice 133
<table>
<thead>
<tr>
<th>Subject</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>weakly meet-complemented lattice</td>
<td>135</td>
</tr>
<tr>
<td>weakly modular lattice</td>
<td>87</td>
</tr>
<tr>
<td>width of a poset</td>
<td>3, 39–40</td>
</tr>
<tr>
<td>wreath product</td>
<td>416–418</td>
</tr>
<tr>
<td>(X)</td>
<td></td>
</tr>
<tr>
<td>(\mathcal{X})-normal subgroup</td>
<td>510</td>
</tr>
<tr>
<td>(\mathcal{X})-subnormal subgroup</td>
<td>510</td>
</tr>
</tbody>
</table>