

GROUP THEORY

Define semigroup, monoid, group.

Definition. A function $f: G \rightarrow H$, where G, H are groups, is a *group homomorphism* if $f(g_1g_2) = f(g_1)f(g_2)$ for all $g_i \in G$. A group homomorphism $f: G \rightarrow H$ is

- 1) a *monomorphism* if it is injective;
- 2) an *epimorphism* if it is surjective;
- 3) an *isomorphism* if it is bijective;
- 4) an *automorphism* if it is bijective and $G = H$;
- 5) an *endomorphism* if $G = H$.

Write $\text{Aut}(G)$ for the set of all automorphisms of a group G . Note that it is a group under composition. This is the usual operation. But the set is also a subgroup of $\text{Maps}(G, G)$, the group of all functions from $G \rightarrow G$ with the operation of multiplication in G .

Let $f: G \rightarrow H$ be a group homomorphism. Define the *kernel* of f , $\ker f$, and the *image* of f , $\text{im } f$.

Proposition. A group homomorphism $f: G \rightarrow H$ is injective iff $\ker f = \langle e_G \rangle$.

Definition. Let G be a group, $S \subseteq G$. We say that S *generates* G if any element of G can be written as a product of elements of S and their inverses. We write $G = \langle S \rangle$.

Definition. A group G which can be generated by one element is called a *cyclic group*, written $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Theorem. Every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$ and every finite cyclic group of order m is isomorphic to the group $(\mathbb{Z}_m, +)$.

Define order of an element, cosets and index.

Lagrange's Theorem. If $H < G$, then $[G : H][H : 1] = [G : 1]$.

Corollary. If $H < G$ and $|G|$ is finite, then $|H|$ divides $|G|$.

Corollary. The order of any element divides the order of the group.

Corollary. *If $|G|$ is prime, then G is cyclic.*

The converse of Lagrange's Theorem is false. The alternating group A_4 , which has order 12, has no subgroup of order 6.

Characterize the kernels of homomorphisms.

Define *normal subgroup*, $K \triangleleft G$. Note that every kernel of a homomorphism is a normal subgroup of the domain. Define the *quotient group* G/K (where $K \triangleleft G$) and the canonical homomorphism $\pi: G \rightarrow G/K$ for which $K = \ker \pi$. Thus kernels of homomorphisms are precisely the normal subgroups.

Definitions. Let G be a group and $S \subseteq G$. The *normalizer* of S in G is the set

$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

The *centralizer* of S in G is the set

$$C_G(S) = \{g \in G \mid gsg^{-1} = s, \forall s \in S\}.$$

We write $Z(G)$ for the set $C_G(G)$ and call it the *center* of G .

Proposition. *Let $H < G$. Then $N_G(H)$ is the largest subgroup of G in which H is normal.*

Proposition. *Let $H < G$ and $K < N_G(H)$. Then KH is a group and $H \triangleleft KH$.*

Definition. A sequence of homomorphisms $G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \dots \xrightarrow{f_{n-1}} G_n$ is *exact* if $\ker f_{i+1} = \text{im } f_i$ for $i = 1, 2, \dots, n-1$. A *short exact sequence* is a five term exact sequence with identity groups on the ends.

Noether Isomorphism Theorems

Theorem 1. *If $f: G \rightarrow H$ is a group homomorphism, then there exists a unique homomorphism $f_*: G/\ker f \rightarrow H$ such that $f_*\pi = f$, where $\pi: G \rightarrow G/\ker f$ is the canonical homomorphism to the quotient group. Furthermore, f_* is surjective and $G/\ker f \cong \text{im } f$.*

Theorem 2. *Let $H, K < G$ and $H \subseteq N_G(K)$. Then $H/(H \cap K) \cong HK/K$.*

Theorem 3. *Let $H \triangleleft G$, $K \triangleleft G$ and $K < H$. Then $H/K \triangleleft G/K$ and $(G/K)/(H/K) \cong G/H$.*

Corollary. *If $f: G \rightarrow H$ is a group homomorphism and $N \triangleleft G$ with $N \subseteq \ker f$, then f factors through G/N .*

Proof. Compose f_* from the first isomorphism theorem with the canonical homomorphisms to quotient groups to obtain $G \rightarrow G/N \rightarrow (G/N)/(\ker f/N) \cong G/\ker f \rightarrow H$, where the isomorphism comes from the third isomorphism theorem. \square

Theorem. *Let $f: G \rightarrow H$ be a group epimorphism. Then $K \rightarrow f(K)$ is a bijective correspondence between subgroups of G containing $\ker f$ and subgroups of H . Under this correspondence, normal subgroups correspond to normal subgroups.*

Definition. By an *action* of a group G on a set S we mean a mapping $G \times S \rightarrow S$ (denoted by $(g, s) \mapsto gs$) such that for all $s \in S$, $g_1, g_2 \in G$, $es = s$ and $(g_1g_2)s = g_1(g_2s)$. We say that G *acts on* (or *operates on*) S .

Examples. 1. Let $N = \{1, 2, \dots, n\}$ and let S_n be the group of all bijections of N onto itself, with composition. S_n is called the *symmetric group* on n elements. The elements of S_n are called *permutations*. S_n acts on N . More generally, we will write $S(X)$ for the group of all permutations of a set X .

2. The *trivial action* of G on S is defined by $gs = s$ for all $g \in G$, $s \in S$.

3. A group G can act on itself as follows: For $g \in G$, define the *translation* $T_g: G \rightarrow G$ by $T_g(x) = gx$. Steinberger calls this the *standard action* of G on G . Similarly, if $H < G$, then G acts by translation on the left cosets of H .

4. Let $H < G$. Then H acts on G by *conjugation*: for $h \in H$, $(h, g) \mapsto hgh^{-1}$. The element hgh^{-1} is called a *conjugate* of g . If $K < G$, then $hKh^{-1} < G$, so H also acts on the set of subgroups of G by conjugation. The group hKh^{-1} is called a *conjugate* of K .

Let G act on S and let $s \in S$. The subset $Gs = \{gs \mid g \in G\}$ is called the *orbit* of s under G .

Proposition. *The orbits partition S into equivalence classes.*

If there is only one orbit, we say G acts *transitively* on S .

Set $G_s = \{g \in G \mid gs = s\}$, called the *subgroup fixing s* or the *isotropy group of s* or the *stabilizer of s* .

Example. If G acts on itself by conjugation, the subgroup fixing an element is the centralizer of the element, and the orbit of an element $x \in G$ is the conjugacy class of x . If G

acts on the set of its subgroups by conjugation, the subgroup of G fixing a subgroup H is the normalizer $N_G(H)$.

Proposition. *The cardinality of Gs is $[G : G_s]$.*

Since the orbits partition S , we can choose one s_i from each orbit to write $S = \bigcup_{i \in I} Gs_i$. If $|S| < \infty$, then

$$|S| = \sum_{i \in I} [G : G_{s_i}],$$

called the *orbit decomposition formula* (G -set counting formula in Steinberger).

Now assume that G acts on itself by conjugation. Then this becomes the *class formula*: $|G| = \sum [G : C_G(x_i)]$, where $\{x_i\}$ is a set of representatives for distinct conjugacy classes. Note that $g \in Z(G)$ iff the conjugacy class of g has only one element. If we separate these out,

$$\text{(Class Formula)} \quad |G| = |Z(G)| + \sum_{i=1}^m [G : C_G(x_i)],$$

where the x_i 's represent the conjugacy classes with more than one element. This version of the class formula has remarkable power as we shall soon see.

Definition. Let p be a prime number. We say G is a p -group if $|G|$ is a power of p . A subgroup H is a p -subgroup of G if H is a p -group. A p -subgroup H is a *Sylow p -subgroup* (or p -Sylow subgroup) if $|H|$ is the highest power of p dividing $|G|$.

Lemma. *Assume that G is a group of order p^n , p prime, and G acts on a finite set S . Let $S_0 = \{s \in S \mid gs = s, \forall g \in G\}$, the set of all one element orbits. Then $|S| \equiv |S_0| \pmod{p}$.*

Corollary. *If G is a nontrivial p -group, then $|Z(G)| > 1$.*

Cauchy's Theorem. *If a prime p divides $|G|$, then G has an element of order p .*

Lemma. *If H is a p -subgroup of G , then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.*

Corollary. *If H is a p -subgroup of G such that $p \mid [G : H]$, then $N_G(H) \neq H$.*

First Sylow Theorem. Assume $|G| = p^n m$ with $n \geq 1$, p prime, $\gcd(p, m) = 1$. Then for each i , $1 \leq i \leq n$, the group G has a subgroup of order p^i and every subgroup of order p^i , $i < n$, is normal in some subgroup of order p^{i+1} .

Corollary. Let G be a finite group with $p \mid |G|$, p prime. Then G contains a Sylow p -subgroup. Every p -subgroup of G is contained in a Sylow p -subgroup.

Second Sylow Theorem. All Sylow p -subgroups of a finite group are conjugate.

Third Sylow Theorem. Let G be a finite group with $p \mid |G|$, p prime. The number of Sylow p -subgroups of G is of the form $1 + kp$ and divides $|G|$.

Lemma. Assume that $H_i \triangleleft G$, $i = 1, 2, \dots, r$, such that $H_i \cap H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_r = \{e\}$ for each i and $G = H_1 H_2 \cdots H_r$. Then $G \cong H_1 \times H_2 \times \cdots \times H_r$.

Proposition. If every Sylow subgroup of a finite group G is normal, then G is isomorphic to the direct product of its Sylow subgroups.

Theorem. Let $p < q$ be prime numbers. If $q \not\equiv 1 \pmod{p}$, there is exactly one group of order pq , namely \mathbb{Z}_{pq} . If $q \equiv 1 \pmod{p}$, there is also a unique nonabelian group of order pq generated by two elements x, y with relations $x^q = e$, $y^p = e$, $xyx^{-1} = x^r$, where $r^p \equiv 1 \pmod{q}$.

Definition. Let G be a group. The ascending central series for G is $C_0 = \{e\}$, $C_1 = Z(G)$; $C_{n+1} =$ the unique subgroup of G containing C_n such that $C_{n+1}/C_n = Z(G/C_n)$. If there exists an n such that $C_n = G$, then we say that G is nilpotent.

As a nonexample, we have seen that for $n \geq 3$, $Z(S_n) = \{e\}$, so S_n is not nilpotent. For examples, if G is abelian, $Z(G) = G$ and G is nilpotent.

Theorem. All p -groups are nilpotent.

Lemma. Let G be nilpotent and H a proper subgroup of G . Then H is a proper subgroup of its normalizer.

Lemma. Let G be nilpotent and M a maximal (proper) subgroup of G . Then $M \triangleleft G$ and $[G : M]$ is prime.

Theorem. *Let G be a finite nilpotent group. Then every Sylow subgroup of G is normal, hence G is isomorphic to the product of its Sylow subgroups.*

Remark. $C_n(G \times H) = C_n(G) \times C_n(H)$, so if G and H are nilpotent, so is $G \times H$. Therefore, G is nilpotent iff it is a direct product of p -groups.

Definition. Let G be a group. The subgroup of G generated by the set $\{aba^{-1}b^{-1} \mid a, b \in G\} = [G, G]$ is the *commutator* subgroup of G (also called the *derived* subgroup and denoted G').

Theorem. *For any group G , we have $[G, G] \triangleleft G$ and $G/[G, G]$ is abelian. If G/N is abelian ($N \triangleleft G$), then $N \supseteq [G, G]$.*

Corollary. *If $f: G \rightarrow H$ is a group homomorphism with H abelian, then f factors through $G/[G, G]$.*

Definition. The *descending central series* of G is $G_0 = G$, $G_{n+1} = [G, G_n]$, the subgroup of G generated by $\{aba^{-1}b^{-1} \mid a \in G, b \in G_n\}$.

Following the proof of the previous theorem and using induction on n , one can show that any automorphism of G takes G_n to itself, so each $G_n \triangleleft G$. Thus $G_{n+1} \subseteq G_n$ for all n .

Theorem. *The descending central series terminates in $\{e\}$ iff the ascending central series reaches G , iff G is nilpotent.*

Definition. The *derived series* of G is defined by $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. If there exists an n such that $G^{(n)} = \{e\}$, then G is *solvable*.

Note that all nilpotent groups are solvable since the derived series is contained in the descending central series.

Feit–Thompson Theorem. *All groups of odd order are solvable.*

We shall see that S_n is not solvable if $n \geq 5$.

Theorem. *Every subgroup and factor group of a solvable group is solvable.*

We will prove the converse of this theorem by first getting a good understanding of certain chains of subgroups of a solvable group. This will be crucial for understanding the origins of these groups in Galois theory (algebraic extensions of fields).

Definition. A *simple* group is one with no normal subgroups. For any group G , a *composition series* for G is a sequence of subgroups $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = \{e\}$ such that each G_{i+1} is a maximal normal subgroup of G_i . (These always exist if G is finite.) Given such a series, each G_i/G_{i+1} is simple and is called a *composition factor* of G , or a Jordan–Hölder component of G .

Jordan–Hölder Theorem. *Let G be any group. Any two composition series for G have the same length and the composition factors are the same up to permutation (and isomorphism).*

Corollary. *A finite group G is solvable iff all of its Jordan–Hölder components are cyclic of prime order.*

Corollary. *If G/N and N are solvable, then so is G .*

Permutation Groups

In your text reading [S, §3.5], you saw that there is a homomorphism $\epsilon: S_n \rightarrow \{\pm 1\}$, where $\epsilon(\sigma)$ is called the *sign* of σ . We denote the kernel of ϵ by A_n and call it the *alternating group of degree n* . Thus A_n is the subgroup of all *even permutations* (products of an even number of transpositions). Since it is the kernel of a homomorphism, $A_n \triangleleft S_n$.

Example. A composition series for S_4 is given by $G_0 = S_4 \supsetneq G_1 = A_4 \supsetneq G_2 = \{(1), (12)(34), (13)(24), (14)(23)\} \supsetneq G_3 = \{(1), (12)(34)\} \supsetneq G_4 = \{(1)\}$. The Jordan–Hölder components are $S_4/A_4 \cong \mathbb{Z}_2$, $A_4/G_2 \cong \mathbb{Z}_3$, $G_2/G_3 \cong \mathbb{Z}_2$, $G_3/G_4 \cong \mathbb{Z}_2$. In particular, S_4 is solvable, hence so are its subgroups S_2 and S_3 .

Proposition. *Two permutations in S_n are conjugate iff they have the same cycle structure (same number of cycles of the same lengths).*

Theorem. *A_n is simple if $n \neq 4$.*

REFERENCES

- [S] M. Steinberger, *Algebra*, PWS Publishing Co., Boston, 1994.