Chapter 7, Groups

We end this semester with a quick introduction to a new algebraic object: groups. We will continue with groups in Math 413. We shall see that many of the ideas from rings will have counterparts for groups, in particular homomorphisms, special types of subgroups that give kernels of homomorphisms, congruence and quotient groups. A group is somewhat like a ring, except that there is only one operation instead of two. Actually, this describes a semigroup. To make it more interesting, we require that inverses always exist.

Definition, p. 163. A group is a nonempty set $G$ with a binary operation $*$ that satisfies

1. Closure: if $a, b \in G$, then $a * b \in G$.
2. Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
3. There exists an element $e \in G$ satisfying $a * e = e * a = a$ for all $a \in G$. $e$ is called the identity element.
4. For each $a \in G$, there exists an element $b \in G$ satisfying $a * b = b * a = e$. $b$ is called the inverse of $a$.

If the operation is commutative ($a * b = b * a$ for all $a, b \in G$), we say that $G$ is abelian.

Much of our work will be with finite groups; that is, one with only finitely many elements. The number of elements in $G$ is called the order of $G$, denoted $|G|$. If $G$ is infinite, we say it has infinite order. We typically use whatever notation is convenient for the operation $*$. We often write it as $+$ if the group is abelian, because it then behaves like addition in a ring. In fact, any ring is a group if we consider only its $+$ operation. If the group is nonabelian, a more common notation is the one we use for multiplication: $ab$ for $a * b$. In the former case, we write inverses as $-a$ and $e$ as $0$. In the latter we write inverses as $a^{-1}$, but $e$ is still the usual name for the identity.

Examples: we have already seen essentially all the abelian finite groups. Theorem 8.7 says they are just the additive subgroups of our rings $\mathbb{Z}_n$. In fact, a little more can be said because these rings are often products (recall $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$), but there is not too much more to learn about these. That means we have to start dealing much more with noncommutativity! Without any doubt, the most important examples are the permutation groups. For any finite set $S = \{1, 2, 3, \ldots, n\}$, a permutation of $S$ is just a bijective function $f: S \rightarrow S$. Since compositions of bijections are again bijective, the identity is a bijection, and bijections have inverses, the set of all permutations of $S$ form a group. We will call the group $S_n$, the symmetric group on $n$ symbols. (Of course, we didn’t have to use the first $n$ positive integers.) The order of $S_n$ is $n!$, as you saw in linear algebra. We shall study these groups in considerable detail next semester. For $n = 3$, the details are all written out in the book, pp 161–163. We shall later use a more compact notation which will help us understand the patterns involved in permutations (cycles).
The oldest examples of groups are those which come from the rigid motions of a geometric object. For example, the group $S_3$ above can be thought of as the group of motions of an equilateral triangle. Label the vertices $\{1, 2, 3\}$: a rigid motion of the triangle is a movement of the triangle onto itself such as a $120^\circ$ rotation. This moves all the vertices. Another type of movement is to hold one vertex fixed and flip the triangle over, switching the other two vertices. All six of the elements of $S_3$ give legitimate movements of the triangle. This is no longer true if we start with a square. Any rigid motion must keep adjacent vertices adjacent—they can never move to where they become diagonal. Therefore, we don’t get all the permutations of the four vertices when we look at the group of rigid motions. Pages 165–167 show that there are just 8 symmetries of the square; that is, only 8 of the 24 permutations correspond to what you can actually do to a square while keeping it rigid, rotating or flipping it. The group of motions is called the **dihedral group of degree 4**, denoted $D_4$ and it has order 8 (confusing, eh?). This generalizes to the group $D_n$, the **dihedral group of degree $n$**, which has order $2n$ and is the group of symmetries of a regular $n$-gon. As we have seen, $S_3$ is the same as $D_3$. The elements of $D_n$ are combinations of a rotation through $360/n$ degrees, which becomes the identity if you do it $n$ times, and a reflection (flip it over), which becomes the identity when done twice. The pictures for the triangle are in the book at the bottom of page 167.

While a ring is a group under addition, it never is under multiplication (except the zero ring) since 0 has no inverse. On the other hand, the set of nonzero elements of a field is an abelian group under multiplication. Another example is the set of positive real numbers, again using multiplication. Finite subgroups of this sort also exist, such as the set $\{1, -1, i, -i\}$ in $\mathbb{C}$. This can be expanded to the subset $\{\pm1, \pm i, \pm j, \pm k\}$ of the quaternions. This is a nonabelian group known as the **quaternion group**; see Exercise 14, page 172 for details. Similarly, it works for rings as long as we use only the set of units in the ring. The book denotes the group of units in $\mathbb{Z}_n$ by $U_n$. For convenience, if you need a notation for the group of units in an arbitrary ring $R$, use $U(R)$ or $R^\ast$. The order of the group $U_n$ is of interest. We know from earlier work that it is the number of integers in $\{1, 2, \ldots, n - 1\}$ which are relatively prime to $n$. This number is denoted by $\phi(n)$ and called the Euler $\phi$-function. It is commonly studied in number theory and can be computed exactly, with the value depending on the factorization of $n$ into primes. For example, $\phi(p) = p - 1$ for a prime $p$.

Other interesting infinite examples come from matrices. The **general linear group** $GL(n, \mathbb{R})$ is the set of all invertible $n \times n$ matrices under the operation of matrix multiplication. The **special linear group** $SL(n, \mathbb{R})$ is the set of all invertible $n \times n$ matrices of determinant 1. Since $\det AB = \det A \det B$, this set is closed under multiplication. Of course, the field $\mathbb{R}$ could be replaced by any other field. It can also be replaced by commutative rings with identity, where one defines the determinant by the same sum over the permutation group as was done for fields in linear algebra.

As with rings, we have a Cartesian product construction of new groups from old ones.
Theorem 7.4. Let $G$ and $H$ be groups. Define an operation on $G \times H$ by

$$(g, h) \circ (g', h') = (gg', hh').$$

This makes $G \times H$ into a group. If $G$ and $H$ are both finite, then $|G \times H| = |G||H|.$

Proof. Check the four axioms: closure is clear since we defined something which makes sense. Associativity comes from associativity in $G$ and $H$. The identity element of $G \times H$ is $(e_G, e_H).$ The inverse of $(g, h)$ is $(g^{-1}, h^{-1}).$ The order statement for finite groups is true because the Cartesian product has that number of elements. \[
\square
\]

Section 7.2 of the book is a collection of easy facts, none of which are worth calling a theorem. Theorem 7.5 points out some easy facts that have the same proofs as in other contexts where they hold. The cancellation results can be used to provide other ways to define a group (see exercises 37–39 on page 181).

Facts about groups:

1. The identity element is unique. [If $e$ and $e'$ are identities, then $e = ee' = e'.$]
2. Cancellation laws hold on both sides. [The usual result whenever you have inverses.]
3. Inverses are unique. [If $x$ and $y$ are both inverses for $g$, then $x = x(gy) = (xy)y = y.$ Notice that this uses only the fact that $x$ is a left inverse and $y$ is a right inverse.]
4. $(ab)^{-1} = b^{-1}a^{-1}$ and $(a^{-1})^{-1} = a.$ [Same proof as for rings when inverses exist.]
5. $a^m a^n = a^{m+n},$ $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}.$ We now define $a^0 = e,$ the identity element of the group. [Same as for rings.]

Sometimes it happens that $a^k = e$ for some $k > 0.$ If so, we say $a$ has finite order. The order of $a$ is denoted $|a|$ and is the smallest $k > 0$ such that $a^k = e.$ $e$ has order 1. $a$ has infinite order if $a^k$ never equals $e$ for $k > 0.$ For example, in $D_4,$ a rotation of the square of $90^\circ$ has order 4. In $\mathbb{Z}$ under addition, all elements other than the identity (0 since it is additive) have infinite order since $k \cdot n \neq 0$ for any $k > 0.$ (Note that when we write the operation as $+,$ we write $ka$ instead of $a^k$ and 0 instead of $e.$) Some less obvious facts about order of elements:

Theorem 7.8.

1. If $a$ has infinite order, then the elements $a^k$ are all distinct.
2. If $a^i = a^j$ with $i \neq j,$ then $a$ has finite order.
3. If $a$ has finite order $n,$ then $a^k = e$ iff $n|k;$ and $a^i = a^j$ iff $i \equiv j \pmod{n}.$
4. If $a$ has order $n = st$ with $s,t > 0,$ then $a^s$ has order $t.$

Proof. (1) $\iff$ (2) since one is the contrapositive of the other. To prove (2), just note that $a^i = a^j$ implies that $a^{i-j} = e,$ so $a$ has finite order.
(3) If $k = nt$, then $a^k = (a^n)^t = e^t = e$. Conversely, if $a^k = e$, we use the division algorithm to write $k = nq + r$ with $0 \leq r < n$. Then $a^r = a^{k-nq} = a^k a^{-nq} = e$ which is only possible if $r = 0$ since $r < n$ and $n$ is the order. Therefore $n|k$. For the second statement, apply the first one to $k = i - j$.

(4) Certainly $(a^*)^t = a^n = e$. If any smaller positive value than $t$ worked, say $r < t$, then $a^{sr} = (a^*)^r = e$, but $sr < n$, a contradiction. □


3. $(abcd)^{-1} = d^{-1}c^{-1}b^{-1}a^{-1}$.

4. Assume $ab = e$. Since $G$ is a group, there is a right inverse for $b$: $bc = e$. Then $a = a(bc) = (ab)c = e$, so $ba = e$.

6. $\mathbb{Z}_2 \times \mathbb{Z}_2$. Or its isomorphic multiplicative version, $\{\pm 1\} \times \{\pm 1\}$.

7. $5^2 \equiv 1 \pmod{8}$; $1 \mapsto 2 \mapsto 3 \mapsto 7 \mapsto 6 \mapsto 4 \mapsto 5 \mapsto 1$, so it has order 7; order 6; order 3.

8. $GL(2, \mathbb{R})$ by #7(d) and \( \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \). Also $\mathbb{Z}_2 \times \mathbb{Z}$.

12. False: $\mathbb{Z}_2 \times \mathbb{Z}_2$ has all elements of order 1 or 2 by #6.

Subgroups.

Following the usual procedure with algebraic objects, we need to understand subsets with the same properties.

Definition, p. 181. A subset $H$ of a group $G$ is a subgroup of $G$ if $H$ is itself a group under the operation of $G$.

Examples. 1. For any group $G$, the set $G$ itself is a subgroup and so is the trivial subgroup $\{e\}$. All other subgroups are called proper to distinguish them from these two which always exist. There is a study of groups with the property that they have no proper subgroups. These are called simple groups and are mentioned on page 225. These are definitely not simple in the everyday sense, but rather are very hard to understand. A few years ago the task of finding all the finite simple groups was finally completed by mathematicians, with the estimate that it required about 5000 pages in journals over many decades. Some of the work required hours of computer time to check the existence of certain large simple groups which had been predicted.
2. Let $R$ be a ring and $I$ an ideal in $R$. Then, considering only the addition operation, $I$ is a subgroup of $R$.

3. Exercises 3 and 5 on page 187 are easy analogues of the corresponding results for ideals in a ring.

As with subrings and ideals, some of the axioms are automatic for $H$ since they use the operation from $G$.

**Theorem 7.10.** A nonempty subset $H$ of a group $G$ is a subgroup iff for any $a, b \in H$, the element $ab^{-1}$ is also in $H$. [The book states this as two separate things to check.]

**Proof.** Associativity is automatic. Since there is some element $a \in H$, our hypothesis implies that $e = aa^{-1} \in H$. And so, for any $h \in H$, we have $h^{-1} = eh^{-1} \in H$. Finally, for closure, if $a, b \in H$, then $b^{-1} \in H$, hence $ab = a(b^{-1})^{-1} \in H$. □

If the subset $H$ is finite, we automatically get inverses using Theorem 7.8, so you only need to check closure under the operation: since the elements $a^k$ cannot all be distinct, we get $a^n = e$ for some $n$ by Theorem 7.8(2). But then $aa^{n-1} = a^n = e$, so $a^{-1} = a^{n-1} \in H$ by closure.

**Example from page 183:** $H = \{ f \in S_5 \mid f(1) = 1 \}$ consists of all permutations fixing the element 1. Since $H$ is finite, we only need to check that it is closed under the operation: for $g, h \in H$, $g(h(1)) = g(1) = 1$, so $g \circ h \in H$. Therefore $H$ is a subgroup of $S_5$. In fact, we expect that as soon as we define isomorphisms for groups, $H$ should be isomorphic to $S_4$ which we think of as permutations of the set $\{2, 3, 4, 5\}$.

Even though a group $G$ may be nonabelian, it may have some elements that commute with everything in the group (as the identity does). We call this set the center of $G$, writing $Z(G) = \{ a \in G \mid ga = ag \text{ for every } g \in G \}$. Then $Z(G) = G$ iff $G$ is abelian. The letter $Z$ comes from the German word *Zentrum*, meaning center.

**Theorem 7.12.** The center $Z(G)$ of a group $G$ is a subgroup of $G$.

**Proof.** Since $e \in Z(G)$, it is nonempty. If $a, b \in Z(G)$, then for any $g \in G$, $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$, so $ab \in Z(G)$. Also, since $ag = ga$, we can multiply by $a^{-1}$ on both the right and left to obtain $ga^{-1} = a^{-1}g$, so $a^{-1} \in Z(G)$. Therefore $Z(G)$ is a subgroup. □

**Example.** The center of the group $S_n$ for $n \geq 3$ is the identity subgroup. (If $n = 2$, $S_2 \cong Z_2$ is abelian, so the center is the whole group.) Let $e \neq \sigma \in S_n$. We may assume
σ(1) = 2. Let τ be the permutation which switches 2 and 3, but fixes everything else. Then τ(σ(1)) = τ(2) = 3, but σ(τ(1)) = σ(1) = 2, so στ ≠ τσ, and therefore σ ∉ Z(Sₙ).

Let G be a group and g ∈ G. The set \{..., g⁻², g⁻¹, e, g, g², ...\} = \{g^n | n ∈ ℤ\} of all powers of g is denoted by ⟨g⟩ and is called the cyclic subgroup generated by g. If it is the whole group G, then G is called a cyclic group. (This is, of course, a subgroup as it is clearly closed under taking inverses and multiplication.) As a corollary of Theorem 7.8 on orders, we get

**Theorem 7.14.** Let G be a group and g ∈ G.

1. If g has infinite order, then ⟨g⟩ is an infinite subgroup of G and all powers of g are distinct.
2. If g has order n < ∞, then ⟨g⟩ is a cyclic subgroup of order n and ⟨g⟩ = \{e, g, g², ..., gⁿ⁻¹\}.

**Proof.** Immediate from parts (1) and (3) of Theorem 7.8. □

If we write the operation additively, we just have the additive groups ℤ for the infinite cyclic group and ℤₙ for the cyclic group of order n. Once we have a definition of isomorphism, it will be clear from this theorem that every cyclic group is isomorphic to one of these groups with the isomorphism given by corresponding the element k ∈ ℤₙ to the element gᵏ ∈ ⟨g⟩.

The next theorem is usually found in a chapter on field theory. It will be useful to us later in the course and provides examples of cyclic groups at the present.

**Theorem 7.15.** If G is a finite subgroup of the multiplicative group of nonzero elements of a field, then G is cyclic.

An example is the set of all n-th roots of 1 in ℂ; if n = 4, this is \{1, −1, i, −i\}.

**Proof.** Note first that G must be abelian. Let c ∈ G be an element of maximum order in G, say of order n. Let a ∈ G. We claim aⁿ = 1. If not, then there exists some prime p in the factorization of |a| that appears to a higher power than it does in n, say n = pʳn₁, \[|a| = pʳm\] and r > s, where n₁ and m are relatively prime to p. But then aᵐ has order pʳ and cᵐ has order n₁ (by Theorem 7.8), hence aᵐcᵐ has order pʳn₁ > pˢn₁ = n (by Exercise 31, p. 180—assigned as homework), a contradiction. But now we have seen that every element of G is a root of the equation xⁿ − 1, which has at most n roots in the field. Since c generates a subgroup of order n, it must actually generate all of G and therefore G is cyclic. □
**Corollary 7.9.** Let $G$ be an abelian group with every element of finite order. Assume that $c$ is an element of maximum order. Then for all $g \in G$, the order of $g$ divides the order of $c$.

*Proof.* The proof is the same as the first part of the proof of Theorem 7.15. □

**Theorem 7.16.** Every subgroup of a cyclic group is cyclic.

*Proof.* Suppose $G = \langle g \rangle$ and $H$ is a subgroup of $G$. Since the trivial group is cyclic, we may assume $H$ is nontrivial, and thus contains a positive power of $g$. Let $k$ be the smallest positive power. We claim $H = \langle g^k \rangle$. Let $h \in H$, so $h = g^m$ for some $m$. We do the usual argument to show that $k|m$: by the division algorithm we can write $m = kq + r$ where $0 \leq r < k$. Then $g^r = g^{m-kq} = h(g^k)^{-q} \in H$, which implies $r = 0$. □

Examples: $2\mathbb{Z}$ is a cyclic subgroup of $\mathbb{Z}$. $2\mathbb{Z}_4 = \{0, 2\}$ is a cyclic subgroup of $\mathbb{Z}_4$; it is isomorphic to $\mathbb{Z}_2$. Note that additively, we write $kg$ rather than $g^k$.

**Corollary.** Every ideal in $\mathbb{Z}_n$ is principle.

*Proof.* $\mathbb{Z}_n$ is a cyclic group under addition and any ideal $I$ is an additive subgroup. By the theorem, $I$ consists of all sums formed from a given element, hence that element also generates $I$ as an ideal. □

As with ideals, we can talk about any set of elements of a group generating some subgroup.

**Theorem 7.17.** Let $S$ be a nonempty subset of a group $G$. Let $\langle S \rangle$ be the set of all products of elements of $S$ and their inverses. (The empty product gives $e \in \langle S \rangle$ and the singleton products give $S \subset \langle S \rangle$; but this convention is not actually needed.) Then

1. $\langle S \rangle$ is a subgroup of $G$ containing $S$.
2. Any subgroup of $G$ containing $S$ contains $\langle S \rangle$.

We call $\langle S \rangle$ the subgroup of $G$ generated by $S$ and call the elements of $S$ the generators of $G$.

*Proof.* (1) Given $a_1 \cdots a_n$ and $b_1 \cdots b_m$ in $\langle S \rangle$, where $a_i, b_j$ are in $S$ or inverses of elements in $S$, then $(a_1 \cdots a_n)(b_1 \cdots b_m)^{-1} = a_1 \cdots a_n b_m^{-1} \cdots b_1^{-1}$ is again in $\langle S \rangle$.

(2) Any subgroup containing $S$ must contain inverses of elements in $S$ and all products by closure, hence contains $\langle S \rangle$. □
Example: in the group $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$, the elements $(1, 0, 0), (0, 1, 0)$ generate a subgroup of order 6, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. The element $(1, 1, 1)$ has order 30 (i.e., $(n, n, n) = (0, 0, 0)$ only if $n$ is a multiple of 30), so $G = \langle (1, 1, 1) \rangle \cong \mathbb{Z}_{30}$.

Exercise 9, page 188: (a) choose any $a \notin Z(G)$. Then $b = a^{-1}$ gives a counterexample. (b) $ab \in Z(G)$ implies that it commutes with $a^{-1}$, in particular. Thus, $b = a^{-1}ab = aba^{-1}$; multiplying by $a$ on the right gives $ba = ab$. This is typical of proving things about groups: you have to find the right element to apply things to. Experimentation becomes more important than grand ideas.

Exercise 45, page 190: $Z_m \times Z_n$ is cyclic iff $\gcd(m, n) = 1$. If $\gcd(m, n) = 1$, then $(1, 1)$ has order $mn$, hence $Z_m \times Z_n = \langle (1, 1) \rangle$ is cyclic. Assume $\gcd(m, n) = d > 1$ and let $(a, b) \in Z_m \times Z_n$. Say $m = dr, n = ds$, so $drs = mn/d < mn$. Now $drs(a, b) = (drsa, drsb) = (smn, rnb) = (0, 0)$, so the order of $(a, b)$ divides $drs$ (Theorem 7.8), and in particular, is less than $mn$. Therefore no single element $(a, b)$ can generate $Z_m \times Z_n$.

The more advanced concepts of centralizer and normalizer are introduced in the exercises on page 189. More fundamental ideas that we shall make use of later are in exercises 30–32.

Exercise 30, page 189: Let $H$ and $K$ be subgroups of a group $G$. We generalize the problem by assuming only that $HK = KH$; that is, the sets $\{hk \mid h \in H, k \in K\}$ and $\{kh \mid h \in H, k \in K\}$ are equal (but it may not be true that any particular $hk = kh$). Then we claim that $HK$ is a subgroup of $G$. Assume that $h_1k_1, h_2k_2 \in HK$. We must show that $(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HK$. Write $k = k_1k_2^{-1} \in K$. By hypothesis, $kh_2^{-1} \in HK$, so there exist $h_3 \in H, k_3 \in K$ with $kh_2^{-1} = h_3k_3$. But then $(h_1k_1)(h_2k_2)^{-1} = (h_1h_3)k_3 \in HK$ as desired, so $HK$ is a subgroup. We shall see that the condition $HK = KH$ is much more general than $G$ being abelian, and is, in fact, closely related to understanding kernels of group homomorphisms.

Homomorphisms and Isomorphisms.

Definition. Let $G$ and $H$ be groups. A homomorphism from $G$ to $H$ is a function $f : G \to H$ satisfying $f(ab) = f(a)f(b)$ for all $a, b \in G$. If a homomorphism is bijective, it is called an isomorphism and the groups are said to be isomorphic, written $G \cong H$. An isomorphism from $G$ to itself is called an automorphism.

As for rings, isomorphism is an equivalence relation.

Examples: 1. Let $G$ be a group and $g \in G$. Define a function $\phi : G \to G$ by $\phi(h) = ghg^{-1}$. $\phi$ is an automorphism of $G$ (check) of a special type called an inner automorphism. If $g \notin Z(G)$, then $\phi$ is not the identity.
2. \( \log : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +) \) is an isomorphism.

3. Every ring homomorphism \( f : R \to S \) induces an group homomorphism of their additive groups. Just ignore the multiplication.

4. Let \( G = \langle g \rangle \) be a cyclic group. Define \( f : \mathbb{Z} \to G \) by \( f(k) = g^k \). Then \( f(j + k) = g^{j+k} = g^j g^k = f(j)f(k), \) so \( f \) is a homomorphism. By our characterization of cyclic groups, \( f \) is surjective. If \( g \) has infinite order, \( f \) is injective by Theorem 7.8, hence is an isomorphism. Otherwise, let \( n = |g| \). Then for any \( k \), write \( k = nq + r, \) \( 0 \leq r < n \), by the division algorithm. We have \( f(k) = (g^n)^rq^r = g^r \). Therefore \( f \) induces a one-to-one correspondence of \( \mathbb{Z} \) with \( G \), namely \( f([k]) = g^k \) is an isomorphism.

The image of a homomorphism \( f : G \to H \), \( \text{Im } f \), is a subset of \( H \) with the property that \( f \) maps onto \( \text{Im } f \). Analogous to a theorem we had for rings, we obtain

**Theorem 7.19.** Let \( f : G \to H \) be a homomorphism of groups. Then

1. \( f(e_G) = e_H \).
2. \( f(a^{-1}) = f(a)^{-1} \) for every \( a \in G \).
3. \( \text{Im } f \) is a subgroup of \( H \).
4. If \( f \) is injective, then \( G \cong \text{Im } f \).

**Proof.**

1. \( f(e_G)f(e_G) = f(e_G) = e_Hf(e_G) \implies f(e_G) = e_H \).

2. \( f(a^{-1}) = f(a)^{-1}e_H = f(a)^{-1}f(e_G) = f(a)^{-1}f(aa^{-1}) = f(a)^{-1}f(a)f(a^{-1}) = f(a^{-1}) \).

3. \( e_H \in \text{Im } f \) by (1). For \( f(a), f(b) \in \text{Im } f \), \( f(a)f(b)^{-1} = f(ab^{-1}) \in \text{Im } f \) by (2).

4. \( f \) is a bijection of \( G \) and \( \text{Im } f \), hence is an isomorphism. \( \square \)

The real complexity of the symmetric groups \( S_n \) can be seen by the next result that every finite group is isomorphic to a subgroup of some \( S_n \). In fact, this can be generalized to infinite groups as well.

**Theorem 7.20 (Cayley’s Theorem).** Every group \( G \) is isomorphic to a group of permutations.

**Proof.** Let \( A(G) \) be the group of all permutations (bijective set functions) of the set \( G \) (ignoring its group structure for the moment). Define a function \( f : G \to A(G) \) by \( f(g) = \phi_g \), where \( \phi_g \in A(G) \) is the function \( \phi_g(x) = gx \). \( \phi_g \) is a bijection of \( G \) onto itself because it has an inverse, namely \( \phi_g^{-1} \). We claim \( f \) is a homomorphism: \( f(gh) = \phi_{gh} \), where \( \phi_{gh}(x) = (gh)x = g(hx) = g\phi_h(x) = \phi_g(\phi_h(x)) = (\phi_g\phi_h)(x) \). Therefore, \( f(gh) = \phi_{gh} = \)
\[ \phi_g \phi_h = f(g)f(h) \]. Next check that \( f \) is injective: if \( f(g) = f(h) \), then \( \phi_g = \phi_h \), so they must agree on \( e \): \( g = ge = \phi_g(e) = \phi_h(e) = he = h \). Now \( f \) is an isomorphism of \( G \) onto the subgroup \( \text{Im} f \subset A(G) \), so is a group of permutations (but not generally all permutations of any set). \( \square \)

When \( G \) has order \( n \), the group \( A(G) \) is \( S_n \), so we obtain

**Corollary 7.21.** Every finite group order \( n \) is isomorphic to a subgroup of \( S_n \).

In practice, it can be very useful to have a specific representation of a group as a set of permutations because it is possible to do computations in a straightforward way. But the abstract proof above is not helpful: for example the group \( Z_{10} \) is given as a subgroup of \( S_{10} \) which has \( 10! = 3,628,800 \) elements—a horrible thing to do to such a nice group!

**Exercises, pages 196–199.**

3. \[ \text{GL}(2, \mathbb{Z}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\} \]

because these are the matrices of nonzero determinant. Each of these 6 elements gives a linear transformation of \( \mathbb{Z}_2^2 \) onto itself, thus permuting the 3 nonzero elements of this space. They must each give a different permutation since otherwise they would be equal as linear transformations and therefore equal as matrices. Thus \( \text{GL}(2, \mathbb{Z}_2) \) consists of 6 permutations of a 3 element set, which means it is isomorphic to \( S_3 \). (This is a more elegant proof than the book's suggestion of writing out the multiplication tables, and is a method that can be applied to larger examples.)

24. Let \( G \) be a group. \( \text{Aut} G \) denotes the set of all automorphisms of \( G \). Since the inverse of an isomorphism is again an isomorphism (same proof as for rings), this is a group. Exercise 42 (homework) asks you to compute \( \text{Aut} \mathbb{Z} \).

28. Discuss in class.

29(a). \( U_8 = \{1, 3, 5, 7\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \), but \( U_{10} = \{1, 3, 7, 9\} \cong \mathbb{Z}_4 \) since it is the cyclic group \( \{1, 3, 3^2 \equiv 9, 3^3 \equiv 7\} \).

**Congruence modulo a subgroup.**

In order to work with quotient groups, we shall need another condition (because of noncommutativity) that we will determine later. But the initial results are completely analogous to what we did for rings. The proofs are exactly the same and will not be repeated.
Definition. Let $K$ be a subgroup of a group $G$ and let $a, b \in G$. We say $a$ is congruent to $b$ modulo $K$, written $a \equiv b \pmod{K}$, if $ab^{-1} \in K$.

Note that this is just like congruence modulo an ideal if we write $a - b$ instead of $ab^{-1}$.

Theorem 7.22. Congruence modulo $K$ is an equivalence relation. □

As before the equivalence classes are called congruence classes and we can talk about cosets just as we did for ideals. But now we write the operation multiplicatively and we must distinguish between left and right cosets. For $a \in G$, the congruence class of $a$ modulo $K$ is $\{ g \in G \mid ga^{-1} \in K \} = \{ g \in G \mid g = ka \text{ for some } k \in K \}$. We write this as $Ka$ and call it a right coset of $K$. We generally write $K$ for the coset $Ke$.

If we wanted to work with left cosets, we would have started by defining congruence by $a^{-1}b \in K$. We shall soon see that the main case of interest is when a subset of $G$ is both a left and right coset. For now, we have the usual results which follow from an equivalence relation: $Ka = Kb$ iff $a \equiv b \pmod{K}$ and any two right cosets are either disjoint or identical (i.e., the collection of all right cosets partitions $G$.) In particular, $G = \bigcup_{a \in G} Ka$.

Before proceeding to analyze kernels of homomorphisms, we use the idea of congruence to obtain some very useful counting results for finite groups. These are the sorts of theorems that make group theory more like combinatorics than like ring theory.

Theorem 7.25. Let $K$ be a subgroup of a group $G$. Then for each $a \in G$, right multiplication by $a$ gives a bijection between $K$ and $Ka$. In particular, if $K$ is finite, then all right cosets have the same number of elements.

Proof. It is a bijection because right multiplication by $a^{-1}$ is an inverse for the function. □

If $G$ is a finite group, then partitioning $G$ into congruence classes, all of size $|K|$, means that $|G|$ equals $|K|$ times the number of distinct right cosets. We denote this number by $[G : K]$ and call it the index of $K$ in $G$. If there are infinitely many congruence classes in an arbitrary group $G$, we say the index is infinite. For example, the infinite group $\mathbb{Z}$ has the subgroup $(2)$ of index 2 and the subgroup $(0)$ of infinite index. The group $\mathbb{Z}_6$ has three right cosets of the subgroup $H = \{0, 3\}$, namely $H, H + 1, H + 2$, where we now write the cosets using the operation $+$. Thus $[\mathbb{Z}_6 : H] = 3$ and $|\mathbb{Z}_6| = 6 = 2 \cdot 3 = |H|[\mathbb{Z}_6 : H]$. This illustrates a major theorem that we have just proved.

Theorem 7.26 (Lagrange’s Theorem). If $K$ is a subgroup of a finite group $G$, then the order of $K$ divides the order of $G$. Indeed, $|G| = |K|[G : K]$. □
The proof was only a matter of noticing that the cosets are the equivalence classes of an equivalence relation and they all have the same size!

At least as useful as this theorem is its corollary obtained by applying it to the cyclic subgroups generated by elements of $G$.

**Corollary 7.27.** Let $G$ be a finite group. Then

1. The order of every element divides the order of the group.
2. If $n = |G|$, then $g^n = e$ for every $g \in G$.

**Proof.** (1) Apply Lagrange's theorem to the subgroup $\langle g \rangle$ and it says that the order of $g$ divides the order of $G$.

(2) If $|g| = r$, then $n = rs$ for some integer $s$ by (1). Hence $g^n = g^{rs} = (g^r)^s = e^s = e$. □

Exercises, page 207:

7. The smallest possible order is $2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 27720$. What is the largest?

8. The order is divisible by 2 and 25 so must be 50 since it is less than 100.

9. Since $|H| = |K| = p$, any nonidentity element of $H$ or $K$ will have order $p$ and thus generate the whole group. Therefore, if $H \cap K \neq \langle e \rangle$, the nonidentity element will generate them both and $H = K$.

17. Let $f : G \to H$ be a group homomorphism, $a \in G$ of order $n$. Then $e_H = f(e_G) = f(a^n) = (f(a))^n$, hence the order of $f(a)$ divides $n$ by Theorem 7.8.

Section 7.5 ends with a computation of all groups of order at most 7 (up to isomorphism). Most of them are covered by

**Theorem 7.28.** Every group of prime order $p$ is isomorphic to $\mathbb{Z}_p$.

**Proof.** As in exercise 9 above, any nonidentity element $g$ in a group $G$ of order $p$ must itself have order $p$, so $G = \langle g \rangle$. We have already seen that any cyclic group of order $p$ is isomorphic to $\mathbb{Z}_p$. □
We claim the groups are all as summarized below:

<table>
<thead>
<tr>
<th>order</th>
<th>groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \langle e \rangle )</td>
</tr>
<tr>
<td>2</td>
<td>( \mathbb{Z}_2 )</td>
</tr>
<tr>
<td>3</td>
<td>( \mathbb{Z}_3 )</td>
</tr>
<tr>
<td>4</td>
<td>( \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 )</td>
</tr>
<tr>
<td>5</td>
<td>( \mathbb{Z}_5 )</td>
</tr>
<tr>
<td>6</td>
<td>( \mathbb{Z}_6, S_3 )</td>
</tr>
<tr>
<td>7</td>
<td>( \mathbb{Z}_7 )</td>
</tr>
</tbody>
</table>

Only the cases of order 4 and 6 are left to decide. We already know the groups given exist and are different. We must convince ourselves that there are no others.

Order 4: if there is an element of order 4, the group is cyclic, hence is isomorphic to \( \mathbb{Z}_4 \). Otherwise, it is \( \{e, a, b, c\} \) where \( a^2 = b^2 = c^2 = e \) (since the only possible other order is 2). Now \( ab \) cannot be \( a, b \) or \( e \), hence \( c = ab \). For the same reason, \( e = ba \), so the group is abelian and thus looks like \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) (think of the possible operation tables).

Order 6: we may assume there is no element of order 6 as this gives the cyclic group \( \mathbb{Z}_6 \). If every element has order 2, then \( G \) is abelian (check) and any two of them generate a subgroup of order 4, impossible by Lagrange’s theorem. So \( G \) has an element \( a \) of order 3; say \( N = \langle a \rangle = \{e, a, a^2\} \). Let \( Nb = \{b, ab, a^2b\} \) be the other right coset of \( N \) in \( G \). We now must consider the possible operation tables for \( G \). It is easy to see that \( b^2 \not\in Nb \). So \( b^2 = a^n \) for \( n = 0, 1 \) or 2. Then \( b^4 = a^{2n} \); if \( |b| = 3 \), then this says \( b = b^4 = a^{2n} \in N \), a contradiction. Thus \( b \) must have order 2 (so \( b^2 = e = a^0 \)). It is easy to see that \( ba \) cannot be in \( N \) (gives wrong order for \( b \)) or equal \( b \). \( ba = ab \) implies that it has order 6, a contradiction. Therefore \( ba = a^2b \) is the only possibility left. So \( G \) has two generators \( a \) and \( b \) and the three relations

\[
a^3 = e \quad b^2 = e \quad ba = a^2b
\]

These determine the operation table—see page 205. Thus there is only one other possible group besides \( \mathbb{Z}_6 \); we know \( S_3 \) has order 6, so we must have \( G \cong S_3 \).

Normal subgroups.

We now wish to determine what kernels of homomorphisms look like; equivalently, we wish to construct quotient groups like we did quotient rings. The main theorem we needed was that the operations of addition and multiplication worked on congruence classes—i.e. the operations were well-defined on the quotient rings. The book provides an example on page 209 to show that the operation may not be well-defined on the cosets \( Ka \) of a subgroup \( K \). We will need an additional condition on the subgroup. The author now goes
through the process that we mentioned earlier: we could define left cosets analogous to the way in which we defined right cosets, namely, by saying that \( a \) is left congruent to \( b \) modulo \( K \) if \( a^{-1}b \in K \). The left coset of \( a \) is written \( aK \) (or \( a + K \) in additive notation). It is a special property of a subgroup \( K \) for these two notions of congruence to be the same.

**Definition.** A subgroup \( N \) of a group \( G \) is **normal** if \( Ng = gN \) for every \( g \in G \). We write \( N \triangleleft G \) to mean that \( N \) is a normal subgroup of \( G \).

Examples: every subgroup of an abelian group \( G \) is normal, for then \( ng = gn \) for every \( g \in G \). More generally, every subgroup of \( \mathbb{Z}(G) \) is normal in \( G \) for the same reason.

In \( S_3 \), the cycle \( 1 \to 2 \to 3 \to 1 \) generates a normal subgroup of order 3, but the transposition \( 1 \leftrightarrow 2 \) generates a subgroup which is not normal. (No, we do not call it abnormal.) Indeed, in cycle notation, \( (23)(12) = (132) \) and \( (12)(23) = (123) \) which shows \( \langle (12) \rangle \) is not normal. On the other hand, \( \langle (123) \rangle \) has order 3, so it has index 2 in \( S_3 \). Thus it is normal by

**Proposition.** If \([G : H] = 2\), then \( H \) is normal in \( G \).

**Proof.** We know that the cosets partition \( G \). Let \( a \in G \setminus H \). Then \( H \cup Ha = G = H \cup aH \), where both \( aH \) and \( Ha \) are disjoint from \( H \). But then \( Ha = aH \) and \( H \) is normal. \( \square \)

Back to our example with \( S_3 \), if we write \( H = \langle (123) \rangle \), we know that \( (12)H = H(12) \) since \( H \) is normal. But (12) does not commute with elements of \( H \): \( (12)(123) = (23) = (132)(12) = (123)^2(12) \).

Other ways to express the normality condition:

**Theorem 7.34.** Let \( N \) be a subgroup of \( G \). The following are equivalent:

1. \( N \triangleleft G \).
2. \( g^{-1}Ng \subseteq N \) for each \( g \in G \).
3. \( gNg^{-1} \subseteq N \) for each \( g \in G \).
4. \( g^{-1}Ng = N \) for each \( g \in G \).
5. \( gNg^{-1} = N \) for each \( g \in G \).

**Proof.** \((2) \iff (3) \) and \((4) \iff (5) \) because \( g^{-1} \) runs through all elements of \( G \) as \( g \) does. \( (1) \implies (2) \)

Let \( n \in N \). We must show that \( g^{-1}ng \in N \). We know that \( Ng = gN \), so there exists some \( n_1 \in N \) with \( ng = gn_1 \). Then \( g^{-1}ng = g^{-1}gn_1 = n_1 \in N \).

\( (3) \implies (4) \)

From \((3) \implies (2) \) we know that \( g^{-1}Ng \subseteq N \); we need to show that
Let \( \ker f \) be a homomorphism and assume \( f(x) = e \). Then we check that 
\[
(fgx^{-1}) = f(g)f(x)f(g^{-1}) = f(g)f(g)^{-1} = e, \text{ so } g(\ker f)g^{-1} \subseteq \ker f \text{ and therefore } \\
\ker f \lhd G \text{ by Theorem 7.34(3)}.
\]

**Theorem 7.33.** Let \( N \triangleleft G \). If \( a \equiv b \pmod{N} \) and \( c \equiv d \pmod{N} \), then \( ac \equiv bd \pmod{N} \).

**Proof.** A translation of our earlier proofs, but now we want to see how normality enters.

By hypothesis, there exist elements \( m, n \in N \) such that \( ab^{-1} = m \) and \( cd^{-1} = n \). Then 
\[
ac(bd)^{-1} = acd^{-1}b^{-1} = ab^{-1} = m(bn)^{-1} \in N \text{ because normality implies that } \\
b^n \in N. \quad \Box
\]

This will enable us to construct quotient groups and prove the isomorphism theorems as we have done for rings. But first, some more examples.

Page 214. 7. \( \{ (g, e) \mid g \in G \} \triangleleft G \times H \). This is part of helping us to recognize when a group can be broken up as a product.

28. Let \( A \triangleleft G, B \triangleleft G, AB = G \) and \( A \cap B = \langle e \rangle \). Then \( A \times B \cong G \). Proof: We first note that \( ab = ba \) for every \( a \in A, b \in B \). Indeed, \( a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in B \) and \( a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in A \) by normality, so \( a^{-1}b^{-1}ab = e; \) therefore \( ab = ba \). Define \( f: A \times B \to G \) by \( f(a, b) = ab \). Check that this is a homomorphism (using the commutativity we have just established). \( f \) is surjective by hypothesis. For injectivity, assume \( f(a_1, b_1) = f(a_2, b_2) \). Then \( a_1b_1 = a_2b_2 \), hence \( a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{ e \} \).

Thus \( a_1 = a_2 \) and \( b_1 = b_2 \). Therefore \( f \) is an isomorphism.

14. Normality is not transitive. See page 165 for the elements of \( D_4 \). We have \( M = \{ v, r_0 \} \triangleleft N = \{ h, v, r_2, r_0 \} \triangleleft D_4 \) since each has index 2. But \( M \) is not normal in \( D_4 \) because \( dM = \{ d, r_1 \} \neq \{ d, r_3 \} = Md, \) using the operation table on page 167.
Quotient groups.

Using the same notation as for rings and ideals, we write \( G/N \) for the set of all right (or left) cosets of \( G \) when \( N \) is a normal subgroup. We define multiplication of cosets by

\[
(NA)(Nb) = Nab
\]

Translating Theorem 7.33 to this language gives

**Theorem 7.35.** The multiplication defined above is well-defined.

**Proof.** Well-defined means, if we use other names for the cosets, say \( Na = Nc \) and \( Nb = Nd \), then we get the same coset as an answer. But \( Na = Nc \) says \( a \equiv c \pmod{N} \), and similarly \( b \equiv d \pmod{N} \), so \( ab \equiv cd \pmod{N} \), or \( Nab = Ncd \).

This means the set of cosets again has an operation under which it is closed. We next show that it is a group. We call the group \( G/N \) the **quotient group** or **factor group** of \( G \) by \( N \).

**Theorem 7.36.** Let \( N \triangleleft G \). Then

1. \( G/N \) is a group under the operation defined above.
2. If \( G \) is finite, then \( |G/N| = |G|/|N| \).
3. If \( G \) is abelian, so is \( G/N \).

**Proof.** (1) The operation is well-defined, the identity is \( N = Ne \), the inverse of \( Na \) is \( Na^{-1} \) and associativity is inherited from \( G \).

(2) Lagrange’s theorem.

(3) Clear, since the operation is inherited from \( G \).

Examples: we saw that \( \langle (123) \rangle \triangleleft S_3 \). Since the index is 2, the quotient group is isomorphic to \( \mathbb{Z}_2 \).

Abelian groups are easy because we don’t have to worry about normality: In \( \mathbb{Z}_{rs} \), the subgroup \( N = \langle r \rangle \) has order \( s \) and the quotient group has order \( r \). The quotient is isomorphic to \( \mathbb{Z}_r \) because the cosets are precisely \( N + k \), \( k = 0, 1, \ldots, r - 1 \). In particular, every quotient of a cyclic group is cyclic.

Among infinite groups, \( \mathbb{Q}/\mathbb{Z} \) is interesting. Every element has finite order and every possible order occurs. Let \( \frac{m}{n} \in \mathbb{Q} \) with \( \gcd(m, n) = 1 \). Then \( n \frac{m}{n} = m \in \mathbb{Z} \) is the smallest multiple of \( \frac{m}{n} \) in \( \mathbb{Z} \). Thus \( \mathbb{Z} + \frac{m}{n} \) has order \( n \) in \( \mathbb{Q}/\mathbb{Z} \).
Lemma 8.22 (Abelian case of Cauchy’s Theorem). Let \( G \) be a finite abelian group with a prime \( p \) dividing \( |G| \). Then \( G \) has an element of order \( p \).

Proof. Induct on \( |G| \). If \( |G| = 1 \), it is vacuously true. Assume \( |G| > 1 \) and the claim holds for every abelian group of order less than \( |G| \). Let \( e \neq a \in G \) be an element of order \( r > 1 \). If \( p|r \), then \( a^{r/p} \) works. If not, then \( p \) divides \( |G/\langle a \rangle| \) (since \( |G| = |\langle a \rangle||G/\langle a \rangle| \)). By the induction hypothesis, \( G/\langle a \rangle \) has an element \( \langle a \rangle b \) of order \( p \). Let \( s = |b| \). Then \( \langle (a)b \rangle = \langle a \rangle b^s = \langle a \rangle \), so \( p|s \). Now \( b^{r/p} \) is the desired element of \( G \) of order \( p \).

As a general principle, factoring out a subgroup makes the group less complicated. One question we might ask is just what needs to be factored out to make the factor group abelian. This is answered in Theorem 7.37 together with Exercise 23, page 221. First assume that \( N \triangleleft G \). What is needed to make \( G/N \) abelian? To have \( ab = ba \), we need \( aba^{-1}b^{-1} = e \). Modulo \( N \), this means \( aba^{-1}b^{-1} \in N \) for every \( a, b \in G \). The set of such products is not usually closed under multiplication. We write \( G' \) for the group generated by all such products. They are called commutators and the group \( G' \) is called the commutator subgroup of \( G \). Note that taking \( a = b \), we see that \( e \) is a commutator; and \( bab^{-1}a^{-1} \) is a commutator, so they are closed under taking inverses. But the general form of an element of \( G' \) is a finite product of commutators in order to have closure.

Next we check that \( G' \triangleleft G \): for any \( g \in G \),
\[
g(abab^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G'.
\]
More generally, if \( c_1, c_2, \ldots, c_k \) are commutators, then \( gc_1\ldots c_k g^{-1} = (gc_1g^{-1})\ldots(gc_kg^{-1}) \) is again a product of commutators, hence is in \( G' \).

Since \( N \) must contain \( G' \) if it contains all commutators, we have proved

Theorem. Let \( N \triangleleft G \). Then \( G/N \) is abelian iff \( G' \subseteq N \).

The center of \( G \) has almost the opposite effect. One might expect that factoring it out would leave only the noncommutative stuff. That is close to being correct (see Exercise 26, page 221), but if the quotient is sufficiently simple, there is no room for noncommutativity.

Theorem 7.38. If \( G \) is a group such that \( G/Z(G) \) is cyclic, then \( G \) is abelian.

Proof. Since \( G/Z(G) \) is cyclic, it has a generator \( Z(G)g \). And every coset looks like \( Z(G)g^n \) for some integer \( n \). So every element of \( G \) has the form \( zg^n \) for some \( z \in Z(G) \), \( n \in \mathbb{Z} \). But then an arbitrary product has the form \((z_1g^n)(z_2g^m) = (z_1z_2)g^{n+m} = (z_2g^m)(z_1g^n)\) and \( G \) is abelian. \( \square \)

An application is given by Exercise 21, page 221. Assume that \( |G| = pq \) with \( p, q \) prime.
Then $Z(G)$ is $\langle e \rangle$ or $G$. We know that $|Z(G)|$ divides $pq$, so is $1, p, q$ or $pq$. We must eliminate the possibility of $p$ or $q$. So assume $|Z(G)| = p$ (the same argument will apply to $q$). Then $G/Z(G)$ has prime order $q$, hence is cyclic. By Theorem 7.38, $G$ is abelian, so $G = Z(G)$, a contradiction of $|Z(G)| = p$. Later we shall see that if $p = q$, then $G$ must be abelian and so $G = Z(G)$. If $p \neq q$, the center may be $\langle e \rangle$ as we saw for $S_3$.

**Theorem 7.39.** Let $f: G \to H$ be a group homomorphism. Then $\ker f$ is a normal subgroup of $G$.

**Proof.** We have already checked the normality condition. We need to check that $\ker f$ is a subgroup. We know it contains the identity of $G$. Assume $a, b \in \ker f$; then $f(ab^{-1}) = f(a)f(b)^{-1} = e$, hence $ab^{-1} \in \ker f$. Therefore $\ker f$ is a subgroup of $G$. □

**Theorem 7.40.** Let $f: G \to H$ be a group homomorphism. Then $\ker f = \langle e \rangle$ iff $f$ is injective.

The proof is the same as for rings or linear transformations. Also, just as for rings, using congruence modulo a subgroup to define a quotient group shows that every normal subgroup is the kernel of a homomorphism: in particular, if $N \triangleleft G$, then $N$ is the kernel of the canonical homomorphism $\pi: G \to G/N$ defined by $\pi(g) = Ng$. The fact that $\pi$ is a homomorphism is just because of the way we defined the operation in $G/N$.

**The Isomorphism Theorems.**

**First Isomorphism Theorem** (Theorem 7.42). Let $f: G \to H$ be a homomorphism of groups with $K = \ker f$. Then the quotient group $G/K$ is isomorphic to the image $\text{Im} f \subseteq H$.

**Proof.** Define $\bar{f}: G/K \to H$ by $\bar{f}(Kg) = f(g)$. The function is well-defined because if $Kg_1 = Kg_2$, then $g_1g_2^{-1} \in K$, so that $f(g_2) = e_Hf(g_2) = f(g_1g_2^{-1})f(g_2) = f(g_1g_2^{-1}g_2) = f(g_1)$. It is a homomorphism because

$$\bar{f}(Kg_1)\bar{f}(Kg_2) = f(g_1)f(g_2) = f(g_1g_2) = \bar{f}(Kg_1g_2) = \bar{f}(Kg_1Kg_2).$$

It is injective since $Kx \in \ker \bar{f}$ implies $f(x) = \bar{f}(Kx) = e_H$, so $x \in K$. Therefore $\ker \bar{f} = \{Ke \} \subseteq G/K$. Since $\bar{f}$ maps surjectively onto $\text{Im} f$, it gives an isomorphism. □

**Second Isomorphism Theorem** (Exercise 24, page 229). Let $K$ and $N$ be subgroups of $G$ with $N \triangleleft G$. Then $N \cap K \triangleleft K$ and $NK/N \cong K/(N \cap K)$. 
Proof. You proved for homework that $N \triangleleft G$ implies $NK$ is a subgroup of $G$. Note that $N \triangleleft NK$ because $gNg^{-1} = N$ for every element of $G \supseteq NK$ so $NK/N$ is a quotient group. Define a function $f: K \to NK/N$ by $f(k) = Nk \in NK/N$. $f$ is the composition of the inclusion $K \to NK$ and the canonical quotient mapping $NK \to NK/N$, so it is a homomorphism. Since every element of $NK/N$ is a coset $Nk$ for some $k \in K$, $f$ is surjective. What is ker $f$? Certainly $N \cap K \subseteq \ker f$ since $f(x) = Nx = N$ for $x \in N \cap K$. Conversely, if $k \in \ker f$ then $k \in K$ and $f(k) = Nk = N$, so $k \in N$. Therefore ker $f = N \cap K$. Since kernels are always normal we have $N \cap K \triangleleft K$. By the first isomorphism theorem, $f$ induces an isomorphism $NK/N \cong K/(N \cap K)$. \hfill \Box

**Third Isomorphism Theorem** (Theorem 7.43). Let $K,N \triangleleft G$ with $N \subseteq K \subseteq G$. Then $K/N$ is a normal subgroup of $G/N$ and the quotient group $(G/N)/(K/N)$ is isomorphic to $G/K$.

Proof. We want to define a homomorphism $f: G/N \to G/K$. Try $f(Ng) = Kg$. Well-defined: if $Ng_1 = Ng_2$, then $g_1g_2^{-1} \in N \subseteq K$, so $Kg_1 = Kg_2$. Homomorphism: $f(NA nb) = f(NAb) = Kab = bKg = f(Na)f(Nb)$

Again we want to apply the first homomorphism theorem and need to know ker $f$. So assume $Ng \in \ker f$; that is, $Kg = f(Ng) = e_{G/K} = K$. So $g \in K$ meaning that $Ng$ in $G/N$ actually lies in the subgroup $K/N$. Conversely, any element of $K/N$ is certainly in the kernel, so we have ker $f = K/N$. Furthermore, it is clear that $f$ is surjective, so the first isomorphism theorem gives us $(G/N)/(K/N) \cong G/K$. The fact that $K/N \triangleleft G/N$ follows from it being a kernel of a homomorphism. \hfill \Box

Look at exercises 2, 3 on page 227.

Exercise 15, page 227. We generalize to $SL(n, \mathbb{R})$, the set of all $n \times n$ matrices in $GL(n, \mathbb{R})$ with determinant 1. Let $A,B \in GL(n, \mathbb{R})$ with det $B = 1$. Then $\det(ABA^{-1}) = \det A \det B (\det A)^{-1} = \det B = 1$. Therefore $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$. But we can also approach this with the first isomorphism theorem. Just consider the determinant mapping $\det: GL(n, \mathbb{R}) \to \mathbb{R}^*$; since $\det(AB) = \det A \det B$, it is a group homomorphism. By definition, its kernel is $SL(n, \mathbb{R})$, so $SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$ and $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^*$ (since $\det$ is surjective).

There is a strong connection between subgroups of $G$ and subgroups of $G/N$, just as there was a connection for ideals of rings modulo an ideal. Part of this is in the 3rd isomorphism theorem. But much more is true.

**Theorem 7.44.** Let $N \triangleleft G$ and let $K \supseteq N$ be a subgroup of $G$. Then

1. $K/N$ is a subgroup of $G/N$.
2. $K/N \triangleleft G/N$ iff $K \triangleleft G$. 


There is a one-to-one correspondence between subgroups of $G/N$ and subgroups $H$ of $G$ containing $N$ given by $H \longrightarrow H/N$. Under this correspondence, normal subgroups correspond to normal subgroups.

**Proof.** (1) By Theorem 7.19(3), the image of a subgroup is a subgroup.

(2) $(\Rightarrow)$ Assume $K/N \triangleleft G/N$ and let $g \in G, k \in K$. Then $\pi(gk)^{-1} = (Ng)(Nk)(Ng)^{-1} \in K/N$. Thus $Ngk^{-1} = Nk_1$ for some $k_1 \in K$, and so $gk^{-1}k_1^{-1} \in N \subseteq K$. Therefore $gk^{-1} \in K$ and so $K \triangleleft G$.

(3) Half of the correspondence is proved in (1). Now assume that $T$ is a subgroup of $G/N$. Let $H = \{ g \in G \mid \pi(g) = Ng \in T \}$. $H$ is a subgroup of $G$ by homework problem 23, page 197. Since we have defined it so that $T = H/N$, this gives half of a one-to-one correspondence. We must also show that if we start with $K \subseteq G$, map it to $K/N$ and then take the inverse image, we get $K$ back. Let $x \in G$ with $Nx \in K/N$. Then $x \in NK = K$, so this does work to give a one-to-one correspondence. The correspondence of normal subgroups is just statement (2). \(\square\)

**Symmetric and Alternating groups.**

We have already seen that Theorem 7.47 holds: every element of $S_n$ can be written a product of disjoint cycles. More precisely, a cycle of length $k$ or $k$-cycle is a cycle of the form $(a_1a_2 \cdots a_k)$ where $a_1, \ldots, a_k$ are distinct elements of $N = \{1, 2, \ldots, n\}$. Cycles are said to be disjoint if they have no elements in common. It should be clear to you from the way we multiply (compose) cycles, that disjoint cycles commute in $S_n$. Using the disjoint cycle decomposition of a permutation shows that any $\sigma \in S_n$ partitions $N$ into equivalence classes called orbits.

2-cycles are usually called transpositions. You should have seen the next result in linear algebra in working with determinants.

**Corollary 7.48.** Every permutation can be written as a product of transpositions.

**Proof.** Since we know every permutation can be written as a product of cycles, it will suffice to show that every cycle is a product of transpositions. One need only check that $(a_1a_2 \cdots a_k) = (a_1a_2)(a_2a_3) \cdots (a_k-1a_k)$. \(\square\)

Another fact you should have seen in linear algebra is that every way of writing a given permutation as a product of transpositions either has an even number or an odd number, but never both. This is needed to define the sign of a permutation, used in the definition of determinant of a matrix. There is a cute way of seeing this, other than the computational method in the book. Let $\Delta$ be the polynomial $\prod_{1 \leq i < j \leq n} (x_i - x_j)$ in $n$
variables. A permutation $\sigma \in S_n$ acts on $\Delta$ by sending $x_i \mapsto x_{\sigma(i)}$. Therefore $\sigma$ takes $\Delta$ to $\pm \Delta$. We call a permutation even if it leaves $\Delta$ unchanged and odd if it sends $\Delta$ to $-\Delta$. The relationship with transpositions is that whenever $i$ and $j$ are interchanged, the sign of $\Delta$ is changed by a factor of $-1$. Thus an even number of transpositions leaves the sign unchanged and an odd number flips it.

**Theorem 7.51.** The set $A_n$ of all even permutations is a normal subgroup of $S_n$ of index 2 in $S_n$ and order $n!/2$. $A_n$ is called the alternating group on $n$ elements.

**Proof.** First we need to check that $A_n$ is a group. But it is clear that the identity permutation does not change $\Delta$. And if $\sigma$ is even, then its inverse also takes $\Delta \mapsto \Delta$, as do compositions of such functions. Thus $A_n$ is a subgroup of $S_n$. Now define a function $\text{sgn}: S_n \to \{\pm 1\}$ by $\text{sgn}(\sigma)$ is 1 if $\sigma$ is even and $-1$ if $\sigma$ is odd. Think of $\{\pm 1\}$ as the 2-element group under multiplication. Continuing the argument above, a composition of two odd permutations gives an even permutation since $\sigma \tau(\Delta) = \sigma(-\Delta) = +\Delta$, and a composition of an odd and an even permutation is odd. Therefore $\text{sgn}$ is a group homomorphism. By definition its kernel is $A_n$, so $A_n \triangleleft S_n$. Since the image of $\text{sgn}$ has order 2 and $|S_n| = n!$, the numerical claims follow from Lagrange’s theorem. □

**Finite simple groups.**

Recall that we discussed simple groups briefly. They are the groups with no normal subgroups. This means that any homomorphism from a simple group to another group has kernel either the trivial group or the whole group and thus they have no nontrivial homomorphic images other than themselves. This gives a way to consider them as the building blocks for all finite groups. For any finite group $G$, one considers maximal chains of subgroups $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = \langle e \rangle$ such that each $G_k$ is a normal subgroup of $G_{k-1}$. If the chain is maximal, there is no normal subgroup of $G_{k-1}$ containing $G_k$, so $G_{k-1}/G_k$ is a simple group. A theorem called the Jordan–Hölder theorem says that the set of all factor groups $G_{k-1}/G_k$ is unique up to isomorphism and order. That is, there can be different chains for a group $G$, but the set of quotient groups (called composition factors) is unique. Example: $\mathbb{Z}_{12} \supseteq \{0, 2, 4, 6, 8, 10\} \supseteq \{0, 6\} \supseteq \{0\}$ with composition factors isomorphic to $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$ and also $\mathbb{Z}_{12} \supseteq \{0, 3, 6, 9\} \supseteq \{0, 6\} \supseteq \{0\}$ with composition factors isomorphic to $\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$. Now the problem of finding all finite groups can be broken into two parts

1. Find all finite simple groups
2. Find all ways to build finite groups from the set of composition factors.

(1) was finally completed in 1981. The simple groups we have encountered are the groups $\mathbb{Z}_p$ for $p$ prime—in fact, these are precisely the groups with no proper subgroups of any kind—and the alternating groups $A_n$ for $n \neq 4$. ($A_2 = \langle e \rangle$, $A_3 \cong \mathbb{Z}_3$ and $A_n$ for $n \geq 5$ is nonabelian with simplicity requiring a computational proof given in section 7.10.)
(2) is much harder. Of course one way to put two groups together is the direct product. We have seen that if $G$ and $H$ are simple, then $G \times H \supseteq G \times \langle e \rangle \supseteq \langle (e,e) \rangle$ is a composition series (i.e. $G \times \langle e \rangle \lhd G \times H$). More generally, they can be put together with what is called a semidirect product. This is mentioned in Exercise 27, page 251, but the general construction is not given in our book. It involves using an automorphism of one of the groups to twist the multiplication of the product. We have seen an example in $S_3$ which was generated by two elements $a, b$ with $\langle a \rangle \cong \mathbb{Z}_3$, $\langle b \rangle \cong \mathbb{Z}_2$, but with multiplication twisted by the formula $ab = ba^2$. But there is no known way to compute all possible ways of constructing such products. This is known as the extension problem: how many ways can you fill in the middle of $H \rightarrow ? \rightarrow G$ in which the first homomorphism is an injection, the second is a surjection and $H$ is isomorphic to the kernel of the second. One way is with $G \times H$.

This brings us to Part 2 of our book, in which we take a more in depth look at the topics we have covered so far: groups, rings and fields. It culminates in a beautiful correspondence between group theory and field theory that leads to a better understanding of both, as well as a solution of the classical Greek geometry problems such as trisecting an angle with straigntedge and compass (shown to be impossible).