Chapter 1

Groups

In this chapter we introduce groups and prove some of the basic theorems in group theory. One of these, the structure theorem for finitely generated abelian groups, we do not prove here but instead derive it as a corollary of the more general structure theorem for finitely generated modules over a PID (see Theorem 3.7.22).

1.1 Definitions and Examples

(1.1) Definition. *A* **group** *is a set G together with a binary operation*

$$\cdot : G \times G \to G$$

satisfying the following three conditions:

(a) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* a, b, $c \in G$. *(Associativity)*
(b) *There exists an element* $e \in G$ *such that* $a \cdot e = e \cdot a = a$ *for all* $a \in G$. *(Existence of an identity element)*
(c) *For each* $a \in G$ *there exists a* $b \in G$ *such that* $a \cdot b = b \cdot a = e$. *(Existence of an inverse for each* $a \in G$*)*

It is customary in working with binary operations to write $a \cdot b$ rather than $\cdot(a, b)$. Moreover, when the binary operation defines a group structure on a set G then it is traditional to write the group operation as ab. One exception to this convention occurs when the group G is **abelian**, i.e., if $ab = ba$ for all a, $b \in G$. If the group G is abelian then the group operation is commonly written additively, i.e., one writes $a + b$ rather than ab. This convention is not rigidly followed; for example, one does not suddenly switch to additive notation when dealing with a group that is a subset of a group written multiplicatively. However, when dealing specifically with abelian groups the additive convention is common. Also, when dealing with abelian groups the identity is commonly written $e = 0$, in conformity with

the additive notation. In this chapter, we will write e for the identity of general groups, i.e., those written multiplicatively, but when we study group representation theory in Chapter 8, we will switch to 1 as the identity for multiplicatively written groups.

To present some examples of groups we must give the set G and the operation $\cdot : G \times G \to G$ and then check that this operation satisfies (a), (b), and (c) of Definition 1.1. For most of the following examples, the fact that the operation satisfies (a), (b), and (c) follows from properties of the various number systems with which you should be quite familiar. Thus details of the verification of the axioms are generally left to the reader.

(1.2) Examples.

(1) The set $\mathbf{Z}$ of integers with the operation being ordinary addition of integers is a group with identity $e = 0$, and the inverse of $m \in \mathbf{Z}$ is $-m$. Similarly, we obtain the additive group $\mathbf{Q}$ of rational numbers, $\mathbf{R}$ of real numbers, and $\mathbf{C}$ of complex numbers.

(2) The set $\mathbf{Q}^*$ of nonzero rational numbers with the operation of ordinary multiplication is a group with identity $e = 1$, and the inverse of $a \in \mathbf{Q}^*$ is $1/a$. $\mathbf{Q}^*$ is abelian, but this is one example of an abelian group that is not normally written with additive notation. Similarly, there are the abelian groups $\mathbf{R}^*$ of nonzero real numbers and $\mathbf{C}^*$ of nonzero complex numbers.

(3) The set $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$ with the operation of addition modulo n is a group with identity 0, and the inverse of $x \in \mathbf{Z}_n$ is $n-x$. Recall that addition modulo n is defined as follows. If x, $y \in \mathbf{Z}_n$, take $x + y \in \mathbf{Z}$ and divide by n to get $x + y = qn + r$ where $0 \leq r < n$. Then define $x + y \pmod{n}$ to be r.

(4) The set U_n of complex n^{th} roots of unity, i.e., $U_n = \{\exp((2k\pi i)/n) : 0 \leq k \leq n-1\}$ with the operation of multiplication of complex numbers is a group with the identity $e = 1 = \exp(0)$, and the inverse of $\exp((2k\pi i)/n)$ is $\exp((2(n-k)\pi i)/n)$.

(5) Let $\mathbf{Z}_n^* = \{m : 1 \leq m < n \text{ and } m \text{ is relatively prime to } n\}$. Under the operation of multiplication modulo n, $\mathbf{Z}_n^*$ is a group with identity 1. Details of the verification are left as an exercise.

(6) If X is a set let S_X be the set of all bijective functions $f : X \to X$. Recall that a function is bijective if it is one-to-one and onto. Functional composition gives a binary operation on S_X and with this operation it becomes a group. S_X is called the group of **permutations** of X or the **symmetric group** on X. If $X = \{1, 2, \ldots, n\}$ then the symmetric group on X is usually denoted S_n and an element α of S_n can be conveniently indicated by a $2 \times n$ matrix

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

where the entry in the second row under k is the image $\alpha(k)$ of k under the function α. To conform with the conventions of functional composition, the product $\alpha\beta$ will be read from right to left, i.e., first do β and then do α. For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

(7) Let $\mathrm{GL}(n, \mathbf{R})$ denote the set of $n \times n$ invertible matrices with real entries. Then $\mathrm{GL}(n, \mathbf{R})$ is a group under matrix multiplication. Let $\mathrm{SL}(n, \mathbf{R}) = \{T \in \mathrm{GL}(n, \mathbf{R}) : \det T = 1\}$. Then $\mathrm{SL}(n, \mathbf{R})$ is a group under matrix multiplication. (In this example, we are assuming familiarity with basic properties of matrix multiplication and determinants. See Chapter 4 for details.) $\mathrm{GL}(n, \mathbf{R})$ (respectively, $\mathrm{SL}(n, \mathbf{R})$) is known as the **general linear group** (respectively, **special linear group**) of degree n over $\mathbf{R}$.

(8) If X is a set let $\mathcal{P}(X)$ denote the power set of X, i.e., $\mathcal{P}(X)$ is the set of all subsets of X. Define a product on $\mathcal{P}(X)$ by the formula $A \triangle B = (A \setminus B) \cup (B \setminus A)$. $A \triangle B$ is called the symmetric difference of A and B. It is a straightforward exercise to verify the associative law for the symmetric difference. Also note that $A \triangle A = \emptyset$ and $\emptyset \triangle A = A \triangle \emptyset = A$. Thus $\mathcal{P}(X)$ with the symmetric difference operation is a group with $\emptyset$ as identity and every element as its own inverse. Note that $\mathcal{P}(X)$ is an abelian group.

(9) Let $\mathcal{C}(\mathbf{R})$ be the set of continuous real-valued functions defined on $\mathbf{R}$ and let $\mathcal{D}(\mathbf{R})$ be the set of differentiable real-valued functions defined on $\mathbf{R}$. Then $\mathcal{C}(\mathbf{R})$ and $\mathcal{D}(\mathbf{R})$ are groups under the operation of function addition.

One way to explicitly describe a group with only finitely many elements is to give a table listing the multiplications. For example the group $\{1, -1\}$ has the multiplcation table

$\cdot$	1	-1
1	1	-1
-1	-1	1

whereas the following table

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

is the table of a group called the **Klein 4-group**. Note that in these tables each entry of the group appears exactly once in each row and column. Also the multiplication is read from left to right; that is, the entry at the intersection of the row headed by α and the column headed by β is the product $\alpha\beta$. Such a table is called a **Cayley diagram** of the group. They are sometimes useful for an explicit listing of the multiplication in small groups.

The following result collects some elementary properties of a group:

(1.3) Proposition. *Let G be a group.*

(1) *The identity e of G is unique.*
(2) *The inverse b of $a \in G$ is unique. We denote it by a^{-1}.*
(3) *$(a^{-1})^{-1} = a$ for all $a \in G$ and $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$.*
(4) *If $a, b \in G$ the equations $ax = b$ and $ya = b$ each have unique solutions in G.*
(5) *If $a, b, c \in G$ then $ab = ac$ implies that $b = c$ and $ab = cb$ implies that $a = c$.*

Proof. (1) Suppose e' is also an identity. Then $e' = e'e = e$.

(2) Suppose $ab = ba = e$ and $ab' = b'a = e$. Then $b = eb = (b'a)b = b'(ab) = b'e = b'$, so inverses are unique.

(3) $a(a^{-1}) = (a^{-1})a = e$, so $(a^{-1})^{-1} = a$. Also $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$ and similarly $(b^{-1}a^{-1})(ab) = e$. Thus $(ab)^{-1} = b^{-1}a^{-1}$.

(4) $x = a^{-1}b$ solves $ax = b$ and $y = ba^{-1}$ solves $ya = b$, and any solution must be the given one as one sees by multiplication on the left or right by a^{-1}.

(5) If $ab = ac$ then $b = a^{-1}(ab) = a^{-1}(ac) = c$. □

The results in part (5) of Proposition 1.3 are known as the cancellation laws for a group.

The associative law for a group G shows that a product of the elements a, b, c of G can be written unambiguously as abc. Since the multiplication is binary, what this means is that any two ways of multiplying a, b, and c (so that the order of occurrence in the product is the given order) produces the same element of G. With three elements there are only two choices for multiplication, that is, $(ab)c$ and $a(bc)$, and the law of associativity says

that these are the same element of G. If there are n elements of G then the law of associativity combined with induction shows that we can write $a_1a_2\cdots a_n$ unambiguously, i.e., it is not necessary to include parentheses to indicate which sequence of binary multiplications occurred to arrive at an element of G involving all of the a_i. This is the content of the next proposition.

(1.4) Proposition. *Any two ways of multiplying the elements a_1, a_2, ..., a_n in a group G in the order given (i.e., removal of all parentheses produces the juxtaposition $a_1a_2\cdots a_n$) produces the same element of G.*

Proof. If $n = 3$ the result is clear from the associative law in G.

Let $n > 3$ and consider two elements g and h obtained as products of a_1, a_2, ..., a_n in the given order. Writing g and h in terms of the last multiplications used to obtain them gives

$$g = (a_1\cdots a_i)\cdot(a_{i+1}\cdots a_n)$$

and

$$h = (a_1\cdots a_j)\cdot(a_{j+1}\cdots a_n).$$

Since i and j are less than n, the induction hypothesis implies that the products $a_1\cdots a_i$, $a_{i+1}\cdots a_n$, $a_1\cdots a_j$, and $a_{j+1}\cdots a_n$ are unambiguously defined elements in G. Without loss of generality we may assume that $i \le j$. If $i = j$ then $g = h$ and we are done. Thus assume that $i < j$. Then, by the induction hypothesis, parentheses can be rearranged so that

$$g = (a_1\cdots a_i)((a_{i+1}\cdots a_j)(a_{j+1}\cdots a_n))$$

and

$$h = ((a_1\cdots a_i)(a_{i+1}\cdots a_j))(a_{j+1}\cdots a_n).$$

Letting $A = (a_1\cdots a_i)$, $B = (a_{i+1}\cdots a_j)$, and $C = (a_{j+1}\cdots a_n)$ the induction hypothesis implies that A, B, and C are unambiguously defined elements of G. Then

$$g = A(BC) = (AB)C = h$$

and the proposition follows by the principle of induction. □

Since products of n elements of G are unambiguous once the order has been specified, we will write $a_1a_2\cdots a_n$ for such a product, without any specification of parentheses. Note that the only property of a group used in Proposition 1.4 is the associative property. Therefore, Proposition 1.4 is valid for *any* associative binary operation. We will use this fact to be able to write unambiguous multiplications of elements of a ring in later chapters. A convenient notation for $a_1\cdots a_n$ is $\prod_{i=1}^{n} a_i$. If $a_i = a$ for all i then $\prod_{i=1}^{n} a$ is denoted a^n and called the n^{th} power of a. Negative powers of a are defined

by $a^{-n} = (a^{-1})^n$ where $n > 0$, and we set $a^0 = e$. With these notations the standard rules for exponents are valid.

(1.5) Proposition. *If G is a group and $a \in G$ then*

(1) $a^m a^n = a^{m+n}$, *and*
(2) $(a^m)^n = a^{mn}$ *for all integers m and n.*

Proof. Part (1) follows from Proposition 1.4 while part (2) is an easy exercise using induction. □

1.2 Subgroups and Cosets

Let G be a group and let $H \subseteq G$ be a subset. H is called a **subgroup** of G if H together with the binary operation of G is a group. The first thing to note is that this requires that H be closed under the multiplication of G, that is, ab is in H whenever a and b are in H. This is no more than the statement that the multiplication on G is defined on H. Furthermore, if H is a subgroup of G then H has an identity e' and G has an identity e. Then $e'e = e'$ since e is the identity of G and $e'e' = e'$ since e' is the identity of H. Thus $e'e = e'e'$ and left cancellation of e' (in the group G) gives $e = e'$. Therefore, the identity of G is also the identity of any subgroup H of G. Also, if $a \in H$ then the inverse of a as an element of H is the same as the inverse of a as an element of G since the inverse of an element is the unique solution to the equations $ax = e = xa$.

(2.1) Proposition. *Let G be a group and let H be a nonempty subset of G. Then H is a subgroup if and only if the following two conditions are satisfied.*

(1) *If $a, b \in H$ then $ab \in H$.*
(2) *If $a \in H$ then $a^{-1} \in H$.*

Proof. If H is a subgroup then (1) and (2) are satisfied as was observed in the previous paragraph. If (1) and (2) are satisfied and $a \in H$ then $a^{-1} \in H$ by (2) and $e = aa^{-1} \in H$ by (1). Thus conditions (a), (b), and (c) in the definition of a group are satisfied for H, and hence H is a subgroup of G. □

(2.2) *Remarks.* (1) Conditions (1) and (2) of Proposition 2.1 can be replaced by the following single condition.

(1)′ If $a, b \in H$ then $ab^{-1} \in H$.

Indeed, if $(1)'$ is satisfied then whenever $a \in H$ it follows that $e = aa^{-1} \in H$ and then $a^{-1} = ea^{-1} \in H$. Thus $a \in H$ implies that $a^{-1} \in H$. Also, if $a, b \in H$ then $b^{-1} \in H$ so that $ab = a(b^{-1})^{-1} \in H$. Therefore, $(1)'$ implies (1) and (2). The other implication is clear.

(2) If H is finite then only condition (1) of Proposition 2.1 is necessary to ensure that H is a subgroup of G. To see this suppose that H is a finite set and suppose that $a, b \in H$ implies that $ab \in H$. We need to show that $a^{-1} \in H$ for every $a \in H$. Thus let $a \in H$ and let $T_a : H \to H$ be defined by $T_a(b) = ab$. Our hypothesis implies that $T_a(H) \subseteq H$. If $T_a(b) = T_a(c)$ then $ab = ac$ and left cancellation in the group G (Proposition 1.3 (5)) shows that $b = c$. Hence T_a is an injective map and, since H is assumed to be finite, it follows that T_a is bijective, so the equation $ax = c$ is solvable in H for any choice of $c \in H$. Taking $c = a$ shows that $e \in H$ and then taking $c = e$ shows that $a^{-1} \in H$. Therefore, condition (2) of Proposition 2.1 is satisfied and H is a subgroup of G.

(3) If G is an abelian group with the additive notation, then $H \subseteq G$ is a subgroup if and only if $a - b \in H$ whenever $a, b \in H$.

(2.3) Proposition. *Let I be an index set and let H_i be a subgroup of G for each $i \in I$. Then $H = \bigcap_{i \in I} H_i$ is a subgroup of G.*

Proof. If $a, b \in H$ then $a, b \in H_i$ for all $i \in I$. Thus $ab^{-1} \in H_i$ for all $i \in I$. Hence $ab^{-1} \in H$ and H is a subgroup by Remark 2.2 (1). □

(2.4) Definition. *Let G and H be groups and let $f : G \to H$ be a function. Then f is a* **group homomorphism** *if $f(ab) = f(a)f(b)$ for all $a, b \in G$. A* **group isomorphism** *is an invertible group homomorphism. If f is a group homomorphism, let*

$$\mathrm{Ker}(f) = \{a \in G : f(a) = e\}$$

and

$$\mathrm{Im}(f) = \{h \in H : h = f(a) \quad \textit{for some } a \in G\}.$$

$\mathrm{Ker}(f)$ *is the* **kernel** *of the homomorphism f and* $\mathrm{Im}(f)$ *is the* **image** *of f.*

It is easy to check that f is invertible as a group homomorphism if and only if it is invertible as a function between sets, i.e., if and only if it is bijective.

(2.5) Proposition. *Let $f : G \to H$ be a group homomorphism. Then* $\mathrm{Ker}(f)$ *and* $\mathrm{Im}(f)$ *are subgroups of G and H respectively.*

Proof. First note that $f(e) = f(ee) = f(e)f(e)$, so by cancellation in H we conclude that $f(e) = e$. Then $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ for all $a \in G$. Thus $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Now let $a, b \in \mathrm{Ker}(f)$. Then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = ee^{-1} = e$, so $ab^{-1} \in \mathrm{Ker}(f)$

and $\mathrm{Ker}(f)$ is a subgroup of G. Similarly, if $f(a), f(b) \in \mathrm{Im}(f)$ then $f(a)f(b)^{-1} = f(ab^{-1}) \in \mathrm{Im}(f)$, so $\mathrm{Im}(f)$ is a subgroup of H. □

(2.6) Definition. *Let S be a subset of a group G. Then $\langle S\rangle$ denotes the intersection of all subgroups of G that contain S. The subgroup $\langle S\rangle$ is called* **the subgroup generated by** S**.** *If S is finite and $G = \langle S\rangle$ we say that G is* **finitely generated.** *If $S = \{a\}$ has only one element and $G = \langle S\rangle$ then we say that G is a* **cyclic** *group.*

(2.7) Proposition. *Let S be a nonempty subset of a group G. Then*

$$\langle S\rangle = \{a_1 a_2 \cdots a_n : n \in \mathbf{N} \text{ and } a_i \text{ or } a_i^{-1} \in S \text{ for } 1 \le i \le n\}.$$

That is, $\langle S\rangle$ is the set of all finite products consisting of elements of S or inverses of elements of S.

Proof. Let H denote the set of elements of G obtained as a finite product of elements of S or $S^{-1} = \{a^{-1} : a \in S\}$. If $a, b \in H$ then ab^{-1} is also a finite product of elements from $S \cup S^{-1}$, so $ab^{-1} \in H$. Thus H is a subgroup of G that contains S. Any subgroup K of G that contains S must be closed under multiplication by elements of $S \cup S^{-1}$, so K must contain H. Therefore, $H = \langle S\rangle$. □

(2.8) Examples. You should provide proofs (where needed) for the claims made in the following examples.

(1) The additive group $\mathbf{Z}$ is an infinite cyclic group generated by the number 1.
(2) The multiplicative group $\mathbf{Q}^*$ is generated by the set $S = \{1/p : p \text{ is a prime number}\}$.
(3) The group $\mathbf{Z}_n$ is cyclic with generator 1.
(4) The group U_n is cyclic with generator $\exp(2\pi i/n)$.
(5) The even integers are a subgroup of $\mathbf{Z}$. More generally, all the multiples of a fixed integer n form a subgroup of $\mathbf{Z}$ and we will see shortly that these are all the subgroups of $\mathbf{Z}$.
(6) If $\alpha = \left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right)$ then $H = \{e, \alpha, \alpha^2\}$ is a subgroup of the symmetric group S_3. Also, S_3 is generated by α and $\beta = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$.
(7) If $\beta = \left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix}1&2&3\\3&2&1\end{smallmatrix}\right)$ then $S_3 = \langle \beta, \gamma\rangle$.
(8) A matrix $A = [a_{ij}]$ is upper triangular if $a_{ij} = 0$ for $i > j$. The subset $T(n, \mathbf{R}) \subseteq \mathrm{GL}(n, \mathbf{R})$ of invertible upper triangular matrices is a subgroup of $\mathrm{GL}(n, \mathbf{R})$.
(9) If G is a group let $Z(G)$, called the **center of** G, be defined by

$$Z(G) = \{a \in G : ab = ba \quad \text{for all } b \in G\}.$$

Then $Z(G)$ is a subgroup of G.

(10) If G is a group and $x \in G$, then the **centralizer of** x is the subset $C(x)$ of G defined by

$$C(x) = \{a \in G : ax = xa\}.$$

$C(x)$ is a subgroup of G and $C(x) = G$ if and only if $x \in Z(G)$. Also note that $C(x)$ always contains the subgroup $\langle x \rangle$ generated by x.

(11) If G is a group and $a, b \in G$, then $[a, b] = a^{-1}b^{-1}ab$ is called the **commutator** of a and b. The subgroup G' generated by all the commutators of elements of G is called the **commutator subgroup** of G. Another common notation for the commutator subgroup is $[G, G]$. See Exercise 22 for some properties of the commutator subgroup.

(12) A convenient way to describe some groups is by giving generators and relations. Rather than giving formal definitions we shall be content to illustrate the method with two examples of groups commonly expressed by generators and relations. For the first, the **quaternion group** is a group with 8 elements. There are two generators a and b subject to the three relations (and no others):

$$a^4 = e; \qquad b^2 = a^2; \qquad b^{-1}ab = a^{-1}.$$

We leave it for the reader to check that

$$Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

For a concrete description of Q as a subgroup of $\mathrm{GL}(2, \mathbf{C})$, see Exercise 24.

(13) As our second example of a group expressed by generators and relations, the **dihedral group of order** $2n$, denoted D_{2n}, is a group generated by two elements x and y subject to the three relations (and no others):

$$x^n = e; \qquad y^2 = e; \qquad yxy^{-1} = x^{-1}.$$

Again, we leave it as an exercise to check that

$$D_{2n} = \{e, x, x^2, \ldots, x^{n-1}, y, yx, yx^2, \ldots, yx^{n-1}\}.$$

Thus, D_{2n} has $2n$ elements. The dihedral group will be presented as a group of symmetries in Section 1.6, and it will be studied in detail from the point of view of representation theory in Chapter 8.

(2.9) Definition. *The* **order** *of G, denoted $|G|$, is the cardinality of the set G. The* **order of an element** *$a \in G$, denoted $o(a)$ is the order of the subgroup generated by a. (In general, $|X|$ will denote the cardinality of the set X, with $|X| = \infty$ used to indicate an infinite set.)*

(2.10) Lemma. *Let G be a group and $a \in G$. Then*

(1) *$o(a) = \infty$ if and only if $a^n \neq e$ for any $n > 0$.*

(2) *If* $o(a) < \infty$, *then* $o(a)$ *is the smallest positive integer* n *such that* $a^n = e$.
(3) $a^k = e$ *if and only if* $o(a) \mid k$.

Proof. (1) If $a^n \neq e$ for any $n > 0$, then $a^r \neq a^s$ for any $r \neq s$ since $a^r = a^s$ implies $a^{r-s} = e = a^{s-r}$, and if $r \neq s$, then $r - s > 0$ or $s - r > 0$, which is excluded by our hypothesis. Thus, if $a^n \neq e$ for $n > 0$, then $|\langle a \rangle| = \infty$, so $o(a) = \infty$. If $a^n = e$ then let a^m be any element of $\langle a \rangle$. Writing $m = qn + r$ where $0 \leq r < n$ we see that $a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = a^r$. Thus $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $o(a) \leq n < \infty$.

(2) By part (1), if $o(a) < \infty$ then there is an $n > 0$ such that $a^n = e$ and for each such n the argument in (1) shows that $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. If we choose n as the smallest positive integer such that $a^n = e$ then we claim that the powers a^i are all distinct for $0 \leq i \leq n - 1$. Suppose that $a^i = a^j$ for $0 \leq i < j \leq n - 1$. Then $a^{j-i} = e$ and $0 < j - i < n$, contradicting the choice of n. Thus $o(a) = n =$ smallest positive integer such that $a^n = e$.

(3) Assume that $a^k = e$, let $n = o(a)$, and write $k = nq + r$ where $0 \leq r < n$. Then $e = a^k = a^{nq+r} = a^{nq}a^r = a^r$. Part (2) shows that we must have $r = 0$ so that $k = nq$. □

We will now characterize all subgroups of cyclic groups. We start with the group $\mathbf{Z}$.

(2.11) Theorem. *If* H *is a subgroup of* $\mathbf{Z}$ *then* H *consists of all the multiples of a fixed integer* m, *i.e.,* $H = \langle m \rangle$.

Proof. If $H = \{0\}$ we are done. Otherwise H contains a positive integer since H contains both n and $-n$ whenever it contains n. Let m be the least positive integer in H. Then we claim that $H = \{km : k \in \mathbf{Z}\} = \langle m \rangle$. Indeed, let $n \in H$. Then write $n = qm + r$ where $0 \leq r < m$. Since $n \in H$ and $m \in H$, it follows that $r = n - qm \in H$ because H is a subgroup of $\mathbf{Z}$. But $0 \leq r < m$ so the choice of m forces $r = 0$, otherwise r is a smaller positive integer in H than m. Hence $n = qm$ so that every element of H is a multiple of m, as required. □

We now determine all subgroups of a cyclic group G. Assume that $G = \langle a \rangle$ and let H be a subgroup of G such that $H \neq \{e\}$. If H contains a power a^{-m} with a negative exponent then it also contains the inverse a^m, which is a positive power of a. Arguing as in Theorem 2.11, let m be the smallest positive integer such that $a^m \in H$. Let a^s be an arbitrary element of H and write $s = qm + r$ where $0 \leq r < m$. Then $a^r = a^{s-qm} = a^s(a^m)^{-q} \in H$ since a^s and a^m are in H. Thus we must have $r = 0$ since $r < m$ and m is the smallest positive integer with $a^m \in H$. Therefore, $s = qm$ and $a^s = (a^m)^q$ so that all elements of H are powers of a^m.

If a is of finite order n so that $a^n = e$ then n must be divisible by m because $e = a^n \in H$ so that $n = qm$ for some q. In this case, $H =$

$\{e, a^m, a^{2m}, \ldots, a^{(q-1)m}\}$. Therefore, $|H| = q = n/m$. However, if the order of a is infinite, then $H = \{e, a^{\pm m}, a^{\pm 2m}, \ldots\} = \langle a^m \rangle$ is also infinite cyclic. Thus we have proved the following result.

(2.12) Theorem. *Any subgroup H of a cyclic group $G = \langle a \rangle$ is cyclic. Moreover, either $H = \langle e \rangle$ or $H = \langle a^m \rangle$ where m is the smallest positive power of a that is in H. If G is infinite then m is arbitrary and H is infinite cyclic. If $|G| = n$ then $m \mid n$ and $|H| = n/m$. If m is any factor of n then there is exactly one subgroup H of G of order n/m, namely, $H = \langle a^m \rangle$.*

The above theorem gives a complete description of cyclic groups and their subgroups. From this description, it is easy to see that any two cyclic groups of order n are isomorphic, as well as any two infinite cyclic groups are isomorphic. Indeed, if $G = \langle a \rangle$ and $H = \langle b \rangle$ where $|G| = |H| = n$ then define $f : G \to H$ by $f(a^m) = b^m$ for all m. One checks that f is a group isomorphism. In particular, every cyclic group of order n is isomorphic to the additive group $\mathbf{Z}_n$ of integers modulo n (see Example 1.2 (3)), and any infinite cyclic group is isomorphic to the additive group $\mathbf{Z}$.

(2.13) Definition. *Let G be a group and H a subgroup. For a fixed element $a \in G$ we define two subsets of G:*

(1) *The* **left coset** *of H in G determined by a is the set $aH = \{ah : h \in H\}$. The element a is called a representative of the left coset aH.*
(2) *The* **right coset** *of H in G determined by a is the set $Ha = \{ha : h \in H\}$. The element a is called a representative of the right coset Ha.*

Remark. Unfortunately, there is no unanimity on this definition in the mathematical world. Some authors define left and right cosets as we do; others have the definitions reversed.

A given left or right coset of H can have many different representatives. The following lemma gives a criterion for two elements to represent the same coset.

(2.14) Lemma. *Let H be a subgroup of G and let $a, b \in G$. Then*

(1) *$aH = bH$ if and only if $a^{-1}b \in H$, and*
(2) *$Ha = Hb$ if and only if $ab^{-1} \in H$.*

Proof. We give the proof of (1). Suppose $a^{-1}b \in H$ and let $b = ah$ for some $h \in H$. Then $bh' = a(hh')$ for all $h' \in H$ and $ah_1 = (ah)(h^{-1}h_1) = b(h^{-1}h_1)$ for all $h_1 \in H$. Thus $aH = bH$. Conversely, suppose $aH = bH$. Then $b = be = ah$ for some $h \in H$. Therefore, $a^{-1}b = h \in H$. □

(2.15) Theorem. *Let H be a subgroup of G. Then the left cosets (right cosets) of H form a partition of G.*

Proof. Define a relation L on G by setting $a \sim_L b$ if and only if $a^{-1}b \in H$. Note that

(1) $a \sim_L a$,
(2) $a \sim_L b$ implies $b \sim_L a$ (since $a^{-1}b \in H$ implies that $b^{-1}a = (a^{-1}b)^{-1} \in H$), and
(3) $a \sim_L b$ and $b \sim_L c$ implies $a \sim_L c$.

Thus, L is an equivalence relation on G and the equivalence classes of L, denoted $[a]_L$, partition G. (See the appendix.) That is, the equivalence classes $[a]_L$ and $[b]_L$ are identical or they do not intersect. But

$$\begin{aligned}[a]_L &= \{b \in G : a \sim_L b\} \\ &= \{b \in G : a^{-1}b \in H\} \\ &= \{b \in G : b = ah \text{ for some } h \in H\} \\ &= aH.\end{aligned}$$

Thus, the left cosets of H partition G and similarly for the right cosets. □

The function $\phi_a : H \to aH$ defined by $\phi_a(h) = ah$ is bijective by the left cancellation property. Thus, every left coset of H has the same cardinality as H, i.e., $|aH| = |H|$ for every $a \in G$. Similarly, by the right cancellation law the function $\psi_a(h) = ha$ from H to Ha is bijective so that every right coset of H also has the same cardinality as H. In particular, all right and left cosets of H have the same cardinality, namely, that of H itself.

(2.16) Definition. *If H is a subgroup of G we define the* **index of H in G,** *denoted $[G : H]$, to be the number of left cosets of H in G. The left cosets of H in G are in one-to-one correspondence with the right cosets via the correspondence $aH \leftrightarrow Ha^{-1} = (aH)^{-1}$. Therefore, $[G : H]$ is also the number of right cosets of H in G.*

(2.17) Theorem. (Lagrange) *If H is a subgroup of a finite group G, then $[G : H] = |G|/|H|$, and in particular, $|H|$ divides $|G|$.*

Proof. The left cosets of H partition G into $[G : H]$ sets, each of which has exactly $|H|$ elements. Thus, $|G| = [G : H]|H|$. □

(2.18) Corollary. *If G is a finite group and $a \in G$ then $o(a) \mid |G|$.*

Proof. □

(2.19) Corollary. *If $|G| = n$, then $a^n = e$ for all $a \in G$.*

Proof. □

(2.20) Corollary. *If $|G| = p$ where p is prime, then G is a cyclic group.*

Proof. Choose $a \in G$ with $a \neq e$ and consider the subgroup $H = \langle a \rangle$. Then $H \neq \{e\}$, and since $|H| \mid |G| = p$, it follows that $|H| = p$, so $H = G$. □

(2.21) *Remark.* The converse of Theorem 2.17 is false in the sense that if m is an integer dividing $|G|$, then there need not exist a subgroup H of G with $|H| = m$. A counterexample is given in Exercise 31. It is true, however, when m is prime. This will be proved in Theorem 4.7.

(2.22) Definition. *If G is any group, then the* **exponent** *of G is the smallest natural number n such that $a^n = e$ for all $a \in G$. If no such n exists, we say that G has infinite exponent.*

If $|G| < \infty$, then Corollaries 2.18 and 2.19 show that the exponent of G divides the order of G.

There is a simple multiplication formula relating indices for a chain of subgroups $K \subseteq H \subseteq G$.

(2.23) Proposition. *Let G be a group and H, K subgroups with $K \subseteq H$. If $[G : K] < \infty$ then*

$$[G : K] = [G : H][H : K].$$

Proof. Choose one representative a_i $(1 \leq i \leq [G : H])$ for each left coset of H in G and one representative b_j $(1 \leq j \leq [H : K])$ for each left coset of K in H. Then we claim that the set

$$\{a_i b_j : 1 \leq i \leq [G : H], \quad 1 \leq j \leq [H : K]\}$$

consists of exactly one representative from each left coset of K in G. To see this, let cK be a left coset of K in G. Then $c \in a_i H$ for a unique a_i so that $c = a_i h$. Then $h \in b_j K$ for a unique b_j so that $c = a_i b_j k$ for uniquely determined a_i, b_j k. Therefore, $cK = a_i b_j K$ for unique a_i, b_j, and we conclude that the number of left cosets of K in G is $[G : H][H : K]$. □

(2.24) *Remark.* If $|G| < \infty$ then Proposition 2.23 follows immediately from Lagrange's theorem. Indeed, in this case $[G : K] = |G|/|K| = (|G|/|H|)(|H|/|K|) = [G : H][H : K]$.

(2.25) Examples.

(1) If $G = \mathbf{Z}$ and $H = 2\mathbf{Z}$ is the subgroup of even integers, then the cosets of H consist of the even integers and the odd integers. Thus,

$[\mathbf{Z} : 2\mathbf{Z}] = 2$. Since $\mathbf{Z}$ is abelian, it is not necessary to distinguish between left and right cosets.

(2) If $G = \mathbf{Z}$ and $H = n\mathbf{Z}$, then $[\mathbf{Z} : n\mathbf{Z}] = n$ where the coset $m+H$ consists of all integers that have the same remainder as m upon division by n.

(3) Let $G = S_3 = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ where $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$ and $\beta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$. If $H = \langle\beta\rangle$, then the left cosets of H in G are

$$H = \{e, \beta\} \qquad \alpha H = \{\alpha, \alpha\beta\} \qquad \alpha^2 H = \{\alpha^2, \alpha^2\beta\},$$

while the right cosets are

$$H = \{e, \beta\} \qquad H\alpha = \{\alpha, \alpha^2\beta\} \qquad H\alpha^2 = \{\alpha^2, \alpha\beta\}.$$

Note that, in this example, left cosets are not the same as right cosets.

(4) Let $G = \mathrm{GL}(2, \mathbf{R})$ and let $H = \mathrm{SL}(2, \mathbf{R})$. Then A, $B \in \mathrm{GL}(2, \mathbf{R})$ are in the same left coset of H if and only if $A^{-1}B \in H$, which means that $\det(A^{-1}B) = 1$. This happens if and only if $\det A = \det B$. Similarly, A and B are in the same right coset of H if and only if $\det A = \det B$. Thus in this example, left cosets of H are also right cosets of H. A set of coset representatives consists of the matrices

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbf{R}^* \right\}.$$

Therefore, the set of cosets of H in G is in one-to-one correspondence with the set of nonzero real numbers.

(5) **Groups of order ≤ 5.** Let G be a group with $|G| \leq 5$. If $|G| = 1$, 2, 3, or 5 then Corollary 2.20 shows that G is cyclic. Suppose now that $|G| = 4$. Then every element $a \neq e \in G$ has order 2 or 4. If G has an element a of order 4 then $G = \langle a\rangle$ and G is cyclic. If G does not have any element of order 4 then $G = \{e, a, b, c\}$ where $a^2 = b^2 = c^2 = e$ since each nonidentity element must have order 2. Now consider the product ab. If $ab = e$ then $ab = a^2$, so $b = a$ by cancellation. But a and b are distinct elements. Similarly, ab cannot be a or b, so we must have $ab = c$. A similar argument shows that $ba = c$, $ac = b = ca$, $bc = a = cb$. Thus, G has the Cayley diagram of the Klein 4-group. Therefore, we have shown that there are exactly two nonisomorphic groups of order 4, namely, the cyclic group of order 4 and the Klein 4-group.

The left cosets of a subgroup were seen (in the proof of Theorem 2.14) to be a partition of G by describing an explicit equivalence relation on G. There are other important equivalence relations that can be defined on a group G. We will conclude this section by describing one such equivalence relation.

(2.26) Definition. *Let G be a group and let a, $b \in G$. Then a is* **conjugate** *to b if there is a $g \in G$ such that $b = gag^{-1}$. It is easy to check that conjugacy*

is an equivalence relation on G. The equivalence classes are called **conjugacy classes**. *Let $[a]_C$ denote the conjugacy class of the element $a \in G$.*

(2.27) Proposition. *Let G be a group and let $a \in G$. Then*

$$|[a]_C| = [G : C(a)]$$

where $C(a)$ is the centralizer of the element a.

Proof. Since

$$\begin{aligned} gag^{-1} = hah^{-1} &\Leftrightarrow g^{-1}h \in C(a) \\ &\Leftrightarrow gC(a) = hC(a), \end{aligned}$$

there is a bijective function $\phi : [a]_C \to G/C(a)$ defined by $\phi(gag^{-1}) = gC(a)$, which gives the result. □

(2.28) Corollary. (Class equation) *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum [G : C(a)]$$

where the sum is over a complete set of nonconjugate a not in $Z(G)$.

Proof. Since $|[a]_C| = 1$ if and only if $a \in Z(G)$, the above equation is nothing more than the partition of G into equivalence classes under conjugation, with the observation that all equivalence classes consisting of a single element have been grouped into $|Z(G)|$. □

1.3 Normal Subgroups, Isomorphism Theorems, and Automorphism Groups

If G is a group, let $\mathcal{P}^*(G)$ denote the set of all nonempty subsets of G and define a multiplication on $\mathcal{P}^*(G)$ by the formula

$$ST = \{st : s \in S, \quad t \in T\}$$

where $S, T \in \mathcal{P}^*(G)$. Since the multiplication in G is associative it follows that the multiplication in $\mathcal{P}^*(G)$ is associative, so that parentheses are not necessary in multiplications such as $STUV$. If $S = \{s\}$ then we will write sT or Ts instead of $\{s\}T$ or $T\{s\}$. In particular, if H is a subgroup of G and $a \in G$ then the left coset aH is just the product in $\mathcal{P}^*(G)$ of the subsets $\{a\}$ and H of G and there is no ambiguity in the notation aH. The subset $\{e\} \in \mathcal{P}^*(G)$ satisfies $eS = Se = S$ for all $S \in \mathcal{P}^*(G)$. Thus $\mathcal{P}^*(G)$ has an identity element for its multiplication, namely, $\{e\}$, and hence $\mathcal{P}^*(G)$ forms what is called a **monoid** (a set with an associative multiplication with an

identity element), but it is not a group except in the trivial case $G = \{e\}$ since an inverse will not exist (using the multiplication on $\mathcal{P}^*(G)$) for any subset S of G with $|S| > 1$. If $S \in \mathcal{P}^*(G)$ let $S^{-1} = \{s^{-1} : s \in S\}$. Note, however, that S^{-1} is not the inverse of S under the multiplication of $\mathcal{P}^*(G)$ except when S contains only one element. If H is a subgroup of G, then $HH = H$, and if $|H| < \infty$, then Remark 2.2 (2) implies that this equality is equivalent to H being a subgroup of G. If H is a subgroup of G then $H^{-1} = H$ since subgroups are closed under inverses.

Now consider the following question. Suppose H, $K \in \mathcal{P}^*(G)$ are subgroups of G. Then under what conditions is HK a subgroup of G? The following lemma gives one answer to this question; another answer will be provided later in this section after the concept of normal subgroup has been introduced.

(3.1) Lemma. *If H and K are subgroups of G then HK is a subgroup if and only if $HK = KH$.*

Proof. If HK is a subgroup, then HK contains all inverses of elements of HK. Thus, $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$.

Conversely, suppose that $HK = KH$. Then HK is closed under inverses since $(HK)^{-1} = KH = HK$, and it is closed under products since $(HK)(HK) = HKHK = HHKK = HK$. Thus, HK is a subgroup by Proposition 2.1. □

The equality $HK = KH$ is an equality of subsets of G; it should not be confused with element by element commutativity. In terms of elements, $HK = KH$ means that any product hk ($h \in H$, $k \in K$) can also be written k_1h_1 for some $k_1 \in K$, $h_1 \in H$. If G is abelian this is of course automatic.

We now consider the question of when the subset of $\mathcal{P}^*(G)$ consisting of all the left cosets of a subgroup H is closed under the multiplication on $\mathcal{P}^*(G)$.

(3.2) Definition. *If H is a subgroup of G then $G/H \subseteq \mathcal{P}^*(G)$ will denote the set of all left cosets of H in G. It is called the* **coset space** *of H in G.*

Consider two left cosets of H, say aH and bH. If $(aH)(bH) = cH$, then $ab \in cH$, and hence $cH = abH$. Therefore, to ask if G/H is closed under multiplication is to ask if the equation $(aH)(bH) = abH$ is true for all a, $b \in G$.

(3.3) Lemma. *If H is a subgroup of G, then $(aH)(bH) = abH$ for all a, $b \in G$ if and only if $cHc^{-1} = H$ for all $c \in G$.*

Proof. Suppose $cHc^{-1} = H$ for all $c \in G$. Then $cH = Hc$ for all $c \in G$, so

$$(aH)(bH) = a(Hb)H = a(bH)H = abHH = abH.$$

Conversely, if $(aH)(bH) = abH$ for all $a, b \in G$, then

$$cHc^{-1} \subseteq cHc^{-1}H = cc^{-1}H = H$$

for all $c \in G$. Replacing c by c^{-1} (since $c^{-1} \in G$) gives an inclusion $c^{-1}Hc \subseteq H$ and multiplying on the left by c and the right by c^{-1} gives $H \subseteq cHc^{-1}$. Hence, $cHc^{-1} = H$ for all $c \in G$. □

(3.4) Definition. *A subgroup N of G is said to be* **normal**, *denoted $N \triangleleft G$, if $aNa^{-1} = N$ for all $a \in G$.*

(3.5) *Remark.* The argument in Lemma 3.3 shows that N is normal in G if and only if $aNa^{-1} \subseteq N$ for all $a \in G$. This is frequently easier to check than the equality $aNa^{-1} = N$. Also note that Definition 3.4 is equivalent to $aN = Na$ for all $a \in G$.

(3.6) Proposition. *If $N \triangleleft G$, then the coset space $G/N \subseteq \mathcal{P}^*(G)$ forms a group under the multiplication inherited from $\mathcal{P}^*(G)$.*

Proof. By Lemma 3.3, G/N is closed under the multiplication on $\mathcal{P}^*(G)$. Since the multiplication on $\mathcal{P}^*(G)$ is already associative, it is only necessary to check the existence of an identity and inverses. But the coset $N = eN$ satisfies

$$(eN)(aN) = eaN = aN = aeN = (aN)(eN),$$

so N is an identity of G/N. Also

$$(aN)(a^{-1}N) = aa^{-1}N = eN = N = a^{-1}aN = (a^{-1}N)(aN)$$

so that $a^{-1}N$ is an inverse of aN. Therefore, the axioms for a group structure on G/N are satisfied. □

(3.7) Definition. *If $N \triangleleft G$, then G/N is called the* **quotient group** *of G by N.*

(3.8) *Remark.* If $N \triangleleft G$ and $|G| < \infty$, then Lagrange's theorem (Theorem 2.17) shows that $|G/N| = [G : N] = |G|/|N|$.

(3.9) Examples.

(1) If G is abelian, then every subgroup of G is normal.
(2) $\mathrm{SL}(n, \mathbf{R})$ is a normal subgroup of $\mathrm{GL}(n, \mathbf{R})$. Indeed, if $A \in \mathrm{GL}(n, \mathbf{R})$ and $B \in \mathrm{SL}(n, \mathbf{R})$ then

$$\det(ABA^{-1}) = (\det A)(\det B)(\det A)^{-1} = 1$$

so that $ABA^{-1} \in \mathrm{SL}(n, \mathbf{R})$ for all $A \in \mathrm{GL}(n, \mathbf{R})$ and $B \in \mathrm{SL}(n, \mathbf{R})$. The quotient group $\mathrm{GL}(n, \mathbf{R})/\mathrm{SL}(n, \mathbf{R})$ is isomorphic to $\mathbf{R}^*$, the multiplicative group of nonzero real numbers. This will follow from Theorem 3.11 (to be proved shortly) by considering the homomorphism $\det : \mathrm{GL}(n, \mathbf{R}) \to \mathbf{R}^*$. The details are left as an exercise.

(3) The subgroup $T(n, \mathbf{R})$ of upper triangular matrices is *not* a normal subgroup of $\mathrm{GL}(n, \mathbf{R})$. For example, take $n = 2$ and let $A = \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Then $ABA^{-1} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 2 \end{smallmatrix}\right] \notin T(2, \mathbf{R})$. A similar example can be constructed for any $n > 1$. Thus the set of cosets $\mathrm{GL}(n, \mathbf{R})/T(n, \mathbf{R})$ does not form a group under the operation of coset multiplication.

(4) If $\alpha = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$, then $H = \{e, \alpha, \alpha^2\}$ is a normal subgroup of the symmetric group S_3 (check it). If $\beta \notin H$ then the cosets are H and βH.

(5) Let $K = \langle \beta \rangle \subseteq S_3$ where $\beta = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$. Then the left cosets of K in G are

$$K = \{e, \alpha\} \qquad \alpha K = \{\alpha, \alpha\beta\} \qquad \alpha^2 K = \{\alpha^2, \alpha^2\beta\}$$

where α is the permutation defined in Example 3.9 (4). Then

$$K(\alpha K) = \{e, \alpha\}\{\alpha, \alpha\beta\} = \{\alpha, \alpha\beta, \alpha^2, \alpha^2\beta\} \neq \alpha K.$$

Therefore, the product of two cosets of K is not a coset of K, and in particular, K is not a normal subgroup of S_3. A straightforward calculation shows that $\alpha K \alpha^{-1} \neq K$.

(3.10) Proposition. *Let $f : G \to H$ be a group homomorphism. Then* $\mathrm{Ker}(f) \triangleleft G$.

Proof. Let $a \in G$ and $b \in \mathrm{Ker}(f)$. Then

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)ef(a)^{-1} = e$$

so $aba^{-1} \in \mathrm{Ker}(f)$ for all $b \in \mathrm{Ker}(f)$, $a \in G$ and $\mathrm{Ker}(f)$ is normal by Remark 3.5. □

In fact, Proposition 3.10 describes *all* possible normal subgroups of a group G. To see this let $N \triangleleft G$ and define a function $\pi : G \to G/N$ by the formula $\pi(a) = aN$. By the definition of multiplication on G/N we see that

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b).$$

Thus, π is a group homomorphism (called the **natural projection** or simply **natural map**) from G to G/N. Note that $\mathrm{Ker}(\pi) = N$ and therefore N is the kernel of a group homomorphism. Since N was an arbitrary normal subgroup of G, it follows that *the normal subgroups of G are precisely the kernels of all possible group homomorphisms from G to some other group.*

We now present some general results, which are commonly called the **noether isomorphism theorems**. Similar results will also be seen in the theory of rings and the theory of modules.

(3.11) Theorem. (First isomorphism theorem) *Let $f : G \to H$ be a group homomorphism with kernel K. Then $G/K \cong \mathrm{Im}(f)$ ($\cong$ means is isomorphic to).*

Proof. Define a function $\overline{f} : G/K \to \mathrm{Im}(f)$ by the formula $\overline{f}(aK) = f(a)$. The first thing that needs to be checked is that this is a well-defined function since the coset aK may also be a coset bK. It is necessary to check that $f(a) = f(b)$ in this case. But $aK = bK$ if and only if $a^{-1}b \in K$, which means that $f(a^{-1}b) = e$ or $f(a) = f(b)$. Therefore, $\overline{f}$ is a well-defined function on G/K. Also

$$\overline{f}((aK)(bK)) = \overline{f}(abK) = f(ab) = f(a)f(b) = \overline{f}(aK)\overline{f}(bK)$$

so that $\overline{f}$ is a homomorphism. $\overline{f}$ is clearly surjective and $\mathrm{Ker}(\overline{f}) = K$ which is the identity of G/K. Hence $\overline{f}$ is an isomorphism. □

Recall from Lemma 3.1 that the product HK of two subgroups H, K is a subgroup if and only if $HK = KH$. There is a simple criterion for this commutativity.

(3.12) Lemma. *Let H, K be subgroups of G. If either H or K is normal in G, then HK is a subgroup of G.*

Proof. Suppose $K \triangleleft G$. Then $aK = Ka$ for all $a \in G$. In particular, $HK = KH$, so HK is a subgroup. □

(3.13) Theorem. (Second isomorphism theorem) *Let H and N be subgroups of G with $N \triangleleft G$. Then $H/(H \cap N) \cong HN/N$.*

Proof. Let $\pi : G \to G/N$ be the natural map and let π_0 be the restriction of π to H. Then π_0 is a homomorphism with $\mathrm{Ker}(\pi_0) = H \cap N$. Thus,

$$H/(H \cap N) = H/\mathrm{Ker}(\pi_0) \cong \mathrm{Im}(\pi_0).$$

But the image of π_0 is the set of all cosets of N having representatives in H. Therefore, $\mathrm{Im}(\pi_0) = HN/N$. □

(3.14) Theorem. (Third isomorphism theorem) *Let $N \triangleleft G$, $H \triangleleft G$ and assume that $N \subseteq H$. Then*

$$G/H \cong (G/N)/(H/N).$$

Proof. Define a function $f : G/N \to G/H$ by the formula $f(aN) = aH$. It is easy to check (do it) that this is a well-defined group homomorphism. Then

$$\mathrm{Ker}(f) = \{aN : aH = H\} = \{aN : a \in H\} = H/N.$$

The result then follows from the first isomorphism theorem. □

(3.15) Theorem. (Correspondence theorem) *Let $N \triangleleft G$ and let $\pi : G \to G/N$ be the natural map. Then the function $H \mapsto H/N$ defines a one-to-one correspondence between the set of all subgroups of G containing N and the set of all subgroups of G/N. This correspondence satisfies the following properties.*

(1) *$H_1 \subseteq H_2$ if and only if $H_1/N \subseteq H_2/N$, and in this case*

$$[H_2 : H_1] = [H_2/N : H_1/N].$$

(2) *$H \triangleleft G$ if and only if $H/N \triangleleft G/N$.*

Proof. Letting

$$S_1 = \{H : H \text{ is a subgroup of } G \text{ containing } N\}$$

and

$$S_2 = \{\text{subgroups of } G/N\},$$

define $\alpha : S_1 \to S_2$ by $\alpha(H) = H/N = \mathrm{Im}(\pi|_H)$. Suppose $H_1/N = H_2/N$ where H_1, $H_2 \in S_1$. We claim that $H_1 = H_2$. Let $h_1 \in H_1$. Then $h_1N \in H_2/N$, so $h_1N = h_2N$ where $h_2 \in H_2$. Therefore, $H_1 \subseteq H_2$ and a similar argument shows that $H_2 \subseteq H_1$ so that $H_1 = H_2$. Thus α is one-to-one. If $K \in S_2$ then $\pi^{-1}(K) \in S_1$ and $\alpha(\pi^{-1}(K)) = K$ so that α is surjective. We conclude that α is a $1-1$ correspondence between S_1 and S_2.

Now consider properties (1) and (2). The fact that $H_1 \subseteq H_2$ if and only if $H_1/N \subseteq H_2/N$ is clear. To show that $[H_2 : H_1] = [H_2/N : H_2/N]$ it is necessary to show that the set of cosets aH_1 (for $a \in H_2$) is in one-to-one correspondence with the set of cosets $\overline{a}H_1/N$ (for $\overline{a} \in H_2/N$). This is left as an exercise.

Suppose $H \triangleleft G$. Then $H/N \triangleleft G/N$ since

$$(aN)(H/N)(aN)^{-1} = (aHa^{-1})/N = H/N.$$

Conversely, let H/N be a normal subgroup of G/N. Then if $\pi_1 : G/N \to (G/N)/(H/N)$ is the natural map we see that $\mathrm{Ker}(\pi_1 \circ \pi) = H$. Thus, $H \triangleleft G$. □

The following result is a simple, but useful, criterion for normality of a subgroup:

(3.16) Proposition. *Let H be a subgroup of G with $[G : H] = 2$. Then $H \triangleleft G$.*

Proof. Let $a \in G$. If $a \in H$ then certainly $aHa^{-1} = H$. If $a \notin H$ then $G = H \cup aH$ (since $[G : H] = 2$), so the left coset of H containing a is $G \setminus H$. But also $G = H \cup Ha$ (since $[G : H] = 2$), so the right coset of H containing a is $G \setminus H$. Hence, $aH = Ha$ so that $aHa^{-1} = H$ for all $a \in G$ and $H \triangleleft G$. □

(3.17) Definition. *If G is a group then an* **automorphism** *of G is a group isomorphism $\phi : G \to G$. $\mathrm{Aut}(G)$ will denote the set of all automorphisms of G. Under the operation of functional composition $\mathrm{Aut}(G)$ is a group; in fact, it is a subgroup of the symmetric group S_G on the set G (Example 1.2 (6)).*

(3.18) Examples.

(1) $\mathrm{Aut}(\mathbf{Z}) \cong \mathbf{Z}_2$. To see this let $\phi \in \mathrm{Aut}(\mathbf{Z})$. Then if $\phi(1) = r$ it follows that $\phi(m) = mr$ so that $\mathbf{Z} = \mathrm{Im}\,(\phi) = \langle r \rangle$. Therefore, r must be a generator of $\mathbf{Z}$, i.e., $r = \pm 1$. Hence $\phi(m) = m$ or $\phi(m) = -m$ for all $m \in \mathbf{Z}$.

(2) Let $G = \{(a,\, b) : a, b \in \mathbf{Z}\}$. Then $\mathrm{Aut}(G)$ is not abelian. Indeed,

$$\mathrm{Aut}(G) \cong \mathrm{GL}(2, \mathbf{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbf{Z} \quad \text{and} \quad ad - bc = \pm 1 \right\}.$$

(3) Let V be the Klein 4-group. Then $\mathrm{Aut}(V) \cong S_3$ (exercise).

(3.19) Definition. *If $a \in G$ define $I_a : G \to G$ by $I_a(b) = aba^{-1}$. Then $I_a \in \mathrm{Aut}(G)$. An automorphism of G of the form I_a for some $a \in G$ is called an* **inner automorphism** *or* **conjugation** *of G. All other automorphisms are called* **outer automorphisms** *of G. Let $\mathrm{Inn}(G)$ denote the set of all inner automorphisms of G. Define a function $\Phi : G \to \mathrm{Aut}(G)$ by $\Phi(a) = I_a$. Thus $\mathrm{Im}(\Phi) = \mathrm{Inn}(G)$.*

(3.20) Proposition. *Φ is a group homomorphism with $\mathrm{Im}(\Phi) = \mathrm{Inn}(G)$ and*

$$\mathrm{Ker}(\Phi) = Z(G).$$

Recall (Example 2.8 (9)) that $Z(G)$ denotes the center of G, i.e.,

$$Z(G) = \{a \in G : ab = ba \quad \textit{for all } b \in G\}.$$

Proof. $\Phi(ab)(c) = I_{ab}(c) = (ab)c(ab)^{-1} = a(bcb^{-1})a^{-1} = I_a(I_b(c)) = I_a \circ I_b(c)$. Thus Φ is a homomorphism, and the rest is clear. □

(3.21) Corollary. $\mathrm{Inn}(G) \cong G/Z(G)$.

Proof. □

(3.22) Example.

(1) The group S_3 has $Z(S_3) = \{e\}$ (check this). Thus $\mathrm{Inn}(S_3) \cong S_3$. Recall that $S_3 = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$ (see Example 2.8 (6)). Note that α and β satisfy $\alpha^3 = e = \beta^2$ and $\alpha\beta = \alpha^2\beta$. The elements α and α^2 have order 3 and $\beta, \alpha\beta$, and $\alpha^2\beta$ all have order 2. Thus if $\phi \in \mathrm{Aut}(S_3)$

then $\phi(\alpha) \in \{\alpha, \alpha^2\}$ and $\phi(\beta) \in \{\beta, \alpha\beta, \alpha^2\beta\}$. Since S_3 is generated by $\{\alpha, \beta\}$, the automorphism ϕ is completely determined once $\phi(\alpha)$ and $\phi(\beta)$ are specified. Thus $|\operatorname{Aut}(S_3)| \leq 6$ and we conclude that

$$\operatorname{Aut}(S_3) = \operatorname{Inn}(S_3) \cong S_3.$$

(2) If G is abelian then every nontrivial automorphism of G is an outer automorphism.

In general it is difficult to compute $\operatorname{Aut}(G)$ for a given group G. There is, however, one important special case where the computation is possible.

(3.23) Proposition. $\operatorname{Aut}(\mathbf{Z}_n) \cong \mathbf{Z}_n^*$.

Proof. Recall that $\mathbf{Z}_n^* = \{m : 1 \leq m < n \text{ and } (m, n) = 1\}$ with the operation of multiplication modulo n, and $\mathbf{Z}_n = \{m : 0 \leq m < n\} = \langle 1 \rangle$ with the operation of addition modulo n. Let $\phi \in \operatorname{Aut}(\mathbf{Z}_n)$. Since 1 is a generator of $\mathbf{Z}_n$, ϕ is completely determined by $\phi(1) = m$. Since ϕ is an isomorphism and $o(1) = n$, we must have $o(m) = o(\phi(1)) = n$. Let $d = (m, n)$, the greatest common divisor of m and n. Then $n \mid (n/d)m$, so $(n/d)m = 0$ in $\mathbf{Z}_n$. Since n is the smallest multiple of m that gives $0 \in \mathbf{Z}_n$, we must have $d = 1$, i.e., $m \in \mathbf{Z}_n^*$.

Also, any $m \in \mathbf{Z}_n^*$ determines an element $\phi_m \in \operatorname{Aut}(\mathbf{Z}_n)$ by the formula $\phi_m(r) = rm$. To see this we need to check that ϕ_m is an automorphism of $\mathbf{Z}_n$. But if $\phi_m(r) = \phi_m(s)$ then $rm = sm$ in $\mathbf{Z}_n$, which implies that $(r - s)m = 0 \in \mathbf{Z}_n$. But $(m, n) = 1$ implies that $r - s$ is a multiple of n, i.e., $r = s$ in $\mathbf{Z}_n$.

Therefore, we have a one-to-one correspondence of sets

$$\operatorname{Aut}(\mathbf{Z}_n) \longleftrightarrow \mathbf{Z}_n^*$$

given by

$$\phi_m \longleftrightarrow m.$$

Furthermore, this is an isomorphism of groups since

$$\phi_{m_1}(\phi_{m_2}(r)) = \phi_{m_1}(m_2 r) = m_1 m_2 r = \phi_{m_1 m_2}(r).$$

□

1.4 Permutation Representations and the Sylow Theorems

If X is any set, then the set $S_X = \{\text{one-to-one correspondences } f : X \to X\}$ is a group under functional composition. S_X is called the **symmetric group**

on X or group of permutations of X. A **permutation group** is a subgroup of S_X for some set X. The following theorem, due to Cayley, shows that *all* groups can be considered as permutation groups if the set X is appropriately chosen:

(4.1) Theorem. (Cayley) *Any group G is isomorphic to a subgroup of the symmetric group S_G.*

Proof. Define $\Phi : G \to S_G$ by the formula $\Phi(a)(b) = ab$. That is, $\Phi(a)$ is the function on G that multiplies each $b \in G$ by a on the left. By Proposition 1.3 (4) and (5) it follows that each $\Phi(a)$ is a bijective function on G so that $\Phi(a) \in S_G$. Also Φ is a group homomorphism since

$$\Phi(ab)(c) = (ab)c = a(bc) = \Phi(a)(bc) = \Phi(a)(\Phi(b)(c)) = (\Phi(a) \circ \Phi(b))(c).$$

Now

$$\mathrm{Ker}(\Phi) = \{a \in G : ab = b \text{ for all } \ b \in G\} = \{e\}.$$

Thus, Φ is injective, so by the first isomorphism theorem $G \cong \mathrm{Im}(\Phi) \subseteq S_G$. □

(4.2) *Remark.* The homomorphism Φ is called the **left regular representation of** G. If $|G| < \infty$ then Φ is an isomorphism only when $|G| \leq 2$ since if $|G| > 2$ then $|S_G| = |G|! > |G|$. This same observation shows that Theorem 4.1 is primarily of interest in showing that nothing is lost if one chooses to restrict consideration to permutation groups. As a practical matter, the size of S_G is so large compared to that of G that rarely is much insight gained with the use of the left regular representation of G in S_G. It does, however, suggest the possibility of looking for smaller permutation groups that might contain a copy of G. One possibility for this will be considered now.

By a **permutation representation** of G we mean any homomorphism $\phi : G \to S_X$ for some set X. The left regular representation is one such example with $X = G$. Another important example, where $|X|$ may be substantially smaller than $|G|$, is obtained by taking $X = G/H$ where H is a subgroup of G. We are not assuming that H is normal in G, so the coset space G/H is only a set, not necessarily a group. Define $\Phi_H : G \to S_{G/H}$ by the formula $\Phi_H(a)(bH) = abH$.

(4.3) Proposition. *If H is a subgroup of G then $\Phi_H : G \to S_{G/H}$ is a group homomorphism and* $\mathrm{Ker}\,(\Phi_H)$ *is the largest normal subgroup of G contained in H.*

Proof. If $abH = acH$, then $bH = cH$, so $\Phi_H(a)$ is a one-to-one function on G/H and it is surjective since $\Phi_H(a)(a^{-1}bH) = bH$. Thus, $\Phi_H(a) \in S_{G/H}$. The fact that Φ_H is a group homomorphism is the same calculation as that

used to show that Φ was a group homomorphism in the proof of Cayley's theorem. Thus, $\mathrm{Ker}(\Phi_H) \triangleleft G$ and if $a \in \mathrm{Ker}(\Phi_H)$ then $\Phi_H(a)$ acts as the identity on G/H. Thus, $aH = \Phi_H(a)(H) = H$ so that $a \in H$. Therefore, $\mathrm{Ker}(\Phi_H)$ is a normal subgroup of G contained in H. Now suppose that $N \triangleleft G$ and $N \subseteq H$. Let $a \in N$. Then $\Phi_H(a)(bH) = abH = ba'H = bH$ since $b^{-1}ab = a' \in N \subseteq H$. Therefore, $N \subseteq \mathrm{Ker}(\Phi_H)$ and $\mathrm{Ker}(\Phi_H)$ is the largest normal subgroup of G contained in H. □

As an example of the usefulness of Proposition 4.3, we will indicate how to use this result to prove the existence of normal subgroups of certain groups.

(4.4) Corollary. *Let H be a subgroup of the finite group G and assume that $|G|$ does not divide $[G : H]!$. Then there is a subgroup $N \subseteq H$ such that $N \neq \{e\}$ and $N \triangleleft G$.*

Proof. Let N be the kernel of the permutation representation Φ_H. By Proposition 4.3 N is the largest normal subgroup of G contained in H. To see that $N \neq \{e\}$, note that $G/N \cong \mathrm{Im}\,(\Phi_H)$, which is a subgroup of $S_{G/H}$. Thus,

$$|G|/|N| = |\,\mathrm{Im}\,(\Phi_H)| \,\Big|\, |S_{G/H}| = [G : H]!.$$

Since $|G|$ does not divide $[G : H]!$, we must have that $|N| > 1$ so that $N \neq \{e\}$. □

(4.5) Corollary. *Let H be a subgroup of the finite group G such that*

$$\big(|H|,\, ([G : H] - 1)!\big) = 1.$$

Then $H \triangleleft G$.

Proof. Let $N = \mathrm{Ker}(\Phi_H)$. Then $N \subseteq H$ and $G/N \cong \mathrm{Im}(\Phi_H)$ so that

$$\big(|G|/|N|\big) \,\Big|\, [G : H]! = \big(|G|/|H|\big)!.$$

Therefore,

$$\big(|G|/|H|\big) \cdot \big(|H|/|N|\big) \,\Big|\, [G : H]!$$

so that $\big(|H|/|N|\big) \mid ([G : H] - 1)!$. But $|H|$ and $([G : H] - 1)!$ have no common factors so that $|H|/|N|$ must be 1, i.e., $H = N$. □

(4.6) Corollary. *Let p be the smallest prime dividing $|G|$. Then any subgroup of G of index p is normal.*

Proof. Let H be a subgroup of G with $[G : H] = p$ and let $r = |H| = |G|/p$. Then every prime divisor of r is $\geq p$ so that

$$\big(|H|, ([G : H] - 1)!\big) = (r, (p - 1)!) = 1.$$

By Corollary 4.5, $H \triangleleft G$. □

The following result is a partial converse of Lagrange's theorem:

(4.7) Theorem. (Cauchy) *Let G be a finite group and let p be a prime dividing $|G|$. Then G has a subgroup of order p.*

Proof. If we can find an element a of order p, then $\langle a \rangle$ is the desired subgroup. To do this consider the set

$$X = \{\overline{a} = (a_0, a_1, \ldots, a_{p-1}) : a_i \in G \quad \text{and} \quad a_0 a_1 \cdots a_{p-1} = e\}.$$

Then we have a permutation representation of the group $\mathbf{Z}_p$ on X where the homomorphism $\phi : \mathbf{Z}_p \to S_X$ is given by

$$\phi(i)(\overline{a}) = \phi(i)(a_0, \ldots, a_{p-1}) = (a_i, a_{i+1}, \ldots, a_p, a_0, \ldots, a_{i-1}).$$

Note that $(a_i \cdots a_p) = (a_0 \cdots a_{i-1})^{-1}$ so that $\phi(i)(\overline{a}) \in X$.

We may define an equivalence relation on X by $\overline{a} \sim \overline{b}$ if $\phi(i)(\overline{a}) = \overline{b}$ for some i. Then X is partitioned into equivalence classes, and it is easy to see that each equivalence class consists of either exactly one or exactly p elements of X. If n_1 and n_p denote the number of equivalence classes with 1 and p elements respectively, then

$$|X| = n_1 \cdot 1 + n_p \cdot p.$$

Now X has $|G|^{p-1}$ elements (since we may choose $a_0, \ldots, a_{p-2}$ arbitrarily, and then $a_{p-1} = (a_0 \cdots a_{p-2})^{-1}$), and this number is a multiple of p. Thus we see that n_1 must be divisible by p as well. Now $n_1 \geq 1$ since there is an equivalence class $\{(e, \ldots, e)\}$. Therefore, there must be other equivalence classes with exactly one element. All of these are of the form $\{(a, \ldots, a)\}$ and by the definition of X, such an element of X gives $a \in G$ with $a^p = e$. □

(4.8) *Remark.* Note that Corollary 4.6 is a generalization of Proposition 3.15. Proposition 4.3 and its corollaries are useful in beginning a study of the structural theory of finite groups. One use of permutation representations in the structure theory of finite groups is the proof of Cauchy's theorem presented above. The next is in proving the Sylow theorems, which are substantial generalizations of Cauchy's theorem. We begin our presentation of the Sylow theorems by indicating what we mean by an action of a group on a set.

(4.9) Definition. *Let G be a group and let X be a set. By an* **action of G on X** *we mean a permutation representation $\Phi : G \to S_X$. In general, we shall write gx for $\Phi(g)(x)$. The fact that Φ is a homomorphism means that $g(hx) = (gh)x$ for all $g, h \in G$ and $x \in X$, while $ex = x$ where $e \in G$ is*

the identity. Associated to $x \in X$ there is a subset Gx of X and a subgroup $G(x)$ of G defined as follows:

(1) $Gx = \{gx : g \in G\}$ *is called the* **orbit** *of x.*
(2) $G(x) = \{g \in G : gx = x\}$ *is called the* **stabilizer** *of x.*

(4.10) Lemma. *Let the group G act on a finite set X. Then*

$$|Gx| = [G : G(x)]$$

for each $x \in G$.

Proof. Since

$$\begin{aligned} gx = hx &\Leftrightarrow g^{-1}h \in G(x) \\ &\Leftrightarrow gG(x) = hG(x), \end{aligned}$$

there is a bijective function $\phi : Gx \to G/G(x)$ defined by $\phi(gx) = gG(x)$, which gives the result. □

(4.11) Lemma. *Let the group G act on a finite set X. Then*

$$|X| = \sum [G : G(x)]$$

where the sum is over a set consisting of one representative of each orbit of G.

Proof. The orbits of G form a partition X, and hence $|X| = \sum |Gx|$ where the sum is over a set consisting of one representative of each orbit of G. The result then follows from Lemma 4.10. □

(4.12) *Remark.* Note that Lemma 4.11 generalizes the class equation (Corollary 2.28), which is the special case of Lemma 4.11 when $X = G$ and G acts on X by conjugation.

(4.13) Definition. (1) *If p is a prime, a finite group G is a* **p-group** *if $|G| = p^n$ for some $n \geq 1$.*
(2) *H is a* **p-subgroup** *of a group G if H is a subgroup of G and H is a p-group.*
(3) *Let G be an arbitrary finite group, p a prime, and p^n the highest power of p dividing $|G|$ (i.e., p^n divides $|G|$, but p^{n+1} does not). H is a* **p-Sylow subgroup** *of G if H is a subgroup of G and $|H| = p^n$.*

The three parts of the following theorem are often known as the three Sylow theorems:

(4.14) Theorem. (Sylow) *Let G be a finite group and let p be a prime dividing $|G|$.*

(1) *G has a p-Sylow subgroup, and furthermore, every p-subgroup of G is contained in some p-Sylow subgroup.*
(2) *The p-Sylow subgroups of G are all mutually conjugate.*
(3) *The number of p-Sylow subgroups of G is congruent to 1 modulo p and divides $|G|$.*

Proof. Let $m = |G|$ and write $m = p^n k$ where k is not divisible by p and $n \geq 1$. We will first prove that G has a p-Sylow subgroup by induction on m. If $m = p$ then G itself is a p-Sylow subgroup. Thus, suppose that $m > p$ and consider the class equation of G (Corollary 2.28):

$$|G| = |Z(G)| + \sum [G : C(a)] \tag{4.1}$$

where the sum is over a complete set of nonconjugate a not in $Z(G)$. There are two possibilities to consider:

(1) For some a, $[G : C(a)]$ is not divisible by p. In that case, $|C(a)| = |G|/[G : C(a)] = p^n k'$ for some k' dividing k. Then p divides $|C(a)|$ and $|C(a)| < |G|$, so by induction $C(a)$ has a subgroup H of order p^n, which is then also a p-Sylow subgroup of G.
(2) $[G : C(a)]$ is divisible by p for all $a \notin Z(G)$. Then, since $|G|$ is divisible by p, we see from Equation (4.1) that p divides $|Z(G)|$. By Cauchy's theorem (Theorem 4.7), there is an $x \in Z(G)$ of order p. Let $N = \langle x \rangle$. If $n = 1$ (i.e., p divides $|G|$, but p^2 does not) then N itself is a p-Sylow subgroup of G. Otherwise, note that since $N \subseteq Z(G)$, it follows that $N \triangleleft G$ (Exercise 21). Consider the projection map $\pi : G \to G/N$. Now $|G/N| = p^{n-1}k < |G|$, so by induction, G/N has a subgroup H with $|H| = p^{n-1}$, and then $\pi^{-1}(H)$ is a p-Sylow subgroup of G.

Thus, we have established that G has a p-Sylow subgroup P. Let X be the set of all subgroups of G conjugate to P. (Of course, any subgroup conjugate to P has the same order as P, so it is also a p-Sylow subgroup of G.) The group G acts on X by conjugation, and since all elements of X are conjugate to P, there is only one orbit. By Lemma 4.11, we have $|X| = [G : G(P)]$. But $P \subseteq G(P)$, so $[G : G(P)]$ divides k and, in particular, is not divisible by p. Thus, $|X|$ is relatively prime to p.

Now let H be an arbitrary p-subgroup of G, and consider the action of H on X by conjugation. Again by Lemma 4.11,

$$|X| = \sum [H : H(x)]. \tag{4.2}$$

Since $|X|$ is not divisible by p, some term on the right-hand side of Equation (4.2) must not be divisible by p; since H is a p-group, that can only happen if it is equal to one. Thus, there is some p-Sylow subgroup P' of G, conjugate to P, with $hP'h^{-1} = P'$ for all $h \in H$, i.e., with $HP' = P'H$. But then Lemma 3.1 implies that HP' is a subgroup of G. Since

$$|HP'| = |H||P'|/|H \cap P'|$$

(see Exercise 17), it follows that HP' is also a p-subgroup of G. Since P' is a p-Sylow subgroup, this can only happen if $HP' = P'$, i.e., if $H \subseteq P'$. Thus part (1) of the theorem is proved.

To see that (2) is true, let H itself be any p-Sylow subgroup of G. Then $H \subseteq P'$ for some conjugate P' of P, and since $|H| = |P'|$, we must have $H = P'$ so that H is conjugate to P. This gives that X consists of all the p-Sylow subgroups of G, and hence, $|X| = [G : G(P)]$ divides $|G|$. Now take $H = P$. Equation (4.2) becomes

$$|X| = \sum [P : P(x)]. \tag{4.3}$$

Then, for $x = P$, $[P : P(x)] = 1$, while if x is a representative of any other orbit, $[P : P(x)]$ is divisible by p, showing that $|X|$ is congruent to 1 modulo p. Thus part (3) is verified. □

The Sylow theorems are a major tool in analyzing the structure of finite groups. In Section 1.7, as an application of these theorems, we will classify all finite groups of order ≤ 15.

1.5 The Symmetric Group and Symmetry Groups

Recall that if $X = \{1, 2, \ldots, n\}$ then we denote S_X by S_n and we can write a typical element $\alpha \in S_n$ as a two-rowed array

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}.$$

This notation is somewhat cumbersome so we introduce a simpler notation which is frequently more useful.

(5.1) Definition. *An element $i \in X = \{1, 2, \ldots, n\}$ is fixed by $\alpha \in S_n$ if $\alpha(i) = i$. $\alpha \in S_n$ is an r-**cycle** or **cycle of length** r if there are r integers $i_1, i_2, \ldots, i_r \in X$ such that*

$$\alpha(i_1) = i_2, \qquad \alpha(i_2) = i_3, \qquad \ldots\ , \qquad \alpha(i_{r-1}) = i_r, \qquad \alpha(i_r) = i_1$$

and such that α fixes all other $i \in X$. The r-cycle α is denoted $(i_1\, i_2 \cdots i_r)$. If α is an r-cycle, note that $o(\alpha) = r$. A 2-cycle is called a **transposition**. *Two cycles $\alpha = (i_1 \cdots i_r)$ and $\beta = (j_1 \cdots j_s)$ are* **disjoint** *if*

$$\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \emptyset.$$

That is, every element moved by α is fixed by β.

As an example of the increased clarity of the cycle notation over the 2-rowed notation, consider the following permutation in S_9.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 7 & 4 & 2 & 1 & 6 & 8 & 5 \end{pmatrix}.$$

α is not a cycle, but it is a product of disjoint cycles, namely,

$$\alpha = (1\,3\,7\,6)(9\,5\,2)(4)(8).$$

Since 1-cycles represent the identity function, it is customary to omit them and write $\alpha = (1\,3\,7\,6)(9\,5\,2)$. This expression for α generally gives more information and is much cleaner than the 2-rowed notation. There are, however, two things worth pointing out concerning the cycle notation. First the cycle notation is not unique. For an r-cycle $(i_1 \cdots i_r)$ there are r different cycle notations for the same r-cycle:

$$(i_1 \cdots i_r) = (i_2\, i_3 \cdots i_r\, i_1) = \cdots = (i_r\, i_1 \cdots i_{r-1}).$$

The second observation is that the cycle notation does not make it clear which symmetric group S_n the cycle belongs to. For example, the transposition $(1\,2)$ has the same notation as an element of every S_n for $n \geq 2$.

In practice, this ambiguity is not a problem. We now prove a factorization theorem for permutations.

(5.2) Lemma. *Disjoint cycles commute.*

Proof. Suppose α and β are disjoint cycles in S_n, and let $i \in X = \{1, 2, \ldots, n\}$. If i is fixed by both α and β then $\alpha\beta(i) = i = \beta\alpha(i)$. If α moves i, then α also moves $\alpha(i)$, and thus, β fixes both of these elements. Therefore, $\alpha\beta(i) = \alpha(i) = \beta\alpha(i)$. Similarly, if β moves i then $\alpha\beta(i) = \beta(i) = \beta\alpha(i)$. □

(5.3) Theorem. *Every $\alpha \in S_n$ with $\alpha \neq e$ can be written uniquely (except for order) as a product of disjoint cycles of length ≥ 2.*

Proof. We first describe an algorithm for producing the factorization. Let k_1 be the smallest integer in $X = \{1, 2, \ldots, n\}$ that is not fixed by α (k_1 exists since $\alpha \neq e$) and then choose the smallest positive r_1 with $\alpha^{r_1}(k_1) = k_1$ (such an r_1 exists since $o(\alpha) < \infty$). Then let α_1 be the r_1-cycle

$$\alpha_1 = (k_1\, \alpha(k_1)\, \alpha^2(k_1) \cdots \alpha^{r_1-1}(k_1)).$$

Now let $X_1 = X \setminus \{k_1, \alpha(k_1), \ldots, \alpha^{r_1-1}\}$.

If every $k \in X_1$ is fixed by α then $\alpha = \alpha_1$ and we are finished. Otherwise let k_2 be the smallest integer in X_1 not fixed by α and then let r_2 be the smallest positive integer with $\alpha^{r_2}(k_2) = k_2$. Then let α_2 be the r_2-cycle

$$\alpha_2 = (k_2\, \alpha(k_2)\, \alpha^2(k_2) \cdots \alpha^{r_2-1}(k_2)).$$

It is clear from the construction that α_1 and α_2 are disjoint cycles. Continuing in this manner we eventually arrive at a factorization

$$\alpha = \alpha_1\alpha_2\cdots\alpha_s$$

of α into a product of disjoint cycles.

We now consider the question of uniqueness of the factorization. Suppose that

$$\alpha = \alpha_1\alpha_2\cdots\alpha_s = \beta_1\beta_2\cdots\beta_t$$

where each of these is a factorization of α into disjoint cycles of length ≥ 2. We must show that $s = t$ and $\alpha_i = \beta_{\phi(i)}$ for some $\phi \in S_s$. Let $m = \max\{s, t\}$. If $m = 1$ then $\alpha = \alpha_1 = \beta_1$ and uniqueness is clear. We proceed by induction on m. Suppose that $m > 1$ and let k be an element of X that is moved by α. Then some α_i and β_j must also move k. Since disjoint cycles commute, we can, without loss of generality, suppose that α_1 and β_1 move k. Since none of the other α_i or β_j move k, it follows that

$$\alpha_1^\ell(k) = \alpha^\ell(k) = \beta_1^\ell(k) \qquad \text{for all } \ell.$$

Thus, $o(\alpha_1) = o(\beta_1) = r =$ smallest r with $\alpha^r(k) = k$. Hence,

$$\alpha_1 = (k\ \alpha(k)\ \cdots\ \alpha^{r-1}(k)) = \beta_1.$$

Multiplying by α_1^{-1} gives a factorization

$$\alpha_1^{-1}\alpha = \alpha_2\cdots\alpha_s = \beta_2\cdots\beta_t,$$

and the proof is completed by induction on m. □

(5.4) Corollary. *Every $\alpha \in S_n$ is a product of transpositions.*

Proof. By Theorem 5.3, it is sufficient to factor any cycle as a product of transpositions. But

$$(i_1\, i_2\, \cdots\, i_r) = (i_1\, i_r)(i_1\, i_{r-1})\cdots(i_1\, i_2)$$

is such a factorization. □

In contrast to the uniqueness of the factorization of a permutation into disjoint cycles, writing a permutation as a product of transpositions is not very well behaved. First, the transpositions may not commute. For example, $(1\,3)(1\,2) = (1\,2\,3) \neq (1\,3\,2) = (1\,2)(1\,3)$. Second, the factorization is not uniquely determined, e.g., $(1\,2\,3) = (1\,3)(1\,2) = (1\,3)(1\,2)(2\,3)(2\,3)$. There is, however, one observation that can be made concerning this factorization; namely, the number of transpositions occurring in both factorizations is even. While we have shown only one example, this is in fact a result that is true in general. Specifically, *the number of transpositions occurring in any factorization of a permutation as a product of transpositions is always odd or always even.* This will be verified now.

If $\alpha = (i_1 \cdots i_r)$ then $\alpha = (i_1\, i_r) \cdots (i_1\, i_2)$ so that an r-cycle α can be written as a product of $(o(\alpha) - 1)$ transpositions. Hence, if $\alpha \neq e \in S_n$ is written in its cycle decomposition $\alpha = \alpha_1 \cdots \alpha_s$ then α is the product of $f(\alpha) = \sum_{i=1}^{s}(o(\alpha_i) - 1)$ transpositions. We also set $f(e) = 0$. Now suppose that

$$\alpha = (a_1\, b_1)(a_2\, b_2) \cdots (a_t\, b_t)$$

is written as an arbitrary product of transpositions. We claim that $f(\alpha) - t$ is even. To see this note that

$$(a\, i_1\, i_2 \cdots i_r\, b\, j_1 \cdots j_s)(a\, b) = (a\, j_1 \cdots j_s)(b\, i_1 \cdots i_r)$$

and (since $(a\, b)^2 = e$)

$$(a\, j_1 \cdots j_s)(b\, i_1 \cdots i_r)(a\, b) = (a\, i_1\, i_2 \cdots i_r\, b\, j_1 \cdots j_s)$$

where it is possible that no i_k or j_k is present. Hence, if a and b both occur in the same cycle in the cycle decomposition of α it follows that $f(\alpha \cdot (a\, b)) = f(\alpha) - 1$, while if they occur in different cycles or are both not moved by α then $f(\alpha \cdot (a\, b)) = f(\alpha) + 1$. In any case

$$f(\alpha \cdot (a\, b)) - f(\alpha) \equiv 1 \pmod 2.$$

Continuing this process gives

$$0 = f(e) = f(\alpha \cdot (a_1\, b_1) \cdots (a_t\, b_t)) \equiv f(\alpha) + t \pmod 2.$$

We conclude that any factorization of α into a product of t transpositions has both $f(\alpha)$ and t even or both odd, which is what we wished to verify. Because of this fact we can make the following definition.

(5.5) Definition. *A permutation $\alpha \in S_n$ is* **even** *if α can be written as a product of an even number of transpositions. α is* **odd** *if α can be written as a product of an odd number of transpositions. Define the* **sign** *of α, denoted* $\operatorname{sgn}(\alpha)$*, by*

$$\operatorname{sgn}(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is even,} \\ -1 & \text{if } \alpha \text{ is odd.} \end{cases}$$

The argument in the previous paragraph shows that a permutation cannot be both even and odd. Thus $\operatorname{sgn} : S_n \to \{1, -1\}$ *is a well-defined function, and moreover, it is a group homomorphism. The kernel of* sgn*, i.e., the set of even permutations, is a normal subgroup of S_n called the* **alternating group** *and denoted A_n.*

(5.6) *Remark.* Note that the above argument gives a method for computing $\operatorname{sgn}(\alpha)$. Namely, decompose $\alpha = \alpha_1 \cdots \alpha_s$ into a product of cycles and compute $f(\alpha) = \sum_{i=1}^{s}(o(\alpha_i) - 1)$. Then $\operatorname{sgn}(\alpha) = 1$ if $f(\alpha)$ is even and $\operatorname{sgn}(\alpha) = -1$ if $f(\alpha)$ is odd.

There is an alternative method that does not require that α be first decomposed into a product of cycles. We have defined α as a bijection of $\{1, \ldots, n\}$. Let

$$\widetilde{f}(\alpha) = |\{(i, j) : 1 \leq i < j \leq n \quad \text{and} \quad \alpha(j) < \alpha(i)\}|.$$

Then $\operatorname{sgn}(\alpha) = 1$ if $\widetilde{f}(\alpha)$ is even and $\operatorname{sgn}(\alpha) = -1$ if $\widetilde{f}(\alpha)$ is odd. We leave the proof of this as an exercise for the reader.

(5.7) Proposition. $|A_n| = n!/2$.

Proof. Since $\operatorname{sgn} : S_n \to \{1, -1\}$ is a group homomorphism, the first isomorphism theorem gives

$$S_n/A_n \cong \operatorname{Im}(\operatorname{sgn}) = \{1, -1\}.$$

Thus, $n! = |S_n| = 2|A_n|$. □

(5.8) Proposition. *If $n > 2$ then A_n is generated by all the 3-cycles in S_n.*

Proof. An element of A_n is a product of terms of the form $(i\,j)(k\,l)$ or $(i\,j)(i\,k)$ where i, j, k, l are distinct. (If $n = 3$, only the latter product is possible.) But

$$(i\,j)(i\,k) = (i\,k\,j)$$

and

$$(i\,j)(k\,l) = (i\,k\,j)(i\,k\,l)$$

so that every element of A_n is a product of 3-cycles. □

If G is a group recall (Definition 2.26) that two elements $a, b \in G$ are conjugate if $b = cac^{-1}$ for some $c \in G$. In general, it is not easy to determine if two elements of G are conjugate, but for the group S_n there is a simple criterion for conjugacy based on the cycle decomposition (factorization) of $\alpha, \beta \in S_n$. We will say that α and β have the same cycle structure if their factorizations into disjoint cycles produce the same number of r-cycles for each r.

(5.9) Proposition. (1) *If $\alpha \in S_n$ and $\beta = (i_1 \cdots i_r)$ is an r-cycle, then $\alpha\beta\alpha^{-1}$ is the r-cycle $(\alpha(i_1) \cdots \alpha(i_r))$.*

(2) *Any two r-cycles in S_n are conjugate.*

Proof. (1) If $j \notin \{\alpha(i_1), \ldots, \alpha(i_r)\}$ then $\alpha^{-1}(j)$ is fixed by β so that $\alpha\beta\alpha^{-1}(j) = j$. Also

$$\begin{aligned} \alpha\beta\alpha^{-1}(\alpha(i_1)) &= \alpha(i_2) \\ &\vdots \\ \alpha\beta\alpha^{-1}(\alpha(i_{r-1})) &= \alpha(i_r) \\ \alpha\beta\alpha^{-1}(\alpha(i_r)) &= \alpha(i_1) \end{aligned}$$

so that $\alpha\beta\alpha^{-1} = (\alpha(i_1) \cdots \alpha(i_r))$.

(2) Let $\beta = (i_1 \cdots i_r)$ and $\gamma = (j_1 \cdots j_r)$ be any two r-cycles in S_n. Define $\alpha \in S_n$ by $\alpha(i_k) = j_k$ for $1 \leq k \leq r$ and extend α to a permutation in any manner. Then by part (1) $\alpha\beta\alpha^{-1} = \gamma$. □

(5.10) Corollary. *Two permutations $\alpha, \beta \in S_n$ are conjugate if and only if they have the same cycle structure.*

Proof. Suppose that $\gamma\alpha\gamma^{-1} = \beta$. Then if $\alpha = \alpha_1 \cdots \alpha_s$ is the cycle decomposition of α, it follows from Proposition 5.9 (1) that

$$\beta = \gamma\alpha\gamma^{-1} = (\gamma\alpha_1\gamma^{-1})(\gamma\alpha_2\gamma^{-1}) \cdots (\gamma\alpha_s\gamma^{-1})$$

is the cycle decomposition of β. Thus, α and β have the same cycle structure.

The converse is analogous to the proof of Proposition 5.9 (2); it is left to the reader. □

(5.11) Example. Let $H = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \subseteq S_4$. Then H is a subgroup of S_4 isomorphic with the Klein 4-group, and since H consists of all permutations in S_4 with cycle type $(a\,b)(c\,d)$ (where a, b, c, d are all distinct), it follows from Corollary 5.10 that $H \triangleleft S_4$. Let $K = \{e, (1\,2)(3\,4)\}$. Then K is a normal subgroup of H (since H is abelian), but K is *not* normal in S_4 since any other permutation of cycle type $(a\,b)(c\,d)$ can be obtained from $(1\,2)(3\,4)$ by conjugation in S_4. Therefore, normality is not a transitive property on the set of all subgroups of a group G.

Let $X \subset \mathbf{R}^n$. By a **symmetry of** X we mean a function $f : X \to X$ such that f preserves distances, i.e., $\|x - y\| = \|f(x) - f(y)\|$ for all $x, y \in X$. The set of all symmetries of X under functional composition forms a group, called the symmetry group of X. If $X = P_n \subseteq \mathbf{R}^2$ is a regular polygon with n vertices then a symmetry is completely determined by the action on the vertices (since it is easy to see from the triangle inequality that lines must go to lines and adjacent vertices must go to adjacent vertices) so that we get a permutation representation of the symmetry group of P_n, denoted D_{2n}, as a subgroup of S_n. D_{2n} is called the **dihedral group of order** $2n$. If P_n is taken on the unit circle centered at $(0, 0)$ with one vertex at $(1, 0)$ then the symmetries of P_n are the rotations through an angle of $\theta_k = 2k\pi/n$ around $(0,\, 0)$ for $0 \leq k < n$ and the reflections through the lines from each vertex and from the midpoint of each side to the center of the circle. (There are always n such distinct lines.) Thus $|D_{2n}| = 2n$ where there are n rotations and n reflections. If we let α be the rotation through the angle θ_1 and β the reflection through the x-axis, then

$$D_{2n} = \{\alpha^i\beta^j : 0 \leq i < n, j = 0, 1\}.$$

It is easy to check that $o(\alpha) = n$ and that $\beta\alpha\beta = \alpha^{-1}$. If the vertices of P_n are numbered n, 1, 2, ..., $n-1$ counterclockwise starting at $(1, 0)$, then D_{2n} is identified as a subgroup of S_n by

$$\alpha \longleftrightarrow (1\,2\,\cdots\,n)$$

$$\beta \longleftrightarrow \begin{cases} (1\,n-1)(2\,n-2)\cdots((n-1)/2\ (n+1)/2) & \text{when } n \text{ is odd,} \\ (1\,n-1)(2\,n-2)\cdots(n/2-1\ (n/2)+1) & \text{when } n \text{ is even.} \end{cases}$$

Thus, we have arrived at a concrete representation of the dihedral group that was described by means of generators and relations in Example 2.8 (13).

(5.12) Examples.

(1) If X is the rectangle in $\mathbf{R}^2$ with vertices (0, 1), (0, 0), (2, 0), and (2, 1) labelled from 1 to 4 in the given order, then the symmetry group of X is the subgroup

$$H = \{e, (1\,3)(2\,4),\ (1\,2)(3\,4),\ (1\,4)(2\,3)\}$$

of S_4, which is isomorphic to the Klein 4-group.

(2) $D_6 \cong S_3$ since D_3 is generated as a subgroup of S_3 by the permutations $\alpha = (1\,2\,3)$ and $\beta = (2\,3)$.

(3) D_8 is a (nonnormal) subgroup of S_4 of order 8. If $\alpha = (1\,2\,3\,4)$ and $\beta = (1\,3)$ then

$$D_8 = \{e, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}.$$

There are two other subgroups of S_4 conjugate to D_8 (exercise).

1.6 Direct and Semidirect Products

(6.1) Definition. *If N and H are groups the* **(external) direct product** *of N and H, denoted $N \times H$, is the cartesian product set $N \times H$ with the multiplication defined componentwise, i.e.,*

$$(n,\, h)(n',\, h') = (nn',\, hh').$$

It is easy to check that $N \times H$ is a group with this multiplication. Associated to $N \times H$ there are some natural homomorphisms

$$\begin{aligned} \pi_N &: N \times H \to N \quad ((n,\, h) \mapsto n) \\ \pi_H &: N \times H \to H \quad ((n,\, h) \mapsto h) \\ \iota_N &: N \to N \times H \quad (n \mapsto (n, e)) \\ \iota_H &: H \to N \times H \quad (h \mapsto (e, h))\,. \end{aligned}$$

The homomorphisms π_N and π_H are called the **natural projections** while ι_N and ι_H are known as the **natural injections**. The word canonical is used interchangeably with natural when referring to projections or injections. Note the following relationships among these homomorphisms

$$\begin{aligned} \mathrm{Ker}(\pi_H) &= \mathrm{Im}(\iota_N) \\ \mathrm{Ker}(\pi_N) &= \mathrm{Im}(\iota_H) \\ \pi_H \circ \iota_H &= 1_H \\ \pi_N \circ \iota_N &= 1_N \end{aligned}$$

(1_G refers to the identity homomorphism of the group G). In particular, $N \times H$ contains a normal subgroup

$$\widetilde{N} = \mathrm{Im}(\iota_N) = \mathrm{Ker}(\pi_N) \cong N$$

and a normal subgroup

$$\widetilde{H} = \mathrm{Im}(\iota_H) = \mathrm{Ker}(\pi_N) \cong H$$

such that $\widetilde{N} \cap \widetilde{H} = \{(e, e)\}$ is the identity in $N \times H$ and $N \times H = \widetilde{N}\widetilde{H}$. Having made this observation, we make the following definition.

(6.2) Definition. *Let G be a group with subgroups N and H such that*

$$N \cap H = \{e\} \quad \textit{and} \quad NH = G.$$

(1) *If N and H are both normal, then we say that G is the* **internal direct product** *of N and H.*
(2) *If N is normal (but not necessarily H), then we say that G is the* **semidirect product** *of N and H.*

The relationship between internal and external direct products is given by the following result. We have already observed that $N \times H$ is the internal direct product of $\widetilde{N}$ and $\widetilde{H}$, which are subgroups of $N \times H$ isomorphic to N and H respectively.

(6.3) Proposition. *If G is the internal direct product of subgroups N and H, then $G \cong N \times H$.*

Proof. Let $a \in G$. Then $a = nh$ for some $n \in N,\ h \in H$. Suppose we may also write $a = n_1 h_1$ for some $n_1 \in N,\ h_1 \in H$. Then $nh = n_1 h_1$ so that $n^{-1} n_1 = h h_1^{-1} \in N \cap H = \{e\}$. Therefore, $n = n_1$ and $h = h_1$ so that the factorization $a = nh$ is unique.

Define $f : G \to N \times H$ by $f(a) = (n, h)$ where $a = nh$. This function is well defined by the previous paragraph, which also shows that f is a one-to-one correspondence. It remains to check that f is a group homomorphism.

Suppose that $a = nh$ and $b = n_1h_1$. Then $ab = nhn_1h_1$. We claim that $hn_1 = n_1h$ for all $n_1 \in N$ and $h \in H$. Indeed, $(hn_1h^{-1})n_1^{-1} \in N$ since N is normal in G and $h(n_1h^{-1}n_1^{-1}) \in H$ since H is normal. But $N \cap H = \{e\}$, so $hn_1h^{-1}n_1^{-1} \in N \cap H = \{e\}$, and thus, $hn_1 = n_1h$. Therefore,

$$f(ab) = f(nhn_1h_1) = f(nn_1hh_1) = (nn_1,\, hh_1) = (n,\, h)(n_1,\, h_1) = f(a)f(b)$$

so that f is a group homomorphism, and, hence, a group isomorphism since it is a one-to-one correspondence. □

(6.4) Examples.

(1) Recall that if G is a group then the **center** of G, denoted $Z(G)$, is the set of elements that commute with all elements of G. It is a normal subgroup of G. Now, if N and H are groups, then it is an easy exercise (do it) to show that $Z(N \times H) = Z(N) \times Z(H)$. As a consequence, one obtains the fact that *the product of abelian groups is abelian.*

(2) The group $\mathbf{Z}_2 \times \mathbf{Z}_2$ is isomorphic to the Klein 4-group. Therefore, the two nonisomorphic groups of order 4 are $\mathbf{Z}_4$ and $\mathbf{Z}_2 \times \mathbf{Z}_2$.

(3) All the hypotheses in the definition of internal direct product are necessary for the validity of Proposition 6.3. For example, let $G = S_3$, $N = A_3$, and $H = \langle(1\,2)\rangle$. Then $N \triangleleft G$ but H is not a normal subgroup of G. It is true that $G = NH$ and $N \cap H = \{e\}$, but $G \ncong N \times H$ since G is not abelian, but $N \times H$ is abelian.

(4) In the previous example S_3 is the semidirect product of $N = A_3$ and $H = \langle(1\,2)\rangle$.

(6.5) Lemma. *If G is the semidirect product of N and H then every $a \in G$ can be written uniquely as $a = nh$ where $n \in N$ and $h \in H$.*

Proof. By hypothesis, $G = NH$, so existence of the factorization is clear. Suppose $a = n_1h_1 = n_2h_2$. Then $n_2^{-1}n_1 = h_2h_1^{-1} \in N \cap H = \{e\}$. Therefore, $n_1 = n_2$ and $h_1 = h_2$. □

According to this lemma, G is set theoretically the cartesian product set $N \times H$, but the group structures are different.

If G is the semidirect product of N and H, then the second isomorphism theorem (Theorem 3.12) shows that

$$H = H/(H \cap N) \cong (HN)/N = (NH)/N = G/N.$$

Thus, H is determined once we have N. A natural question is then, given groups N and H, identify all groups G such that G is the semidirect product of subgroups $\widetilde{N}$ and $\widetilde{H}$ where $\widetilde{N} \cong N$ and $\widetilde{H} \cong H$. As one answer to this problem, we will present a construction showing how to produce all semidirect products. We start with the following definition:

(6.6) Definition. *Let N and H be groups. An* **extension of N by H** *is a group G such that*

(1) *G contains N as a normal subgroup.*
(2) *$G/N \cong H$.*

The first isomorphism theorem shows that for G to be an extension of N by H means that there is an **exact sequence** of groups and group homomorphisms

$$1 \longrightarrow N \xrightarrow{\theta} G \xrightarrow{\pi} H \longrightarrow 1.$$

In this sequence, $1 = \{e\}$ and exactness means that π is surjective, θ is injective, and $\mathrm{Ker}(\pi) = \mathrm{Im}(\theta)$.

The extension G of N by H is a **split extension** if there is a homomorphism $\alpha : H \to G$ such that $\pi \circ \alpha = 1_H$. In this case we say that the above sequence is a **split exact sequence**.

The relationship between semidirect products and extensions is given by the following result:

(6.7) Proposition. *G is a semidirect product of N and H if and only if G is a split extension of N by H.*

Proof. Suppose G is a semidirect product of N and H with $N \triangleleft G$. Define $\pi : G \to H$ by $\pi(a) = h$ where $a = nh$. Lemma 6.5 shows that π is well defined. To see that π is a homomorphism, note that $h_1 n_2 h_1^{-1} = n_2' \in N$ whenever $h_1, n_2 \in N$ (because $N \triangleleft G$). Thus,

$$\pi(n_1 h_1 n_2 h_2) = \pi(n_1 n_2' h_1 h_2) = h_1 h_2 = \pi(n_1 h_1)\pi(n_2 h_2),$$

so π is a homomorphism. It is clear that $\mathrm{Im}(\pi) = H$ and $\mathrm{Ker}(\pi) = N$. Let $\alpha : H \to G$ be the inclusion map, i.e., $\alpha(h) = h$. Then $\pi \circ \alpha(h) = h$ for all $h \in H$, so the extension determined by π is split.

Conversely, assume that G is a split extension of N by H with $\pi : G \to H$ and $\alpha : H \to G$ the homomorphisms given by the definition of split extension. Then $N = \mathrm{Ker}(\pi) \triangleleft G$ and $\widetilde{H} = \mathrm{Im}(\alpha)$ is a subgroup of G. Suppose that $a \in N \cap \widetilde{H}$. Then $\pi(a) = e$ and $a = \alpha(h)$ for some $h \in H$ so that $h = \pi(\alpha(h)) = \pi(a) = e$. Therefore, $a = \alpha(e) = e$, and we conclude that $N \cap \widetilde{H} = \{e\}$. Now let $a \in G$ and write

$$a = (a \cdot \alpha(\pi(a))^{-1}) \cdot \alpha(\pi(a)) = nh.$$

Clearly, $h \in \widetilde{H}$ and

$$\pi(n) = \pi(a \cdot \alpha(\pi(a))^{-1}) = \pi(a)\pi(\alpha(\pi(a))^{-1}) = \pi(a)\pi(a)^{-1} = e,$$

so $n \in N$. Therefore, G is a semidirect product of N and $\widetilde{H} \cong H$. □

(6.8) *Remark.* Comparing the definitions of semidirect product and direct product, we see that if G is the semidirect product of N and H with H normal (in addition to N), then G is in fact the (internal) direct product of these subgroups. Of course, in an abelian group every subgroup is normal, so for abelian groups the notion of semidirect product reduces to that of direct product. In particular, we see from Proposition 6.7 that given a *split* exact sequence of *abelian* groups

$$1 \longrightarrow N \xrightarrow{\theta} G \xrightarrow{\pi} H \longrightarrow 1$$

we have that $G \cong N \times H$.

We now consider a way to construct split extensions of N by H, which according to Proposition 6.7 is equivalent to constructing semidirect products. Let N and H be groups and let $\phi : H \to \mathrm{Aut}(N)$ be a group homomorphism. We will write $\phi_h \in \mathrm{Aut}(N)$ instead of $\phi(h)$. Then define $G = N \rtimes_\phi H = N \rtimes H$ to be the set $N \times H$ with the multiplication defined by

$$(n_1, h_1)(n_2, h_2) = (n_1\phi_{h_1}(n_2), h_1h_2).$$

We identify N and H with the subsets $N \times \{e\}$ and $\{e\} \times H$, respectively.

(6.9) Theorem. *With the above notation,*

(1) $G = N \rtimes_\phi H$ *is a group,*
(2) H *is a subgroup of* G *and* $N \triangleleft G$*,*
(3) G *is a split extension of* N *by* H*, and*
(4) $hnh^{-1} = \phi_h(n)$ *for all* $h \in H \subseteq G$ *and* $n \in N \subseteq G$*.*

Proof. (1) (e, e) is easily seen to be the identity of G. For inverses, note that

$$\begin{aligned}(\phi_{h^{-1}}(n^{-1}), h^{-1})(n, h) &= (\phi_{h^{-1}}(n^{-1}) \cdot \phi_{h^{-1}}(n), h^{-1}h) \\ &= (\phi_{h^{-1}}(e), e) = (e, e)\end{aligned}$$

and

$$\begin{aligned}(n, h)(\phi_{h^{-1}}(n^{-1}), h^{-1}) &= (n\phi_h(\phi_{h^{-1}}(n^{-1}), hh^{-1}) \\ &= (n\phi_e(n^{-1}), e) = (nn^{-1}, e) = (e, e).\end{aligned}$$

Thus, $(n, h)^{-1} = (\phi_{h^{-1}}(n^{-1}), h^{-1})$.

To check associativity, note that

$$\begin{aligned}((n_1, h_1)(n_2, h_2))(n_3, h_3) &= (n_1\phi_{h_1}(n_2), h_1h_2)(n_3, h_3) \\ &= (n_1\phi_{h_1}(n_2)\phi_{h_1h_2}(n_3), h_1h_2h_3) \\ &= (n_1\phi_{h_1}(n_2)\phi_{h_1}(\phi_{h_2}(n_3)), h_1h_2h_3) \\ &= (n_1\phi_{h_1}(n_2\phi_{h_2}(n_3)), h_1h_2h_3) \\ &= (n_1, h_1)(n_2\phi_{h_2}(n_3), h_2h_3) \\ &= (n_1, h_1)((n_2, h_2)(n_3, h_3)).\end{aligned}$$

(2) It is clear from the definition that N and H are subgroups of G. Let $\pi : N \rtimes_\phi H \to H$ be defined by $\phi(n,h) = h$. Then π is a group homomorphism since $\pi((n_1,h_1)(n_2,h_2)) = \pi(n_1\phi_{h_1}(n_2), h_1h_2) = h_1h_2 = \pi(n_1,h_1)\pi(n_2,h_2)$ and $N = \mathrm{Ker}(\pi)$, so $N \lhd G$.

(3) Let $\alpha : H \to G$ be defined by $\alpha(h) = (e,h)$. Then α is a homomorphism and $\pi \circ \alpha = 1_H$.

(4)

$$\begin{aligned}(e,h)(n,e)(e,h)^{-1} &= (e,h)(n,e)(e,h^{-1}) \\ &= (\phi_h(n),h)(e,h^{-1}) \\ &= (\phi_h(n)\phi_h(e), hh^{-1}) \\ &= (\phi_h(n),e).\end{aligned}$$

□

(6.10) Examples.

(1) Let $\phi : H \to \mathrm{Aut}(N)$ be defined by $\phi(h) = 1_N$ for all $h \in H$. Then $N \rtimes_\phi H$ is just the direct product of N and H.

(2) If $\phi : \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_n)$ is defined by $1 \mapsto \phi_1(a) = -a$ where $\mathbf{Z}_2 = \{0,1\}$, then $\mathbf{Z}_n \rtimes_\phi \mathbf{Z}_2 \cong D_n$.

(3) The construction in Example (2) works for any abelian group A in place of $\mathbf{Z}_n$ and gives a group $A \rtimes_\phi \mathbf{Z}_2$. Note that $A \rtimes_\phi \mathbf{Z}_2 \ncong A \times \mathbf{Z}_2$ unless $a^2 = e$ for all $a \in A$.

(4) $\mathbf{Z}_{p^2}$ is a nonsplit extension of $\mathbf{Z}_p$ by $\mathbf{Z}_p$. Indeed, define $\pi : \mathbf{Z}_{p^2} \to \mathbf{Z}_p$ by $\pi(r) = r \pmod p$. Then $\mathrm{Ker}(\pi)$ is the unique subgroup of $\mathbf{Z}_{p^2}$ of order p, i.e., $\mathrm{Ker}(\pi) = \langle p \rangle \subseteq \mathbf{Z}_{p^2}$. But then any nonzero homomorphism $\alpha : \mathbf{Z}_p \to \mathbf{Z}_{p^2}$ must have $|\mathrm{Im}(\alpha)| = p$ and, since there is only one subgroup of $\mathbf{Z}_{p^2}$ of order p, it follows that $\mathrm{Im}(\alpha) = \mathrm{Ker}(\pi)$. Therefore, $\pi \circ \alpha = 0 \neq 1_{\mathbf{Z}_p}$ so that the extension is nonsplit.

(6.11) *Remark.* Note that *all* semidirect products arise via the construction of Theorem 6.9 as follows. Suppose $G = NH$ is a semidirect product. Define $\phi : H \to \mathrm{Aut}(N)$ by $\phi_h(n) = hnh^{-1}$. Then the map $\Phi : G \to N \rtimes_\phi H$, defined by $\Phi(nh) = (n,h)$, is easily seen to be an isomorphism. Note that Φ is well defined by Lemma 6.5 and is a homomorphism by Theorem 6.9 (4).

1.7 Groups of Low Order

This section will illustrate the group theoretic techniques introduced in this chapter by producing a list (up to isomorphism) of all groups of order at most 15. The basic approach will be to consider the prime factorization of

$|G|$ and study groups with particularly simple prime factorizations for their order. First note that groups of prime order are cyclic (Corollary 2.20) so that every group of order 2, 3, 5, 7, 11, or 13 is cyclic. Next we consider groups of order p^2 and pq where p and q are distinct primes.

(7.1) Proposition. *If p is a prime and G is a group of order p^2, then $G \cong \mathbf{Z}_{p^2}$ or $G \cong \mathbf{Z}_p \times \mathbf{Z}_p$.*

Proof. If G has an element of order p^2, then $G \cong \mathbf{Z}_{p^2}$. Assume not. Let $e \neq a \in G$. Then $o(a) = p$. Set $N = \langle a \rangle$. Let $b \in G$ with $b \notin N$, and set $H = \langle b \rangle$. Then $N \cong \mathbf{Z}_p$ and $H \cong \mathbf{Z}_p$, and by Corollary 4.6, $N \triangleleft G$ and $H \triangleleft G$; so

$$G \cong N \times H \cong \mathbf{Z}_p \times \mathbf{Z}_p$$

by Proposition 6.3. □

(7.2) Proposition. *Let p and q be primes such that $p > q$ and let G be a group of order pq.*

(1) *If q does not divide $p - 1$, then $G \cong \mathbf{Z}_{pq}$.*
(2) *If $q \mid p - 1$, then $G \cong \mathbf{Z}_{pq}$ or $G \cong \mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q$ where*

$$\phi : \mathbf{Z}_q \to \mathrm{Aut}(\mathbf{Z}_p) \cong \mathbf{Z}_p^*$$

is a nontrivial homomorphism. All nontrivial homomorphisms produce isomorphic groups.

Proof. By Cauchy's theorem (Theorem 4.7) G has a subgroup N of order p and a subgroup H of order p, both of which are necessarily cyclic. Then $N \triangleleft G$ since $[G : N] = q$ and q is the smallest prime dividing $|G|$ (Corollary 4.6). Since it is clear that $N \cap H = \langle e \rangle$ and $NH = G$, it follows that G is the semidirect product of N and H.

The map $\phi : H \to \mathrm{Aut}(N)$ given by $\phi_h(n) = hnh^{-1}$ is a group homomorphism, so if q does not divide $|\mathrm{Aut}(N)| = |\mathrm{Aut}(\mathbf{Z}_p)| = |\mathbf{Z}_p^*| = p - 1$, then ϕ is the trivial homomorphism. Hence $\phi_h = 1_N$ for all $h \in H$, i.e., $nh = hn$ for all $h \in H$, $n \in N$. Hence $H \triangleleft G$ and $G \cong \mathbf{Z}_p \times \mathbf{Z}_q \cong \mathbf{Z}_{pq}$ (see Exercise 11). If $q \mid p - 1$ then there are nontrivial homomorphisms

$$\phi : \mathbf{Z}_q \to \mathrm{Aut}(N) \cong \mathbf{Z}_p^*$$

and for some homomorphism ϕ,

$$G \cong \mathbf{Z}_p \rtimes_\phi \mathbf{Z}_q.$$

Therefore, if $N = \langle a \rangle$ and $H = \langle b \rangle$, then $G = \langle a, b \rangle$, subject to the relations

$$a^p = e, \qquad b^q = e, \qquad b^{-1}ab = a^r$$

where $r^q \equiv 1 \pmod{p}$. If $r = 1$ then ϕ is trivial, H is normal, and $G \cong \mathbf{Z}_p \times \mathbf{Z}_q$. Otherwise, G is nonabelian. We leave it as an exercise to verify

that all choices of $r \neq 1$ produce isomorphic groups. Thus, if $q \mid p-1$, then there are exactly two nonisomorphic groups of order pq. □

(7.3) Corollary. *If $|G| = 2p$, where p is an odd prime, then $G \cong \mathbf{Z}_{2p}$ or $G \cong D_{2p}$.*

Proof. The only nontrivial homomorphism $\phi : \mathbf{Z}_2 \to \mathrm{Aut}(\mathbf{Z}_p) = \mathbf{Z}_p^*$ is the homomorphism $1 \mapsto \phi_1$ with $\phi_1(a) = -a$. Apply Example 6.10 (2). □

(7.4) *Remark.* The results obtained so far completely describe all groups of order ≤ 15, except for groups of order 8 and 12. We shall analyze each of these two cases separately.

Groups of Order 8

We will consider first the case of abelian groups of order 8.

(7.5) Proposition. *If G is an abelian group of order 8, then G is isomorphic to exactly one of the following groups:*

(1) $\mathbf{Z}_8$,
(2) $\mathbf{Z}_4 \times \mathbf{Z}_2$, *or*
(3) $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

Proof. Case 1: Suppose that G has an element of order 8. Then G is cyclic and, hence, isomorphic to $\mathbf{Z}_8$.

Case 2: Suppose every element of G has order 2. Let $\{a, b, c\} \subseteq G \setminus \{e\}$ with $c \neq ab$. Then $H = \langle a, b\rangle$ is a subgroup of G isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$. Furthermore, $H \cap \langle c\rangle = \langle e\rangle$ and $H\langle c\rangle = G$ so that

$$G \cong H \times \langle c\rangle \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Case 3: If G does not come under Case 1 or Case 2, then G is not cyclic and not every element has order 2. Therefore, G has an element a of order 4. We claim that there is an element $b \notin \langle a\rangle$ such that $b^2 = e$. To see this, let c be any element not in $\langle a\rangle$. If $c^2 = e$, take $b = c$. Otherwise, we must have $o(c) = 4$. Since $|G/\langle a\rangle| = 2$, it follows that $c^2 \in \langle a\rangle$. Since a^2 is the only element of $\langle a\rangle$ of order 2, it follows that $c^2 = a^2$. Let $b = ac$. Then

$$b^2 = a^2c^2 = a^4 = e.$$

Proposition 6.3 then shows that

$$G \cong \langle a\rangle \times \langle b\rangle \cong \mathbf{Z}_4 \times \mathbf{Z}_2.$$

Since every abelian group of order 8 is covered by Case 1, Case 2, or Case 3, the proof is complete. □

Now consider the case of nonabelian groups of order 8.

(7.6) Proposition. *If G is a nonabelian group of order 8, then G is isomorphic to exactly one of the following two groups:*

(1) Q = *the quaternion group, or*
(2) D_8 = *the dihedral group of order 8.*

Proof. Since G is not abelian, it is not cyclic so G does not have an element of order 8. Similarly, if $a^2 = e$ for all $a \in G$, then G is abelian (Exercise 8); therefore, there is an element $a \in G$ of order 4. Let b be an element of G not in $\langle a \rangle$. Since $[G : \langle a \rangle] = 2$, the subgroup $\langle a \rangle \triangleleft G$. But $|G/\langle a \rangle| = 2$ so that $b^2 \in \langle a \rangle$. Since $o(b)$ is 2 or 4, we must have $b^2 = e$ or $b^2 = a^2$. Since $\langle a \rangle \triangleleft G$, $b^{-1}ab$ is in $\langle a \rangle$ and has order 4. Since G is not abelian, it follows that $b^{-1}ab = a^3$. Therefore, G has two generators a and b subject to one of the following sets of relations:

(1) $a^4 = e, \quad b^2 = e, \quad b^{-1}ab = a^3;$
(2) $a^4 = e, \quad b^2 = a^2, \quad b^{-1}ab = a^3.$

In case (1), G is isomorphic to D_8, while in case (2) G is isomorphic to Q. We leave it as an exercise to check that Q and D_8 are not isomorphic. □

(7.7) *Remarks.* (1) Propositions 7.5 and 7.6 together show that there are precisely 5 distinct isomorphism classes of groups of order 8; 3 are abelian and 2 are nonabelian.

(2) D_8 is a semidirect product of $\mathbf{Z}_4$ and $\mathbf{Z}_2$ as was observed in Example 6.10 (2). However, Q is a nonsplit extension of $\mathbf{Z}_2$ by $\mathbf{Z}_2 \times \mathbf{Z}_2$. In fact Q is not a semidirect product of proper subgroups.

Groups of Order 12

To classify groups of order 12, we start with the following result.

(7.8) Proposition. *Let G be a group of order p^2q where p and q are distinct primes. Then G is the semidirect product of a p-Sylow subgroup H and a q-Sylow subgroup K.*

Proof. If $p > q$ then $H \triangleleft G$ by Corollary 4.6.

If $q > p$ then $1 + kq \mid p^2$ for some $k \geq 0$. Since $q > p$, this can only occur if $k = 0$ or $1 + kq = p^2$. The latter case forces q to divide $p^2 - 1 = (p+1)(p-1)$. Since $q > p$, we must have $q = p+1$. This can happen only if $p = 2$ and $q = 3$. Therefore, in the case $q > p$, the q-Sylow subgroup K is a normal subgroup of G, except possibly when $|G| = 2^2 \cdot 3 = 12$.

To analyze this case, let K be a 3-Sylow subgroup of a group G of order 12. If K is not normal in G, then the number of 3-Sylow subgroups of G is 4. Let these 3-Sylow subgroups be K_1, K_2, K_3, and K_4. Then $K_1 \cup K_2 \cup K_3 \cup K_4$ accounts for 9 distinct elements of G.

The remaining elements, together with the identity e, must form the 2-Sylow subgroup H of G. Hence, we must have $H \lhd G$.

Therefore, we have shown that at least one of H (a p-Sylow subgroup of G) or K (a q-Sylow subgroup of G) is normal in G. Since it is clear that $H \cap K = \langle e \rangle$ and $HK = G$, it follows that G is a semidirect product of H and K. □

(7.9) Proposition. *A nonabelian group G of order 12 is isomorphic to exactly one of the following groups:*

(1) A_4,
(2) D_{12}, *or*
(3) $T = \mathbf{Z}_3 \rtimes_\phi \mathbf{Z}_4$ *where* $\phi : \mathbf{Z}_4 \to \mathrm{Aut}(\mathbf{Z}_3) \cong \mathbf{Z}_2$ *is the nontrivial homomorphism.*

Proof. Let H be a 2-Sylow subgroup and K a 3-Sylow subgroup of G. By Proposition 7.8 and the fact that G is nonabelian, exactly one of H and K is normal in G.

Case 1: Suppose $H \lhd G$. Then K is not normal in G. Since $[G : K] = 4$, there is a permutation representation $\Phi_K : G \to S_4$. By Proposition 4.3, $\mathrm{Ker}(\Phi_K)$ is the largest normal subgroup of G contained in K. Since K has prime order and is not normal, it follows that G is injective so that

$$G \cong \mathrm{Im}(\Phi_K) \subseteq S_4.$$

It is an easy exercise to show that A_4 is the only subgroup of S_4 of order 12; therefore, $G \cong A_4$ if the 2-Sylow subgroup is normal in G.

Case 2: Suppose $K \lhd G$ and $H \cong \mathbf{Z}_4$. In this case

$$G \cong \mathbf{Z}_3 \rtimes_\phi \mathbf{Z}_4$$

where $\phi : \mathbf{Z}_4 \to \mathrm{Aut}(K)$ is a nontrivial homomorphism, but the only nontrivial automorphism of $\mathbf{Z}_3$ is $a \mapsto a^{-1}$ where $K = \langle a \rangle$. In this case $G \cong T$.

Case 3: Suppose $K \lhd G$ and $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$. Let $K = \langle a \rangle$ and let

$$\phi : H \to \mathrm{Aut}(K) \cong \mathbf{Z}_2$$

be the conjugation homomorphism. Then $H \cong (\mathrm{Ker}(\phi)) \times \mathbf{Z}_2$, so let $\mathrm{Ker}(\phi) = \langle c \rangle$ and let $d \in H$ with $\phi(d) \neq 1_K$. Then $c^{-1}ac = a$ and $d^{-1}ad = a^{-1} = a^2$. Let $b = ac$. Then $o(b) = 6$, $d \notin \langle b \rangle$, and

$$d^{-1}bd = d^{-1}acd = d^{-1}adc = a^2c = (ac)^{-1} = b^{-1}.$$

Thus, $G \cong D_{12}$. □

It remains to consider the case of abelian groups of order 12.

(7.10) Proposition. *If G is an abelian group of order 12, then G is isomorphic to exactly one of the following groups:*

(1) $\mathbf{Z}_{12}$, *or*
(2) $\mathbf{Z}_2 \times \mathbf{Z}_6$.

Proof. Exercise. □

By combining the results of this section we arrive at the following table of distinct groups of order at most 15. That is, every group of order ≤ 15 is isomorphic to exactly one group in this table.

Table 7.1. Groups of order ≤ 15

Order	Abelian Groups	Nonabelian Groups	Total Number
1	$\{e\}$		1
2	$\mathbf{Z}_2$		1
3	$\mathbf{Z}_3$		1
4	$\mathbf{Z}_4$		2
	$\mathbf{Z}_2 \times \mathbf{Z}_2$		
5	$\mathbf{Z}_5$		1
6	$\mathbf{Z}_6$	S_3	2
7	$\mathbf{Z}_7$		1
8	$\mathbf{Z}_8$	Q	5
	$\mathbf{Z}_4 \times \mathbf{Z}_2$	D_8	
	$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$		
9	$\mathbf{Z}_9$		2
	$\mathbf{Z}_3 \times \mathbf{Z}_3$		
10	$\mathbf{Z}_{10}$	D_{10}	2
11	$\mathbf{Z}_{11}$		1
12	$\mathbf{Z}_{12}$	A_4	5
	$\mathbf{Z}_2 \times \mathbf{Z}_6$	D_{12}	
		$\mathbf{Z}_3 \rtimes_\phi \mathbf{Z}_4$	
13	$\mathbf{Z}_{13}$		1
14	$\mathbf{Z}_{14}$	D_{14}	2
15	$\mathbf{Z}_{15}$		1

1.8 Exercises

1. Prove that $\mathbf{Z}_n^*$ is a group. (See Example 1.2 (5).)
2. Prove that $\mathcal{P}(X)$ (Example 1.2 (8)) with the symmetric difference operation is a group.
3. Write the Cayley diagram for the group S_3.
4. Write the Cayley diagram for the group $\mathbf{Z}_{12}^*$.
5. Let G be a group, $g \in G$, and define a new multiplication $\cdot$ on G by the formula $a \cdot b = agb$ for all $a, b \in G$. Prove that G with the multiplication $\cdot$ is a group. What is the identity of G under $\cdot$? If $a \in G$ what is the inverse of a under $\cdot$?
6. Suppose that G is a set and $\cdot$ is an associative binary operation on G such that there is an element $e \in G$ with $e \cdot a = a$ for all $a \in G$ and such that for each $a \in G$ there is an element $b \in G$ with $b \cdot a = e$. Prove that $(G, \cdot)$ is a group. The point of this exercise is that it is sufficient to assume associativity, a left identity, and left inverses in order to have a group. Similarly, left can be replaced with right in the hypotheses.
7. Prove that $\mathbf{R}^* \times \mathbf{R}$ is a group under the multiplication defined by
$$(a,\, b)(c,\, d) = (ac,\, ad + b).$$
Is this group abelian?
8. Prove that if $a^2 = e$ for all a in a group G, then G is abelian.
9. Let $V \subseteq \mathrm{GL}(2, \mathbf{R})$ be the set
$$V = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$
Prove that V is a subgroup of $\mathrm{GL}(2, \mathbf{R})$ that is isomorphic to the Klein 4-group.
10. For fixed positive integers b_0, m_0, and n_0 consider the subset $S \subset \mathrm{GL}(3, \mathbf{Z})$ defined by
$$S = \left\{ \begin{bmatrix} 1 & m & n \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} : m_0 \mid m,\ n_0 \mid n,\ b_0 \mid b \right\}.$$
When is S a subgroup? The notation $a \mid b$ for integers a and b means that a divides b.
11. Let G be a group and let $a, b \in G$ be elements such that $ab = ba$.
    (a) Prove that $o(ab) \mid o(a)o(b)$.
    (b) If $ab = ba$ and $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$, show that
    $$o(ab) = \mathrm{lcm}\{o(a),\, o(b)\}.$$
    ($\mathrm{lcm}\{n,\, m\}$ refers to the least common multiple of the integers n and m.)
    (c) If $ab = ba$ and $o(a)$ and $o(b)$ are relatively prime, then $o(ab) = o(a)o(b)$.
    (d) Give a counterexample to show that these results are false if we do not assume commutativity of a and b.
12. If $\sigma : G \to H$ is a group homomorphism then $o(\sigma(a)) \mid o(a)$ for all $a \in G$ with $o(a) < \infty$. If σ is an isomorphism then $o(\sigma(a)) = o(a)$.
13. (a) A group G is abelian if and only if the function $f : G \to G$ defined by $f(a) = a^{-1}$ is a group homomorphism.

(b) A group G is abelian if and only if the function $g : G \to G$ defined by $g(a) = a^2$ is a group homomorphism.

14. Let G be the multiplicative group of positive real numbers and let H be the additive group of all reals. Prove that $G \cong H$. (Hint: Remember the properties of the logarithm function.)
15. Write all the subgroups of S_3.
16. Let G be a group and let H_1, H_2 be subgroups of G. Prove that $H_1 \cup H_2$ is a subgroup of G if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. Is the analogous result true for three subgroups H_1, H_2, H_3?
17. If G is a finite group and H and K are subgroups, prove that

$$|H||K| = |H \cap K||HK|.$$

18. Prove that the intersection of two subgroups of finite index is a subgroup of finite index. Prove that the intersection of finitely many subgroups of finite index is a subgroup of finite index.
19. Let X be a finite set and let $Y \subseteq X$. Let G be the symmetric group S_X and define H and K by

$$H = \{f \in G : f(y) = y \text{ for all } y \in Y\}$$
$$K = \{f \in G : f(y) \in Y \text{ for all } \ y \in Y\}.$$

If $|X| = n$ and $|Y| = m$ compute $[G : H]$, $[G : K]$, and $[K : H]$.

20. If G is a group let $Z(G) = \{a \in G : ab = ba \text{ for all } b \in G\}$. Then prove that $Z(G)$ is an abelian subgroup of G. $Z(G)$ is called the *center* of G. If $G = GL(n, \mathbf{R})$ show that

$$Z(G) = \{aI_n : a \in \mathbf{R}^*\}.$$

21. Let G be a group and let $H \subseteq Z(G)$ be a subgroup of the center of G. Prove that $H \triangleleft G$.
22. (a) If G is a group, prove that the commutator subgroup G' is a normal subgroup of G, and show that G/G' is abelian.
    (b) If H is any normal subgroup of G such that G/H is abelian, show that $G' \subseteq H$.
23. If G is a group of order $2n$ show that the number of elements of G of order 2 is odd.
24. Let Q be the multiplicative subgroup of GL(2, $\mathbf{C}$) generated by

$$A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

    (a) Show that A and B satisfy the relations $A^4 = I, A^2 = B^2, B^{-1}AB = A^{-1}$. (Thus, Q is a concrete representation of the quaternion group.)
    (b) Prove that $|Q| = 8$ and list all the elements of Q in terms of A and B.
    (c) Compute $Z(Q)$ and prove that $Q/Z(Q)$ is abelian.
    (d) Prove that every subgroup of Q is normal.
25. Let n be a fixed positive integer. Suppose a group G has exactly one subgroup H of order n. Prove that $H \triangleleft G$.
26. Let $H \triangleleft G$ and assume that G/H is abelian. Show that every subgroup $K \subseteq G$ containing H is normal.
27. Let G_n be the multiplicative subgroup of GL(2, $\mathbf{C}$) generated by

$$A = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

where $\zeta = \exp(2\pi i/n)$. Verify that G_n is isomorphic to the dihedral group D_{2n}. (See Example 2.8 (13).)

28. Let G be a group of order n. If G is generated by two elements of order 2, show that $G \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ if $n = 4$ and $G \cong D_n$ if $n > 4$.

29. Let G be a nonabelian group of order 6. Prove that $G \cong S_3$.

30. (a) If $H \triangleleft G$ and $[G : H] = n$, then show that $a^n \in H$ for all $a \in G$.
(b) Show that the result in part (a) is false if H is not normal in G.

31. Show that the alternating group A_4 of order 12 does not have a subgroup of order 6. (Hint: Find at least 8 elements of A_4 that are squares, and apply Exercise 30.)

32. Recall (Definition 4.13) that a group G is called a p-group if $|G| = p^n$ for some integer $n \geq 1$.
(a) If G is a p-group, show that $Z(G) \neq \langle e \rangle$. (Hint: Use the class equation (Corollary 2.28).)
(b) If $|G| = p^n$, show that G has a subgroup of order p^m for every $0 \leq m \leq n$.

33. Let $G = \left\{ \left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right] \in \mathrm{GL}(2, \mathbf{R}) \right\}$. Prove that G is a subgroup of $\mathrm{GL}(2, \mathbf{R})$ and that G is isomorphic to the group $\mathbf{R}^* \times \mathbf{R}$ with the multiplication defined in Exercise 7.

34. (a) Find all homomorphisms $\phi : \mathbf{Z} \to \mathbf{Z}_n$.
(b) Find all homomorphisms $\phi : \mathbf{Z}_7 \to \mathbf{Z}_{16}$.
(c) What is a condition on finite cyclic groups G and H that ensures there is a homomorphism $\phi : G \to H$ other than the zero homomorphism?

35. Let $\mathrm{Hom}(\mathbf{Z}_n, \mathbf{Z}_m)$ be the set of all group homomorphisms from $\mathbf{Z}_n$ to $\mathbf{Z}_m$. Let d be the greatest common divisor of m and n. Show that $|\mathrm{Hom}(\mathbf{Z}_n, \mathbf{Z}_m)| = d$.

36. If n is odd, show that $D_{4n} \cong D_{2n} \times \mathbf{Z}_2$.

37. Write the class equations (Corollary 2.28) for the quaternion group Q and the dihedral group D_8.

38. Verify that the alternating group A_5 has no nontrivial normal subgroups. (Hint: The class equation.) (The trivial subgroups of a group G are $\{e\}$ and G.) A group with no nontrivial normal subgroups is called **simple**. It is known that A_n is simple for all $n \neq 4$.

39. Suppose that G is an abelian group of order n. If $m \mid n$ show that G has a subgroup of order m. Compare this result with Exercise 31.

40. (a) Write each of the following permutations as a product of disjoint cycles:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 6 & 5 & 7 & 4 & 2 \end{pmatrix}$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 1 \end{pmatrix}$$
$$\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 8 & 9 & 2 & 1 & 4 & 3 & 6 & 7 \end{pmatrix}.$$

(b) Let $\sigma \in S_{10}$ be the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 4 & 1 & 7 & 10 & 2 & 6 & 9 & 8 \end{pmatrix}.$$

Compute $o(\sigma)$ and calculate σ^{100}.

41. Let $H \subseteq S_n$ be defined by $H = \{f \in S_n : f(1) = 1\}$. Prove that H is a subgroup of S_n that is isomorphic to S_{n-1}. Is $H \triangleleft S_n$?

42. (a) Prove that an $r-$cycle is even (odd) if and only if r is odd (even).

(b) Prove that a permutation σ is even if and only if there are an even number of even order cycles in the cycle decomposition of σ.

43. Show that if a subgroup G of S_n contains an odd permutation then G has a normal subgroup H with $[G : H] = 2$.

44. For $\alpha \in S_n$, let

$$\widetilde{f}(\alpha) = |\{(i, j) : 1 \leq i < j \quad \text{and} \quad \alpha(j) < \alpha(i)\}|.$$

(For example, if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} \in S_5,$$

then $\widetilde{f}(\alpha) = 5$.) Show that $\operatorname{sgn}(\alpha) = 1$ if $\widetilde{f}(\alpha)$ is even and $\operatorname{sgn}(\alpha) = -1$ if $\widetilde{f}(\alpha)$ is odd. Thus, $\widetilde{f}$ provides a method of determining if a permutation is even or odd without the factorization into disjoint cycles.

45. (a) Prove that S_n is generated by the transpositions $(1\,2)$, $(1\,3)$, ..., $(1\,n)$.
(b) Prove that S_n is generated by $(1\,2)$ and $(1\,2\,\cdots\,n)$.

46. In the group S_4 compute the number of permutations conjugate to each of the following permutations: $e = (1)$, $\alpha = (1\,2)$, $\beta = (1\,2\,3)$, $\gamma = (1\,2\,3\,4)$, and $\delta = (1\,2)(3\,4)$.

47. (a) Find all the subgroups of the dihedral group D_8.
(b) Show that D_8 is not isomorphic to the quaternion group Q. Note, however, that both groups are nonabelian groups of order 8. (Hint: Count the number of elements of order 2 in each group.)

48. Construct two nonisomorphic nonabelian groups of order p^3 where p is an odd prime.

49. Show that any group of order 312 has a nontrivial normal subgroup.

50. Show that any group of order 56 has a nontrivial normal subgroup.

51. Show $\operatorname{Aut}(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$.

52. How many elements are there of order 7 in a simple group of order 168? (See Exercise 38 for the definition of simple.)

53. Classify all groups (up to isomorphism) of order 18.

54. Classify all groups (up to isomorphism) of order 20.