CHAPTER I

GROUPS

The concept of a group is of fundamental importance in the study of algebra. Groups which are, from the point of view of algebraic structure, essentially the same are said to be isomorphic. Ideally the goal in studying groups is to classify all groups up to isomorphism, which in practice means finding necessary and sufficient conditions for two groups to be isomorphic. At present there is little hope of classifying arbitrary groups. But it is possible to obtain complete structure theorems for various restricted classes of groups, such as cyclic groups (Section 3), finitely generated abelian groups (Section II.2), groups satisfying chain conditions (Section II.3) and finite groups of small order (Section II.6). In order to prove even these limited structure theorems, it is necessary to develop a large amount of miscellaneous information about the structure of (more or less) arbitrary groups (Sections 1, 2, 4, 5, and 8 of Chapter I and Sections 4 and 5 of Chapter II). In addition we shall study some classes of groups whose structure is known in large part and which have useful applications in other areas of mathematics, such as symmetric groups (Section 6), free [abelian] groups (Sections 9 and II.1), nilpotent and solvable groups (Sections II.7 and II.8).

There is a basic truth that applies not only to groups but also to many other algebraic objects (for example, rings, modules, vector spaces, fields): in order to study effectively an object with a given algebraic structure, it is necessary to study as well the functions that preserve the given algebraic structure (such functions are called homomorphisms). Indeed a number of concepts that are common to the theory of groups, rings, modules, etc. may be described completely in terms of objects and homomorphisms. In order to provide a convenient language and a useful conceptual framework in which to view these common concepts, the notion of a category is introduced in Section 7 and used frequently thereafter. Of course it is quite possible to study groups, rings, etc. without ever mentioning categories. However, the small amount of effort needed to comprehend this notion now will pay large dividends later in terms of increased understanding of the fundamental relationships among the various algebraic structures to be encountered.

With occasional exceptions such as Section 7, each section in this chapter depends on the sections preceding it.

1. SEMIGROUPS, MONOIDS AND GROUPS

If G is a nonempty set, a **binary operation** on G is a function $G \times G \to G$. There are several commonly used notations for the image of (a,b) under a binary operation: ab (multiplicative notation), $a + b$ (additive notation), $a \cdot b$, $a * b$, etc. For convenience we shall generally use the multiplicative notation throughout this chapter and refer to ab as the **product** of a and b. A set may have several binary operations defined on it (for example, ordinary addition and multiplication on $\mathbf{Z}$ given by $(a,b) \mapsto a + b$ and $(a,b) \mapsto ab$ respectively).

Definition 1.1. *A* **semigroup** *is a nonempty set* G *together with a binary operation on* G *which is*

(i) *associative:* $a(bc) = (ab)c$ *for all* $a, b, c \in G$;

a **monoid** *is a semigroup* G *which contains a*

(ii) *(two-sided) identity element* $e \in G$ *such that* $ae = ea = a$ *for all* $a \in G$.

A **group** *is a monoid* G *such that*

(iii) *for every* $a \in G$ *there exists a (two-sided) inverse element* $a^{-1} \in G$ *such that* $a^{-1}a = aa^{-1} = e$.

A semigroup G *is said to be* **abelian** *or* **commutative** *if its binary operation is*

(iv) *commutative:* $ab = ba$ *for all* $a,b \in G$.

Our principal interest is in groups. However, semigroups and monoids are convenient for stating certain theorems in the greatest generality. Examples are given below. The **order** of a group G is the cardinal number $|G|$. G is said to be finite [resp. infinite] if $|G|$ is finite [resp. infinite].

Theorem 1.2. *If* G *is a monoid, then the identity element* e *is unique. If* G *is a group, then*

(i) $c \in G$ *and* $cc = c \Rightarrow c = e$;
(ii) *for all* $a, b, c \in G$ $ab = ac \Rightarrow b = c$ *and* $ba = ca \Rightarrow b = c$ (*left and right cancellation*);
(iii) *for each* $a \in G$, *the inverse element* a^{-1} *is unique;*
(iv) *for each* $a \in G$, $(a^{-1})^{-1} = a$;
(v) *for* $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;
(vi) *for* $a, b \in G$ *the equations* $ax = b$ *and* $ya = b$ *have unique solutions in* G : $x = a^{-1}b$ *and* $y = ba^{-1}$.

SKETCH OF PROOF. If e' is also a two-sided identity, then $e = ee' = e'$. (i) $cc = c \Rightarrow c^{-1}(cc) = c^{-1}c \Rightarrow (c^{-1}c)c = c^{-1}c \Rightarrow ec = e \Rightarrow c = e$; (ii), (iii) and (vi) are proved similarly. (v) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = (ae)a^{-1} = aa^{-1} = e \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$ by (iii); (iv) is proved similarly. ■

If G is a monoid and the binary operation is written multiplicatively, then the identity element of G will always be denoted e. If the binary operation is written additively, then $a + b$ $(a, b \in G)$ is called the **sum** of a and b, and the identity element is denoted 0; if G is a group the inverse of $a \in G$ is denoted by $-a$. We write $a - b$ for $a + (-b)$. Abelian groups are frequently written additively.

The axioms used in Definition 1.1 to define a group can actually be weakened considerably.

Proposition 1.3. *Let* G *be a semigroup. Then* G *is a group if and only if the following conditions hold:*

(i) *there exists an element* $e \in G$ *such that* $ea = a$ *for all* $a \in G$ (*left identity element*);

(ii) *for each* $a \in G$, *there exists an element* $a^{-1} \in G$ *such that* $a^{-1}a = e$ (*left inverse*).

REMARK. An analogous result holds for "right inverses" and a "right identity."

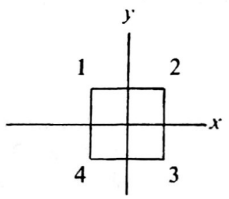
SKETCH OF PROOF OF 1.3. ($\Rightarrow$) Trivial. ($\Leftarrow$) Note that Theorem 1.2(i) is true under these hypotheses. $G \neq \varnothing$ since $e \in G$. If $a \in G$, then by (ii) $(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = a(ea^{-1}) = aa^{-1}$ and hence $aa^{-1} = e$ by Theorem 1.2(i). Thus a^{-1} is a two-sided inverse of a. Since $ae = a(a^{-1}a) = (aa^{-1})a = ea = a$ for every $a \in G$, e is a two-sided identity. Therefore G is a group by Definition 1.1. ■

Proposition 1.4. *Let* G *be a semigroup. Then* G *is a group if and only if for all* $a, b \in G$ *the equations* $ax = b$ *and* $ya = b$ *have solutions in* G.

PROOF. Exercise; use Proposition 1.3. ■

EXAMPLES. The integers **Z**, the rational numbers **Q**, and the real numbers **R** are each infinite abelian groups under ordinary addition. Each is a monoid under ordinary multiplication, but not a group (0 has no inverse). However, the nonzero elements of **Q** and **R** respectively form infinite abelian groups under multiplication. The even integers under multiplication form a semigroup that is not a monoid.

EXAMPLE. Consider the square with vertices consecutively numbered 1,2,3,4, center at the origin of the x-y plane, and sides parallel to the axes.



Let D_4^* be the following set of "transformations" of the square. $D_4^* = \{R, R^2, R^3, I, T_x, T_y, T_{1,3}, T_{2,4}\}$, where R is a counterclockwise rotation about the center of 90°, R^2 a counterclockwise rotation of 180°, R^3 a counterclockwise rotation of 270°

and I a rotation of 360° (= 0°); T_x is a reflection about the x axis, $T_{1,3}$ a reflection about the diagonal through vertices 1 and 3; similarly for T_y and $T_{2,4}$. Note that each $U \in D_4^*$ is a bijection of the square onto itself. Define the binary operation in D_4^* to be composition of functions: for $U,V \in D_4^*$, $U \circ V$ is the transformation V followed by the transformation U. D_4^* is a nonabelian group of order 8 called the **group of symmetries of the square.** Notice that each symmetry (element of D_4^*) is completely determined by its action on the vertices.

EXAMPLE. Let S be a nonempty set and $A(S)$ the set of all bijections $S \to S$. Under the operation of composition of functions, $f \circ g$, $A(S)$ is a group, since composition is associative, composition of bijections is a bijection, 1_S is a bijection, and every bijection has an inverse (see (13) of Introduction, Section 3). The elements of $A(S)$ are called **permutations** and $A(S)$ is called the group of permutations on the set S. If $S = \{1,2,3,\ldots,n\}$, then $A(S)$ is called the **symmetric group on n letters** and denoted S_n. Verify that $|S_n| = n!$ (Exercise 5). The groups S_n play an important role in the theory of finite groups.

Since an element σ of S_n is a function on the finite set $S = \{1,2,\ldots,n\}$, it can be described by listing the elements of S on a line and the image of each element under σ directly below it: $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & & i_n \end{pmatrix}$. The product $\sigma\tau$ of two elements of S_n is the composition function τ *followed by* σ; that is, the function on S given by $k \mapsto \sigma(\tau(k))$.[1] For instance, let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ be elements of S_4. Then under $\sigma\tau$, $1 \mapsto \sigma(\tau(1)) = \sigma(4) = 4$, etc.; thus $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ $= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$; similarly, $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ This example also shows that S_n need not be abelian.

Another source of examples is the following method of constructing new groups from old. Let G and H be groups with identities e_G, e_H respectively, and define the **direct product** of G and H to be the group whose underlying set is $G \times H$ and whose binary operation is given by:

$$(a,b)(a',b') = (aa',bb'), \quad \text{where} \quad a,a' \in G; b,b' \in H.$$

Observe that there are three different operations in G, H and $G \times H$ involved in this statement. It is easy to verify that $G \times H$ is, in fact, a group that is abelian if both G and H are; (e_G,e_H) is the identity and (a^{-1},b^{-1}) the inverse of (a,b). Clearly $|G \times H| = |G||H|$ (Introduction, Definition 8.3). If G and H are written additively, then we write $G \oplus H$ in place of $G \times H$.

Theorem 1.5. *Let* R ($\sim$) *be an equivalence relation on a monoid* G *such that* $a_1 \sim a_2$ *and* $b_1 \sim b_2$ *imply* $a_1b_1 \sim a_2b_2$ *for all* $a_i,b_i \in G$. *Then the set* G/R *of all equivalence classes of* G *under* R *is a monoid under the binary operation defined by* $(\bar{a})(\bar{b}) = \overline{ab}$, *where* $\bar{x}$ *denotes the equivalence class of* $x \in G$. *If* G *is an [abelian] group, then so is* G/R.

[1] In many books, however, the product $\sigma\tau$ is defined to be "σ followed by τ."

An equivalence relation on a monoid G that satisfies the hypothesis of the theorem is called a **congruence relation** on G.

PROOF OF 1.5. If $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$ ($a_i, b_i \in G$), then $a_1 \sim a_2$ and $b_1 \sim b_2$ by (20) of Introduction, Section 4. Then by hypothesis $a_1b_1 \sim a_2b_2$ so that $\overline{a_1b_1} = \overline{a_2b_2}$ by (20) again. Therefore the binary operation in G/R is well defined (that is, independent of the choice of equivalence class representatives). It is associative since $\bar{a}(\bar{b}\,\bar{c}) = \bar{a}(\overline{bc}) = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\bar{c} = (\bar{a}\,\bar{b})\bar{c}$. $\bar{e}$ is the identity element since $(\bar{a})(\bar{e}) = \overline{ae} = \bar{a} = \overline{ea} = (\bar{e})(\bar{a})$. Therefore G/R is a monoid. If G is a group, then $\bar{a} \in G/R$ clearly has inverse $\overline{a^{-1}}$ so that G/R is also a group. Similarly, G abelian implies G/R abelian. ■

EXAMPLE. Let m be a fixed integer. Congruence modulo m is a congruence relation on the additive group $\mathbf{Z}$ by Introduction, Theorem 6.8. Let Z_m denote the set of equivalence classes of $\mathbf{Z}$ under congruence modulo m. By Theorem 1.5 (with additive notation) Z_m is an abelian group, with addition given by $\bar{a} + \bar{b} = \overline{a + b}$ ($a,b \in \mathbf{Z}$). The proof of Introduction, Theorem 6.8 shows that $Z_m = \{\bar{0},\bar{1}, \ldots, \overline{m-1}\}$ so that Z_m is a finite group of order m under addition. Z_m is called the (additive) group of **integers modulo m.** Similarly since $\mathbf{Z}$ is a commutative monoid under multiplication, and congruence modulo m is also a congruence relation with respect to multiplication (Introduction, Theorem 6.8), Z_m is a commutative monoid, with multiplication given by $(\bar{a})(\bar{b}) = \overline{ab}$ ($a,b \in \mathbf{Z}$). Verify that for all $\bar{a}, \bar{b}, \bar{c} \in Z_m$:

$$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c} \quad \text{and} \quad (\bar{a} + \bar{b})\bar{c} = \bar{a}\bar{c} + \bar{b}\bar{c} \text{ (distributivity).}$$

Furthermore if p is prime, then the nonzero elements of Z_p form a multiplicative group of order $p - 1$ (Exercise 7). It is customary to denote the elements of Z_m as $0,1, \ldots, m-1$ rather than $\bar{0},\bar{1}, \ldots, \overline{m-1}$. In context this ambiguous notation will cause no difficulty and will be used whenever convenient.

EXAMPLE. The following relation on the additive group $\mathbf{Q}$ of rational numbers is a congruence relation (Exercise 8):

$$a \sim b \Leftrightarrow a - b \in \mathbf{Z}.$$

By Theorem 1.5 the set of equivalence classes (denoted $\mathbf{Q}/\mathbf{Z}$) is an (infinite) abelian group, with addition given by $\bar{a} + \bar{b} = \overline{a + b}$. $\mathbf{Q}/\mathbf{Z}$ is called the **group of rationals modulo one.**

Given $a_1, \ldots, a_n \in G$ ($n \geq 3$) it is intuitively plausible that there are many ways of inserting parentheses in the expression $a_1a_2 \cdots a_n$ so as to yield a "meaningful" product in G of these n elements in this order. Furthermore it is plausible that any two such products can be proved equal by repeated use of the associative law. A necessary prerequisite for further study of groups and rings is a precise statement and proof of these conjectures and related ones.

Given any sequence of elements of a semigroup G, $\{a_1,a_2 \ldots\}$ define inductively a **meaningful product** of $a_1, \ldots, a_n$ (in this order) as follows. If $n = 1$, the only meaningful product is a_1. If $n > 1$, then a meaningful product is defined to be any product of the form $(a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ where $m < n$ and $(a_1 \cdots a_m)$ and $(a_{m+1} \cdots a_n)$ are meaningful products of m and $n - m$ elements respectively.[2] Note that for each

[2]To show that this definition is in fact well defined requires a stronger version of the Recursion Theorem 6.2 of the Introduction; see C. W. Burrill [56; p. 57].

$n \geq 3$ there may be many meaningful products of $a_1, \ldots, a_n$. For each $n \in \mathbf{N}^*$ we single out a particular meaningful product by defining inductively the **standard n product** $\prod_{i=1}^{n} a_i$ of $a_1, \ldots, a_n$ as follows:

$$\prod_{i=1}^{1} a_i = a_1; \quad \text{and for } n > 1, \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n.$$

The fact that this definition defines for each $n \in \mathbf{N}^*$ a unique element of G (which is clearly a meaningful product) is a consequence of the Recursion Theorem 6.2 of the Introduction (Exercise 16).

Theorem 1.6. (*Generalized Associative Law*) *If* G *is a semigroup and* $a_1, \ldots, a_n \in G$, *then any two meaningful products of* $a_1, \ldots, a_n$ *in this order are equal.*

PROOF. We use induction to show that for every n any meaningful product $a_1 \cdots a_n$ is equal to the standard n product $\prod_{i=1}^{n} a_i$. This is certainly true for $n = 1, 2$. If $n > 2$, then by definition $(a_1 \cdots a_n) = (a_1 \cdots a_m)(a_{m+1} \cdots a_n)$ for some $m < n$. Therefore, by induction and associativity:

$$(a_1 \cdots a_n) = (a_1 \cdots a_m)(a_{m+1} \cdots a_n) = \left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m} a_{m+i}\right)$$

$$= \left(\prod_{i=1}^{m} a_i\right)\left(\left(\prod_{i=1}^{n-m-1} a_{m+i}\right) a_n\right) = \left(\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m-1} a_{m+i}\right)\right) a_n$$

$$= \left(\prod_{i=1}^{n-1} a_i\right) a_n = \prod_{i=1}^{n} a_i. \quad \blacksquare$$

In view of Theorem 1.6 we can and do write any meaningful product of $a_1, \ldots, a_n \in G$ (G a semigroup) as $a_1 a_2 \cdots a_n$ without parentheses or ambiguity.

Corollary 1.7. (*Generalized Commutative Law*) *If* G *is a commutative semigroup and* $a_1, \ldots, a_n \in G$, *then for any permutation* $i_1, \ldots, i_n$ *of* $1, 2, \ldots n$, $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.

PROOF. Exercise. ■

Definition 1.8. *Let* G *be a semigroup,* $a \in G$ *and* $n \in \mathbf{N}^*$. *The element* $a^n \in G$ *is defined to be the standard* n *product* $\prod_{i=1}^{n} a_i$ *with* $a_i = a$ *for* $1 \leq i \leq n$. *If* G *is a monoid,* a^0 *is defined to be the identity element* e. *If* G *is a group, then for each* $n \in \mathbf{N}^*$, a^{-n} *is defined to be* $(a^{-1})^n \in G$.

The remarks preceding Theorem 1.6 and Exercise 16 show that exponentiation is well defined. By definition, then, $a^1 = a$, $a^2 = aa$, $a^3 = (aa)a = aaa, \ldots, a^n = a^{n-1}a$

$= aa\cdots a$ (n factors). Note that we may have $a^m = a^n$ with $m \neq n$ (for example, in $\mathbf{C}$, $-1 = i^2 = i^6$).

ADDITIVE NOTATION. If the binary operation in G is written additively, then we write na in place of a^n. Thus $0a = 0$, $1a = a$, $na = (n-1)a + a$, etc.

Theorem 1.9. *If* G *is a group* [*resp. semigroup, monoid*] *and* $a \in G$, *then for all* $m, n \in \mathbf{Z}$ [*resp.* $\mathbf{N}^*$, N]:

(i) $a^m a^n = a^{m+n}$ (*additive notation:* $ma + na = (m+n)a$);
(ii) $(a^m)^n = a^{mn}$ (*additive notation:* $n(ma) = mna$).

SKETCH OF PROOF. Verify that $(a^n)^{-1} = (a^{-1})^n$ for all $n \in \mathbf{N}$ and that $a^{-n} = (a^{-1})^n$ for all $n \in \mathbf{Z}$. (i) is true for $m > 0$ and $n > 0$ since the product of a standard n product and a standard m product is a meaningful product equal to the standard $(m+n)$ product by Theorem 1.6. For $m < 0$, and $n < 0$ replace a, m, n by $a^{-1}, -m, -n$ and use the preceding argument. The case $m = 0$ or $n = 0$ is trivial and the cases $m \geq 0$, $n < 0$ and $m < 0$, $n \geq 0$ are handled by induction on m and n respectively. (ii) is trivial if $m = 0$. The case when $m > 0$ and $n \in \mathbf{Z}$ is proved by induction on m. Use this result to prove the case $m < 0$ and $n \in \mathbf{Z}$. ■

EXERCISES

1. Give examples other than those in the text of semigroups and monoids that are not groups.
2. Let G be a group (written additively), S a nonempty set, and $M(S,G)$ the set of all functions $f: S \to G$. Define addition in $M(S,G)$ as follows: $(f+g): S \to G$ is given by $s \mapsto f(s) + g(s) \in G$. Prove that $M(S,G)$ is a group, which is abelian if G is.
3. Is it true that a semigroup which has a *left* identity element and in which every element has a *right* inverse (see Proposition 1.3) is a group?
4. Write out a multiplication table for the group D_4*.
5. Prove that the symmetric group on n letters, S_n, has order $n!$.
6. Write out an addition table for $Z_2 \oplus Z_2$. $Z_2 \oplus Z_2$ is called the **Klein four group**.
7. If p is prime, then the nonzero elements of Z_p form a group of order $p-1$ under multiplication. [*Hint:* $\bar{a} \neq \bar{0} \Rightarrow (a,p) = 1$; use Introduction, Theorem 6.5.] Show that this statement is false if p is not prime.
8. (a) The relation given by $a \sim b \Leftrightarrow a - b \in \mathbf{Z}$ is a congruence relation on the additive group $\mathbf{Q}$ [see Theorem 1.5].
   (b) The set $\mathbf{Q}/\mathbf{Z}$ of equivalence classes is an infinite abelian group.
9. Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of p (p^i, $i \geq 0$). Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.

10. Let p be a prime and let $Z(p^\infty)$ be the following subset of the group $\mathbf{Q/Z}$ (see pg. 27):

$$Z(p^\infty) = \{\overline{a/b} \in \mathbf{Q/Z} \mid a,b \in \mathbf{Z} \quad \text{and} \quad b = p^i \text{ for some } i \geq 0\}.$$

Show that $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbf{Q/Z}$.

11. The following conditions on a group G are equivalent: (i) G is abelian; (ii) $(ab)^2 = a^2b^2$ for all $a,b \in G$; (iii) $(ab)^{-1} = a^{-1}b^{-1}$ for all $a,b \in G$; (iv) $(ab)^n = a^nb^n$ for all $n \in \mathbf{Z}$ and all $a,b \in G$; (v) $(ab)^n = a^nb^n$ for three consecutive integers n and all $a,b \in G$. Show that (v) $\Rightarrow$ (i) is false if "three" is replaced by "two."

12. If G is a group, $a,b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbf{N}$, then $b^iab^{-i} = a^{r^i}$ for all $j \in \mathbf{N}$.

13. If $a^2 = e$ for all elements a of a group G, then G is abelian.

14. If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

15. Let G be a nonempty finite set with an associative binary operation such that for all $a,b,c \in G$ $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Then G is a group. Show that this conclusion may be false if G is infinite.

16. Let $a_1,a_2, \ldots$ be a sequence of elements in a semigroup G. Then there exists a unique function $\psi : \mathbf{N}^* \to G$ such that $\psi(1) = a_1$, $\psi(2) = a_1a_2$, $\psi(3) = (a_1a_2)a_3$ and for $n \geq 1$, $\psi(n+1) = (\psi(n))a_{n+1}$. Note that $\psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$. [*Hint:* Applying the Recursion Theorem 6.2 of the Introduction with $a = a_1$, $S = G$ and $f_n : G \to G$ given by $x \mapsto xa_{n+2}$ yields a function $\varphi : \mathbf{N} \to G$. Let $\psi = \varphi\theta$, where $\theta : \mathbf{N}^* \to \mathbf{N}$ is given by $k \mapsto k - 1$.]

2. HOMOMORPHISMS AND SUBGROUPS

Essential to the study of any class of algebraic objects are the functions that preserve the given algebraic structure in the following sense.

Definition 2.1. *Let* G *and* H *be semigroups. A function* $f : G \to H$ *is a* **homomorphism** *provided*

$$f(ab) = f(a)f(b) \quad \textit{for all} \quad a,b \in G.$$

If f *is injective as a map of sets,* f *is said to be a* **monomorphism.** *If* f *is surjective,* f *is called an* **epimorphism.** *If* f *is bijective,* f *is called an* **isomorphism.** *In this case* G *and* H *are said to be* **isomorphic** (*written* $G \cong H$). *A homomorphism* $f : G \to G$ *is called an* **endomorphism** *of* G *and an isomorphism* $f : G \to G$ *is called an* **automorphism** *of* G.

If $f : G \to H$ and $g : H \to K$ are homomorphisms of semigroups, it is easy to see that $gf : G \to K$ is also a homomorphism. Likewise the composition of monomorphisms is a monomorphism; similarly for epimorphisms, isomorphisms and automorphisms. If G and H are groups with identities e_G and e_H respectively and

$f: G \to H$ is a homomorphism, then $f(e_G) = e_H$; however, this is not true for monoids (Exercise 1). Furthermore $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$ (Exercise 1).

EXAMPLE. The map $f: \mathbf{Z} \to Z_m$ given by $x \mapsto \bar{x}$ (that is, each integer is mapped onto its equivalence class in Z_m) is an epimorphism of additive groups. f is called the canonical epimorphism of $\mathbf{Z}$ onto Z_m. Similarly, the map $g: \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ given by $r \mapsto \bar{r}$ is also an epimorphism of additive groups.

EXAMPLE. If A is an abelian group, then the map given by $a \mapsto a^{-1}$ is an automorphism of A. The map given by $a \mapsto a^2$ is an endomorphism of A.

EXAMPLE. Let $1 < m$, $k \in \mathbf{N}^*$. The map $g: Z_m \to Z_{mk}$ given by $\bar{x} \mapsto \overline{kx}$ is a monomorphism.

EXAMPLE. Given groups G and H, there are four homomorphisms: $G \underset{\pi_1}{\overset{\iota_1}{\rightleftarrows}} G \times H \underset{\pi_2}{\overset{\iota_2}{\leftrightarrows}} H$, given by $\iota_1(g) = (g,e)$; $\iota_2(h) = (e,h)$; $\pi_1(g,h) = g$; $\pi_2(g,h) = h$. ι_i is a monomorphism and π_j is an epimorphism $(i,j = 1,2)$.

Definition 2.2. *Let* $\mathrm{f}: \mathrm{G} \to \mathrm{H}$ *be a homomorphism of groups. The* **kernel** *of* f (*denoted Ker* f) *is* $\{\mathrm{a} \in \mathrm{G} \mid \mathrm{f(a)} = \mathrm{e} \in \mathrm{H}\}$. *If* A *is a subset of* G, *then* $\mathrm{f(A)} = \{\mathrm{b} \in \mathrm{H} \mid \mathrm{b} = \mathrm{f(a)}$ *for some* $\mathrm{a} \in \mathrm{A}\}$ *is the* **image of A.** f(G) *is called the* **image of** f *and denoted Im* f. *If* B *is a subset of* H, $\mathrm{f^{-1}(B)} = \{\mathrm{a} \in \mathrm{G} \mid \mathrm{f(a)} \in \mathrm{B}\}$ *is the* **inverse image** *of* B.

Theorem 2.3. *Let* $\mathrm{f}: \mathrm{G} \to \mathrm{H}$ *be a homomorphism of groups. Then*

(i) f *is a monomorphism if and only if Ker* $\mathrm{f} = \{\mathrm{e}\}$;

(ii) f *is an isomorphism if and only if there is a homomorphism* $\mathrm{f^{-1}}: \mathrm{H} \to \mathrm{G}$ *such that* $\mathrm{ff^{-1}} = 1_{\mathrm{H}}$ *and* $\mathrm{f^{-1}f} = 1_{\mathrm{G}}$.

PROOF. (i) If f is a monomorphism and $a \in \operatorname{Ker} f$, then $f(a) = e_H = f(e)$, whence $a = e$ and $\operatorname{Ker} f = \{e\}$. If $\operatorname{Ker} f = \{e\}$ and $f(a) = f(b)$, then $e_H = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ so that $ab^{-1} \in \operatorname{Ker} f$. Therefore, $ab^{-1} = e$ (that is, $a = b$) and f is a monomorphism.

(ii) If f is an isomorphism, then by (13) of Introduction, Section 3 there is a map of sets $f^{-1}: H \to G$ such that $f^{-1}f = 1_G$ and $ff^{-1} = 1_H$. f^{-1} is easily seen to be a homomorphism. The converse is an immediate consequence of (13) of Introduction, Section 3 and Definition 2.1. ■

Let G be a semigroup and H a nonempty subset of G. If for every $a,b \in H$ we have $ab \in H$, we say that H is **closed** under the product in G. This amounts to saying that the binary operation on G, when restricted to H, is in fact a binary operation on H.

Definition 2.4. *Let* G *be a group and* H *a nonempty subset that is closed under the product in* G. *If* H *is itself a group under the product in* G, *then* H *is said to be a* **subgroup** *of* G. *This is denoted by* $\mathrm{H} < \mathrm{G}$.

Two examples of subgroups of a group G are G itself and the **trivial subgroup** $\langle e \rangle$ consisting only of the identity element. A subgroup H such that $H \neq G$, $H \neq \langle e \rangle$ is called a **proper subgroup.**

EXAMPLE. The set of all multiples of some fixed integer n is a subgroup of $\mathbf{Z}$, which is isomorphic to $\mathbf{Z}$ (Exercise 7).

EXAMPLE. In S_n, the group of all permutations of $\{1,2,\ldots,n\}$, the set of all permutations that leave n fixed forms a subgroup isomorphic to S_{n-1} (Exercise 8).

EXAMPLE. In $Z_6 = \{0,1,2,3,4,5\}$, both $\{0,3\}$ and $\{0,2,4\}$ are subgroups under addition. If p is prime, $(Z_p,+)$ has no proper subgroups.

EXAMPLE. If $f: G \to H$ is a homomorphism of groups, then Ker f is a subgroup of G. If A is a subgroup of G, $f(A)$ is a subgroup of H; in particular Im f is a subgroup of H. If B is a subgroup of H, $f^{-1}(B)$ is a subgroup of G (Exercise 9).

EXAMPLE. If G is a group, then the set Aut G of all automorphisms of G is a group, with composition of functions as binary operation (Exercise 15).

By Theorem 1.2 the identity element of any subgroup H is the identity element of G and the inverse of $a \in H$ is the inverse a^{-1} of a in G.

Theorem 2.5. *Let* H *be a nonempty subset of a group* G. *Then* H *is a subgroup of* G *if and only if* $ab^{-1} \in H$ *for all* $a,b \in H$.

PROOF. ($\Leftarrow$) There exists $a \in H$ and hence $e = aa^{-1} \in H$. Thus for any $b \in H$, $b^{-1} = eb^{-1} \in H$. If $a,b \in H$, then $b^{-1} \in H$ and hence $ab = a(b^{-1})^{-1} \in H$. The product in H is associative since G is a group. Therefore H is a (sub)group. The converse is trivial. ■

Corollary 2.6. *If* G *is a group and* $\{H_i \mid i \in I\}$ *is a nonempty family of subgroups, then* $\bigcap_{i \in I} H_i$ is a subgroup of G.

PROOF. Exercise. ■

Definition 2.7. *Let* G *be a group and* X *a subset of* G. *Let* $\{H_i \mid i \in I\}$ *be the family of all subgroups of* G *which contain* X. *Then* $\bigcap_{i \in I} H_i$ *is called the* **subgroup** *of* G **generated by the set** X *and denoted* $\langle X \rangle$.

The elements of X are the **generators** of the subgroup $\langle X \rangle$, which may also be generated by other subsets (that is, we may have $\langle X \rangle = \langle Y \rangle$ with $X \neq Y$). If $X = \{a_1,\ldots,a_n\}$, we write $\langle a_1,\ldots,a_n \rangle$ in place of $\langle X \rangle$. If $G = \langle a_1,\ldots,a_n \rangle$, $(a_i \in G)$, G is said to be **finitely generated.** If $a \in G$, the subgroup $\langle a \rangle$ is called the **cyclic (sub)-group** generated by a.

Theorem 2.8. *If* G *is a group and* X *is a nonempty subset of* G, *then the subgroup* $\langle X \rangle$ *generated by* X *consists of all finite products* $a_1^{n_1}a_2^{n_2}\cdots a_t^{n_t}$ ($a_i \in X$; $n_i \in \mathbf{Z}$). *In particular for every* $a \in G$, $\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$.

SKETCH OF PROOF. Show that the set H of all such products is a subgroup of G that contains X and is contained in every subgroup containing X. Therefore $H < \langle X \rangle < H$. ■

EXAMPLES. The additive group $\mathbf{Z}$ is an infinite cyclic group with generator 1, since by Definition 1.8 (additive notation), $m1 = m$ for all $m \in \mathbf{Z}$. Of course *the "powers" of the generating element need not all be distinct* as they are in $\mathbf{Z}$. The trivial subgroup $\langle e \rangle$ of any group is cyclic; the multiplicative subgroup $\langle i \rangle$ in $\mathbf{C}$ is cyclic of order 4 and for each m the additive group Z_m is cyclic of order m with generator $1 \in Z_m$. In Section 3 we shall prove that every cyclic subgroup is isomorphic either to $\mathbf{Z}$ or Z_m for some m. Also, see Exercise 12.

If $\{H_i \mid i \in I\}$ is a family of subgroups of a group G, then $\bigcup_{i \in I} H_i$ is not a subgroup of G in general. The subgroup $\langle \bigcup_{i \in I} H_i \rangle$ generated by the set $\bigcup_{i \in I} H_i$ is called the **subgroup generated by the groups** $\{H_i \mid i \in I\}$. If H and K are subgroups, the subgroup $\langle H \cup K \rangle$ generated by H and K is called the **join** of H and K and is denoted $H \vee K$ (additive notation: $H + K$).

EXERCISES

1. If $f: G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are not groups.

2. A group G is abelian if and only if the map $G \to G$ given by $x \mapsto x^{-1}$ is an automorphism.

3. Let Q_8 be the group (under ordinary matrix multiplication) generated by the complex matrices $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, where $i^2 = -1$. Show that Q_8 is a nonabelian group of order 8. Q_8 is called the **quaternion group.** [*Hint:* Observe that $BA = A^3B$, whence every element of Q_8 is of the form A^iB^j. Note also that $A^4 = B^4 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of Q_8.]

4. Let H be the group (under matrix multiplication) of real matrices generated by $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that H is a nonabelian group of order 8 which is *not* isomorphic to the quaternion group of Exercise 3, but is isomorphic to the group D_4*.

5. Let S be a nonempty subset of a group G and define a relation on G by $a \sim b$ if and only if $ab^{-1} \in S$. Show that $\sim$ is an equivalence relation if and only if S is a subgroup of G.

6. A nonempty finite subset of a group is a subgroup if and only if it is closed under the product in G.

7. If n is a fixed integer, then $\{kn \mid k \in \mathbf{Z}\} \subset \mathbf{Z}$ is an additive subgroup of $\mathbf{Z}$, which is isomorphic to $\mathbf{Z}$.

8. The set $\{\sigma \in S_n \mid \sigma(n) = n\}$ is a subgroup of S_n which is isomorphic to S_{n-1}.

9. Let $f: G \to H$ be a homomorphism of groups, A a subgroup of G, and B a subgroup of H.
   (a) Ker f and $f^{-1}(B)$ are subgroups of G.
   (b) $f(A)$ is a subgroup of H.

10. List all subgroups of $Z_2 \oplus Z_2$. Is $Z_2 \oplus Z_2$ isomorphic to Z_4?

11. If G is a group, then $C = \{a \in G \mid ax = xa \text{ for all } x \in G\}$ is an abelian subgroup of G. C is called the **center** of G.

12. The group D_4* is not cyclic, but can be generated by two elements. The same is true of S_n (nontrivial). What is the minimal number of generators of the additive group $\mathbf{Z} \oplus \mathbf{Z}$?

13. If $G = \langle a \rangle$ is a cyclic group and H is any group, then every homomorphism $f: G \to H$ is completely determined by the element $f(a) \in H$.

14. The following cyclic subgroups are all isomorphic: the multiplicative group $\langle i \rangle$ in $\mathbf{C}$, the additive group Z_4 and the subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle$ of S_4.

15. Let G be a group and Aut G the set of all automorphisms of G.
   (a) Aut G is a group with composition of functions as binary operation. [*Hint:* $1_G \in$ Aut G is an identity; inverses exist by Theorem 2.3.]
   (b) Aut $\mathbf{Z} \cong Z_2$ and Aut $Z_6 \cong Z_2$; Aut $Z_8 \cong Z_2 \oplus Z_2$; Aut $Z_p \cong Z_{p-1}$ (p prime).
   (c) What is Aut Z_n for arbitrary $n \in \mathbf{N}$*?

16. For each prime p the additive subgroup $Z(p^\infty)$ of $\mathbf{Q}/\mathbf{Z}$ (Exercise 1.10) is generated by the set $\{\overline{1/p^n} \mid n \in \mathbf{N}^*\}$.

17. Let G be an abelian group and let H,K be subgroups of G. Show that the join $H \vee K$ is the set $\{ab \mid a \in H, b \in K\}$. Extend this result to any finite number of subgroups of G.

18. (a) Let G be a group and $\{H_i \mid i \in I\}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i \in I} H_i$ is a subgroup, that is, that $\bigcup_{i \in I} H_i = \langle \bigcup_{i \in I} H_i \rangle$.
   (b) Give an example of a group G and a family of subgroups $\{H_i \mid i \in I\}$ such that $\bigcup_{i \in I} H_i \neq \langle \bigcup_{i \in I} H_i \rangle$.

19. (a) The set of all subgroups of a group G, partially ordered by set theoretic inclusion, forms a complete lattice (Introduction, Exercises 7.1 and 7.2) in which the g.l.b. of $\{H_i \mid i \in I\}$ is $\bigcap_{i \in I} H_i$ and the l.u.b. is $\langle \bigcup_{i \in I} H_i \rangle$.
   (b) Exhibit the lattice of subgroups of the groups S_3, D_4*, Z_6, Z_{27}, and Z_{36}.

3. CYCLIC GROUPS

The structure of cyclic groups is relatively simple. We shall completely characterize all cyclic groups (up to isomorphism).

Theorem 3.1. *Every subgroup* H *of the additive group* **Z** *is cyclic. Either* $H = \langle 0 \rangle$ *or* $H = \langle m \rangle$, *where* m *is the least positive integer in* H. *If* $H \neq \langle 0 \rangle$, *then* H *is infinite.*

PROOF. Either $H = \langle 0 \rangle$ or H contains a least positive integer m. Clearly $\langle m \rangle = \{km \mid k \in \mathbf{Z}\} \subset H$. Conversely if $h \in H$, then $h = qm + r$ with $q, r \in \mathbf{Z}$ and $0 \leq r < m$ (division algorithm). Since $r = h - qm \in H$ the minimality of m implies $r = 0$ and $h = qm$. Hence $H \subset \langle m \rangle$. If $H \neq \langle 0 \rangle$, it is clear that $H = \langle m \rangle$ is infinite. ■

Theorem 3.2. *Every infinite cyclic group is isomorphic to the additive group* **Z** *and every finite cyclic group of order* m *is isomorphic to the additive group* $\mathbf{Z}_m$.

PROOF. If $G = \langle a \rangle$ is a cyclic group then the map $\alpha : \mathbf{Z} \to G$ given by $k \mapsto a^k$ is an epimorphism by Theorems 1.9 and 2.8. If Ker $\alpha = 0$, then $\mathbf{Z} \cong G$ by Theorem 2.3 (i). Otherwise Ker α is a nontrivial subgroup of **Z** (Exercise 2.9) and hence Ker $\alpha = \langle m \rangle$, where m is the least positive integer such that $a^m = e$ (Theorem 3.1). For all $r, s \in \mathbf{Z}$,

$$a^r = a^s \iff a^{r-s} = e \iff r - s \in \text{Ker } \alpha = \langle m \rangle$$
$$\iff m \mid (r - s) \iff \bar{r} = \bar{s} \text{ in } Z_m,$$

(where $\bar{k}$ is the congruence class of $k \in \mathbf{Z}$). Therefore the map $\beta : Z_m \to G$ given by $\bar{k} \mapsto a^k$ is a well-defined epimorphism. Since

$$\beta(\bar{k}) = e \iff a^k = e = a^0 \iff \bar{k} = \bar{0} \text{ in } Z_m,$$

β is a monomorphism (Theorem 2.3(i)), and hence an isomorphism $Z_m \cong G$. ■

Definition 3.3. *Let* G *be a group and* $a \in G$. *The* **order** *of* a *is the order of the cyclic subgroup* $\langle a \rangle$ *and is denoted* $|a|$.

Theorem 3.4. *Let* G *be a group and* $a \in G$. *If* a *has infinite order, then*

(i) $a^k = e$ *if and only if* $k = 0$;
(ii) *the elements* a^k $(k \in \mathbf{Z})$ *are all distinct.*

If a *has finite order* $m > 0$, *then*

(iii) m *is the least positive integer such that* $a^m = e$;
(iv) $a^k = e$ *if and only if* $m \mid k$;
(v) $a^r = a^s$ *if and only if* $r \equiv s \pmod{m}$;
(vi) $\langle a \rangle$ *consists of the distinct elements* $a, a^2, \ldots, a^{m-1}, a^m = e$;
(vii) *for each* k *such that* $k \mid m$, $|a^k| = m/k$.

SKETCH OF PROOF. (i)–(vi) are immediate consequences of the proof of Theorem 3.2. (vii) $(a^k)^{m/k} = a^m = e$ and $(a^k)^r \neq e$ for all $0 < r < m/k$ since otherwise $a^{kr} = e$ with $kr < k(m/k) = m$ contradicting (iii). Therefore, $|a^k| = m/k$ by (iii). ■

Theorem 3.5. *Every homomorphic image and every subgroup of a cyclic group* G *is cyclic. In particular, if* H *is a nontrivial subgroup of* $G = \langle a \rangle$ *and* m *is the least positive integer such that* $a^m \in H$, *then* $H = \langle a^m \rangle$.

SKETCH OF PROOF. If $f: G \to K$ is a homomorphism of groups, then $\text{Im } f = \langle f(a) \rangle$. To prove the second statement simply translate the proof of Theorem 3.1 into multiplicative notation (that is, replace every $t \in \mathbf{Z}$ by a^t throughout). This proof works even if G is finite. ■

Recall that two distinct elements in a group may generate the same cyclic subgroup.

Theorem 3.6. *Let* $G = \langle a \rangle$ *be a cyclic group. If* G *is infinite, then* a *and* a^{-1} *are the only generators of* G. *If* G *is finite of order* m, *then* a^k *is a generator of* G *if and only if* (k,m) = 1.

SKETCH OF PROOF. It suffices to assume either that $G = \mathbf{Z}$, in which case the conclusion is easy to prove, or that $G = Z_m$. If $(k,m) = 1$, there are $c,d \in \mathbf{Z}$ such that $ck + dm = 1$; use this fact to show that $\bar{k}$ generates Z_m. If $(k,m) = r > 1$, show that for $n = m/r < m$, $n\bar{k} = \overline{nk} = \bar{0}$ and hence $\bar{k}$ cannot generate Z_m. ■

A naive hope might be that the techniques used above could be extended to groups with two generators and eventually to all finitely generated groups, and thus provide a description of the structure of such groups. Unfortunately, however, even groups with only two generators may have a very complex structure. (They need not be abelian for one thing; see Exercises 2.3 and 2.4.) Eventually we shall be able to characterize all finitely generated abelian groups, but even this will require a great deal more machinery.

EXERCISES

1. Let a,b be elements of group G. Show that $|a| = |a^{-1}|$; $|ab| = |ba|$, and $|a| = |cac^{-1}|$ for all $c \in G$.
2. Let G be an abelian group containing elements a and b of orders m and n respectively. Show that G contains an element whose order is the least common multiple of m and n. [*Hint:* first try the case when $(m,n) = 1$.]
3. Let G be an abelian group of order pq, with $(p,q) = 1$. Assume there exist $a,b \in G$ such that $|a| = p$, $|b| = q$ and show that G is cyclic.
4. If $f: G \to H$ is a homomorphism, $a \in G$, and $f(a)$ has finite order in H, then $|a|$ is infinite or $|f(a)|$ divides $|a|$.

5. Let G be the multiplicative group of all nonsingular 2×2 matrices with rational entries. Show that $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4 and $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ has order 3, but ab has infinite order. Conversely, show that the additive group $Z_2 \oplus \mathbf{Z}$ contains nonzero elements a,b of infinite order such that $a + b$ has finite order.

6. If G is a cyclic group of order n and $k \mid n$, then G has exactly one subgroup of order k.

7. Let p be prime and H a subgroup of $Z(p^\infty)$ (Exercise 1.10).
   (a) Every element of $Z(p^\infty)$ has finite order p^n for some $n \geq 0$.
   (b) If at least one element of H has order p^k and no element of H has order greater than p^k, then H is the cyclic subgroup generated by $\overline{1/p^k}$, whence $H \cong Z_{p^k}$.
   (c) If there is no upper bound on the orders of elements of H, then $H = Z(p^\infty)$; [see Exercise 2.16].
   (d) The only proper subgroups of $Z(p^\infty)$ are the finite cyclic groups $C_n = \langle \overline{1/p^n} \rangle$ $(n = 1,2, \ldots)$. Furthermore, $\langle 0 \rangle = C_0 < C_1 < C_2 < C_3 < \cdots$.
   (e) Let $x_1, x_2, \ldots$ be elements of an abelian group G such that $|x_1| = p$, $px_2 = x_1$, $px_3 = x_2, \ldots, px_{n+1} = x_n, \ldots$. The subgroup generated by the x_i $(i \geq 1)$ is isomorphic to $Z(p^\infty)$. [*Hint:* Verify that the map induced by $x_i \mapsto \overline{1/p^i}$ is a well-defined isomorphism.]

8. A group that has only a finite number of subgroups must be finite.

9. If G is an abelian group, then the set T of all elements of G with finite order is a subgroup of G. [Compare Exercise 5.]

10. An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.

4. COSETS AND COUNTING

In this section we obtain the first significant theorems relating the structure of a finite group G with the number theoretic properties of its order $|G|$. We begin by extending the concept of congruence modulo m in the group $\mathbf{Z}$. By definition $a \equiv b \pmod{m}$ if and only if $m \mid a - b$, that is, if and only if $a - b$ is an element of the subgroup $\langle m \rangle = \{mk \mid k \in \mathbf{Z}\}$. More generally (and in multiplicative notation) we have

Definition 4.1. *Let* H *be a subgroup of a group* G *and* a,b ε G. a *is* **right congruent** *to* b **modulo** H, *denoted* a $\equiv_r$ b (*mod* H) *if* ab^{-1} ε H. a *is* **left congruent** *to* b **modulo** H, *denoted* a $\equiv_l$ b (*mod* H), *if* $a^{-1}b$ ε H.

If G is abelian, then right and left congruence modulo H coincide (since $ab^{-1} \in H \Leftrightarrow (ab^{-1})^{-1} \in H$ and $(ab^{-1})^{-1} = ba^{-1} = a^{-1}b$). There also exist nonabelian groups G and subgroups H such that right and left congruence coincide (Section 5), but this is not true in general.

Theorem 4.2. *Let* H *be a subgroup of a group* G.

(i) *Right* [*resp. left*] *congruence modulo* H *is an equivalence relation on* G.
(ii) *The equivalence class of* a ε G *under right* [*resp. left*] *congruence modulo* H *is the set* Ha = {ha | h ε H} [*resp.* aH = {ah | h ε H}].
(iii) |Ha| = |H| = |aH| *for all* a ε G.

The set Ha is called a **right coset** of H in G and aH is called a **left coset** of H in G. In general it is *not* the case that a right coset is also a left coset (Exercise 2).

PROOF OF 4.2. We write $a \equiv b$ for $a \equiv_r b \pmod{H}$ and prove the theorem for right congruence and right cosets. Analogous arguments apply to left congruence.

(i) Let $a,b,c \in G$. Then $a \equiv a$ since $aa^{-1} = e \in H$; hence $\equiv$ is reflexive. $\equiv$ is clearly symmetric ($a \equiv b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow b \equiv a$). Finally $a \equiv b$ and $b \equiv c$ imply $ab^{-1} \in H$ and $bc^{-1} \in H$. Thus $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$ and $a \equiv c$; hence $\equiv$ is transitive. Therefore, right congruence modulo H is an equivalence relation.
(ii) The equivalence class of $a \in G$ under right congruence is $\{x \in G \mid x \equiv a\}$ $= \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h \in H\} = \{x \in G \mid x = ha; h \in H\}$ $= \{ha \mid h \in H\} = Ha$.
(iii) The map $Ha \to H$ given by $ha \mapsto h$ is easily seen to be a bijection. ■

Corollary 4.3. *Let* H *be a subgroup of a group* G.

(i) G *is the union of the right* [*resp. left*] *cosets of* H *in* G.
(ii) *Two right* [*resp. left*] *cosets of* H *in* G *are either disjoint or equal.*
(iii) *For all* a,b ε G, Ha = Hb ⇔ ab^{-1} ε H *and* aH = bH ⇔ $a^{-1}b$ ε H.
(iv) *If* $\mathcal{R}$ *is the set of distinct right cosets of* H *in* G *and* $\mathcal{L}$ *is the set of distinct left cosets of* H *in* G, *then* $|\mathcal{R}| = |\mathcal{L}|$.

PROOF. (i)–(iii) are immediate consequences of the theorem and statements (19)–(21) of Introduction, Section 4. (iv) The map $\mathcal{R} \to \mathcal{L}$ given by $Ha \mapsto a^{-1}H$ is a bijection since $Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow (a^{-1})^{-1}b^{-1} \in H \Leftrightarrow a^{-1}H = b^{-1}H$. ■

ADDITIVE NOTATION. If H is a subgroup of an additive group, then right congruence modulo H is defined by: $a \equiv_r b \pmod{H} \Leftrightarrow a - b \in H$. The equivalence class of $a \in G$ is the right coset $H + a = \{h + a \mid h \in H\}$; similarly for left congruence and left cosets.

Definition 4.4. *Let* H *be a subgroup of a group* G. *The* **index of H in G,** *denoted* [G : H], *is the cardinal number of the set of distinct right* [*resp. left*] *cosets of* H *in* G.

In view of Corollary 4.3 (iv), $[G : H]$ does not depend on whether right or left cosets are used in the definition. Our principal interest is in the case when $[G : H]$ is finite, which can occur even when G and H are infinite groups (for example, $[\mathbf{Z} : \langle m \rangle] = m$ by Introduction, Theorem 6.8(i)). Note that if $H = \langle e \rangle$, then $Ha = \{a\}$ for every $a \in G$ and $[G : H] = |G|$.

A **complete set of right coset representatives** of a subgroup H in a group G is a set $\{a_i\}$ consisting of precisely one element from each right coset of H in G. Clearly the set $\{a_i\}$ has cardinality $[G : H]$. Note that such a set contains exactly one element of H since $H = He$ is itself a right coset. Analogous statements apply to left cosets.

Theorem 4.5. *If* $\mathrm{K,H,G}$ *are groups with* $\mathrm{K} < \mathrm{H} < \mathrm{G}$, *then* $[\mathrm{G} : \mathrm{K}] = [\mathrm{G} : \mathrm{H}][\mathrm{H} : \mathrm{K}]$. *If any two of these indices are finite, then so is the third.*

PROOF. By Corollary 4.3 $G = \bigcup_{i \in I} Ha_i$ with $a_i \in G$, $|I| = [G : H]$ and the cosets Ha_i mutually disjoint (that is, $Ha_i = Ha_j \Leftrightarrow i = j$). Similarly $H = \bigcup_{j \in J} Kb_j$ with $b_j \in H$, $|J| = [H : K]$ and the cosets Kb_j are mutually disjoint. Therefore $G = \bigcup_{i \in I} Ha_i = \bigcup_{i \in I} (\bigcup_{j \in J} Kb_j)a_i = \bigcup_{(i,j) \in I \times J} Kb_j a_i$. It suffices to show that the cosets $Kb_j a_i$ are mutually disjoint. For then by Corollary 4.3. we must have $[G : K] = |I \times J|$, whence $[G : K] = |I \times J| = |I||J| = [G : H][H : K]$. If $Kb_j a_i = Kb_r a_t$, then $b_j a_i = kb_r a_t$ $(k \in K)$. Since $b_j, b_r, k \in H$ we have $Ha_i = Hb_j a_i = Hkb_r a_t = Ha_t$; hence $i = t$ and $b_j = kb_r$. Thus $Kb_j = Kkb_r = Kb_r$ and $j = r$. Therefore, the cosets $Kb_j a_i$ are mutually disjoint. The last statement of the theorem is obvious. ■

Corollary 4.6. (*Lagrange*). *If* H *is a subgroup of a group* G, *then* $|\mathrm{G}| = [\mathrm{G} : \mathrm{H}]|\mathrm{H}|$. *In particular if* G *is finite, the order* $|\mathrm{a}|$ *of* $\mathrm{a} \in \mathrm{G}$ *divides* $|\mathrm{G}|$.

PROOF. Apply the theorem with $K = \langle e \rangle$ for the first statement. The second is a special case of the first with $H = \langle a \rangle$. ■

A number of proofs in the theory of (finite) groups rely on various "counting" techniques, some of which we now introduce. If G is a group and H,K are subsets of G, we denote by HK the set $\{ab \mid a \in H, b \in K\}$; a right or left coset of a subgroup is a special case. If H,K are subgroups, HK may *not* be a subgroup (Exercise 7).

Theorem 4.7. *Let* H *and* K *be finite subgroups of a group* G. *Then* $|\mathrm{HK}| = |\mathrm{H}||\mathrm{K}|/|\mathrm{H} \cap \mathrm{K}|$.

SKETCH OF PROOF. $C = H \cap K$ is a subgroup of K of index $n = |K|/|H \cap K|$ and K is the disjoint union of right cosets $Ck_1 \cup Ck_2 \cup \cdots \cup Ck_n$ for some $k_i \in K$. Since $HC = H$, this implies that HK is the disjoint union $Hk_1 \cup Hk_2 \cup \cdots \cup Hk_n$. Therefore, $|HK| = |H| \cdot n = |H||K|/|H \cap K|$. ■

Proposition 4.8. *If* H *and* K *are subgroups of a group* G, *then* $[\mathrm{H} : \mathrm{H} \cap \mathrm{K}] \leq [\mathrm{G} : \mathrm{K}]$. *If* $[\mathrm{G} : \mathrm{K}]$ *is finite, then* $[\mathrm{H} : \mathrm{H} \cap \mathrm{K}] = [\mathrm{G} : \mathrm{K}]$ *if and only if* $G = KH$.

SKETCH OF PROOF. Let A be the set of all right cosets of $H \cap K$ in H and B the set of all right cosets of K in G. The map $\varphi : A \to B$ given by $(H \cap K)h \mapsto Kh$

($h \in H$) is well defined since $(H \cap K)h' = (H \cap K)h$ implies $h'h^{-1} \in H \cap K \subset K$ and hence $Kh' = Kh$. Show that φ is injective. Then $[H : H \cap K] = |A| \leq |B| = [G : K]$. If $[G : K]$ is finite, then show that $[H : H \cap K] = [G : K]$ if and only if φ is surjective and that φ is surjective if and only if $G = KH$. Note that for $h \in H$, $k \in K$, $Kkh = Kh$ since $(kh)h^{-1} = k \in K$. ■

Proposition 4.9. *Let* H *and* K *be subgroups of finite index of a group* G. *Then* $[G : H \cap K]$ *is finite and* $[G : H \cap K] \leq [G : H][G : K]$. *Furthermore,* $[G : H \cap K] = [G : H][G : K]$ *if and only if* $G = HK$.

PROOF. Exercise; use Theorem 4.5 and Proposition 4.8. ■

EXERCISES

1. Let G be a group and $\{H_i \mid i \in I\}$ a family of subgroups. Then for any $a \in G$, $(\bigcap_i H_i)a = \bigcap_i H_i a$.

2. (a) Let H be the cyclic subgroup (of order 2) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then no left coset of H (except H itself) is also a right coset. There exists $a \in S_3$ such that $aH \cap Ha = \{a\}$.

   (b) If K is the cyclic subgroup (of order 3) of S_3 generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, then every left coset of K is also a right coset of K.

3. The following conditions on a finite group G are equivalent.
   (i) $|G|$ is prime.
   (ii) $G \neq \langle e \rangle$ and G has no proper subgroups.
   (iii) $G \cong Z_p$ for some prime p.

4. (Euler-Fermat) Let a be an integer and p a prime such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$. [*Hint:* Consider $\bar{a} \in Z_p$ and the multiplicative group of nonzero elements of Z_p; see Exercise 1.7.] It follows that $a^p \equiv a \pmod{p}$ for any integer a.

5. Prove that there are only two distinct groups of order 4 (up to isomorphism), namely Z_4 and $Z_2 \oplus Z_2$. [*Hint:* By Lagrange's Theorem 4.6 a group of order 4 that is not cyclic must consist of an identity and three elements of order 2.]

6. Let H,K be subgroups of a group G. Then HK is a subgroup of G if and only if $HK = KH$.

7. Let G be a group of order $p^k m$, with p prime and $(p,m) = 1$. Let H be a subgroup of order p^k and K a subgroup of order p^d, with $0 < d \leq k$ and $K \not\subset H$. Show that HK is not a subgroup of G.

8. If H and K are subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime, then $G = HK$.

9. If H,K and N are subgroups of a group G such that $H < N$, then $HK \cap N = H(K \cap N)$.

10. Let H,K,N be subgroups of a group G such that $H < K$, $H \cap N = K \cap N$, and $HN = KN$. Show that $H = K$.

11. Let G be a group of order $2n$; then G contains an element of order 2. If n is odd and G abelian, there is only one element of order 2.

12. If H and K are subgroups of a group G, then $[H \vee K : H] \geq [K : H \cap K]$.

13. If $p > q$ are primes, a group of order pq has at most one subgroup of order p. [*Hint:* Suppose H,K are distinct subgroups of order p. Show $H \cap K = \langle e \rangle$; use Exercise 12 to get a contradiction.]

14. Let G be a group and $a,b \in G$ such that (i) $|a| = 4 = |b|$; (ii) $a^2 = b^2$; (iii) $ba = a^3b = a^{-1}b$; (iv) $a \neq b$; (v) $G = \langle a,b \rangle$. Show that $|G| = 8$ and $G \cong Q_8$. (See Exercise 2.3; observe that the generators A,B of Q_8 also satisfy (i)–(v).)

5. NORMALITY, QUOTIENT GROUPS, AND HOMOMORPHISMS

We shall study those subgroups N of a group G such that left and right congruence modulo N coincide. Such subgroups play an important role in determining both the structure of a group G and the nature of homomorphisms with domain G.

Theorem 5.1. *If* N *is a subgroup of a group* G, *then the following conditions are equivalent.*

(i) *Left and right congruence modulo* N *coincide (that is, define the same equivalence relation on* G);
(ii) *every left coset of* N *in* G *is a right coset of* N *in* G;
(iii) $aN = Na$ *for all* $a \in G$;
(iv) *for all* $a \in G$, $aNa^{-1} \subset N$, *where* $aNa^{-1} = \{ana^{-1} \mid n \in N\}$;
(v) *for all* $a \in G$, $aNa^{-1} = N$.

PROOF. (i) $\Leftrightarrow$ (iii) Two equivalence relations R and S are identical if and only if the equivalence class of each element under R is equal to its equivalence class under S. In this case the equivalence classes are the left and right cosets respectively of N. (ii) $\Rightarrow$ (iii) If $aN = Nb$ for some $b \in G$, then $a \in Nb \cap Na$, which implies $Nb = Na$ since two *right* cosets are either disjoint or equal. (iii) $\Rightarrow$ (iv) is trivial. (iv) $\Rightarrow$ (v) We have $aNa^{-1} \subset N$. Since (iv) also holds for $a^{-1} \in G$, $a^{-1}Na \subset N$. Therefore for every $n \in N$, $n = a(a^{-1}na)a^{-1} \in aNa^{-1}$ and $N \subset aNa^{-1}$. (v) $\Rightarrow$ (ii) is immediate. ■

Definition 5.2. *A subgroup* N *of a group* G *which satisfies the equivalent conditions of Theorem 5.1 is said to be* **normal** *in* G (*or a* **normal subgroup** *of* G); *we write* $N \lhd G$ *if* N *is normal in* G.

In view of Theorem 5.1 we may omit the subscripts "r" and "l" when denoting congruence modulo a normal subgroup.

EXAMPLES. Every subgroup of an abelian group is trivially normal. The subgroup H generated by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ in S_3 is normal (Exercise 4.2). More generally any subgroup N of index 2 in a group G is normal (Exercise 1). The intersection of any family of normal subgroups is a normal subgroup (Exercise 2).

If G is a group with subgroups N and M such that $N \lhd M$ and $M \lhd G$, it does not follow that $N \lhd G$ (Exercise 10). However, it is easy to see that if N is normal in G, then N is normal in every subgroup of G containing N.

Recall that the join $H \vee K$ of two subgroups is the subgroup $\langle H \cup K \rangle$ generated by H and K.

Theorem 5.3. *Let* K *and* N *be subgroups of a group* G *with* N *normal in* G. *Then*

(i) $\mathrm{N} \cap \mathrm{K}$ *is a normal subgroup of* K;
(ii) N *is a normal subgroup of* $\mathrm{N} \vee \mathrm{K}$;
(iii) $\mathrm{NK} = \mathrm{N} \vee \mathrm{K} = \mathrm{KN}$;
(iv) *if* K *is normal in* G *and* $\mathrm{K} \cap \mathrm{N} = \langle \mathrm{e} \rangle$, *then* $\mathrm{nk} = \mathrm{kn}$ *for all* $\mathrm{k} \in \mathrm{K}$ *and* $\mathrm{n} \in \mathrm{N}$.

PROOF. (i) If $n \in N \cap K$ and $a \in K$, then $ana^{-1} \in N$ since $N \lhd G$ and $ana^{-1} \in K$ since $K < G$. Thus $a(N \cap K)a^{-1} \subset N \cap K$ and $N \cap K \lhd K$. (ii) is trivial since $N < N \vee K$. (iii) Clearly $NK \subset N \vee K$. An element x of $N \vee K$ is a product of the form $n_1k_1n_2k_2 \cdots n_rk_r$, with $n_i \in N$, $k_i \in K$ (Theorem 2.8). Since $N \lhd G$, $n_ik_j = k_jn_i'$, $n_i' \in N$ and therefore x can be written in the form $n(k_1 \cdots k_r)$, $n \in N$. Thus $N \vee K \subset NK$. Similarly $KN = N \vee K$. (iv) Let $k \in K$ and $n \in N$. Then $nkn^{-1} \in K$ since $K \lhd G$ and $kn^{-1}k^{-1} \in N$ since $N \lhd G$. Hence $(nkn^{-1})k^{-1} = n(kn^{-1}k^{-1}) \in N \cap K = \langle e \rangle$, which implies $kn = nk$. ■

Theorem 5.4. *If* N *is a normal subgroup of a group* G *and* $\mathrm{G/N}$ *is the set of all (left) cosets of* N *in* G, *then* $\mathrm{G/N}$ *is a group of order* $[\mathrm{G} : \mathrm{N}]$ *under the binary operation given by* $(\mathrm{aN})(\mathrm{bN}) = \mathrm{abN}$.

PROOF. Since the coset aN [resp. bN, abN] is simply the equivalence class of $a \in G$ [resp. $b \in G$, $ab \in G$] under the equivalence relation of congruence modulo N, it suffices by Theorem 1.5 to show that congruence modulo N is a congruence relation, that is, that $a_1 \equiv a \pmod{N}$ and $b_1 \equiv b \pmod{N}$ imply $a_1b_1 \equiv ab \pmod{N}$. By assumption $a_1a^{-1} = n_1 \in N$ and $b_1b^{-1} = n_2 \in N$. Hence $(a_1b_1)(ab)^{-1} = a_1b_1b^{-1}a^{-1} = (a_1n_2)a^{-1}$. But since N is normal, $a_1N = Na_1$ which implies that $a_1n_2 = n_3a_1$ for some $n_3 \in N$. Consequently $(a_1b_1)(ab)^{-1} = (a_1n_2)a^{-1} = n_3a_1a^{-1} = n_3n_1 \in N$, whence $a_1b_1 \equiv ab \pmod{N}$. ■

If N is a normal subgroup of a group G, then the group G/N, as in Theorem 5.4, is called the **quotient group** or **factor group** of G by N. If G is written additively, then the group operation in G/N is given by $(a + N) + (b + N) = (a + b) + N$.

REMARK. If $m > 1$ is a (fixed) integer and $k \in \mathbf{Z}$, then the remarks preceding Definition 4.1 show that the equivalence class of k under congruence modulo m is

precisely the coset of $\langle m \rangle$ in $\mathbf{Z}$ which contains k; that is, as sets, $Z_m = \mathbf{Z}/\langle m \rangle$. Theorems 1.5 and 5.4 show that the group operations coincide, whence $Z_m = \mathbf{Z}/\langle m \rangle$ as groups.

We now explore the relationships between normal subgroups, quotient groups, and homomorphisms.

Theorem 5.5. If $f: \mathrm{G} \to \mathrm{H}$ *is a homomorphism of groups, then the kernel of* f *is a normal subgroup of* G. *Conversely, if* N *is a normal subgroup of* G, *then the map* $\pi : \mathrm{G} \to \mathrm{G/N}$ *given by* $\pi(\mathrm{a}) = \mathrm{aN}$ *is an epimorphism with kernel* N.

PROOF. If $x \in \operatorname{Ker} f$ and $a \in G$, then

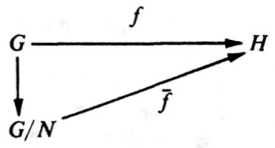
$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)ef(a)^{-1} = e$$

and $axa^{-1} \in \operatorname{Ker} f$. Therefore $a(\operatorname{Ker} f)a^{-1} \subset \operatorname{Ker} f$ and $\operatorname{Ker} f \lhd G$. The map $\pi : G \to G/N$ is clearly surjective and since $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$, π is an epimorphism. $\operatorname{Ker} \pi = \{a \in G \mid \pi(a) = eN = N\} = \{a \in G \mid aN = N\}$ $= \{a \in G \mid a \in N\} = N$. ■

The map $\pi : G \to G/N$ is called the **canonical epimorphism** or **projection.** Hereafter unless stated otherwise $G \to G/N$ $(N \lhd G)$ always denotes the canonical epimorphism.

Theorem 5.6. *If* $\mathrm{f} : \mathrm{G} \to \mathrm{H}$ *is a homomorphism of groups and* N *is a normal subgroup of* G *contained in the kernel of* f, *then there is a unique homomorphism* $\bar{\mathrm{f}} : \mathrm{G/N} \to \mathrm{H}$ *such that* $\bar{\mathrm{f}}(\mathrm{aN}) = \mathrm{f(a)}$ *for all* $\mathrm{a} \in \mathrm{G}$. *Im* f = *Im* $\bar{\mathrm{f}}$ *and Ker* $\bar{\mathrm{f}}$ = (*Ker* f)/N. $\bar{\mathrm{f}}$ *is an isomorphism if and only if* f *is an epimorphism and* N = *Ker* f.

The essential part of the conclusion may be rephrased: there exists a unique homomorphism $\bar{f}: G/N \to H$ such that the diagram:



is commutative. Corollary 5.8 below may also be stated in terms of commutative diagrams.

PROOF OF 5.6. If $b \in aN$, then $b = an$, $n \in N$, and $f(b) = f(an) = f(a)f(n)$ $= f(a)e = f(a)$, since $N < \operatorname{Ker} f$. Therefore, f has the same effect on every element of the coset aN and the map $\bar{f}: G/N \to H$ given by $\bar{f}(aN) = f(a)$ is a well-defined function. Since $\bar{f}(aNbN) = \bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$, $\bar{f}$ is a homomorphism. Clearly $\operatorname{Im} \bar{f} = \operatorname{Im} f$ and

$$aN \in \operatorname{Ker} \bar{f} \Leftrightarrow f(a) = e \Leftrightarrow a \in \operatorname{Ker} f,$$

whence $\operatorname{Ker} \bar{f} = \{aN \mid a \in \operatorname{Ker} f\} = (\operatorname{Ker} f)/N$. $\bar{f}$ is unique since it is completely determined by f. Finally it is clear that $\bar{f}$ is an epimorphism if and only if f is. By Theorem 2.3 $\bar{f}$ is a monomorphism if and only if $\operatorname{Ker} \bar{f} = (\operatorname{Ker} f)/N$ is the trivial subgroup of G/N, which occurs if and only if $\operatorname{Ker} f = N$. ■

Corollary 5.7. (*First Isomorphism Theorem*) *If* $\mathrm{f} : \mathrm{G} \to \mathrm{H}$ *is a homomorphism of groups, then* f *induces an isomorphism* $\mathrm{G}/\mathit{Ker}\ \mathrm{f} \cong \mathit{Im}\ \mathrm{f}$.

PROOF. $f : G \twoheadrightarrow \operatorname{Im} f$ is an epimorphism. Apply Theorem 5.6 with $N = \operatorname{Ker} f$. ■

Corollary 5.8. *If* $\mathrm{f} : \mathrm{G} \to \mathrm{H}$ *is a homomorphism of groups,* $\mathrm{N} \lhd \mathrm{G}$, $\mathrm{M} \lhd \mathrm{H}$, *and* $\mathrm{f}(N) < \mathrm{M}$, *then* f *induces a homomorphism* $\bar{\mathrm{f}} : \mathrm{G/N} \to \mathrm{H/M}$, *given by* $\mathrm{aN} \mapsto \mathrm{f(a)M}$.

$\bar{\mathrm{f}}$ *is an isomorphism if and only if Im* $\mathrm{f} \vee \mathrm{M} = \mathrm{H}$ *and* $\mathrm{f}^{-1}(\mathrm{M}) \subset \mathrm{N}$. *In particular if f is an epimorphism such that* $\mathrm{f(N)} = \mathrm{M}$ *and Ker* $\mathrm{f} \subset \mathrm{N}$, *then* $\bar{\mathrm{f}}$ *is an isomorphism.*

SKETCH OF PROOF. Consider the composition $G \xrightarrow{f} H \xrightarrow{\pi} H/M$ and verify that $N \subset f^{-1}(M) = \operatorname{Ker} \pi f$. By Theorem 5.6 (applied to πf) the map $G/N \to H/M$ given by $aN \mapsto (\pi f)(a) = f(a)M$ is a homomorphism that is an isomorphism if and only if πf is an epimorphism and $N = \operatorname{Ker} \pi f$. But the latter conditions hold if and only if $\operatorname{Im} f \vee M = H$ and $f^{-1}(M) \subset N$. If f is an epimorphism, then $H = \operatorname{Im} f = \operatorname{Im} f \vee M$. If $f(N) = M$ and $\operatorname{Ker} f \subset N$, then $f^{-1}(M) \subset N$, whence $\bar{f}$ is an isomorphism. ■

Corollary 5.9. (*Second Isomorphism Theorem*) *If* K *and* N *are subgroups of a group* G, *with* N *normal in* G, *then* $\mathrm{K}/(\mathrm{N} \cap \mathrm{K}) \cong \mathrm{NK/N}$.

PROOF. $N \lhd NK = N \vee K$ by Theorem 5.3. The composition $K \xrightarrow{\subseteq} NK \xrightarrow{\pi} NK/N$ is a homomorphism f with kernel $K \cap N$, whence $\bar{f} : K/K \cap N \cong \operatorname{Im} f$ by Corollary 5.7. Every element in NK/N is of the form nkN ($n \in N, k \in K$). The normality of N implies that $nk = kn_1$ ($n_1 \in N$), whence $nkN = kn_1N = kN = f(k)$. Therefore f is an epimorphism and hence $\operatorname{Im} f = NK/N$. ■

Corollary 5.10. (*Third Isomorphism Theorem*). *If* H *and* K *are normal subgroups of a group* G *such that* $\mathrm{K} < \mathrm{H}$, *then* H/K *is a normal subgroup of* G/K *and* $(\mathrm{G/K})/(\mathrm{H/K}) \cong \mathrm{G/H}$.

PROOF. The identity map $1_G : G \to G$ has $1_G(K) < H$ and therefore induces an epimorphism $I : G/K \to G/H$, with $I(aK) = aH$. Since $H = I(aK)$ if and only if $a \in H$, $\operatorname{Ker} I = \{aK \mid a \in H\} = H/K$. Hence $H/K \lhd G/K$ by Theorem 5.5 and $G/H = \operatorname{Im} I \cong (G/K)/\operatorname{Ker} I = (G/K)/(H/K)$ by Corollary 5.7. ■

Theorem 5.11. *If* $f : G \to H$ *is an epimorphism of groups, then the assignment* $K \mapsto f(K)$ *defines a one-to-one correspondence between the set* $S_f(G)$ *of all subgroups* K *of* G *which contain* $\operatorname{Ker} f$ *and the set* $S(H)$ *of all subgroups of* H. *Under this correspondence normal subgroups correspond to normal subgroups.*

SKETCH OF PROOF. By Exercise 2.9 the assignment $K \mapsto f(K)$ defines a function $\varphi : S_f(G) \to S(H)$ and $f^{-1}(J)$ is a subgroup of G for every subgroup J of H. Since $J < H$ implies $\operatorname{Ker} f < f^{-1}(J)$ and $f(f^{-1}(J)) = J$, φ is surjective. Exercise 18 shows that $f^{-1}(f(K)) = K$ if and only if $\operatorname{Ker} f < K$. It follows that φ is injective. To prove the last statement verify that $K \lhd G$ implies $f(K) \lhd H$ and $J \lhd H$ implies $f^{-1}(J) \lhd G$. ■

Corollary 5.12. *If* N *is a normal subgroup of a group* G, *then every subgroup of* G/N *is of the form* K/N, *where* K *is a subgroup of* G *that contains* N. *Furthermore,* K/N *is normal in* G/N *if and only if* K *is normal in* G.

PROOF. Apply Theorem 5.11 to the canonical epimorphism $\pi : G \to G/N$. If $N < K < G$, then $\pi(K) = K/N$. ■

EXERCISES

1. If N is a subgroup of index 2 in a group G, then N is normal in G.
2. If $\{N_i \mid i \in I\}$ is a family of normal subgroups of a group G, then $\bigcap_{i \in I} N_i$ is a normal subgroup of G.
3. Let N be a subgroup of a group G. N is normal in G if and only if (right) congruence modulo N is a congruence relation on G.
4. Let $\sim$ be an equivalence relation on a group G and let $N = \{a \in G \mid a \sim e\}$. Then $\sim$ is a congruence relation on G if and only if N is a normal subgroup of G and $\sim$ is congruence modulo N.
5. Let $N < S_4$ consist of all those permutations σ such that $\sigma(4) = 4$. Is N normal in S_4?
6. Let $H < G$; then the set aHa^{-1} is a subgroup for each $a \in G$, and $H \cong aHa^{-1}$.
7. Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, then H is normal in G.
8. All subgroups of the quaternion group are normal (see Exercises 2.3 and 4.14).
9. (a) If G is a group, then the center of G is a normal subgroup of G (see Exercise 2.11);
   (b) the center of S_n is the identity subgroup for all $n > 2$.
10. Find subgroups H and K of D_4^* such that $H \lhd K$ and $K \lhd D_4^*$, but H is not normal in D_4^*.
11. If H is a cyclic subgroup of a group G and H is normal in G, then every subgroup of H is normal in G. [Compare Exercise 10.]

12. If H is a normal subgroup of a group G such that H and G/H are finitely generated, then so is G.

13. (a) Let $H \lhd G$, $K \lhd G$. Show that $H \vee K$ is normal in G.
(b) Prove that the set of all normal subgroups of G forms a complete lattice under inclusion (Introduction, Exercise 7.2).

14. If $N_1 \lhd G_1$, $N_2 \lhd G_2$ then $(N_1 \times N_2) \lhd (G_1 \times G_2)$ and $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

15. Let $N \lhd G$ and $K \lhd G$. If $N \cap K = \langle e \rangle$ and $N \vee K = G$, then $G/N \cong K$.

16. If $f: G \to H$ is a homomorphism, H is abelian and N is a subgroup of G containing Ker f, then N is normal in G.

17. (a) Consider the subgroups $\langle 6 \rangle$ and $\langle 30 \rangle$ of $\mathbf{Z}$ and show that $\langle 6 \rangle/\langle 30 \rangle \cong Z_5$.
(b) For any $k,m > 0$, $\langle k \rangle/\langle km \rangle \cong Z_m$; in particular, $\mathbf{Z}/\langle m \rangle = \langle 1 \rangle/\langle m \rangle \cong Z_m$.

18. If $f: G \to H$ is a homomorphism with kernel N and $K < G$, then prove that $f^{-1}(f(K)) = KN$. Hence $f^{-1}(f(K)) = K$ if and only if $N < K$.

19. If $N \lhd G$, $[G : N]$ finite, $H < G$, $|H|$ finite, and $[G : N]$ and $|H|$ are relatively prime, then $H < N$.

20. If $N \lhd G$, $|N|$ finite, $H < G$, $[G : H]$ finite, and $[G : H]$ and $|N|$ are relatively prime, then $N < H$.

21. If H is a subgroup of $Z(p^\infty)$ and $H \neq Z(p^\infty)$, then $Z(p^\infty)/H \cong Z(p^\infty)$. [*Hint:* if $H = \langle \overline{1/p^n} \rangle$, let $x_i = \overline{1/p^{n+i}} + H$ and apply Exercise 3.7(e).]

6. SYMMETRIC, ALTERNATING, AND DIHEDRAL GROUPS

In this section we shall study in some detail the symmetric group S_n and certain of its subgroups. By definition S_n is the group of all bijections $I_n \to I_n$, where $I_n = \{1,2,\ldots,n\}$. The elements of S_n are called permutations. In addition to the notation given on page 26 for permutations in S_n there is another standard notation:

Definition 6.1. *Let* $i_1,i_2,\ldots,i_r$, $(r \leq n)$ *be distinct elements of* $I_n = \{1,2,\ldots n\}$. *Then* $(i_1i_2i_3\cdots i_r)$ *denotes the permutation that maps* $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $i_3 \mapsto i_4, \ldots,$ $i_{r-1} \mapsto i_r$, *and* $i_r \mapsto i_1$, *and maps every other element of* I_n *onto itself.* $(i_1i_2\cdots i_r)$ *is called a* **cycle** *of length* r *or an* r*-cycle; a* 2*-cycle is called a* **transposition**.

The cycle notation is not unique (see below); indeed, strictly speaking, the cycle notation is ambiguous since $(i_1\cdots i_r)$ may be an element of any S_n, $n \geq r$. In context, however, this will cause no confusion. A 1-cycle (k) is the identity permutation. Clearly, an r-cycle is an element of order r in S_n. Also observe that if τ is a cycle and $\tau(x) \neq x$ for some $x \in I_n$, then $\tau = (x\tau(x)\tau^2(x)\cdots\tau^d(x))$ for some $d \geq 1$. The inverse of the cycle $(i_1i_2\cdots i_r)$ is the cycle $(i_ri_{r-1}i_{r-2}\cdots i_2i_1) = (i_1i_ri_{r-1}i_{r-2}\cdots i_2)$ (verify!).

EXAMPLES. The permutation $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ is a 4-cycle: $\tau = (1432)$ $= (4321) = (3214) = (2143)$. If σ is the 3-cycle (125), then $\sigma\tau = (125)(1432) = (1435)$

(remember: permutations are functions and $\sigma\tau$ means τ followed by σ); similarly $\tau\sigma = (1432)(125) = (2543)$ so that $\sigma\tau \neq \tau\sigma$. There is one case, however, when two permutations do commute.

Definition 6.2. *The permutations* $\sigma_1,\sigma_2, \ldots, \sigma_r$ *of* S_n *are said to be* **disjoint** *provided that for each* $1 \leq i \leq r$, *and every* $k \in I_n$, $\sigma_i(k) \neq k$ *implies* $\sigma_j(k) = k$ *for all* $j \neq i$.

In other words $\sigma_1,\sigma_2, \ldots, \sigma_r$ are disjoint if and only if no element of I_n is moved by more than one of $\sigma_1, \ldots, \sigma_r$. It is easy to see that $\tau\sigma = \sigma\tau$ whenever σ and τ are disjoint.

Theorem 6.3. *Every nonidentity permutation in* S_n *is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least* 2.

SKETCH OF PROOF. Let $\sigma \in S_n$, $\sigma \neq (1)$. Verify that the following is an equivalence relation on I_n: for $x,y \in I_n$, $x \sim y$ if and only if $y = \sigma^m(x)$ for some $m \in \mathbf{Z}$. The equivalence classes $\{B_i \mid 1 \leq i \leq s\}$ of this equivalence relation are called the *orbits* of σ and form a partition of I_n (Introduction, Theorem 4.1). Note that if $x \in B_i$, then $B_i = \{u \mid x \sim u\} = \{\sigma^m(x) \mid m \in \mathbf{Z}\}$. Let $B_1,B_2, \ldots, B_r$ $(1 \leq r \leq s)$ be those orbits that contain more than one element each ($r \geq 1$ since $\sigma \neq (1)$). For each $i \leq r$ define $\sigma_i \in S_n$ by:

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{if } x \in B_i; \\ x & \text{if } x \notin B_i. \end{cases}$$

Each σ_i is a well-defined nonidentity permutation of I_n since $\sigma \mid B_i$ is a bijection $B_i \to B_i$. $\sigma_1,\sigma_2, \ldots, \sigma_r$ are disjoint permutations since the sets $B_1, \ldots, B_r$ are mutually disjoint. Finally verify that $\sigma = \sigma_1\sigma_2\cdots\sigma_r$; (note that $x \in B_i$ implies $\sigma(x) = \sigma_i(x)$ if $i \leq r$ and $\sigma(x) = x$ if $i > r$; use disjointness). We must show that each σ_i is a cycle.

If $x \in B_i$ $(i \leq r)$, then since B_i is finite there is a least positive integer d such that $\sigma^d(x) = \sigma^j(x)$ for some j $(0 \leq j < d)$. Since $\sigma^{d-j}(x) = x$ and $0 < d - j \leq d$, we must have $j = 0$ and $\sigma^d(x) = x$. Hence $(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x))$ is a well-defined cycle of length at least 2. If $\sigma^m(x) \in B_i$, then $m = ad + b$ for some $a,b \in \mathbf{Z}$ such that $0 \leq b < d$. Hence $\sigma^m(x) = \sigma^{b+ad}(x) = \sigma^b\sigma^{ad}(x) = \sigma^b(x) \in \{x,\sigma(x),\sigma^2(x), \ldots, \sigma^{d-1}(x)\}$. Therefore $B_i = \{x,\sigma(x),\sigma^2(x), \ldots, \sigma^{d-1}(x)\}$ and it follows that σ_i is the cycle

$$(x\sigma(x)\sigma^2(x)\cdots\sigma^{d-1}(x)).$$

Suppose $\tau_1, \ldots, \tau_t$ are disjoint cycles such that $\sigma = \tau_1\tau_2\cdots\tau_t$. Let $x \in I_n$ be such that $\sigma(x) \neq x$. By disjointness there exists a unique j $(1 \leq j \leq t)$ with $\sigma(x) = \tau_j(x)$. Since $\sigma\tau_j = \tau_j\sigma$, we have $\sigma^k(x) = \tau_j^k(x)$ for all $k \in \mathbf{Z}$. Therefore, the orbit of x under τ_j is precisely the orbit of x under σ, say B_i. Consequently, $\tau_j(y) = \sigma(y)$ for every $y \in B_i$ (since $y = \sigma^n(x) = \tau_j^n(x)$ for some $n \in \mathbf{Z}$). Since τ_j is a cycle it has only one nontrivial orbit (verify!), which must be B_i since $x \neq \sigma(x) = \tau_j(x)$. Therefore $\tau_j(y) = y$ for all $y \notin B_i$, whence $\tau_j = \sigma_i$. A suitable inductive argument shows that $r = t$ and (after reindexing) $\sigma_i = \tau_i$ for each $i = 1,2, \ldots, r$. ■

Corollary 6.4. *The order of a permutation $\sigma \in S_n$ is the least common multiple of the orders of its disjoint cycles.*

PROOF. Let $\sigma = \sigma_1 \cdots \sigma_r$, with $\{\sigma_i\}$ disjoint cycles. Since disjoint cycles commute, $\sigma^m = \sigma_1^m \cdots \sigma_r^m$ for all $m \in \mathbf{Z}$ and $\sigma^m = (1)$ if and only if $\sigma_i^m = (1)$ for all i. Therefore $\sigma^m = (1)$ if and only if $|\sigma_i|$ divides m for all i (Theorem 3.4). Since $|\sigma|$ is the least such m, the conclusion follows. ■

Corollary 6.5. *Every permutation in S_n can be written as a product of (not necessarily disjoint) transpositions.*

PROOF. It suffices by Theorem 6.3 to show that every cycle is a product of transpositions. This is easy: $(x_1) = (x_1x_2)(x_1x_2)$ and for $r > 1$, $(x_1x_2x_3 \cdots x_r) = (x_1x_r)(x_1x_{r-1}) \cdots (x_1x_3)(x_1x_2)$. ■

Definition 6.6. *A permutation $\tau \in S_n$ is said to be* **even** *[resp.* **odd***] if τ can be written as a product of an even [resp. odd] number of transpositions.*

The **sign of a permutation** τ, denoted sgn τ, is 1 or -1 according as τ is even or odd. The fact that sgn τ is well defined is an immediate consequence of

Theorem 6.7. *A permutation in S_n ($n \geq 2$) cannot be both even and odd.*

PROOF. Let $i_1, i_2, \ldots, i_n$ be the integers $1,2, \ldots, n$ in some order and define $\Delta(i_1, \ldots, i_n)$ to be the integer $\prod (i_j - i_k)$, where the product is taken over all pairs (j,k) such that $1 \leq j < k \leq n$. Note that $\Delta(i_1, \ldots, i_n) \neq 0$. We first compute $\Delta(\sigma(i_1), \ldots, \sigma(i_n))$ when $\sigma \in S_n$ is a transposition, say $\sigma = (i_c i_d)$ with $c < d$. We have $\Delta(i_1, \ldots, i_n) = (i_c - i_d)ABCDEFG$, where

$$A = \prod_{\substack{j<k \\ j,k \neq c,d}} (i_j - i_k); \qquad B = \prod_{j<c} (i_j - i_c); \qquad C = \prod_{j<c} (i_j - i_d);$$

$$D = \prod_{c<j<d} (i_j - i_d); \qquad E = \prod_{c<k<d} (i_c - i_k); \qquad F = \prod_{d<k} (i_c - i_k);$$

$$G = \prod_{d<k} (i_d - i_k).$$

We write $\sigma(A)$ for $\prod_{\substack{j<k \\ j,k \neq c,d}} (\sigma(i_j) - \sigma(i_k))$ and similarly for $\sigma(B)$, $\sigma(C)$, etc. Verify that $\sigma(A) = A$; $\sigma(B) = C$ and $\sigma(C) = B$; $\sigma(D) = (-1)^{d-c-1}E$ and $\sigma(E) = (-1)^{d-c-1}D$; $\sigma(F) = G$, and $\sigma(G) = F$. Finally, $\sigma(i_c - i_d) = \sigma(i_c) - \sigma(i_d) = i_d - i_c = -(i_c - i_d)$. Consequently,

$$\Delta(\sigma(i_1), \ldots, \sigma(i_n)) = \sigma(i_c - i_d)\sigma(A)\sigma(B) \cdots \sigma(G) = (-1)^{1+2(d-c-1)}(i_c - i_d)ABCDEFG$$
$$= -\Delta(i_1, \ldots, i_n).$$

Suppose for some $\tau \in S_n$, $\tau = \tau_1 \cdots \tau_r$ and $\tau = \sigma_1 \cdots \sigma_s$ with τ_i, σ_j transpositions, r even and s odd. Then for $(i_1, \ldots, i_n) = (1,2, \ldots, n)$ the previous paragraph implies $\Delta(\tau(1), \ldots, \tau(n)) = \Delta(\tau_1 \cdots \tau_r(1), \ldots, \tau_1 \cdots \tau_r(n)) = -\Delta(\tau_2 \cdots \tau_r(1), \ldots,$

$\tau_2 \cdots \tau_r(n)) = \cdots = (-1)^r \Delta(1,2,\ldots,n) = \Delta(1,2,\ldots,n)$. Similarly $\Delta(\tau(1),\ldots,\tau(n))$ $= (-1)^s \Delta(1,2,\ldots,n) = -\Delta(1,2,\ldots,n)$, whence $\Delta(1,2,\ldots,n) = -\Delta(1,2,\ldots,n)$. This is a contradiction since $\Delta(1,2,\ldots,n) \neq 0$. ■

Theorem 6.8. *For each* $n \geq 2$, *let* A_n *be the set of all even permutations of* S_n. *Then* A_n *is a normal subgroup of* S_n *of index* 2 *and order* $|S_n|/2 = n!/2$. *Furthermore* A_n *is the only subgroup of* S_n *of index* 2.

The group A_n is called the **alternating group on n letters** or the **alternating group of degree n.**

SKETCH OF PROOF OF 6.8. Let C be the multiplicative subgroup $\{1,-1\}$ of the integers. Define a map $f: S_n \to C$ by $\sigma \mapsto \operatorname{sgn} \sigma$ and verify that f is an epimorphism of groups. Since the kernel of f is clearly A_n, A_n is normal in S_n. By the First Isomorphism Theorem $S_n/A_n \cong C$, which implies $[S_n : A_n] = 2$ and $|A_n| = |S_n|/2$. A_n is the unique subgroup of S_n of index 2 by Exercise 6. ■

Definition 6.9. *A group* G *is said to be* **simple** *if* G *has no proper normal subgroups.*

The only simple abelian groups are the Z_p with p prime (Exercise 4.3). There are a number of nonabelian simple groups; in particular, we have

Theorem 6.10. *The alternating group* A_n *is simple if and only if* $n \neq 4$.

The proof we shall give is quite elementary. It will be preceded by two lemmas. Recall that if τ is a 2-cycle, $\tau^2 = (1)$ and hence $\tau = \tau^{-1}$.

Lemma 6.11. *Let* r,s *be distinct elements of* $\{1,2,\ldots,n\}$. *Then* A_n $(n \geq 3)$ *is generated by the* 3*-cycles* $\{(rsk) \mid 1 \leq k \leq n,\ k \neq r,s\}$.

PROOF. Assume $n > 3$ (the case $n = 3$ is trivial). Every element of A_n is a product of terms of the form $(ab)(cd)$ or $(ab)(ac)$, where a,b,c,d are distinct elements of $\{1,2,\ldots,n\}$. Since $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$, A_n is generated by the set of all 3-cycles. Any 3-cycle is of the form (rsa), (ras), (rab), (sab), or (abc), where a,b,c are distinct and $a,b,c \neq r,s$. Since $(ras) = (rsa)^2$, $(rab) = (rsb)(rsa)^2$, $(sab) = (rsb)^2(rsa)$, and $(abc) = (rsa)^2(rsc)(rsb)^2(rsa)$, A_n is generated by

$$\{(rsk) \mid 1 \leq k \leq n,\ k \neq r,s\}. \quad \blacksquare$$

Lemma 6.12. *If* N *is a normal subgroup of* A_n $(n \geq 3)$ *and* N *contains a* 3*-cycle, then* $N = A_n$.

PROOF. If $(rsc) \in N$, then for any $k \neq r,s,c$, $(rsk) = (rs)(ck)(rsc)^2(ck)(rs)$ $= [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N$. Hence $N = A_n$ by Lemma 6.11. ■

PROOF OF THEOREM 6.10. $A_2 = (1)$ and A_3 is the simple cyclic group of order 3. It is easy to verify that $\{(1),(12)(34),(13)(24),(14)(23)\}$ is a normal subgroup of A_4 (Exercise 7). If $n \geq 5$ and N is a nontrivial normal subgroup of A_n we shall show $N = A_n$ by considering the possible cases.

CASE 1. N contains a 3-cycle; hence $N = A_n$ by Lemma 6.12.

CASE 2. N contains an element σ, the product of disjoint cycles, at least one of which has length $r \geq 4$. Thus $\sigma = (a_1a_2\cdots a_r)\tau$ (disjoint). Let $\delta = (a_1a_2a_3) \in A_n$. Then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ by normality. But

$$\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_1a_ra_{r-1}\cdots a_2)(a_1a_2a_3)(a_1a_2\cdots a_r)\tau(a_1a_3a_2) = (a_1a_3a_r) \in N.$$

Hence $N = A_n$ by Lemma 6.12.

CASE 3. N contains an element σ, the product of disjoint cycles, at least two of which have length 3, so that $\sigma = (a_1a_2a_3)(a_4a_5a_6)\tau$ (disjoint). Let $\delta = (a_1a_2a_4) \in A_n$. Then as above, N contains $\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)\tau$ $(a_1a_4a_2) = (a_1a_4a_2a_6a_3)$. Hence $N = A_n$ by case 2.

CASE 4. N contains an element σ that is the product of one 3-cycle and some 2-cycles, say $\sigma = (a_1a_2a_3)\tau$ (disjoint), with τ a product of disjoint 2-cycles. Then $\sigma^2 \in N$ and $\sigma^2 = (a_1a_2a_3)\tau(a_1a_2a_3)\tau = (a_1a_2a_3)^2\tau^2 = (a_1a_2a_3)^2 = (a_1a_3a_2)$, whence $N = A_n$ by Lemma 6.12.

CASE 5. Every element of N is the product of (an even number of) disjoint 2-cycles. Let $\sigma \in N$, with $\sigma = (a_1a_2)(a_3a_4)\tau$ (disjoint). Let $\delta = (a_1a_2a_3) \in A_n$; then $\sigma^{-1}(\delta\sigma\delta^{-1}) \in N$ as above. Now $\sigma^{-1}(\delta\sigma\delta^{-1}) = \tau^{-1}(a_3a_4)(a_1a_2)(a_1a_2a_3)(a_1a_2)(a_3a_4)\tau(a_1a_3a_2)$ $= (a_1a_3)(a_2a_4)$. Since $n \geq 5$, there is an element $b \in \{1,2,\ldots,n\}$ distinct from a_1,a_2,a_3,a_4. Since $\xi = (a_1a_3b) \in A_n$ and $\zeta = (a_1a_3)(a_2a_4) \in N$, $\zeta(\xi\zeta\xi^{-1}) \in N$. But $\zeta(\xi\zeta\xi^{-1})$ $= (a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4)(a_1ba_3) = (a_1a_3b) \in N$. Hence $N = A_n$ by Lemma 6.12.

Since the cases listed cover all the possibilities, A_n has no proper normal subgroups and hence is simple. ■

Another important subgroup of S_n ($n \geq 3$) is the subgroup D_n generated by $a = (123\cdots n)$ and

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & i & \cdots & n-1 & n \\ 1 & n & n-1 & n-2 & n-3 & \cdots & n+2-i & \cdots & 3 & 2 \end{pmatrix}$$

$$= \prod_{2 \leq i < n+2-i} (i\ n+2-i).$$ D_n is called the **dihedral group of degree n.** The group D_n is isomorphic to and usually identified with the group of all symmetries of a regular polygon with n sides (Exercise 13). In particular D_4 is (isomorphic to) the group D_4^* of symmetries of the square (see pages 25–26).

Theorem 6.13. *For each* $n \geq 3$ *the dihedral group* D_n *is a group of order* $2n$ *whose generators* a *and* b *satisfy:*

(i) $a^n = (1)$; $b^2 = (1)$; $a^k \neq (1)$ if $0 < k < n$;
(ii) $ba = a^{-1}b$.

Any group G *which is generated by elements* a,b ε G *satisfying* (*i*) *and* (*ii*) *for some* n ≥ 3 (*with* e ε G *in place of* (1)) *is isomorphic to* D_n.

SKETCH OF PROOF. Verify that $a,b \in D_n$ as defined above satisfy (i) and (ii), whence $D_n = \langle a,b \rangle = \{a^i b^j \mid 0 \leq i < n;\ j = 0,1\}$ (see Theorem 2.8). Then verify that the $2n$ elements $a^i b^j$ $(0 \leq i < n; j = 0,1)$ are all distinct (just check their action on 1 and 2), whence $|D_n| = 2n$.

Suppose G is a group generated by $a,b \in G$ and a,b satisfy (i) and (ii) for some $n \geq 3$. By Theorem 2.8 every element of G is a finite product $a^{m_1}b^{m_2}a^{m_3}b^{m_4}\cdots b^{m_k}$ $(m_i \in \mathbf{Z})$. By repeated use of (i) and (ii) any such product may be written in the form $a^i b^j$ with $0 \leq i < n$ and $j = 0,1$ (in particular note that $b^2 = e$ and (ii) imply $b = b^{-1}$ and $ab = ba^{-1}$). Denote the generators of D_n by a_1, b_1 to avoid confusion and verify that the map $f: D_n \to G$ given by $a_1^i b_1^j \to a^i b^j$ is an epimorphism of groups. To complete the proof we show that f is a monomorphism. Suppose $f(a_1^i b_1^j) = a^i b^j = e \in G$ with $0 \leq i < n$ and $j = 0,1$. If $j = 1$, then $a^i = b$, and by (ii) $a^{i+1} = a^i a = ba = a^{-1}b = a^{-1}a^i = a^{i-1}$, which implies $a^2 = e$. This contradicts (i) since $n \geq 3$. Therefore $j = 0$ and $e = a^i b^0 = a^i$ with $0 \leq i < n$, which implies $i = 0$ by (i). Thus $f(a_1^i b_1^j) = e$ implies $a_1^i b_1^j = a_1^0 b_1^0 = (1)$. Therefore f is a monomorphism by Theorem 2.3. ■

This theorem is an example of a characterization of a group in terms of "generators and relations." A detailed discussion of this idea will be given in Section 9.

EXERCISES

1. Find four different subgroups of S_4 that are isomorphic to S_3 and nine isomorphic to S_2.

2. (a) S_n is generated by the $n - 1$ transpositions (12), (13), (14), . . . , (1n). [*Hint:* $(1i)(1j)(1i) = (ij)$.]
   (b) S_n is generated by the $n - 1$ transpositions (12), (23), (34), . . . , ($n - 1$ n). [*Hint:* $(1j) = (1\ j-1)(j-1\ j)(1\ j-1)$; use (a).]

3. If $\sigma = (i_1 i_2 \cdots i_r) \in S_n$ and $\tau \in S_n$, then $\tau\sigma\tau^{-1}$ is the r-cycle $(\tau(i_1)\tau(i_2)\cdots\tau(i_r))$.

4. (a) S_n is generated by $\sigma_1 = (12)$ and $\tau = (123\cdots n)$. [*Hint:* Apply Exercise 3 to σ_1, $\sigma_2 = \tau\sigma_1\tau^{-1}$, $\sigma_3 = \tau\sigma_2\tau^{-1}$, . . . , $\sigma_{n-1} = \tau\sigma_{n-2}\tau^{-1}$ and use Exercise 2(b).]
   (b) S_n is generated by (12) and $(23\cdots n)$.

5. Let $\sigma,\tau \in S_n$. If σ is even (odd), then so is $\tau\sigma\tau^{-1}$.

6. A_n is the only subgroup of S_n of index 2. [*Hint:* Show that a subgroup of index 2 must contain all 3-cycles of S_n and apply Lemma 6.11.]

7. Show that $N = \{(1),(12)(34),(13)(24),(14)(23)\}$ is a normal subgroup of S_4 contained in A_4 such that $S_4/N \cong S_3$ and $A_4/N \cong Z_3$.

8. The group A_4 has no subgroup of order 6.

9. For $n \geq 3$ let G_n be the multiplicative group of complex matrices generated by $x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$, where $i^2 = -1$. Show that $G_n \cong D_n$. (*Hint:* recall that $e^{2\pi i} = 1$ and $e^{k2\pi i} \neq 1$, where k is real, unless $k \in \mathbf{Z}$.)

10. Let a be the generator of order n of D_n. Show that $\langle a\rangle \lhd D_n$ and $D_n/\langle a\rangle \cong Z_2$.

11. Find all normal subgroups of D_n.

12. The center (Exercise 2.11) of the group D_n is $\langle e\rangle$ if n is odd and isomorphic to Z_2 if n is even.

13. For each $n \geq 3$ let P_n be a regular polygon of n sides (for $n = 3$, P_n is an equilateral triangle; for $n = 4$, a square). A *symmetry* of P_n is a bijection $P_n \to P_n$ that preserves distances and maps adjacent vertices onto adjacent vertices.
    (a) The set D_n^* of all symmetries of P_n is a group under the binary operation of composition of functions.
    (b) Every $f \in D_n^*$ is completely determined by its action on the vertices of P_n. Number the vertices consecutively $1,2,\ldots,n$; then each $f \in D_n^*$ determines a unique permutation σ_f of $\{1,2,\ldots,n\}$. The assignment $f \mapsto \sigma_f$ defines a monomorphism of groups $\varphi : D_n^* \to S_n$.
    (c) D_n^* is generated by f and g, where f is a rotation of $2\pi/n$ degrees about the center of P_n and g is a reflection about the "diameter" through the center and vertex 1.
    (d) $\sigma_f = (123\cdots n)$ and $\sigma_g = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$, whence $Im\ \varphi = D_n$ and $D_n^* \cong D_n$.

7. CATEGORIES: PRODUCTS, COPRODUCTS, AND FREE OBJECTS

Since we now have several examples at hand, this is an appropriate time to introduce the concept of a category. Categories will serve as a useful language and provide a general context for dealing with a number of different mathematical situations. They are studied in more detail in Chapter X.

The intuitive idea underlying the definition of a category is that several of the mathematical objects already introduced (sets, groups, monoids) or to be introduced (rings, modules) together with the appropriate maps of these objects (functions for sets; homomorphisms for groups, etc.) have a number of formal properties in common. For example, in each case composition of maps (when defined) is associative; each object A has an identity map $1_A : A \to A$ with certain properties. These notions are formalized in

Definition 7.1. *A* **category** *is a class* $\mathcal{C}$ *of objects (denoted* A,B,C, . . .*) together with*

(i) *a class of disjoint sets, denoted hom*(A,B)*, one for each pair of objects in* $\mathcal{C}$ *;(an element* f *of hom*(A,B) *is called a* **morphism** *from* A *to* B *and is denoted* $f : A \to B$*);*
(ii) *for each triple* (A,B,C) *of objects of* $\mathcal{C}$ *a function*

$$hom(B,C) \times hom(A,B) \to hom(A,C);$$

(for morphisms $f : A \to B$, $g : B \to C$, *this function is written* $(g,f) \mapsto g \circ f$ *and* $g \circ f : A \to C$ *is called the* **composite** *of* f *and* g*); all subject to the two axioms:*

(I) Associativity. *If* $f : A \to B$ $g : B \to C$, $h : C \to D$ *are morphisms of* $\mathcal{C}$, *then* $h \circ (g \circ f) = (h \circ g) \circ f$.