PART I

Groups and Subgroups

SECTION 1 BINARY OPERATIONS

The transition from elementary school arithmetic to high school algebra involves using letters to represent unknown numbers and studying the basic properties of equations and expressions. The two main binary operations used in high school algebra are addition and multiplication. Abstract algebra takes the next step in abstraction. Not only are the variables unknown, but the actual operations involved may be unknown! We will study sets that have binary operations with properties similar to those of addition and multiplication of numbers. In Part I, our goal will be to develop some of the basic properties of a group. In this section we start our investigation of groups by defining binary operations, naming properties possessed by some binary operations, and giving examples.

Definitions and Examples

The first step in our journey to understand groups is to give a precise mathematical definition of a binary operation that generalizes the familiar addition and multiplication of numbers. Recall that for any set S, Definition 0.4 defines the set $S \times S$ to contain all ordered pairs (a, b) with $a, b \in S$.

1.1 Definition A **binary operation** $*$ on a set S is a function mapping $S \times S$ into S. For each $(a, b) \in S \times S$, we will denote the element $*((a, b))$ of S by $a * b$. ■

Intuitively, we may regard a binary operation $*$ on S as assigning, to each ordered pair (a, b) of elements of S, an element $a * b$ of S.

Binary refers to the fact that we are mapping *pairs* of elements from S into S. We could also define a ternary operation as a function mapping triples of elements of S to S, but we will have no need for this type of operation. Throughout this book we will often drop the term binary and use the term operation to mean binary operation.

1.2 Example Our usual addition $+$ is an operation on the set $\mathbb{R}$. Our usual multiplication $\cdot$ is a different operation on $\mathbb{R}$. In this example, we could replace $\mathbb{R}$ by any of the sets $\mathbb{C}, \mathbb{Z}$, $\mathbb{R}^+$, or $\mathbb{Z}^+$. ▲

Note that we require an operation on a set S to be defined for *every* ordered pair (a, b) of elements from S.

1.3 Example Let $M(\mathbb{R})$ be the set of all matrices[†] with real entries. The usual matrix addition $+$ is *not* an operation on this set since $A + B$ is not defined for an ordered pair (A, B) of matrices having different numbers of rows or of columns. ▲

Sometimes an operation on S provides an operation on a subset H of S also. We make a formal definition.

1.4 Definition Let $*$ be an operation on S and let H be a subset of S. The subset H is **closed under** $*$ if for all $a, b \in H$ we also have $a * b \in H$. In this case, the operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H. ■

By our very definition of an operation $*$ on S, the set S is closed under $*$, but a subset may not be, as the following example shows.

1.5 Example Our usual addition $+$ on the set $\mathbb{R}$ of real numbers does not induce an operation on the set $\mathbb{R}^*$ of nonzero real numbers because $2 \in \mathbb{R}^*$ and $-2 \in \mathbb{R}^*$, but $2 + (-2) = 0$ and $0 \notin \mathbb{R}^*$. Thus $\mathbb{R}^*$ is not closed under $*$. ▲

In our text, we will often have occasion to decide whether a subset H of S is closed under a binary operation $*$ on S. To arrive at a correct conclusion, *we have to know what it means for an element to be in H*, and to use this fact. Students often have trouble here. Be sure you understand the next example.

1.6 Example Let $+$ and $\cdot$ be the usual operations of addition and multiplication on the set $\mathbb{Z}$, and let $H = \{n^2 | n \in \mathbb{Z}^+\}$. Determine whether H is closed under (a) addition and (b) multiplication.

For part (a), we need only observe that $1^2 = 1$ and $2^2 = 4$ are in H, but that $1 + 4 = 5$ and $5 \notin H$. Thus H is not closed under addition.

For part (b), suppose that $r \in H$ and $s \in H$. Using what it means for r and s to be in H, we see that there must be integers n and m in $\mathbb{Z}^+$ such that $r = n^2$ and $s = m^2$. Consequently, $rs = n^2m^2 = (nm)^2$. By the characterization of elements in H and the fact that $nm \in \mathbb{Z}^+$, this means that $rs \in H$, so H is closed under multiplication. ▲

1.7 Example Let F be the set of all real-valued functions f having as domain the set $\mathbb{R}$ of real numbers. We are familiar from calculus with the operations $+$, $-$, $\cdot$, and $\circ$ on F. Namely, for each ordered pair (f, g) of functions in F, we define for each $x \in \mathbb{R}$

$$\begin{array}{rll} f + g \text{ by } (f + g)(x) = f(x) + g(x) & & \text{addition,} \\ f - g \text{ by } (f - g)(x) = f(x) - g(x) & & \text{subtraction,} \\ f \cdot g \text{ by } (f \cdot g)(x) = f(x)g(x) & & \text{multiplication, and} \\ f \circ g \text{ by } (f \circ g)(x) = f(g(x)) & & \text{composition.} \end{array}$$

All four of these functions are again real valued with domain $\mathbb{R}$, so F is closed under all four operations $+$, $-$, $\cdot$, and $\circ$. ▲

The operations described in the examples above are very familiar to you. In this text, we want to *abstract* basic structural concepts from our familiar algebra. To empha-

[†] Most students of abstract algebra have studied linear algebra and are familiar with matrices and matrix operations. For the benefit of those students, examples involving matrices are often given. The reader who is not familiar with matrices can either skip all references to them or turn to the Appendix at the back of the text, where there is a short summary.

size this concept of *abstraction* from the familiar, we should illustrate these structural concepts with unfamiliar examples.

The most important method of describing a particular binary operation $*$ on a given set is to characterize the element $a * b$ assigned to each pair (a, b) by some property defined in terms of a and b.

1.8 Example On $\mathbb{Z}^+$, we define an operation $*$ by $a * b$ equals the smaller of a and b, or the common value if $a = b$. Thus $2 * 11 = 2$; $15 * 10 = 10$; and $3 * 3 = 3$. ▲

1.9 Example On $\mathbb{Z}^+$, we define an operation $*'$ by $a *' b = a$. Thus $2 *' 3 = 2$; $25 *' 10 = 25$; and $5 *' 5 = 5$. ▲

1.10 Example On $\mathbb{Z}^+$, we define an operation $*''$ by $a *'' b = (a * b) + 2$, where $*$ is defined in Example 1.8. Thus $4 *'' 7 = 6$; $25 *'' 9 = 11$; and $6 *'' 6 = 8$. ▲

It may seem that these examples are of no importance, but in fact they are used millions of times each day. For example, consider the GPS navigational system installed in most cars and cell phones. It searches alternative driving routes, computes the travel time, and determines which route takes less time. The operation in Example 1.8 is programmed into modern GPS systems and it plays an essential role.

Examples 1.8 and 1.9 were chosen to demonstrate that an operation may or may not depend on the order of the given pair. Thus in Example 1.8, $a * b = b * a$ for all $a, b \in \mathbb{Z}^+$, and in Example 1.9 this is not the case, for $5 *' 7 = 5$ but $7 *' 5 = 7$.

1.11 Definition An operation $*$ on a set S is **commutative** if (and only if) $a * b = b * a$ for all $a, b \in S$. ■

As was pointed out in Section 0, it is customary in mathematics to omit the words *and only if* from a definition. Definitions are always understood to be if and only if statements. *Theorems are not always if and only if statements, and no such convention is ever used for theorems.*

Now suppose we wish to consider an expression of the form $a * b * c$. A binary operation $*$ enables us to combine only two elements, and here we have three. The obvious attempts to combine the three elements are to form either $(a * b) * c$ or $a * (b * c)$. With $*$ defined as in Example 1.8, $(2 * 5) * 9$ is computed by $2 * 5 = 2$ and then $2 * 9 = 2$. Likewise, $2 * (5 * 9)$ is computed by $5 * 9 = 5$ and then $2 * 5 = 2$. Hence $(2 * 5) * 9 = 2 * (5 * 9)$, and it is not hard to see that for this $*$,

$$(a * b) * c = a * (b * c),$$

so there is no ambiguity in writing $a * b * c$. But for $*''$ of Example 1.10,

$$(2 *'' 5) *'' 9 = 4 *'' 9 = 6,$$

while

$$2 *'' (5 *'' 9) = 2 *'' 7 = 4.$$

Thus $(a *'' b) *'' c$ need not equal $a *'' (b *'' c)$, and the expression $a *'' b *'' c$ is ambiguous.

1.12 Definition An operation on a set S is **associative** if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$. ■

It can be shown that if $*$ is associative, then longer expressions such as $a * b * c * d$ are not ambiguous. Parentheses may be inserted in any fashion for purposes of computation; the final results of two such computations will be the same.

Composition of functions mapping $\mathbb{R}$ into $\mathbb{R}$ was reviewed in Example 1.7. For any set S and any functions f and g mapping S into S, we similarly define the composition $f \circ g$ of g followed by f as the function mapping S into S such that $(f \circ g)(x) = f(g(x))$ for all $x \in S$. Some of the most important binary operations we consider are defined using composition of functions. It is important to know that function composition is always associative whenever it is defined.

1.13 Theorem **(Associativity of Composition)** Let S be a set and let f, g, and h be functions mapping S into S. Then $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof To show these two functions are equal, we must show that they give the same assignment to each $x \in S$. Computing we find that

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

and

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))),$$

so the same element $f(g(h(x)))$ of S is indeed obtained. ◆

As an example of using Theorem 1.13 to save work, recall that it is a fairly painful exercise in summation notation to show that multiplication of $n \times n$ matrices is an associative operation. If, in a linear algebra course, we first show that there is a one-to-one correspondence between matrices and linear transformations and that multiplication of matrices corresponds to the composition of the linear transformations (functions), we obtain this associativity at once from Theorem 1.13.

There is another property that an operation on a set may have that is of particular importance in algebra. The numbers 0 and 1 play special roles as real numbers because for any real number a, $a + 0 = a$ and $a \times 1 = a$. Because of these properties, 0 is called the *additive identity* in $\mathbb{R}$ and 1 is called the *multiplicative identity* in $\mathbb{R}$. In general we have the following definition of an identity.

1.14 Definition Let S be a set with binary operation $*$. If $e \in S$ has the property that for all $a \in S$, $a * e = e * a = a$, then e is called an **identity element for** $*$. ■

We included both conditions $a * e = a$ and $e * a = a$ in the definition of an identity because we are not assuming that the operation on S is commutative. Of course, if the operation is commutative, such as $+$ and $\times$ on the real numbers, then we would only have to check one of the conditions and the other follows from commutativity.

1.15 Theorem **(Uniqueness of Identity)** A set with binary operation $*$ has at most one identity element.

Proof We need to show that there cannot be two different identity elements. To do this, we assume that both e and e' are identities and show that $e = e'$. Consider the element $e * e'$. Since e is an identity, $e * e' = e'$. But $e * e' = e$ because e' is also an identity. Therefore $e = e'$. ◆

1.16 Example Continuing with Example 1.7, let F be the set of all functions mapping the real numbers to the real numbers. We verify that the function defined by $\iota(x) = x$ is the identity for the operation function composition. Let $f \in F$. Then $f \circ \iota(x) = f(\iota(x)) = f(x)$ and $\iota \circ f(x) = \iota(f(x)) = f(x)$.

The function $m(x) = 1$ is the identity for the operation function multiplication, $a(x) = 0$ is the identity for function addition, but function subtraction has no identity element. ▲

The last property that we consider in this section is the existance of inverse elements. For addition, the inverse of a real number a is $-a$. Using multiplication, the inverse of a nonzero real number a is $\frac{1}{a}$. We now give the formal definition of an inverse for an element x.

1.17 Definition If $*$ is an operation on the set S and S has an identity e, then for any $x \in S$, the inverse of x is an element x' such that $x * x' = x' * x = e$. ■

1.18 Example Continuing Example 1.16, let F be the set of functions mapping the real numbers to the real numbers with operation function composition. We have two definitions for the inverse of a function $f \in F$, the usual definition of an inverse function and Definition 1.17. The two definitions match since both say that an inverse for f is a function f' such that $f \circ f' = f' \circ f = \iota$. So $f \in F$ has an inverse if and only if f is one-to-one and onto. ▲

Tables

For a finite set, a binary operation on the set can be defined by means of a table in which the elements of the set are listed across the top as heads of columns and at the left side as heads of rows. We always require that the elements of the set be listed as heads across the top in the same order as heads down the left side. The next example illustrates the use of a table to define a binary operation.

1.19 Example Table 1.20 defines the binary operation $*$ on $S = \{a, b, c\}$ by the following rule:

(*i*th *entry on the left*) $*$ (*j*th *entry on the top*)
= (*entry in the i*th *row and j*th *column of the table body*).

1.20 Table

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

Thus $a * b = c$ and $b * a = a$, so $*$ is not commutative. ▲

We can easily see that *a binary operation defined by a table is commutative if and only if the entries in the table are symmetric with respect to the diagonal that starts at the upper left corner of the table and terminates at the lower right corner.*

1.21 Example Complete Table 1.22 so that $*$ is a commutative operation on the set $S = \{a, b, c, d\}$.

Solution From Table 1.22, we see that $b * a = d$. For $*$ to be commutative, we must have $a * b = d$ also. Thus we place d in the appropriate square defining $a * b$, which is located symmetrically across the diagonal in Table 1.23 from the square defining $b * a$. We obtain the rest of Table 1.23 in this fashion to give our solution. ▲

1.22 Table

$*$	a	b	c	d
a	b			
b	d	a		
c	a	c	d	
d	a	b	b	c

1.23 Table

$*$	a	b	c	d
a	b	d	a	a
b	d	a	c	b
c	a	c	d	b
d	a	b	b	c

1.24 Example When an operation has an identity element, it is customary to put the identity first in the list of heads. This makes the first row and the first column match the head row and head column as seen in Table 1.25. ▲

1.25 Table

$*$	e	a	b	c
e	e	a	b	c
a	a	c	c	a
b	b	a	e	c
c	c	e	a	b

Some Words of Warning

Classroom experience shows the chaos that may result if a student is given a set and asked to define some binary operation on it. Remember that in an attempt to define a binary operation $*$ on a set S we must be sure that

1. *exactly one element is assigned to each possible ordered pair of elements of S,*
2. *for each ordered pair of elements of S, the element assigned to it is again in S.*

Regarding Condition 1, a student will often make an attempt that assigns an element of S to "most" ordered pairs, but for a few pairs, determines no element. In this event, $*$ is **not everywhere defined** on S. It may also happen that for some pairs, the attempt could assign any of several elements of S, that is, there is ambiguity. In any case of ambiguity, $*$ is **not well defined**. If Condition 2 is violated, then S is **not closed under** $*$.

1.26 Example On which of the sets $\mathbb{Q}$, $\mathbb{Q}^*$, and Z^+ does the formula $a * b = a/b$ define an operation? Note that this formula does not make sense in the case that $b = 0$. So for example, $2 * 0 = 2/0$ is not defined, which means Condition 1 is not satisfied. So $*$ is not an operation on $\mathbb{Q}$.

If we throw out 0, we do have an operation on $\mathbb{Q}^*$ since both Conditions 1 and 2 are satisfied. That is, for any $a, b \in \mathbb{Q}^*$, $a * b = a/b$ is a nonzero rational number.

The set $\mathbb{Z}^+$ does not include 0, but there is another issue. For example, $1 * 2 = 1/2 \notin \mathbb{Z}^+$, which means that Condition 2 is violated and $*$ is not an operation on $\mathbb{Z}^+$.▲

Following are several illustrations of attempts to define operations on sets. Some of them need some work! The symbol $*$ is used for the attempted operation in all these examples.

1.27 Example Let F be the set of all real-valued functions with domain $\mathbb{R}$ as in Example 1.7. Suppose we "define" $*$ to give the usual quotient of f by g, that is, $f * g = h$, where $h(x) = f(x)/g(x)$. Here Condition 2 is violated, for the functions in F are defined for *all* real numbers, and for some $g \in F$, $g(x)$ will be zero for some values of x in $\mathbb{R}$ and $h(x)$ would not be defined at those numbers in $\mathbb{R}$. For example, if $f(x) = \cos x$ and $g(x) = x^2$, then $h(0)$ is undefined, so $h \notin F$. ▲

1.28 Example Let F be as in Example 1.27 and let $f * g = h$, where h is the function greater than both f and g. This "definition" is extremely vague. In the first place, we have not defined what it means for one function to be greater than another. Even if we had, any sensible definition would result in there being many functions greater than both f and g, and $*$ would still be *not well defined.* ▲

1.29 Example Let S be a set consisting of 20 people, no two of whom are of the same height. Define $*$ by $a * b = c$, where c is the tallest person among the 20 in S. This is a perfectly good binary operation on the set, although not a particularly interesting one. ▲

1.30 Example Let S be as in Example 1.29 and let $a * b = c$, where c is the shortest person in S who is taller than both a and b. This $*$ is *not everywhere defined,* since if either a or b is the tallest person in the set, $a * b$ is not determined. ▲

EXERCISES 1

Computations

Exercises 1 through 4 concern the binary operation $*$ defined on $S = \{a, b, c, d, e\}$ by means of Table 1.31.

1. Compute $b * d$, $c * c$, and $[(a * c) * e] * a$.
2. Compute $(a * b) * c$ and $a * (b * c)$. Can you say on the basis of this computation whether $*$ is associative?
3. Compute $(b * d) * c$ and $b * (d * c)$. Can you say on the basis of this computation whether $*$ is associative?
4. Is $*$ commutative? Why?
5. Complete Table 1.32 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d\}$.
6. Table 1.33 can be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries. Does S have an identity element?

1.31 Table

$*$	a	b	c	d	e
a	a	b	c	b	d
b	b	c	a	e	c
c	c	a	b	b	a
d	b	e	b	e	d
e	d	b	a	d	c

1.32 Table

$*$	a	b	c	d
a	a	b	c	
b	b	d		c
c	c	a	d	b
d	d			a

1.33 Table

$*$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

In Exercises 7 through 11, determine whether the operation $*$ is associative, whether the operation is commutative, and whether the set has an identity element.

7. $*$ defined on $\mathbb{Z}$ by letting $a * b = a - b$
8. $*$ defined on $\mathbb{Q}$ by letting $a * b = 2ab + 3$
9. $*$ defined on $\mathbb{Z}$ by letting $a * b = ab + a + b$
10. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = 2^{ab}$
11. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = a^b$
12. Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements; exactly 3 elements; exactly n elements.
13. How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements?
14. How many different binary operations on a set S with n elements have the property that for all $x \in S$, $x * x = x$?
15. How many different binary operations on a set S with n elements have an identity element?

Concepts

In Exercises 16 through 19, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

16. A binary operation $*$ is *commutative* if and only if $a * b = b * a$.
17. A binary operation $*$ on a set S is *associative* if and only if, for all $a, b, c \in S$, we have $(b * c) * a = b * (c * a)$.
18. A subset H of a set S is *closed* under a binary operation $*$ on S if and only if $(a * b) \in H$ for all $a, b \in S$.
19. An identity in the set S with operation $*$ is an element $e \in S$ such that $a * e = e * a = a$.
20. Is there an example of a set S, a binary operation on S, and two different elements $e_1, e_2 \in S$ such that for all $a \in S$, $e_1 * a = a$ and $a * e_2 = a$? If so, give an example and if not, prove there is not one.

In Exercises 21 through 26, determine whether the definition of $*$ does give a binary operation on the set. In the event that $*$ is not a binary operation, state whether Condition 1, Condition 2, or both conditions regarding defining binary operations are violated.

21. On $\mathbb{Z}^+$, define $a * b = b^a$.

22. On $\mathbb{R}^+$, define $*$ by letting $a * b = 2a - b$.

23. On $\mathbb{R}^+$, define $*$ by $a * b$ to be the minimum of a and $b - 1$ if they are different and their common value if they are the same.

24. On $\mathbb{R}$, define $a * b$ to be the number c so that $c^b = a$.

25. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is at least 5 more than $a + b$.

26. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is the largest integer less than the product of a and b.

27. Let H be the subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. Is H closed under

a. matrix addition? **b.** matrix multiplication?

28. Determine whether each of the following is true or false.

a. If $*$ is any binary operation on any set S, then $a * a = a$ for all $a \in S$.

b. If $*$ is any commutative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

c. If $*$ is any associative binary operation on any set S, then $a * (b * c) = (b * c) * a$ for all $a, b, c \in S$.

d. The only binary operations of any importance are those defined on sets of numbers.

e. A binary operation $*$ on a set S is commutative if there exist $a, b \in S$ such that $a * b = b * a$.

f. Every binary operation defined on a set having exactly one element is both commutative and associative.

g. A binary operation on a set S assigns at least one element of S to each ordered pair of elements of S.

h. A binary operation on a set S assigns at most one element of S to each ordered pair of elements of S.

i. A binary operation on a set S assigns exactly one element of S to each ordered pair of elements of S.

j. A binary operation on a set S may assign more than one element of S to some ordered pair of elements of S.

k. For any binary operation $*$ on the set S, if $a, b, c \in S$ and $a * b = a * c$, then $b = c$.

l. For any binary operation $*$ on the set S, there is an element $e \in S$ such that for all $x \in S$, $x * e = x$.

m. There is an operation on the set $S = \{e_1, e_2, a\}$ so that for all $x \in S$, $e_1 * x = e_2 * x = x$.

n. Identity elements are always called e.

29. Give a set different from any of those described in the examples of the text and not a set of numbers. Define two different binary operations $*$ and $*'$ on this set. Be sure that your set is *well defined*.

Theory

30. Prove that if $*$ is an associative and commutative binary operation on a set S, then

$$(a * b) * (c * d) = [(d * c) * a] * b$$

for all $a, b, c, d \in S$. Assume the associative law only for triples as in the definition, that is, assume only

$$(x * y) * z = x * (y * z)$$

for all $x, y, z \in S$.

In Exercises 31 and 32, either prove the statement or give a counterexample.

31. Every binary operation on a set consisting of a single element is both commutative and associative.

32. Every commutative binary operation on a set having just two elements is associative.

Let F be the set of all real-valued functions having as domain the set $\mathbb{R}$ of all real numbers. Example 1.7 defined the binary operations $+, -, \cdot$, and $\circ$ on F. In Exercises 33 through 41, either prove the given statement or give a counterexample.

33. Function addition $+$ on F is associative.

34. Function subtraction $-$ on F is commutative.

35. Function subtraction $-$ on F is associative.

36. Under function subtraction $-$ F has an identity.

37. Under function multiplication $\cdot$ F has an identity.

38. Function multiplication $\cdot$ on F is commutative.

39. Function multiplication $\cdot$ on F is associative.

40. Function composition $\circ$ on F is commutative.

41. If $*$ and $*'$ are any two binary operations on a set S, then

$$a * (b *' c) = (a * b) *' (a * c) \qquad \text{for all} \quad a, b, c \in S.$$

42. Suppose that $*$ is an *associative binary* operation on a set S. Let $H = \{a \in S \mid a * x = x * a \text{ for all } x \in S\}$. Show that H is closed under $*$. (We think of H as consisting of all elements of S that *commute* with every element in S.)

43. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that $H = \{a \in S \mid a * a = a\}$ is closed under $*$. (The elements of H are **idempotents** of the binary operation $*$.)

44. Let S be a set and let $*$ be a binary operation on S satisfying the two laws

- $x * x = x$ for all $s \in S$, and
- $(x * y) * z = (y * z) * x$ for all $x, y, z \in S$.

Show that $*$ is associative and commutative. (This is problem B-1 on the 1971 Putnam Competition.)

SECTION 2 GROUPS

In high school algebra, one of the key objectives is to learn how to solve equations. Even before learning algebra, students in elementary school are given problems like $5 + \square = 2$ or $2 \times \square = 3$, which become $5 + x = 2$ and $2x = 3$ in high school algebra. Let us closely examine the steps we use to solve these equations:

$$\begin{aligned}
5 + x &= 2, && \text{given,}\\
-5 + (5 + x) &= -5 + 2, && \text{adding } -5,\\
(-5 + 5) + x &= -5 + 2, && \text{associative law,}\\
0 + x &= -5 + 2, && \text{computing } -5 + 5,\\
x &= -5 + 2, && \text{property of 0,}\\
x &= -3, && \text{computing } -5 + 2.
\end{aligned}$$

Strictly speaking, we have not shown here that -3 is a solution, but rather that it is the only possibility for a solution. To show that -3 is a solution, one merely computes $5 + (-3)$. A similar analysis could be made for the equation $2x = 3$ in the rational numbers with the operation of multiplication:

$$\begin{aligned}
2x &= 3, && \text{given,}\\
\tfrac{1}{2}(2x) &= \tfrac{1}{2}(3), && \text{multiplying by } \tfrac{1}{2},\\
(\tfrac{1}{2} \cdot 2)x &= \tfrac{1}{2}3, && \text{associative law,}\\
1 \cdot x &= \tfrac{1}{2}3, && \text{computing } \tfrac{1}{2}2,\\
x &= \tfrac{1}{2}3, && \text{property of 1,}\\
x &= \tfrac{3}{2}, && \text{computing } \tfrac{1}{2}3.
\end{aligned}$$

Now suppose that we have a set with a binary operation $*$. What properties does the operation need to have in order to solve an equation of the form $a * x = b$ where a and b are fixed elements of S? Both equations $5 + x = 2$ and $2x = 3$ have this form; the

first uses the operation $+$, and the second uses the operation $\times$. By examining the steps used we can see what properties of the operation $*$ are required as summarized in the table below.

Property	$+$	$\times$
Associative Property	$-5+(5+x)=(-5+5)+x$	$\frac{1}{2}(2x)=(\frac{1}{2}\cdot 2)x$
Identity Element	0: $0+x=x$	1: $1\cdot x=x$
Inverse Element	-5: $-5+5=0$	$\frac{1}{2}$: $\frac{1}{2}\cdot 2=1$

If S is a set with an operation $*$ satisfying these three properties, then an equation of the form $a*x=b$ could be solved for x using exactly the same steps used to solve $5+x=2$ or $2x=3$. These three essential properties are all that is required in order to have a group. We are now ready to present the precise definition.

Definition and Examples

2.1 Definition A **group** $\langle G,*\rangle$ is a set G, closed under a binary operation $*$, such that the following axioms are satisfied:

$\mathscr{G}_1$: For all $a,b,c\in G$, we have

$$(a*b)*c=a*(b*c). \quad \textbf{associativity of } *$$

$\mathscr{G}_2$: There is an element e in G such that for all $x\in G$,

$$e*x=x*e=x. \quad \textbf{identity element } e \text{ for } *$$

$\mathscr{G}_3$: Corresponding to each $a\in G$, there is an element a' in G such that

$$a*a'=a'*a=e. \quad \textbf{inverse } a' \text{ of } a$$ ■

2.2 Example $\langle\mathbb{R},+\rangle$ is a group with identity element 0 and the inverse of any real number a is $-a$. However, $\langle\mathbb{R},\cdot\rangle$ is not a group since 0 has no multiplicative inverse. We were still able to solve $2x=3$ in the example above because $\langle\mathbb{R}^*,\cdot\rangle$ is a group since multiplication of real numbers is associative, 1 is an identity, and every real number except 0 has an inverse. ▲

It is often convenient to say that G is a group under the operation $*$ rather than write $\langle G,*\rangle$ is a group. At times, there is only one obvious operation that makes $\langle G,*\rangle$ a group. In this case, we may abuse notation and say that G is a group. For example, if we say that $\mathbb{R}$ is a group, we mean that $\mathbb{R}$ is a group under addition.

2.3 Definition A group G is **abelian** if its binary operation is commutative. ■

Let us give some examples of some sets with binary operations that give groups and also of some that do not give groups.

2.4 Example The set $\mathbb{Z}^+$ under addition is *not* a group. There is no identity element for $+$ in $\mathbb{Z}^+$. ▲

2.5 Example The set of all nonnegative integers (including 0) under addition is still *not* a group. There is an identity element 0, but no inverse for 2. ▲

Historical Note

There are three historical roots of the development of abstract group theory evident in the mathematical literature of the nineteenth century: the theory of algebraic equations, number theory, and geometry. All three of these areas used group-theoretic methods of reasoning, although the methods were considerably more explicit in the first area than in the other two.

One of the central themes of geometry in the nineteenth century was the search for invariants under various types of geometric transformations. Gradually attention became focused on the transformations themselves, which in many cases can be thought of as elements of groups.

In number theory, already in the eighteenth century Leonhard Euler had considered the remainders on division of powers a^n by a fixed prime p. These remainders have "group" properties. Similarly, Carl F. Gauss, in his *Disquisitiones Arithmeticae* (1800), dealt extensively with quadratic forms $ax^2 + 2bxy + cy^2$, and in particular showed that equivalence classes of these forms under composition possessed what amounted to group properties.

Finally, the theory of algebraic equations provided the most explicit prefiguring of the group concept. Joseph-Louis Lagrange (1736–1813) in fact initiated the study of permutations of the roots of an equation as a tool for solving it. These permutations, of course, were ultimately considered as elements of a group.

It was Walther von Dyck (1856–1934) and Heinrich Weber (1842–1913) who in 1882 were able independently to combine the three historical roots and give clear definitions of the notion of an abstract group.

2.6 Example The familiar additive properties of integers and of rational, real, and complex numbers show that $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ under addition are abelian groups. ▲

2.7 Example The set $\mathbb{Z}^+$ under multiplication is *not* a group. There is an identity 1, but no inverse of 3. ▲

Historical Note

Commutative groups are called *abelian* in honor of the Norwegian mathematician Niels Henrik Abel (1802–1829). Abel was interested in the question of solvability of polynomial equations. In a paper written in 1828, he proved that if all the roots of such an equation can be expressed as rational functions $f, g, \ldots, h$ of one of them, say x, and if for any two of these roots, $f(x)$ and $g(x)$, the relation $f(g(x)) = g(f(x))$ always holds, then the equation is solvable by radicals. Abel showed that each of these functions in fact permutes the roots of the equation; hence, these functions are elements of the group of permutations of the roots. It was this property of commutativity in these permutation groups associated with solvable equations that led Camille Jordan in his 1870 treatise on algebra to name such groups *abelian;* the name since then has been applied to commutative groups in general.

Abel was attracted to mathematics as a teenager and soon surpassed all his teachers in Norway. He finally received a government travel grant to study elsewhere in 1825 and proceeded to Berlin, where he befriended August Crelle, the founder of the most influential German mathematical journal. Abel contributed numerous papers to Crelle's *Journal* during the next several years, including many in the field of elliptic functions, whose theory he created virtually single-handedly. Abel returned to Norway in 1827 with no position and an abundance of debts. He nevertheless continued to write brilliant papers, but died of tuberculosis at the age of 26, two days before Crelle succeeded in finding a university position for him in Berlin.

2.8 Example The familiar multiplicative properties of rational, real, and complex numbers show that the sets $\mathbb{Q}^+$ and $\mathbb{R}^+$ of positive numbers and the sets $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$ of nonzero numbers under multiplication are abelian groups. ▲

2.9 Example The set of all real-valued functions with domain $\mathbb{R}$ under function addition is a group. This group is abelian. ▲

2.10 Example **(Linear Algebra)** Those who have studied vector spaces should note that the axioms for a vector space V pertaining just to vector addition can be summarized by asserting that V under vector addition is an abelian group. ▲

2.11 Example The set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices under matrix addition is a group. The $m \times n$ matrix with all entries 0 is the identity matrix. This group is abelian. ▲

2.12 Example The set $M_n(\mathbb{R})$ of all $n \times n$ matrices under matrix multiplication is *not* a group. The $n \times n$ matrix with all entries 0 has no inverse. ▲

Each of the groups we have seen in the above examples is an abelian group. There are many examples of groups which are not abelian, two of which we now present.

2.13 Example Here we give an example of a group that is not abelian. We let T be the set of all isometries of the plane. An **isometry of the plane** is a function mapping the plane to the plane which preserves distance. So if ϕ is an isometry of the plane and P, Q are points in the plane, then the distance between P and Q is the same as the distance between $\phi(P)$ and $\phi(Q)$. Isometries of the plane map the plane one-to-one and onto itself. Examples of isometries include translations and rotations of the plane. The set T under the operation of composition forms a group. To verify this we first must check that function composition is an operation. Certainly, the composition of two isometries is an isometry since each preserves distance. So function composition gives an operation on T. Theorem 1.13 states that function composition is associative, so $\mathscr{G}_1$ is satisfied. The identity function ι that maps each point P in the plane to itself gives an identity element in T, which means that $\mathscr{G}_2$ is satisfied. Finally, for any isometry ϕ, the inverse function ϕ^{-1} is also an isometry and it serves as an inverse as defined in $\mathscr{G}_3$. Therefore T is a group under function composition.

To show that T is not abelian, we only need to find two isometries ϕ and θ such that $\phi \circ \theta \neq \theta \circ \phi$. The functions $\phi(x, y) = (-x, y)$ (reflection across the y-axis) and $\theta(x, y) = (-y, x)$ (rotation by $\pi/2$ about the origin) foot the bill. Note that $\phi \circ \theta(1, 0) = \phi(\theta(1, 0)) = \phi(0, 1) = (0, 1)$ and $\theta \circ \phi(1, 0) = \theta(\phi(1, 0)) = \theta(-1, 0) = (0, -1)$, which implies that $\phi \circ \theta \neq \theta \circ \phi$ and T is not an abelian group under function composition. ▲

2.14 Example Show that the subset S of $M_n(\mathbb{R})$ consisting of all *invertible* $n \times n$ matrices under matrix multiplication is a group.

Solution We start by showing that S is closed under matrix multiplication. Let A and B be in S, so that both A^{-1} and B^{-1} exist and $AA^{-1} = BB^{-1} = I_n$. Then

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = I_n,$$

so that AB is invertible and consequently is also in S.

Since matrix multiplication is associative and I_n acts as the identity element, and since each element of S has an inverse by definition of S, we see that S is indeed a group. This group is *not* commutative. ▲

The group of invertible $n \times n$ matrices described in the preceding example is of fundamental importance in linear algebra. It is the **general linear group of degree** n,

and is usually denoted by $GL(n, \mathbb{R})$. Those of you who have studied linear algebra know that a matrix A in $GL(n, \mathbb{R})$ gives rise to an invertible linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$, defined by $T(\mathbf{x}) = A\mathbf{x}$, and that conversely, every invertible linear transformation of $\mathbb{R}^n$ into itself is defined in this fashion by some matrix in $GL(n, \mathbb{R})$. Also, matrix multiplication corresponds to composition of linear transformations. Thus all invertible linear transformations of $\mathbb{R}^n$ into itself form a group under function composition; this group is usually denoted by $GL(\mathbb{R}^n)$. Since the sets $\mathrm{GL}(\mathbb{R}^n)$ and $\mathrm{GL}(n, \mathbb{R})$ and their operations are essentially the same, we say that the two groups are *isomorphic*. We give a formal definition later in this section.

We conclude our list of examples of groups with one that may seem a bit contrived. We include it to show that there are many ways to define groups and to illustrate the steps needed to verify that a given set with an operation is a group.

2.15 Example Let $*$ be defined on $\mathbb{Q}^+$ by $a * b = ab/2$. Then

$$(a * b) * c = \frac{ab}{2} * c = \frac{abc}{4},$$

and likewise

$$a * (b * c) = a * \frac{bc}{2} = \frac{abc}{4}.$$

Thus $*$ is associative. Computation shows that

$$2 * a = a * 2 = a$$

for all $a \in \mathbb{Q}^+$, so 2 is an identity element for $*$. Finally,

$$a * \frac{4}{a} = \frac{4}{a} * a = 2,$$

so $a' = 4/a$ is an inverse for a. Hence $\mathbb{Q}^+$ with the operation $*$ is a group. ▲

Elementary Properties of Groups

As we proceed to prove our first theorem about groups, we must use Definition 2.1, which is the only thing we know about groups at the moment. The proof of a second theorem can employ both Definition 2.1 and the first theorem; the proof of a third theorem can use the definition and the first two theorems, and so on.

Our first theorem will establish cancellation laws. In real number arithmetic, we know that $2a = 2b$ implies that $a = b$. We need only divide both sides of the equation $2a = 2b$ by 2, or equivalently, multiply both sides by $\frac{1}{2}$, which is the multiplicative inverse of 2. We parrot this proof to establish cancellation laws for any group. Note that we will also use the associative law.

2.16 Theorem If G is a group with binary operation $*$, then the **left and right cancellation laws** hold in G, that is, $a * b = a * c$ implies $b = c$, and $b * a = c * a$ implies $b = c$ for all $a, b, c \in G$.

Proof Suppose $a * b = a * c$. Then by $\mathscr{G}_3$, there exists a', and

$$a' * (a * b) = a' * (a * c).$$

By the associative law,

$$(a' * a) * b = (a' * a) * c.$$

By the definition of a' in $\mathscr{G}_3$, $a' * a = e$, so

$$e * b = e * c.$$

By the definition of e in $\mathscr{G}_2$,

$$b = c.$$

Similarly, from $b * a = c * a$ one can deduce that $b = c$ upon multiplication on the right by a' and use of the axioms for a group. ◆

Our next proof can make use of Theorem 2.16. We show that a "linear equation" in a group has a *unique* solution. Recall that we chose our group properties to allow us to find solutions of such equations.

2.17 Theorem If G is a group with binary operation $*$, and if a and b are any elements of G, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions x and y in G.

Proof First we show the existence of *at least* one solution by just computing that $a' * b$ is a solution of $a * x = b$. Note that

$$\begin{aligned} a * (a' * b) &= (a * a') * b, && \text{associative law,} \\ &= e * b, && \text{definition of } a', \\ &= b, && \text{property of } e. \end{aligned}$$

Thus $x = a' * b$ is a solution of $a * x = b$. In a similar fashion, $y = b * a'$ is a solution of $y * a = b$.

To show uniqueness of y, we use the standard method of assuming that we have two solutions, y_1 and y_2, so that $y_1 * a = b$ and $y_2 * a = b$. Then $y_1 * a = y_2 * a$, and by Theorem 2.16, $y_1 = y_2$. The uniqueness of x follows similarly. ◆

Of course, to prove the uniqueness in the last theorem, we could have followed the procedure we used in motivating the definition of a group, showing that if $a * x = b$, then $x = a' * b$. However, we chose to illustrate the standard way to prove an object is unique; namely, suppose you have two such objects, and then prove they must be the same. Note that the solutions $x = a' * b$ and $y = b * a'$ need not be the same unless $*$ is commutative.

Because a group has a binary operation, we know from Theorem 1.15 that the identity e in a group is unique. We state this again as part of the next theorem for easy reference.

2.18 Theorem In a group G with binary operation $*$, there is only one element e in G such that

$$e * x = x * e = x$$

for all $x \in G$. Likewise for each $a \in G$, there is only one element a' in G such that

$$a' * a = a * a' = e.$$

In summary, the identity element and inverse of each element are unique in a group.

Proof Theorem 1.15 shows that an identity element for any binary operation is unique. No use of the other group axioms was required to show this.

Turning to the uniqueness of an inverse, suppose that $a \in G$ has inverses a' and a'' so that $a' * a = a * a' = e$ and $a'' * a = a * a'' = e$. Then

$$a * a'' = a * a' = e$$

and, by Theorem 2.16,

$$a'' = a',$$

so the inverse of a in a group is unique. ◆

Note that in a group G, we have

$$(a * b) * (b' * a') = a * (b * b') * a' = (a * e) * a' = a * a' = e.$$

This equation and Theorem 2.18 show that $b' * a'$ is the unique inverse of $a * b$. That is, $(a * b)' = b' * a'$. We state this as a corollary.

2.19 Corollary Let G be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$. ◆

For your information, we remark that binary algebraic structures with weaker axioms than those for a group have also been studied quite extensively. Of these weaker structures, the **semigroup,** a set with an associative binary operation, has perhaps had the most attention. A **monoid** is a semigroup that has an identity element for the binary operation. Note that every group is both a semigroup and a monoid.

Finally, it is possible to give axioms for a group $\langle G, * \rangle$ that seem at first glance to be weaker, namely:

1. The binary operation $*$ on G is associative.
2. There exists a **left identity element** e in G such that $e * x = x$ for all $x \in G$.
3. For each $a \in G$, there exists **a left inverse** a' in G such that $a' * a = e$.

From this *one-sided definition*, one can prove that the left identity element is also a right identity element, and a left inverse is also a right inverse for the same element. Thus these axioms should not be called *weaker*, since they result in exactly the same structures being called groups. It is conceivable that it might be easier in some cases to check these *left axioms* than to check our *two-sided axioms*. Of course, by symmetry it is clear that there are also *right axioms* for a group.

Group Isomorphisms

All our examples have been of infinite groups, that is, groups where the set G has an infinite number of elements. We turn to finite groups, starting with the smallest finite sets.

Since a group has to have at least one element, namely, the identity, a minimal set that might give rise to a group is a one-element set $\{e\}$. The only possible binary operation $*$ on $\{e\}$ is defined by $e * e = e$. The three group axioms hold. The identity element is always its own inverse in every group.

2.20 Table

$\times$	1	-1
1	1	-1
-1	-1	1

There is a group with only two elements, namely $G = \{1, -1\}$ with operation the usual multiplication. It is clear that G is closed under multiplication and we know that multiplication is associative. Furthermore, 1 is the identity, the inverse of 1 is 1, and the inverse of -1 is -1. Table 2.20 is the group table for G.

Is this the only group with exactly two elements? To see, let us try to put a group structure on a set with two elements. Since one of the elements must be the identity, we will label the identity element e and we will label the other element a. Following tradition, we place the identity first both on the top and to the left as in the following table.

$*$	e	a
e		
a		

Since e is to be the identity,

$$e * x = x * e = x$$

for all $x \in \{e, a\}$. We are forced to fill in the table as follows, if $*$ is to give a group:

$*$	e	a
e	e	a
a	a	

Also, a must have an inverse a' such that

$$a * a' = a' * a = e.$$

2.21 Table

$*$	e	a
e	e	a
a	a	e

In our case, a' must be either e or a. Since $a' = e$ obviously does not work, we must have $a' = a$, so we have to complete the table as shown in Table 2.21.

All the group axioms are now satisfied, except possibly associativity. But if we relabel 1 as e and -1 as a in Table 2.20 we obtain Table 2.21. Therefore, the table we constructed for $\{e, a\}$ must also satisfy $\mathscr{G}_1$, the associative property. The table also shows clearly that properties $\mathscr{G}_2$ and $\mathscr{G}_3$ are satisfied, so $\langle \{e, a\}, * \rangle$ is a group. The groups $\{1, -1\}$ and $\{e, a\}$ are not the same, but they are essentially the same since by relabeling elements of one with the names of the other, the operations match. When the elements of one group can be matched with another in such a way that the operations are the same, we say that the groups are **isomorphic** and the matching is called a **group isomorphism**. We showed that any group with two elements is isomorphic with $\{1, -1\}$ under multiplication. The notation used to indicate isomorphism is $\simeq$, so we could write $\langle \{1, -1\}, \times \rangle \simeq \langle \{e, a\}, * \rangle$. Of course the matching is a one-to-one function from one group onto the other. If we were only interested in groups whose tables are easy to compute, then we would not need a more precise definition for isomorphism. We would simply see if we can relabel one group table to make it look like the other. However, in the case of infinite groups or even groups with more than a few elements, we need a better way to verify that groups are isomorphic. We now give a more precise definition of a group isomorphism.

2.22 Definition Let $\langle G_1, *_1 \rangle$ and $\langle G_2, *_2 \rangle$ be groups and $f : G_1 \to G_2$. We say that f is a **group isomorphism** if the following two conditions are satisfied.

1. The function f is one-to-one and maps onto G_2.
2. For all $a, b \in G_1, f(a *_1 b) = f(a) *_2 f(b)$. ■

Note that Condition 1 simply gives a way to relabel the elements of G_1 with elements in G_2. Condition 2, which we will refer to as the **homomorphism property**, says that with this relabeling, the operations $*_1$ on G_1 and $*_2$ on G_2 match. If we are in the context of groups, we will often use the term isomorphism to mean group isomorphism. If there is an isomorphism from a group G_1 to G_2, we say that G_1 is **isomorphic** with (or to) G_2. In Exercise 44, you are asked to show that if $f : G_1 \to G_2$ is an isomorphism, then $f^{-1} : G_2 \to G_1$, the inverse function, is also an isomorphism. So if G_1 is isomorphic with G_2, then G_2 is isomorphic with G_1. If you wish to verify that two groups, G_1 and G_2, are isomorphic, you can either construct an isomorphism mapping G_1 to G_2 or one mapping G_2 to G_1.

2.23 Example In Exercise 10 you will be asked to show that $2\mathbb{Z}$, the even integers, forms a group under addition. Here we show $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic groups. In this case, the operations on the groups are both addition. We need a function $f : \mathbb{Z} \to 2\mathbb{Z}$ that is both one-to-one and onto $2\mathbb{Z}$. Let $f : \mathbb{Z} \to 2\mathbb{Z}$ be given by $f(m) = 2m$. We need to verify Condition 1 for an isomorphism, which says that f is one-to-one and onto. Suppose that $a, b \in \mathbb{Z}$ and $f(a) = f(b)$. Then $2a = 2b$, which implies that $a = b$, so f is one-to-one. We now show f

is onto. Let $y \in 2\mathbb{Z}$. Since y is even, $y = 2c$ for some $c \in \mathbb{Z}$. Therefore, $y = 2c = f(c)$, so f maps onto $2\mathbb{Z}$. We now turn our attention to the homomorphism property and consider arbitrary $a, b \in \mathbb{Z}$. Then

$$f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b),$$

which verifies Condition 2. Therefore f is a group isomorphism and $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic groups.

As noted above, we could have defined an isomorphism by using the inverse function $f^{-1} : 2\mathbb{Z} \to \mathbb{Z}$, which is defined by $f^{-1}(x) = x/2$. ▲

Properties of Group Tables

With Table 2.21 as background, we should be able to list some necessary conditions that a table giving a binary operation on a finite set must satisfy for the operation to give a group structure on the set. There must be one element of the set, which we may as well denote by e, that acts as the identity element. The condition $e * x = x$ means that the row of the table opposite e at the extreme left must contain exactly the elements appearing across the very top of the table in the same order. Similarly, the condition $x * e = x$ means that the column of the table under e at the very top must contain exactly the elements appearing at the extreme left in the same order. The fact that every element a has a right and a left inverse means that in the row having a at the extreme left, the element e must appear, and in the column under a at the very top, the e must appear. Thus e must appear in each row and in each column. We can do even better than this, however. By Theorem 2.17, not only do the equations $a * x = e$ and $y * a = e$ have unique solutions, but also the equations $a * x = b$ and $y * a = b$. By a similar argument, this means that *each element b of the group must appear once and only once in each row and each column of the table*.

Suppose conversely that a table for a binary operation on a finite set is such that there is an element acting as identity and that in each row and each column, each element of the set appears exactly once. Then it can be seen that the structure is a group structure if and only if the associative law holds. If a binary operation $*$ is given by a table, the associative law is usually messy to check. If the operation $*$ is defined by some characterizing property of $a * b$, the associative law is often easy to check. Fortunately, this second case turns out to be the one usually encountered.

2.24 Table

$*$	e	a	b
e	e	a	b
a	a		
b	b		

2.25 Table

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We saw that there was essentially only one group of two elements in the sense that if the elements are denoted by e and a with the identity element e appearing first, the table must be as shown in Table 2.21. Suppose that a set has three elements. As before, we may as well let the set be $\{e, a, b\}$. For e to be an identity element, a binary operation $*$ on this set has to have a table of the form shown in Table 2.24. This leaves four places to be filled in. You can quickly see that Table 2.24 must be completed as shown in Table 2.25 if each row and each column are to contain each element exactly once. We find a group whose table is the same as Table 2.25. The elements of the group are the three matrices $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $a = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$, and $b = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$. We let $G = \{e, a, b\}$. In Exercise 18 you will show that G is a group under matrix multiplication. By computing matix products it is easy to check that the group table for G is identical with Table 2.25. Therefore Table 2.25 gives a group.

Now suppose that G' is any other group of three elements and imagine a table for G' with identity element appearing first. Since our filling out of the table for $G = \{e, a, b\}$ could be done in only one way, we see that if we take the table for G' and rename the identity e, the next element listed a, and the last element b, the resulting table for G' must be the same as the one we had for G. As explained above, this renaming gives an isomorphism of the group G' with the group G. Thus our work above can be summarized

by saying that all groups with a single element are isomorphic, all groups with just two elements are isomorphic, and all groups with just three elements are isomorphic. We use the phrase *up to isomorphism* to express this identification. Thus we may say, "There is only one group of three elements, up to isomorphism."

An interesting problem in group theory is to determine up to isomorphism all the groups with a given number of elements n. In Exercise 20, you will be asked to show that there are up to isomorphism exactly two groups of order 4. It is beyond the scope of this book to give a thorough investigation of this problem, but we will solve the problem for some other special values of n in later sections.

EXERCISES 2

Computations

In Exercises 1 through 9, determine whether the binary operation $*$ gives a group structure on the given set. If no group results, give the first axiom in the order $\mathscr{G}_1, \mathscr{G}_2, \mathscr{G}_3$ from Definition 2.1 that does not hold.

1. Let $*$ be defined on $\mathbb{Z}$ by letting $a * b = ab$.

2. Let $*$ be defined on $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$ by letting $a * b = a + b$.

3. Let $*$ be defined on $\mathbb{R}^+$ by letting $a * b = \sqrt{ab}$.

4. Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$.

5. Let $*$ be defined on the set $\mathbb{R}^*$ of nonzero real numbers by letting $a * b = a/b$.

6. Let $*$ be defined on $\mathbb{C}$ by letting $a * b = |ab|$.

7. Let $*$ be defined on the set $\{a, b\}$ by Table 2.26.

8. Let $*$ be defined on the set $\{a, b\}$ by Table 2.27.

9. Let $*$ be defined on the set $\{e, a, b\}$ by Table 2.28.

2.26 Table

$*$	a	b
a	a	b
b	b	b

2.27 Table

$*$	a	b
a	a	b
b	a	b

2.28 Table

$*$	e	a	b
e	e	a	b
a	a	e	b
b	b	b	e

10. Let n be a positive integer and let $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\}$.

a. Show that $\langle n\mathbb{Z}, + \rangle$ is a group.

b. Show that $\langle n\mathbb{Z}, + \rangle \simeq \langle \mathbb{Z}, + \rangle$.

In Exercises 11 through 18, determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group. Recall that a **diagonal matrix** is a square matrix whose only nonzero entries lie on the **main diagonal,** from the upper left to the lower right corner. An **upper-triangular matrix** is a square matrix with only zero entries below the main diagonal. Associated with each $n \times n$ matrix A is a number called the determinant of A, denoted by $\det(A)$. If A and B are both $n \times n$ matrices, then $\det(AB) = \det(A)\det(B)$. Also, $\det(I_n) = 1$ and A is invertible if and only if $\det(A) \neq 0$.

11. All $n \times n$ diagonal matrices under matrix addition.

12. All $n \times n$ diagonal matrices under matrix multiplication.

13. All $n \times n$ diagonal matrices with no zero diagonal entry under matrix multiplication.

14. All $n \times n$ diagonal matrices with all diagonal entries 1 or -1 under matrix multiplication.

15. All $n \times n$ upper-triangular matrices under matrix multiplication.

16. All $n \times n$ upper-triangular matrices under matrix addition.

17. All $n \times n$ upper-triangular matrices with determinant 1 under matrix multiplication.

18. The set of 2×2 matrices $G = \{e, a, b\}$ where $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $a = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$, and $b = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$ under matrix multiplication.

19. Let S be the set of all real numbers except -1. Define $*$ on S by

$$a * b = a + b + ab.$$

a. Show that $*$ gives a binary operation on S.

b. Show that $\langle S, * \rangle$ is a group.

c. Find the solution of the equation $2 * x * 3 = 7$ in S.

20. This exercise shows that there are two nonisomorphic group structures on a set of 4 elements.

Let the set be $\{e, a, b, c\}$, with e the identity element for the group operation. A group table would then have to start in the manner shown in Table 2.29. The square indicated by the question mark cannot be filled in with a. It must be filled in either with the identity element e or with an element different from both e and a. In this latter case, it is no loss of generality to assume that this element is b. If this square is filled in with e, the table can then be completed in two ways to give a group. Find these two tables. (You need not check the associative law.) If this square is filled in with b, then the table can only be completed in one way to give a group. Find this table. (Again, you need not check the associative law.) Of the three tables you now have, two give isomorphic groups. Determine which two tables these are, and give the one-to-one onto relabeling function which is an isomorphism.

a. Are all groups of 4 elements commutative?

b. Find a way to relabel the four matrices

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}$$

so the matrix multiplication table is identical to one you constructed. This shows that the table you constructed defines an associative operation and therefore gives a group.

c. Show that for a particular value of n, the group elements given in Exercise 14 can be relabeled so their group table is identical to one you constructed. This implies the operation in the table is also associative.

21. According to Exercise 12 of Section 1, there are 16 possible binary operations on a set of 2 elements. How many of these give a structure of a group? How many of the 19,683 possible binary operations on a set of 3 elements give a group structure?

Concepts

22. Consider our axioms $\mathscr{G}_1$, $\mathscr{G}_2$, and $\mathscr{G}_3$ for a group. We gave them in the order $\mathscr{G}_1\mathscr{G}_2\mathscr{G}_3$. Conceivable other orders to state the axioms are $\mathscr{G}_1\mathscr{G}_3\mathscr{G}_2$, $\mathscr{G}_2\mathscr{G}_1\mathscr{G}_3$, $\mathscr{G}_2\mathscr{G}_3\mathscr{G}_1$, $\mathscr{G}_3\mathscr{G}_1\mathscr{G}_2$, and $\mathscr{G}_3\mathscr{G}_2\mathscr{G}_1$. Of these six possible orders, exactly three are acceptable for a definition. Which orders are not acceptable, and why? (Remember this. Most instructors ask the student to define a group on at least one test.)

2.29 Table

$*$	e	a	b	c
e	e	a	b	c
a	a	?		
b	b			
c	c			

23. The following "definitions" of a group are taken verbatim, including spelling and punctuation, from papers of students who wrote a bit too quickly and carelessly. Criticize them.

a. A group G is a set of elements together with a binary operation $*$ such that the following conditions are satisfied

$*$ is associative
There exists $e \in G$ such that

$$e * x = x * e = x = \text{identity}.$$

For every $a \in G$ there exists an a' (inverse) such that

$$a \cdot a' = a' \cdot a = e$$

b. A group is a set G such that
The operation on G is associative.
there is an identity element (e) in G.
for every $a \in G$, there is an a' (inverse for each element)

c. A group is a set with a binary operation such
the binary operation is defined
an inverse exists
an identity element exists

d. A set G is called a group over the binery operation $*$ such that for all $a, b \in G$
Binary operation $*$ is associative under addition
there exist an element $\{e\}$ such that

$$a * e = e * a = e$$

Fore every element a there exists an element a' such that

$$a * a' = a' * a = e$$

24. Give a table defining an operation satisfying axioms $\mathscr{G}_2$ and $\mathscr{G}_3$ in the definition of a group, but not satisfying axiom $\mathscr{G}_1$ for the set

a. $\{e, a, b\}$

b. $\{e, a, b, c\}$

25. Mark each of the following true or false.

_____ **a.** A group may have more than one identity element.

_____ **b.** Any two groups of three elements are isomorphic.

_____ **c.** In a group, each linear equation has a solution.

_____ **d.** The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.

_____ **e.** Any definition a person gives for a group is correct provided that everything that is a group by that person's definition is also a group by the definition in the text.

_____ **f.** Any definition a person gives for a group is correct provided he or she can show that everything that satisfies the definition satisfies the one in the text and conversely.

_____ **g.** Every finite group of at most three elements is abelian.

_____ **h.** An equation of the form $a * x * b = c$ always has a unique solution in a group.

_____ **i.** The empty set can be considered a group.

_____ **j.** Every group is a binary algebraic structure.

Proof synopsis

We give an example of a proof synopsis. Here is a one-sentence synopsis of the proof that the inverse of an element a in a group $\langle G, * \rangle$ is unique.

> Assuming that $a * a' = e$ and $a * a'' = e$, apply the left cancellation law to the equation $a * a' = a * a''$.

Note that we said "the left cancellation law" and not "Theorem 2.16." We always suppose that our synopsis was given as an explanation given during a conversation at lunch, with no reference to text numbering and as little notation as is practical.

26. Give a one-sentence synopsis of the proof of the left cancellation law in Theorem 2.16.

27. Give at most a two-sentence synopsis of the proof in Theorem 2.17 that an equation $ax = b$ has a unique solution in a group.

Theory

28. An element $a \neq e$ in a group is said to have order 2 if $a * a = e$. Prove that if G is a group and $a \in G$ has order 2, then for any $b \in G$, $b' * a * b$ also has order 2.

29. Show that if G is a finite group with identity e and with an even number of elements, then there is $a \neq e$ in G such that $a * a = e$.

30. Let $\mathbb{R}^*$ be the set of all real numbers except 0. Define $*$ on $\mathbb{R}^*$ by letting $a * b = |a|b$.

a. Show that $*$ gives an associative binary operation on $\mathbb{R}^*$.

b. Show that there is a left identity for $*$ and a right inverse for each element in $\mathbb{R}^*$.

c. Is $\mathbb{R}^*$ with this binary operation a group?

d. Explain the significance of this exercise.

31. If $*$ is a binary operation on a set S, an element x of S is an **idempotent for** $*$ if $x * x = x$. Prove that a group has exactly one idempotent element. (You may use any theorems proved so far in the text.)

32. Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian. [*Hint:* Consider $(a * b) * (a * b)$.]

33. Let G be an abelian group and let $c^n = c * c * \cdots * c$ for n factors c, where $c \in G$ and $n \in \mathbb{Z}^+$. Give a mathematical induction proof that $(a * b)^n = (a^n) * (b^n)$ for all $a, b \in G$.

34. Suppose that G is a group and $a, b \in G$ satisfy $a * b = b * a'$ where as usual, a' is the inverse for a. Prove that $b * a = a' * b$.

35. Suppose that G is a group and a and b are elements of G that satisfy $a * b = b * a^3$. Rewrite the element $(a * b)^2$ in the form $b^k a^r$. (See Exercise 33 for power notation.)

36. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$. See Exercise 33 for the meaning of a^n. [*Hint:* Consider $e, a, a^2, a^3, \ldots, a^m$, where m is the number of elements in G, and use the cancellation laws.]

37. Show that if $(a * b)^2 = a^2 * b^2$ for a and b in a group G, then $a * b = b * a$. See Exercise 33 for the meaning of a^2.

38. Let G be a group and let $a, b \in G$. Show that $(a * b)' = a' * b'$ if and only if $a * b = b * a$.

39. Let G be a group and suppose that $a * b * c = e$ for $a, b, c \in G$. Show that $b * c * a = e$ also.

40. Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given after Corollary 2.19, is a group.

41. Prove that a nonempty set G, together with an associative binary operation $*$ on G such that

$$a * x = b \text{ and } y * a = b \text{ have solutions in } G \text{ for all } a, b \in G,$$

is a group. [*Hint:* Use Exercise 40.]

42. Let G be a group. Prove that $(a')' = a$.

43. Let $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ be an isometry of the plane.

a. Prove that ϕ is a one-to-one function.

b. Prove that ϕ maps onto $\mathbb{R}^2$.

44. Prove that if $f : G_1 \to G_2$ is a group isomorphism from the group $\langle G_1, *_1 \rangle$ to the group $\langle G_2, *_2 \rangle$, then $f^{-1} : G_2 \to G_1$ is also a group isomorphism.

45. Suppose that G is a group with n elements and $A \subseteq G$ has more than $\frac{n}{2}$ elements. Prove that for every $g \in G$, there exists $a, b \in A$ such that $a * b = g$. (This was Problem B-2 on the 1968 Putnam exam.)

SECTION 3 ABELIAN EXAMPLES

In this section we introduce two families of abelian groups and one special abelian group. These groups will be very useful in our study of groups in that they provide examples we can use to help understand concepts and test conjectures. Furthermore, we will see that some of them arise frequently in the study of groups.

We start by defining the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, the first $n-1$ positive integers together with 0, which makes a total of n elements. To define an operation $+_n$ on $\mathbb{Z}_n$, we let $a, b \in \mathbb{Z}_n$. Then

$$a +_n b = \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{if } a+b \geq n \end{cases}.$$

Note that for any $a, b \in \mathbb{Z}_n$, $0 \leq a+b \leq 2n-2$, so $0 \leq a +_n b \leq n-1$ is an operation which we call **addition modulo n**. Addition modulo n is clearly commutative: $a +_n b = b +_n a$ for any $a, b \in \mathbb{Z}_n$. The number 0 is an identity, the inverse of $a \in \mathbb{Z}_n$ is $n-a$ for $a \neq 0$, and the inverse of 0 is 0. To show that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group, it only remains to show that $+_n$ is associative. Although it is not difficult to show directly that $+_n$ is associative, it is a little tedious, so we defer the proof until we develop the circle group and then use properties of that group to conclude that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group.

3.1 Example For $n = 1$, $\mathbb{Z}_1 = \{0\}$, which is the trivial group with just one element. For $n = 2$, $\mathbb{Z}_2 = \{0, 1\}$, which as we saw in Section 2 is isomorphic with $\{1, -1\}$ under multiplication. It is important to note that completely different operations on sets can still define isomorphic groups. We also saw in Section 2 that any group with exactly three elements is isomorphic with any other group with exactly three elements. Therefore $\mathbb{Z}_3$ under addition modulo 3 is isomorphic with the group consisting of the three matrices

$$\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \right\}$$

under matrix multiplication. Again we see that two groups can be isomorphic, but have completely different sets and operations. ▲

3.2 Example

Let us look more closely at the group table for $\mathbb{Z}_4$, Table 3.3. We see that the inverse for 0 is 0, the inverse for 1 is $4-1=3$, and the inverse for 2 is $4-2=2$. In Exercise 20 in Section 2, you were asked to show that there are two groups with exactly four elements. The other group is the **Klein 4-group** denoted V, which stands for Vier, German for "four." The group table for V is displayed as Table 3.4. How can we tell that the two groups $\mathbb{Z}_4$ and V are not isomorphic? We could try all possible one-to-one functions from $\mathbb{Z}_4$ onto K_4 to see if any of them make the table for $\mathbb{Z}_4$ look like the table for K_4. This is tedious, so instead we look for a sneaky method. Notice that the diagonal entries of the table for K_4 are all the identity. No matter how we relabel

3.3 Table

$\mathbb{Z}_4$:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

3.4 Table

V:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

the entries in the table for $\mathbb{Z}_4$, only two entries along the diagonal will be the same. Therefore $\mathbb{Z}_4$ and K_4 are not isomorphic. ▲

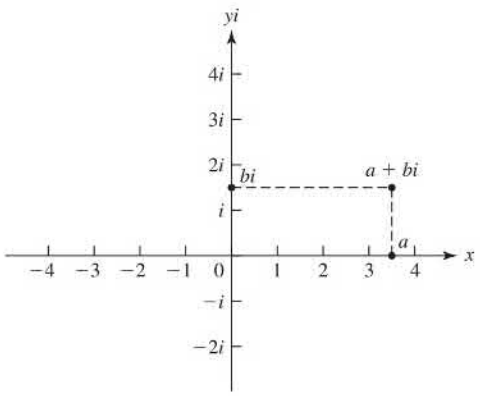
Looking back at the definition of $+_n$ there is no reason we had to restrict our set to integers a with $0 \leq a < n$. In fact, the same formula defines an operation on all real numbers a with $0 \leq a < n$. In general, let c be any positive real number and $a, b \in [0, c)$. We define $+_c$ by

$$a +_c b = \begin{cases} a + b & \text{if } a + b < c \\ a + b - c & \text{if } a + b \geq c \end{cases}.$$

This operation is called **addition modulo** c. It is easy to see that addition modulo c is an operation on $[0, c)$, it is commutative, 0 is an identity, the inverse of 0 is 0, and the inverse of any $a \in (0, c)$ is $c - a$. Instead of writing $[0, c)$ we will denote this set as $\mathbb{R}_c$. In order to show that $\langle \mathbb{R}_c, +_c \rangle$ is an abelian group, it remains to show that $+_c$ is associative. Again, we defer the proof until after we develop the circle group.

3.5 Example Let $c = 2\pi$. Then $\frac{2}{5}\pi +_{2\pi} \frac{6}{5}\pi = \frac{8}{5}\pi$ and $\frac{7}{5}\pi +_{2\pi} \frac{6}{5}\pi = \frac{3}{5}\pi$. The inverse of $\frac{\pi}{2}$ is $2\pi - \frac{\pi}{2} = \frac{3}{2}\pi$. ▲

In the group $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$, we are essentially equating 0 with 2π in the sense that if a and b add to give 2π, we know that $a +_{2\pi} b = 0$. Intuitively, we can think of this geometrically as taking a string of length 2π and attaching the ends together to form a circle of radius 1. Our next goal is to make this idea more precise by defining a group on the unit circle in the plane and showing that this group is isomorphic with $\mathbb{R}_{2\pi}$. To do this, we first review some facts about complex numbers.



3.6 Figure

Complex Numbers

A real number can be visualized geometrically as a point on a line that we often regard as an x-axis. A complex number can be regarded as a point in the Euclidean plane, as shown in Fig. 3.6. Note that we label the vertical axis as the yi-axis rather than just the y-axis, and label the point one unit above the origin with i rather than 1. The point with Cartesian coordinates (a, b) is labeled $a + bi$ in Fig. 3.6. The set $\mathbb{C}$ of **complex numbers** is defined by

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

We consider $\mathbb{R}$ to be a subset of the complex numbers by identifying a real number r with the complex number $r + 0i$. For example, we write $3 + 0i$ as 3 and $-\pi + 0i$ as $-\pi$ and $0 + 0i$ as 0. Similarly, we write $0 + 1i$ as i and $0 + si$ as si.

Complex numbers were developed after the development of real numbers. The complex number i was *invented* to provide a solution to the quadratic equation $x^2 = -1$, so we require that

$$i^2 = -1. \tag{1}$$

Unfortunately, i has been called an **imaginary number,** and this terminology has led generations of students to view the complex numbers with more skepticism than the real numbers. Actually, *all* numbers, such as 1, 3, π, $-\sqrt{3}$, and i are inventions of our minds. There is no physical entity that *is* the number 1. If there were, it would surely be in a place of honor in some great scientific museum, and past it would file a steady stream of mathematicians, gazing at 1 in wonder and awe. A basic goal of this text is to show how we can invent solutions of polynomial equations when the coefficients of the polynomial may not even be real numbers!

Multiplication of Complex Numbers

The product $(a + bi)(c + di)$ is defined in the way it must be if we are to enjoy the familiar properties of real arithmetic and require that $i^2 = -1$, in accord with Eq. (1). Namely, we see that we want to have

$$\begin{aligned}(a + bi)(c + di) &= ac + adi + bci + bdi^2 \\ &= ac + adi + bci + bd(-1) \\ &= (ac - bd) + (ad + bc)i.\end{aligned}$$

Consequently, we define multiplication of $z_1 = a + bi$ and $z_2 = c + di$ as

$$z_1 z_2 = (a + bi)(c + di) = (ac - bd) + (ad + bc)i, \tag{2}$$

which is of the form $r + si$ with $r = ac - bd$ and $s = ad + bc$. It is routine to check that the usual properties $z_1 z_2 = z_2 z_1$(commutative), $z_1(z_2 z_3) = (z_1 z_2)z_3$ (associative), and $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$ (distributive) all hold for all $z_1, z_2, z_3 \in \mathbb{C}$.

3.7 Example Compute $(2 - 5i)(8 + 3i)$.

Solution We don't memorize Eq. (2), but rather we compute the product as we did to motivate that equation. We have

$$(2 - 5i)(8 + 3i) = 16 + 6i - 40i + 15 = 31 - 34i. \quad \blacktriangle$$

To establish the geometric meaning of complex multiplication, we first define the **absolute value** $|a + bi|$ of $a + bi$ by

$$|a + bi| = \sqrt{a^2 + b^2}. \tag{3}$$

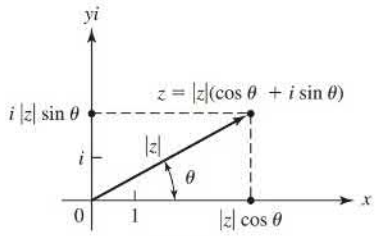
This absolute value is a nonnegative real number and is the distance from $a + bi$ to the origin in Fig. 3.6. We can now describe a complex number z in the polar-coordinate form

$$z = |z|(\cos\theta + i\sin\theta), \tag{4}$$

where θ is the angle measured counterclockwise from the positive x-axis to the vector from 0 to z, as shown in Fig. 3.8. A famous formula due to Leonard Euler states that

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Euler's Formula



3.8 Figure

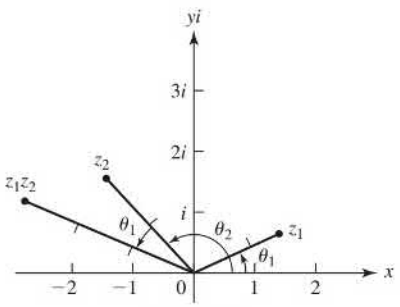
We ask you to derive Euler's formula formally from the power series expansions for $e^{\theta}, \cos\theta$, and $\sin\theta$ in Exercise 43. Using this formula, we can express z in Eq. (4) as $z = |z|e^{i\theta}$. Let us set

$$z_1 = |z_1|e^{i\theta_1} \qquad \text{and} \qquad z_2 = |z_2|e^{i\theta_2}$$

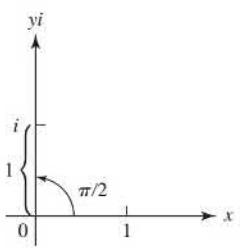
and compute their product in this form, assuming that the usual laws of exponentiation hold with complex number exponents. We obtain

$$\begin{aligned} z_1 z_2 &= |z_1|e^{i\theta_1}|z_2|e^{i\theta_2} = |z_1||z_2|e^{i(\theta_1+\theta_2)} \\ &= |z_1||z_2|[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)]. \end{aligned} \tag{5}$$

Note that Eq. 5 concludes in the polar form of Eq. 4 where $|z_1 z_2| = |z_1||z_2|$ and the polar angle θ for $z_1 z_2$ is the sum $\theta = \theta_1 + \theta_2$. Thus, geometrically, we multiply complex numbers by multiplying their absolute values and adding their polar angles, as shown in Fig. 3.9. Exercise 41 indicates how this can be derived via trigonometric identities without recourse to Euler's formula and assumptions about complex exponentiation.



3.9 Figure



3.10 Figure

Note that i has polar angle $\pi/2$ and absolute value 1, as shown in Fig. 3.10. Thus i^2 has polar angle $2(\pi/2) = \pi$ and $|1 \cdot 1| = 1$, so that $i^2 = -1$.

3.11 Example Find all solutions in $\mathbb{C}$ of the equation $z^2 = i$.

Solution Writing the equation $z^2 = i$ in polar form and using Eq. (5), we obtain

$$|z|^2(\cos 2\theta + i\sin 2\theta) = 1(0 + i).$$

Thus $|z|^2 = 1$, so $|z| = 1$. The angle θ for z must satisfy $\cos 2\theta = 0$ and $\sin 2\theta = 1$. Consequently, $2\theta = (\pi/2) + n(2\pi)$, so $\theta = (\pi/4) + n\pi$ for an integer n. The values of

n yielding values θ where $0 \le \theta < 2\pi$ are 0 and 1, yielding $\theta = \pi/4$ or $\theta = 5\pi/4$. Our solutions are

$$z_1 = 1\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \quad \text{and} \quad z_2 = 1\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right)$$

or

$$z_1 = \frac{1}{\sqrt{2}}(1+i) \quad \text{and} \quad z_2 = \frac{-1}{\sqrt{2}}(1+i). \qquad \blacktriangle$$

3.12 Example Find all solutions of $z^4 = -16$.

Solution As in Example 3.11 we write the equation in polar form, obtaining

$$|z|^4(\cos 4\theta + i\sin 4\theta) = 16(-1+0i).$$

Consequently, $|z|^4 = 16$, so $|z| = 2$ while $\cos 4\theta = -1$ and $\sin 4\theta = 0$. We find that $4\theta = \pi + n(2\pi)$, so $\theta = (\pi/4) + n(\pi/2)$ for integers n. The different values of θ obtained where $0 \le \theta < 2\pi$ are $\pi/4, 3\pi/4, 5\pi/4$, and $7\pi/4$. Thus one solution of $z^4 = -16$ is

$$2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 2\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i\right) = \sqrt{2}(1+i).$$

In a similar way, we find three more solutions,

$$\sqrt{2}(-1+i), \qquad \sqrt{2}(-1-i), \qquad \text{and} \qquad \sqrt{2}(1-i). \qquad \blacktriangle$$

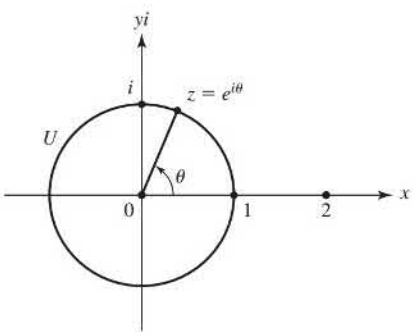
The last two examples illustrate that we can find solutions of an equation $z^n = a + bi$ by writing the equation in polar form. There will always be n solutions, provided that $a + bi \neq 0$. Exercises 16 through 21 ask you to solve equations of this type.

We will not use addition or division of complex numbers, but we probably should mention that addition is given by

$$(a+bi) + (c+di) = (a+c) + (b+d)i. \tag{6}$$

and division of $a + bi$ by nonzero $c + di$ can be performed using only division of real numbers as follows:

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2}$$
$$= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i. \tag{7}$$



3.13 Figure

Algebra on the Unit Circle

Let $U = \{z \in \mathbb{C} \mid |z| = 1\}$, so that U is the circle in the Euclidean plane with center at the origin and radius 1, as shown in Fig. 3.13.

3.14 Theorem $\langle U, \cdot \rangle$ is an abelian group.

Proof We first check that U is closed under multiplication. Let $z_1, z_2 \in U$. Then $|z_1| = |z_2| = 1$, which implies that $|z_1 z_1| = 1$, showing $z_1 z_2 \in U$.

Since multiplication of complex numbers is associative and commutative in general, multiplication in U is also associative and commutative, which verifies $\mathscr{G}_1$ and the condition for abelian.

The number $1 \in U$ is the identity, verifying condition $\mathscr{G}_2$.

For each $a + bi \in U$,

$$(a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 = |a + bi|^2 = 1.$$

So the inverse of $a + bi$ is $a - bi$, which verifies condition $\mathscr{G}_3$. Thus U is an abelian group under multiplication. ◆

Figure 3.13 gives us a way of relabeling points in U as points in $\mathbb{R}_{2\pi}$. We simply relabel z as θ where $0 \le \theta < 2\pi$. Let $f : U \to \mathbb{R}_{2\pi}$ be given by $f(z) = \theta$ according to this relabeling. Then for $z_1, z_2 \in U, f(z_1 z_2) = f(z_1) +_{2\pi} f(z_2)$ since multiplying in U simply adds the corresponding angles:

$$\text{if} \quad z_1 \leftrightarrow \theta_1 \quad \text{and} \quad z_2 \leftrightarrow \theta_2, \quad \text{then} \quad z_1 \cdot z_2 \leftrightarrow (\theta_1 +_{2\pi} \theta_2). \tag{8}$$

Recall that all that remains to show that $\mathbb{R}_{2\pi}$ is a group is to show that $+_{2\pi}$ is associative. Since the operations of multiplication in U and addition modulo 2π in $\mathbb{R}_{2\pi}$ are the same using the above relabeling and multiplication in U is associative, addition modulo 2π is also associative. This completes the proof that $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$ is a group. Furthermore, the relabeling (8) shows that the two groups $\langle U, \cdot \rangle$ and $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$ are isomorphic. In Exercise 45, you will be asked to prove that for any $b > 0$ and $c > 0$, $\langle \mathbb{R}_b, +_b \rangle$ is an abelian group and $\langle \mathbb{R}_b, +_b \rangle \simeq \langle \mathbb{R}_c, +_c \rangle$. Since $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$ is isomorphic with $\langle U, \cdot \rangle$, for every $c > 0$, $\langle \mathbb{R}_c, +_c \rangle$ is also isomorphic with $\langle U, \cdot \rangle$, meaning they have the same algebraic properties.

3.15 Example The equation $z \cdot z \cdot z \cdot z = 1$ in U has exactly four solutions, namely, $1, i, -1$, and $-i$. Now $1 \in U$ and $0 \in \mathbb{R}_{2\pi}$ correspond, and the equation $x +_{2\pi} x +_{2\pi} x +_{2\pi} x = 0$ in $\mathbb{R}_{2\pi}$ has exactly four solutions, namely, $0, \pi/2, \pi$, and $3\pi/2$, which, of course, correspond to $1, i, -1$, and $-i$, respectively. ▲

Roots of Unity

The elements of the set $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$ are called the n^{th} **roots of unity**. In Exercise 46 you are asked to prove that U_n is a group under multiplication. Using the techniques from Examples 3.11 and 3.12, we see that the elements of this set are the numbers

$$e^{(m\frac{2\pi}{n})i} = \cos\left(m\frac{2\pi}{n}\right) + i\sin\left(m\frac{2\pi}{n}\right) \quad \text{for } m = 0, 1, 2, \ldots, n-1.$$

They all have absolute value 1, so $U_n \subset U$. If we let $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, then these n^{th} roots of unity can be written as

$$1 = \zeta^0, \zeta^1, \zeta^2, \zeta^3, \cdots, \zeta^{n-1}. \tag{9}$$

Because $\zeta^n = 1$, these n powers of ζ are closed under multiplication. For example, with $n = 10$, we have

$$\zeta^6 \zeta^8 = \zeta^{14} = \zeta^{10}\zeta^4 = 1 \cdot \zeta^4 = \zeta^4.$$

Thus we see that we can compute $\zeta^i\zeta^j$ by computing $i +_n j$, viewing i and j as elements of $\mathbb{Z}_n$.

By relabeling an element $\zeta^m \in U_n$ to $m \in \mathbb{Z}_n$ we can see that addition modulo n in $\mathbb{Z}_n$ is also associative, which completes the proof that $\langle \mathbb{Z}_n, +_n \rangle$ is an abelian group.

3.16 Example We solve the equation $x +_8 x +_8 x = 1$ in $\mathbb{Z}_8$ using trial and error. We note that neither 0, 1, nor 2 is a solution simply by substitution. However, substituting $x = 3$ gives $3 +_8 3 +_8 3 = 6 +_8 3 = 1$, which shows $x = 3$ is a solution. We can also check by substituting that neither 4, 5, 6, nor 7 are solutions. So the only solution is $x = 3$. Because $\mathbb{Z}_8$ is isomorphic with U_8 by the correspondence $k \in \mathbb{Z}_8$ corresponds with ζ^k, the corresponding equation in U_8 is $z \cdot z \cdot z = \zeta = e^{\frac{2\pi}{8}i}$. Without further calculations we know that there is only one solution to $z \cdot z \cdot z = \zeta$ in U_8 and that solution is $z = \zeta^3 = e^{3\frac{2\pi}{8}i} = \cos(6\pi/8) + i\sin(6\pi/8) = -\dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$ since this is the corresponding solution in $\mathbb{Z}_8$.

There are three solutions to $z^3 = \zeta$ in U. We leave it to the reader to find the solutions and check that only one of them, ζ^3, is in U_8. ▲

We summarize the results of this section.

1. For any $n \in \mathbb{Z}^+$, $\mathbb{Z}_n$ is an abelian group under addition modulo n.
2. For any $n \in \mathbb{Z}^+$, $\mathbb{Z}_n$ is isomorphic with U_n, an abelian group under complex number multiplication.
3. For any $c > 0$, R_c under addition modulo c is a group.
4. U under multiplication is a group.
5. For any $c \in \mathbb{R}^+$, $\mathbb{R}_c$ under addition modulo c is isomorphic with U under multiplication.

EXERCISES 3

In Exercises 1 through 9 compute the given arithmetic expression and give the answer in the form $a + bi$ for $a, b \in \mathbb{R}$.

1. i^3 **2.** i^4 **3.** i^{26}

4. $(-i)^{39}$ **5.** $(3 - 2i)(6 + i)$ **6.** $(8 + 2i)(3 - i)$

7. $(2 - 3i)(4 + i) + (6 - 5i)$ **8.** $(1 + i)^3$ **9.** $(1 - i)^5$ (Use the binomial theorem.)

10. Find $|5 - 12i|$. **11.** Find $|\pi + ei|$.

In Exercises 12 through 15 write the given complex number z in the polar form $|z|(p + qi)$ where $|p + qi| = 1$.

12. $3 - 4i$ **13.** $-1 - i$ **14.** $12 + 5i$ **15.** $-3 + 5i$

In Exercises 16 through 21, find all solutions in $\mathbb{C}$ of the given equation.

16. $z^4 = 1$ **17.** $z^4 = -1$ **18.** $z^3 = -125$ **19.** $z^3 = -27i$

20. $z^6 = 1$ **21.** $z^6 = -64$

In Exercises 22 through 27, compute the given expression using the indicated modular addition.

22. $10 +_{17} 16$ **23.** $14 +_{99} 92$ **24.** $3.141 +_4 2.718$

25. $\frac{1}{2} +_1 \frac{7}{8}$ **26.** $\frac{3\pi}{4} +_{2\pi} \frac{3\pi}{2}$ **27.** $2\sqrt{2} +_{\sqrt{32}} 3\sqrt{2}$

28. Explain why the expression $5 +_6 8$ in $\mathbb{R}_6$ makes no sense.

In Exercises 29 through 34, find *all* solutions x of the given equation.

29. $x +_{10} 7 = 3$ in $\mathbb{Z}_{10}$

30. $x +_{2\pi} \pi = \frac{\pi}{2}$ in $\mathbb{R}_{2\pi}$

31. $x +_7 x = 3$ in $\mathbb{Z}_7$

32. $x +_{13} x +_{13} x = 5$ in $\mathbb{Z}_{13}$

33. $x +_{12} x = 2$ in $\mathbb{Z}_{12}$

34. $x +_8 x +_8 x +_8 x = 4$ in $\mathbb{Z}_8$

35. Prove or give a counterexample to the statement that for any $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n$, the equation $x +_n x = a$ has at most two solutions in $\mathbb{Z}_n$.

36. Prove or give a counterexample to the statement that for any $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}_n$, if n is not a multiple of 3, then the equation $x +_n x +_n x = a$ has exactly one solution in $\mathbb{Z}_n$.

37. There is an isomorphism of U_8 with $\mathbb{Z}_8$ in which $\zeta = e^{i(\pi/4)} \leftrightarrow 5$ and $\zeta^2 \leftrightarrow 2$. Find the element of $\mathbb{Z}_8$ that corresponds to each of the remaining six elements ζ^m in U_8 for $m = 0, 3, 4, 5, 6$, and 7.

38. There is an isomorphism of U_7 with $\mathbb{Z}_7$ in which $\zeta = e^{i(2\pi/7)} \leftrightarrow 4$. Find the element in $\mathbb{Z}_7$ to which ζ^m must correspond for $m = 0, 2, 3, 4, 5$, and 6.

39. Why can there be no isomorphism of U_6 with $\mathbb{Z}_6$ in which $\zeta = e^{i(\pi/3)}$ corresponds to 4?

40. Derive the formulas

$$\sin(a + b) = \sin a \cos b + \cos a \sin b$$

and

$$\cos(a + b) = \cos a \cos b - \sin a \sin b$$

by using Euler's formula and computing $e^{ia}e^{ib}$.

41. Let $z_1 = |z_1|(\cos\theta_1 + i \sin\theta_1)$ and $z_2 = |z_2|(\cos\theta_2 + i \sin\theta_2)$. Use the trigonometric identities in Exercise 40 to derive $z_1 z_2 = |z_1||z_2|[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)]$.

42. **a.** Derive a formula for $\cos 3\theta$ in terms of $\sin\theta$ and $\cos\theta$ using Euler's formula.

b. Derive the formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ from part (a) and the identity $\sin^2\theta + \cos^2\theta = 1$. (We will have use for this identity in Section 41.)

43. Recall the power series expansions

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots + \frac{x^n}{n!} + \cdots,$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots + (-1)^{n-1}\frac{x^{2n-1}}{(2n-1)!} + \cdots, \text{ and}$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots + (-1)^n\frac{x^{2n}}{(2n)!} + \cdots$$

from calculus. Derive Euler's formula $e^{i\theta} = \cos\theta + i \sin\theta$ formally from these three series expansions.

44. Prove that for any $n \in \mathbb{Z}^+$, $\langle \mathbb{Z}_n, +_n \rangle$ is associative without using the fact that U_n is associative.

45. Let $b, c \in \mathbb{R}^+$. Find a one-to-one and onto function $f : \mathbb{R}_b \to \mathbb{R}_c$ that has the homomorphism property. Conclude that $\mathbb{R}_c$ is an abelian group that is isomorphic with U.

46. Prove that for any $n \geq 1$, U_n is a group.

SECTION 4 NONABELIAN EXAMPLES

Notation and Terminology

It is time to explain some conventional notation and terminology used in group theory. Algebraists as a rule do not use a special symbol $*$ to denote a binary operation different from the usual addition and multiplication. They stick with the conventional additive or multiplicative notation and even call the operation *addition* or *multiplication,* depending

on the symbol used. The symbol for addition is, of course, $+$, and usually multiplication is denoted by juxtaposition without a dot, if no confusion results. Thus in place of the notation $a * b$, we shall be using either $a + b$ to be read "the *sum* of a and b," or ab to be read "the *product* of a and b." There is a sort of unwritten agreement that the symbol $+$ should be used only to designate commutative operations. Algebraists feel very uncomfortable when they see $a + b \neq b + a$. For this reason, when developing our theory in a general situation where the operation may or may not be commutative, we shall always use multiplicative notation.

Algebraists frequently use the symbol 0 to denote an additive identity element and the symbol 1 to denote a multiplicative identity element, even though they may not be actually denoting the integers 0 and 1. Of course, if they are also talking about numbers at the same time, so that confusion would result, symbols such as e or u are used as identity elements. Thus a table for a group of three elements might be one like Table 4.1 or, since such a group is commutative, the table might look like Table 4.2. In general situations we shall continue to use e to denote the identity element of a group.

4.1 Table

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

4.2 Table

$+$	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

It is customary to denote the inverse of an element a in a group by a^{-1} in multiplicative notation and by $-a$ in additive notation. From now on, we shall use these notations in place of the symbol a'.

Let n be a positive integer. If a is an element of a group G, written multiplicatively, we denote the product $aaa\ldots a$ for n factors a by a^n. We let a^0 be the identity element e, and denote the product $a^{-1}a^{-1}a^{-1}\ldots a^{-1}$ for n factors by a^{-n}. It is easy to see that our usual law of exponents, $a^m a^n = a^{m+n}$ for $m, n \in \mathbb{Z}$, holds. For $m, n \in \mathbb{Z}^+$, it is clear. We illustrate another type of case by an example:

$$a^{-2}a^5 = a^{-1}a^{-1}aaaaa = a^{-1}(a^{-1}a)aaaa = a^{-1}eaaaa = a^{-1}(ea)aaa$$
$$= a^{-1}aaaa = (a^{-1}a)aaa = eaaa = (ea)aa = aaa = a^3.$$

In additive notation, we denote $a + a + a + \cdots + a$ for n summands by na, denote $(-a) + (-a) + (-a) + \cdots + (-a)$ for n summands by $-na$, and let $0a$ be the identity element. Be careful: In the notation na, the number n is in $\mathbb{Z}$, not in G. One reason we prefer to present group theory using multiplicative notation, even if G is abelian, is the confusion caused by regarding n as being in G in this notation na. No one ever misinterprets the n when it appears in an exponent.

The following table summarizes basic notations and facts using both additive and multiplicative notation. We assume that a is an element of a group, n, m are integers, and k is a positive integer.

$*$ **Notation**	$+$ **Notation**	$\cdot$ **Notation**
May or may not be abelian	Abelian	May or may not be abelian
e	0	1
a'	$-a$	a^{-1}
$a * b$	$a + b$	ab
$\underbrace{a * a * \cdots * a}_{k}$	ka	a^k
$\underbrace{(a' * a' * \cdots * a')}_{k}$	$-ka$	a^{-k}
	$0a = 0$	$a^0 = 1$
	$(n + m)a = na + ma$	$a^{n+m} = a^n a^m$
	$n(ma) = (nm)a$	$(a^n)^m = a^{nm}$

Typically when stating a theorem we will use multiplicative notation, but the theorem also applies when using additive notation by using the above table to translate.

We often refer to the number of elements in a group, so we have a term for this number.

4.3 Definition If G is a group, then the **order** of G is the number of elements or cardinality of G. The order of G is denoted $|G|$. ■

Permutations

We have seen examples of groups of numbers, like the groups $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ under addition. We have also introduced groups of matrices, like the group $GL(2, \mathbb{R})$. Each element A of $GL(2, \mathbb{R})$ yields a transformation of the plane $\mathbb{R}^2$ into itself; namely, if we regard $\mathbf{x}$ as a 2-component column vector, then $A\mathbf{x}$ is also a 2-component column vector. The group $GL(2, \mathbb{R})$ is typical of many of the most useful groups in that its elements *act on things* to transform them. Often, an action produced by a group element can be regarded as a *function*, and the binary operation of the group can be regarded as *function composition*. In this section, we construct some finite groups whose elements, called *permutations*, act on finite sets. These groups will provide us with examples of finite nonabelian groups.

You may be familiar with the notion of a permutation of a set as a rearrangement of the elements of the set. Thus for the set {1, 2, 3, 4, 5}, a rearrangement of the elements could be given schematically as in Fig. 4.4, resulting in the new arrangement {4, 2, 5, 3, 1}. Let us think of this schematic diagram in Fig. 4.4 as a function mapping each element listed in the left column into a single (not necessarily different) element from the same set listed at the right. Thus 1 is carried into 4, 2 is mapped into 2, and so on. Furthermore, to be a permutation of the set, this mapping must be such that each element appears in the right column once and only once. For example, the diagram in Fig. 4.5 does *not* give a permutation, for 3 appears twice while 1 does not appear at all in the right column. We now define a permutation to be such a mapping.

1→4	1→3
2→2	2→2
3→5	3→4
4→3	4→5
5→1	5→3
4.4 Figure	**4.5 Figure**

4.6 Definition A **permutation of a set** A is a function $\phi : A \to A$ that is both one-to-one and onto. ■

Permutation Groups

We now show that function composition $\circ$ is a binary operation on the collection of all permutations of a set A. We call this operation *permutation multiplication*. Let A be a set, and let σ and τ be permutations of A so that σ and τ are both one-to-one functions mapping A onto A. The composite function $\sigma \circ \tau$ defined schematically by

$$A \xrightarrow{\tau} A \xrightarrow{\sigma} A,$$

gives a mapping of A into A. Rather than keep the symbol $\circ$ for permutation multiplication, we will denote $\sigma \circ \tau$ by the juxtaposition $\sigma\tau$. Now $\sigma\tau$ will be a permutation if it is one-to-one and onto A. *Remember that the action of $\sigma\tau$ on A must be read in right-to-left order: first apply τ and then σ.* Let us show that $\sigma\tau$ is one-to-one. If

$$(\sigma\tau)(a_1) = (\sigma\tau)(a_2),$$

then

$$\sigma(\tau(a_1)) = \sigma(\tau(a_2)),$$

and since σ is given to be one-to-one, we know that $\tau(a_1) = \tau(a_2)$. But then, since τ is one-to-one, this gives $a_1 = a_2$. Hence $\sigma\tau$ is one-to-one. To show that $\sigma\tau$ is onto A, let $a \in A$. Since σ is onto A, there exists $a' \in A$ such that $\sigma(a') = a$. Since τ is onto A, there exists $a'' \in A$ such that $\tau(a'') = a'$. Thus

$$a = \sigma(a') = \sigma(\tau(a'')) = (\sigma\tau)(a''),$$

so $\sigma\tau$ is onto A.

4.7 Example Suppose that

$$A = \{1, 2, 3, 4, 5\}$$

and that σ is the permutation given by Fig. 4.4. We write σ in a more standard notation, changing the columns to rows in parentheses and omitting the arrows, as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix},$$

so that $\sigma(1) = 4, \sigma(2) = 2$, and so on. Let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

For example, multiplying in right-to-left order,

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 5.$$

▲

■ HISTORICAL NOTE

One of the earliest recorded studies of permutations occurs in the *Sefer Yetsirah,* or *Book of Creation,* written by an unknown Jewish author sometime before the eighth century. The author was interested in counting the various ways in which the letters of the Hebrew alphabet can be arranged. The question was in some sense a mystical one. It was believed that the letters had magical powers; therefore, suitable arrangements could subjugate the forces of nature. The actual text of the *Sefer Yetsirah* is very sparse: "Two letters build two words, three build six words, four build 24 words, five build 120, six build 720, seven build 5040." Interestingly enough, the idea of counting the arrangements of the letters of the alphabet also occurred in Islamic mathematics in the eighth and ninth centuries. By the thirteenth century, in both the Islamic and Hebrew cultures, the abstract idea of a permutation had taken root so that both Abu-l-' Abbas ibn al-Banna (1256–1321), a mathematician from Marrakech in what is now Morocco, and Levi ben Gerson, a French rabbi, philosopher, and mathematician, were able to give rigorous proofs that the number of permutations of any set of n elements is $n!$, as well as prove various results about counting combinations.

Levi and his predecessors, however, were concerned with permutations as simply arrangements of a given finite set. It was the search for solutions of polynomial equations that led Lagrange and others in the late eighteenth century to think of permutations as functions from a finite set to itself, the set being that of the roots of a given equation. And it was Augustin-Louis Cauchy (1789–1857) who developed in detail the basic theorems of permutation theory and who introduced the standard notation used in this text.

We now show that the collection of all permutations of a nonempty set A forms a group under this permutation multiplication.

4.8 Theorem Let A be a nonempty set, and let S_A be the collection of all permutations of A. Then S_A is a group under permutation multiplication.

Proof We have shown that composition of two permutations of A yields a permutation of A, so S_A is closed under permutation multiplication.

Now permutation multiplication is defined as function composition, and in Section 1, we showed that *function composition is associative*. Hence $\mathscr{G}_1$ is satisfied.

The permutation ι such that $\iota(a) = a$, for all $a \in A$ acts as identity. Therefore $\mathscr{G}_2$ is satisfied.

For a permutation σ, the inverse function, σ^{-1}, is the permutation that reverses the direction of the mapping σ, that is, $\sigma^{-1}(a)$ is the element a' of A such that $a = \sigma(a')$. The existence of exactly one such element a' is a consequence of the fact that, as a function, σ is both one-to-one and onto. For each $a \in A$ we have

$$\iota(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a)) = (\sigma\sigma^{-1})(a)$$

and also

$$\iota(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a'),$$

so that $\sigma^{-1}\sigma$ and $\sigma\sigma^{-1}$ are both the permutation ι. Thus $\mathscr{G}_3$ is satisfied. ◆

Warning: Some texts compute a product $\sigma\mu$ of permutations in left-to-right order, so that $(\sigma\mu)(a) = \mu(\sigma(a))$. Thus the permutation they get for $\sigma\mu$ is the one we would get by computing $\mu\sigma$. Exercise 34 asks us to check in two ways that we still get a group. If you refer to another text on this material, be sure to check its order for permutation multiplication.

There was nothing in our definition of a permutation to require that the set A be finite. However, most of our examples of permutation groups will be concerned with permutations of finite sets. Note that the *structure* of the group S_A is concerned only with the number of elements in the set A, and not what the elements in A are. If sets A and B have the same cardinality, then $S_A \simeq S_B$. To define an isomorphism $\phi : S_A \to S_B$, we let $f : A \to B$ be a one-to-one function mapping A onto B, which establishes that A and B have the same cardinality. For $\sigma \in S_A$, we let $\phi(\sigma)$ be the permutation $\bar{\sigma} \in S_B$ such that $\bar{\sigma}(f(a)) = f(\sigma(a))$ for all $a \in A$. To illustrate this for $A = \{1, 2, 3\}$ and $B = \{\#, \$, \%\}$ and the function $f : A \to B$ defined as

$$f(1) = \#, \quad f(2) = \$, \quad f(3) = \%,$$

ϕ maps

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ into } \begin{pmatrix} \# & \$ & \% \\ \% & \$ & \# \end{pmatrix}.$$

We simply rename the elements of A in our two-row notation by elements in B using the renaming function f, thus renaming elements of S_A to be those of S_B. We can take $\{1, 2, 3, \cdots, n\}$ to be a prototype for a finite set A of n elements.

4.9 Definition Let A be the finite set $\{1, 2, \cdots, n\}$. The group of all permutations of A is the **symmetric group on n letters**, and is denoted by S_n. ■

Note that S_n has $n!$ elements, where

$$n! = n(n-1)(n-2)\cdots(3)(2)(1).$$

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Then

$$\sigma\tau(1) = \sigma(1) = 2$$

and

$$\tau\sigma(1) = 3$$

which says that $\sigma\tau \neq \tau\sigma$. Therefore S_3 is not abelian. We have seen that any group with at most four elements is abelian. Furthermore we will see later that up to isomorphism, the abelian group $\mathbb{Z}_5$ is the only group of order 5. Thus S_3 is the smallest group which is not abelian.

4.10 Example Suppose that $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 4 & 5 \end{pmatrix}$. We find the inverse σ^{-1}. We saw in the proof of Theorem 4.8 that the inverse function of a permutation is the group inverse. So it is easy to find inverses for permutations, we simply turn the tables! That is, we switch the top and bottom rows and sort the columns so the top row is in order:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 5 & 6 & 3 \end{pmatrix}. \quad \blacktriangle$$

Disjoint Cycles

There is a more efficient way of specifying the action of a permutation. In the two-row notation that we have been using, we list each number 1 through n twice, once in the top row and once in the bottom row. Disjoint cycle notation allows us to write the permutation using each number only once. We illustrate with an example. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$. To write in disjoint cycle notation we start by writing

$$(1$$

We see that $\sigma(1) = 3$, so we place 3 just to the right of 1:

$$(1, 3$$

Now we see that σ maps 3 to 6, so we write:

$$(1, 3, 6$$

Our permutation maps 6 to 1, but there is no reason to write 1 again, so we just place a parenthesis after the 6 to indicate that 6 maps back to the first element listed:

$$(1, 3, 6)$$

This is called a **cycle** because when we apply σ repeatedly, we cycle through the numbers 1, 3, and 6. A cycle containing exactly k numbers is called a ***k*-cycle**. So the cycle $(1, 3, 6)$ is a 3-cycle. This is not the end of the story for σ because we have not indicated that 2 maps to 4. So we start another cycle and write

$$(1, 3, 6)(2, 4$$

to indicate that σ maps 2 to 4. Since 4 maps back to 2, we obtain a 2-cycle:

$$(1, 3, 6)(2, 4)$$

We still have not indicated what σ does to 5. We can write $(1, 3, 6)(2, 4)(5)$ to indicate that 5 maps to itself, but usually we will simply leave out 1-cycles with the understanding that any number not listed maps to itself. So in disjoint cycle notation

$$\sigma = (1, 3, 6)(2, 4).$$

We see that σ is a product of a 3-cycle and a 2-cycle. Sometimes we refer to a 2-cycle as a **transposition**.

A collection of cycles is said to be **disjoint** if no entry is in more than one cycle. Note that σ could also be written as $(3,6,1)(4,2)$, $(2,4)(1,3,6)$, or in a number of other ways. In general it doesn't matter which order we write the disjoint cycles, and inside each cycle we can start with any number as long as we keep the cyclic order the same. It is clear that any permutation in S_n can be written in disjoint cycle notation and that the representation is unique up to the order the cycles are written and the cyclic order within each cycle.

4.11 Example In disjoint cycle notation, $\sigma \in S_9$ is written as $(1,5,2,7)(3,4,9)$. Let us rewrite σ in two-row notation. Reading off the disjoint cycle notation we see that $\sigma(1) = 5$, $\sigma(5) = 2$, $\sigma(2) = 7$, $\sigma(7) = 1$, $\sigma(3) = 4$, $\sigma(4) = 9$, and $\sigma(9) = 3$. Since 6 and 8 do not appear in either cycle, we know that $\sigma(6) = 6$ and $\sigma(8) = 8$. Therefore,

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

The operation that makes S_n a group is composition of functions. Keeping this in mind, we can see how to multiply permutations written in disjoint cycle notation.

4.12 Example Let $\sigma = (1,5,3,2,6)$ and $\tau = (1,2,4,3,6)$ in S_6. Let us find $\sigma\tau$ in disjoint cycle notation without resorting to using two-row notation. So

$$\sigma\tau = (1,5,3,2,6)(1,2,4,3,6).$$

We need to rewrite this product in disjoint cycles. So we ask where 1 is mapped. Since the operation is function composition, we see that the cycle τ on the right sends 1 to 2 and then the cycle on the left sends 2 to 6. So $\sigma\tau(1) = 6$ and we start our cycle by writing

$$(1,6$$

Now we see that τ maps 6 to 1 and σ maps 1 to 5, so we write

$$(1,6,5$$

We note that 5 is not in the cycle $(1,2,4,3,6)$, so $\tau(5) = 5$ and $\sigma\tau(5) = \sigma(5) = 3$. So we write

$$(1,6,5,3$$

Continuing in the same manner, we see that 3 maps to 1 and we complete the first cycle:

$$(1,6,5,3)$$

We are now ready to start the second cycle. We note that we have still not seen where 2 maps, so we start the next cycle with 2 and we write

$$\sigma\tau = (1,5,3,2,6)(1,2,4,3,6) = (1,6,5,3)(2,4)$$

using the same method we used for the first cycle. We know we are through since we have used every number 1 through 6. $\blacktriangle$

Example 4.12 illustrates the process of multiplying permutations in general. We move from right to left between the cycles, and within the cycles we move from left to right.

4.13 Example We compute the product of the permutations

$$\sigma = (1,5)(2,4)(1,4,3)(2,5)(4,2,1)$$

using disjoint cycle notation.

We start by seeing where 1 is mapped. The first cycle on the right maps 1 to 4. We are using function composition, so we next check what $(2,5)$ does to 4, which is nothing. So we move to the cycle $(1,4,3)$ and note that 4 is mapped to 3. Next, 3 is not in the cycle $(2,4)$ and so $(2,4)$ does not move 3 . Finally, $(1,5)$ also does not move 3 and we conclude that $\sigma(1) = 3$. We next need to determine where 3 is mapped by σ and continue until we arrive at

$$\sigma = (1,3,5,4)(2) = (1,3,5,4). \qquad \blacktriangle$$

It is interesting to note that in Example 4.13 the group was never specified. The same calculation is valid whether the group is S_5, S_6, or S_n for any $n \geq 5$.

4.14 Example We compute the inverse of $\sigma = (1,5,7)(3,8,2,4,6)$. We first note that in general for a group $(ab)^{-1} = b^{-1}a^{-1}$, so

$$\sigma^{-1} = (3,8,2,4,6)^{-1}(1,5,7)^{-1}.$$

The inverse of a cycle is simply the cycle written backward:

$$\sigma^{-1} = (6,4,2,8,3)(7,5,1).$$

This is a perfectly good way of writing σ^{-1}, but since disjoint cycles commute and we can start each cycle with any entry in the cycle, we could write

$$\sigma^{-1} = (1,7,5)(2,8,3,6,4). \qquad \blacktriangle$$

With a little practice, computing products of permutations in disjoint cycle notation becomes routine. We give the table for S_3.

4.15 Table

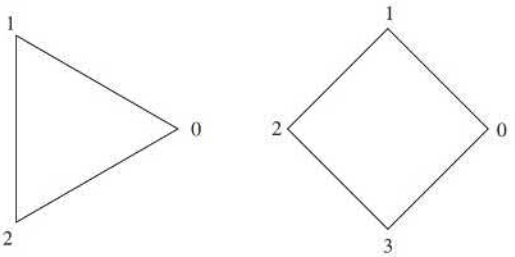
S_3 $\circ$	ι	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
ι	ι	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	ι	$(1,3)$	$(2,3)$	$(1,2)$
$(1,3,2)$	$(1,3,2)$	ι	$(1,2,3)$	$(2,3)$	$(1,2)$	$(1,3)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	ι	$(1,3,2)$	$(1,2,3)$
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,2,3)$	ι	$(1,3,2)$
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	$(1,3,2)$	$(1,2,3)$	ι

Again we can see that S_3 is not abelian since the table is not symmetric about the main diagonal. We also notice that although disjoint cycles commute, the same cannot be said for cycles that are not disjoint. For example we see in Table 4.15 that $(1,2)(2,3) = (1,2,3) \neq (1,3,2) = (2,3)(1,2)$.

The Dihedral Group

We next define a collection of finite groups based on the symmetries of regular n-gons. To be specific, we use as our standard regular n-gon the one whose points are U_n. Recall that U_n includes the point $(1,0)$ and the other points are spaced uniformly around the unit circle to form the vertices of a regular n-gon, which we denote by P_n. We label the points starting at $(1,0)$ with 0 and continue labeling them $1,2,3,\ldots,n-1$ around the circle counterclockwise. Note that this is the same labeling as the isomorphism between U_n and $\mathbb{Z}_n$ that we saw in Section 3. When we refer to a vertex we will reference it by its label. So vertex 0 is the point $(1,0)$. Note that the edges of P_n consist of the line segments between vertices k and $k +_n 1$ for $0 \leq k \leq n-1$.

4.16 Definition Let $n \geq 3$. Then D_n is the set of all one-to-one functions $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ that map onto $\mathbb{Z}_n$ with the property that the line segment between vertices i and j is an edge in P_n if and only if the line segment between $\phi(i)$ and $\phi(j)$ is an edge of P_n. The n^{th} **dihedral group** is the set D_n with binary operation function composition. ■



We justify calling $\langle D_n, \circ \rangle$ a group with Theorem 4.17.

4.17 Theorem For any $n \geq 3$, $\langle D_n, \circ \rangle$ is a group.

Proof We first show that function composition is an operation on D_n. Let $\phi, \theta \in D_n$ and suppose that the line between vertices i and j is an edge in P_n. Since $\theta \in D_n$, the line between $\theta(i)$ and $\theta(j)$ is an edge of P_n. Because $\phi \in D_n$, and the line between $\theta(i)$ and $\theta(j)$ is an edge, the line between $\phi(\theta(i)) = \phi \circ \theta(i)$ and $\phi(\theta(j)) = \phi \circ \theta(j)$ is an edge of P_n.

We leave it to the reader to check that if the line segment between $\phi(\theta(i)) = \phi \circ \theta(i)$ and $\phi(\theta(j)) = \phi \circ \theta(j)$ is an edge of P_n, then the line segment between i and j is an edge of P_n.

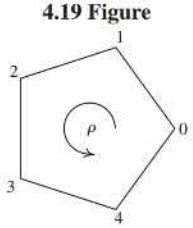
We also know that the composition of one-to-one and onto functions is one-to-one and onto, so $\phi \circ \theta \in D_n$. Therefore, function composition is an operation on D_n.

The operation of composition of functions is associative, so $\mathscr{G}_1$ is satisfied. The function $\iota : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by $\iota(k) = k$ is an identity in D_n, so $\mathscr{G}_2$ is satisfied. Finally, if $\phi \in D_n$, then $\phi^{-1} \in D_n$; the inverse function for f acts as the inverse in the group sense, so $\mathscr{G}_3$ is satisfied. Therefore, $\langle D_n, \circ \rangle$ is a group. ◆

Following tradition, we will use multiplicative notation in the dihedral groups instead of using $\circ$. If the operation on D_n were abelian, we could use additive notation, but in Example 4.18 we find that D_n is not abelian.

4.18 Example Let $n \geq 3$ and $\rho : Z_n \to Z_n$ be given by rotating the n-gon P_n by $\frac{2\pi}{n}$, which just rotates each vertex to the next one. That is,

4.19 Figure



$$\rho(k) = k +_n 1$$

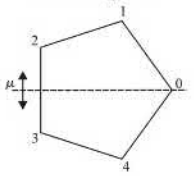
for each $k \in \mathbb{Z}_n$, as can be visualized in Figure 4.19. The function ρ matches edges to edges and it is one-to-one and onto. So $\rho \in D_n$.

A second element in D_n is reflection about the x-axis, which we call μ. By glancing at Figure 4.20 we see that in D_5, $\mu(0) = 0$, $\mu(1) = 4$, $\mu(2) = 3$, $\mu(3) = 2$, and $\mu(4) = 1$. For any $n \geq 3$ in general, if $k \in \mathbb{Z}_n$, then

$$\mu(k) = -k.$$

(Recall that in $\mathbb{Z}_n$, $-k$ is the additive inverse of k, which is $n - k$ for $k > 0$ and $-0 = 0$.)

4.20 Figure



Let us check if $\mu\rho = \rho\mu$. We start by checking what each function does to 0.

$$\begin{aligned}\mu(\rho(0)) &= \mu(1)\\ &= n-1\end{aligned}$$

$$\begin{aligned}\rho(\mu(0)) &= \rho(0)\\ &= 1\end{aligned}$$

Since $n \geq 3$, $n-1 \neq 1$, which implies that $\mu\rho \neq \rho\mu$. Thus for all $n \geq 3$, D_n is not abelian. ▲

4.21 Theorem Let $n \geq 3$. The order of the dihedral group D_n is $2n$ and

$$D_n = \{\iota, \rho, \rho^2, \rho^3, \cdots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \mu\rho^3, \cdots, \mu\rho^{n-1}\}.$$

Proof We first show there can be at most $2n$ elements of D_n. If we map the vertices $\mathbb{Z}_n$ to the vertices $\mathbb{Z}_n$, vertex 0 has n possible images. Let y be the image of vertex 0. Since y is connected by an edge to just two vertices, 1 must map to one of these two vertices. So after the image of vertex 0 is determined, there are only two choices for the image of 1. After the images of vertices 0 and 1 are determined, the rest are fixed. This means that there are at most $2n$ elements of D_n.

To show that $|D_n| = 2n$ we only need to show that no two of the functions $\iota = \rho^0, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \mu\rho^3, \ldots, \mu\rho^{n-1}$ are the same. We first suppose that $\rho^k = \rho^r$ for some integers $0 \leq k \leq n-1$ and $0 \leq r \leq n-1$. Then:

$$\begin{aligned}\rho^k(0) &= \rho^r(0)\\ k +_n 0 &= r +_n 0\\ k &= r\end{aligned}$$

This shows that no two of $\iota = \rho^0, \rho, \rho^2, \rho^3, \ldots, \rho^{n-1}$ are the same.

We next show that no two of $\mu = \mu\rho^0, \mu\rho, \mu\rho^2, \mu\rho^3, \ldots, \mu\rho^{n-1}$ are the same. As before we assume that $\mu\rho^k = \mu\rho^r$ where $0 \leq k \leq n-1$ and $0 \leq r \leq n-1$ are integers. By cancellation, we have $\rho^k = \rho^r$. But then $k = r$ as shown above. Therefore no two of $\mu = \mu\rho^0, \mu\rho, \mu\rho^2, \mu\rho^3, \ldots, \mu\rho^{n-1}$ are the same.

It now only remains to show that there are no values for k and r with $\rho^k = \mu\rho^r$. Note that traversing the n-gon in the order

$$\rho^k(0), \rho^k(1), \rho^k(2), \cdots, \rho^k(n-1)$$

progresses in a counterclockwise manner regardless of which k we use. On the other hand,

$$\mu\rho^k(0), \mu\rho^k(1), \mu\rho^k(3), \cdots, \mu\rho^k(n)$$

traverses the n-gon in a clockwise manner. This shows that there are no values of k and r for which $\rho^k = \mu\rho^r$. Therefore, D_n has at least $2n$ elements. Combining this with the fact that D_n has at most $2n$ elements shows that $|D_n| = 2n$ and

$$D_n = \{\iota, \rho, \rho^2, \rho^3, \cdots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \mu\rho^3, \cdots, \mu\rho^{n-1}\}.$$ ◆

Theorem 4.21 says that if $\phi \in D_n$, then there is an integer $0 \leq k \leq n-1$ such that either $\phi = \rho^k$ or else $\phi = \mu\rho^k$. We refer to this representation of ϕ as the **standard form**. We notice that each application of μ reverses the direction traversed by the images of $0, 1, 2, 3, \ldots, n$. We use this fact in the following example.

4.22 Example Let $n \geq 3$. We know $\rho\mu \neq \mu\rho$ from Example 4.18, so let us determine $\rho\mu \in D_n$ in standard form. Each time we apply μ we reverse the clock direction of the images of $0, 1, 2, 3, \ldots, n-1$. This means that $\mu\rho\mu$ reverses direction twice, so the rotation is

back to counterclockwise. Thus $\mu\rho\mu = \rho^k$ for some k. We determine the value of k by determining where 0 is sent:

$$k = \rho^k(0) = \mu\rho\mu(0) = \mu\rho(0) = \mu(1) = n - 1$$

Therefore,

$$\mu\rho\mu = \rho^{n-1}.$$

Multiplying both sides on the left by μ yields:

$$\mu\mu\rho\mu = \mu\rho^{n-1}$$

Since $\mu\mu = \iota$, we conclude that

$$\rho\mu = \mu\rho^{n-1}.$$ ▲

When computing products in D_n we normally want our answer in standard form. This is not difficult if we keep in mind a few basic facts about the group D_n. We have shown some of the properties listed below, and the rest you will be asked to verify in the exercises.

1. $\rho^n = \iota$ (Rotation by 2π is the identity map.)
2. $(\rho^k)^{-1} = \rho^{n-k}$
3. $\mu^2 = \iota$, which implies $\mu^{-1} = \mu$ (Reflect across a line twice is the identity map.)
4. $\rho^k\mu = \mu\rho^{n-k}$ (Example 4.22 for $k = 1$ and Exercise 30 for any k.)

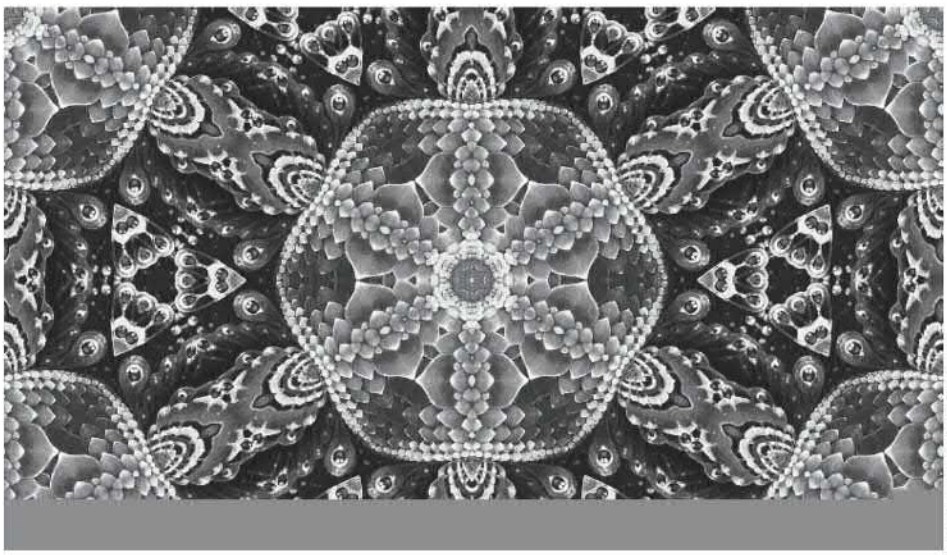
4.23 Example In the group D_5 compute $(\mu\rho^2)(\mu\rho)$. We see that

$$\begin{aligned}(\mu\rho^2)(\mu\rho) &= \mu\rho^2\mu\rho \\ &= \mu(\rho^2\mu)\rho \\ &= \mu(\mu\rho^{5-2})\rho \\ &= \mu^2\rho^4 \\ &= \rho^4\end{aligned}$$ ▲

4.24 Example In the dihedral group D_n compute $(\mu\rho^k)^{-1}$.

$$\begin{aligned}(\mu\rho^k)^{-1} &= (\rho^k)^{-1}\mu^{-1} \\ &= \rho^{n-k}\mu \\ &= \mu\rho^{n-(n-k)} \\ &= \mu\rho^k\end{aligned}$$ ▲

In Example 4.24 we determined that the inverse of $\mu\rho^k$ is itself, which suggests that $\mu\rho^k$ could be reflection across a line of symmetry. In Exercise 37, you will be asked to show this is the case. Geometrically, we can see that each of the elements of the form $\mu\rho^k$ is reflection across a line. Placing one mirror along the line of reflection for μ and another mirror along the line of reflection for $\mu\rho$ is the basis for designing a kaleidoscope. Any element in D_n can be written as a product using only the elements μ and $\mu\rho$ since we can write $\rho = \mu\mu\rho$. In a kaleidoscope successive reflections across the mirrors correspond to taking products involving μ and $\mu\rho$. So the image you see in the kaleidoscope has all the symmetries in D_n. That is, you can rotate the image by $\frac{360^\circ}{n}$ or reflect it across any one of the lines of reflection for the elements $\mu\rho^k$. Figure 4.25 is a typical image from a kaleidoscope with dihedral group D_{16} symmetries.



IZI_creation/Shutterstock

4.25 Figure

EXERCISES 4

Computation

In Exercises 1 through 5, compute the indicated product involving the following permutations in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}, \quad \mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}.$$

1. $\tau\sigma$ **2.** $\tau^2\sigma$ **3.** $\mu\sigma^2$ **4.** $\sigma^{-2}\tau$ **5.** $\sigma^{-1}\tau\sigma$

In Exercises 6 through 9, compute the expressions shown for the permutations σ, τ, and μ defined prior to Exercise 1.

6. σ^6 **7.** μ^2 **8.** σ^{100} **9.** μ^{100}

10. Convert the permutations σ, τ, and μ defined prior to Exercise 1 to disjoint cycle notation.

11. Convert the following permutations in S_8 from disjoint cycle notation to two-row notation.

a. $(1,4,5)(2,3)$
b. $(1,8,5)(2,6,7,3,4)$
c. $(1,2,3)(4,5)(6,7,8)$

12. Compute the permutation products.

a. $(1,5,2,4)(1,5,2,3)$
b. $(1,5,3)(1,2,3,4,5,6)(1,5,3)^{-1}$
c. $[(1,6,7,2)^2(4,5,2,6)^{-1}(1,7,3)]^{-1}$
d. $(1,6)(1,5)(1,4)(1,3)(1,2)$

13. Compute the following elements of D_{12}. Write your answer in standard form.

a. $\mu\rho^2\mu\rho^8$
b. $\mu\rho^{10}\mu\rho^{-1}$
c. $\rho\mu\rho^{-1}$
d. $(\mu\rho^3\mu^{-1}\rho^{-1})^{-1}$

14. Write the group table for D_3. Compare the group tables for D_3 and S_3. Are the groups isomorphic?

Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

is the **orbit** of a **under** σ. In Exercises 15 through 17, find the orbit of 1 under the permutation defined prior to Exercise 1.

15. σ **16.** τ **17.** μ

18. Verify that $H = \{\iota, \mu, \rho^2, \mu\rho^2\} \subseteq D_4$ is a group using the operation function composition.

19. a. Verify that the six matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

form a group under matrix multiplication. [*Hint*: Don't try to compute all products of these matrices. Instead, think how the column vector $\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$ is transformed by multiplying it on the left by each of the matrices.]

b. What group discussed in this section is isomorphic to this group of six matrices?

20. After working Exercise 18, write down eight matrices that form a group under matrix multiplication that is isomorphic to D_4.

Concepts

In Exercises 21 through 23, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

21. The *dihedral group* D_n is the set of all functions $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ such that the line segment between vertex i and vertex j of U_n is an edge of P_n if and only if the line segment between vertices $\phi(i)$ and $\phi(j)$ in U_n is an edge of P_n.

22. A *permutation* of a set S is a one-to-one map from S to S.

23. The *order* of a group is the number of elements in the group.

In Exercises 24 through 28, determine whether the given function is a permutation of $\mathbb{R}$.

24. $f_1 : \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x + 1$

25. $f_2 : \mathbb{R} \to \mathbb{R}$ defined by $f_2(x) = x^2$

26. $f_3 : \mathbb{R} \to \mathbb{R}$ defined by $f_3(x) = -x^3$

27. $f_4 : \mathbb{R} \to \mathbb{R}$ defined by $f_4(x) = e^x$

28. $f_5 : \mathbb{R} \to \mathbb{R}$ defined by $f_5(x) = x^3 - x^2 - 2x$

29. Determine whether each of the following is true or false.

a. Every permutation is a one-to-one function.

b. Every function is a permutation if and only if it is one-to-one.

c. Every function from a finite set onto itself must be one-to-one.

d. Every subset of an abelian group G that is also a group using the same operation as G is abelian.

e. The symmetric group S_{10} has 10 elements.

f. If $\phi \in D_n$, then ϕ is a permutation on the set $\mathbb{Z}_n$.

g. The group D_n has exactly n elements.

h. D_3 is a subset of D_4.

Theory

30. Let $n \geq 3$ and $k \in \mathbb{Z}_n$. Prove that in D_n, $\rho^k\mu = \mu\rho^{n-k}$.

31. Show that S_n is a nonabelian group for $n \geq 3$.

32. Strengthening Exercise 31, show that if $n \geq 3$, then the only element of σ of S_n satisfying $\sigma\gamma = \gamma\sigma$ for all $\gamma \in S_n$ is $\sigma = \iota$, the identity permutation.

33. Orbits were defined before Exercise 15. Let $a, b \in A$ and $\sigma \in S_A$. Show that if $\mathcal{O}_{a,\sigma}$ and $\mathcal{O}_{b,\sigma}$ have an element in common, then $\mathcal{O}_{a,\sigma} = \mathcal{O}_{b,\sigma}$.

34. (See the warning following Theorem 4.8.) Let G be a group with binary operation $*$. Let G' be the same set as G, and define a binary operation $*'$ on G' by $x *' y = y * x$ for all $x, y \in G'$.

a. (Intuitive argument that G' under $*'$ is a group.) Suppose the front wall of your classroom were made of transparent glass, and that all possible products $a * b = c$ and all possible instances $a * (b * c) = (a * b) * c$ of the associative property for G under $*$ were written on the wall with a magic marker. What would a person see when looking at the other side of the wall from the next room in front of yours?

b. Show from the mathematical definition of $*'$ that G' is a group under $*'$.

35. Give a careful proof using the definition of isomorphism that if G and G' are both groups with G abelian and G' not abelian, then G and G' are not isomorphic.

36. Prove that for any integer $n \geq 2$, there are at least two nonisomorphic groups with exactly $2n$ elements.

37. Let $n \geq 3$ and $0 \leq k \leq n - 1$. Prove that the map $\mu\rho^k \in D_n$ is reflection about the line through the origin that makes an angle of $-\frac{\pi k}{n}$ with the $x-$axis.

38. Let $n \geq 3$ and $k, r \in \mathbb{Z}_n$. Based on Exercise 37, determine the element of D_n that corresponds to first reflecting across the line through the origin at an angle of $-\frac{2\pi k}{n}$ and then reflection across the line through the origin making an angle of $-\frac{2\pi r}{n}$. Prove your answer.

SECTION 5 SUBGROUPS

Subsets and Subgroups

You may have noticed that we sometimes have had groups contained within larger groups. For example, the group $\mathbb{Z}$ under addition is contained within the group $\mathbb{Q}$ under addition, which in turn is contained in the group $\mathbb{R}$ under addition. When we view the group $\langle \mathbb{Z}, + \rangle$ as contained in the group $\langle \mathbb{R}, + \rangle$, it is very important to notice that the operation $+$ on integers n and m as elements of $\langle \mathbb{Z}, + \rangle$ produces the same element $n + m$ as would result if you were to think of n and m as elements in $\langle \mathbb{R}, + \rangle$. Thus we should *not* regard the group $\langle \mathbb{Q}^+, \cdot \rangle$ as contained in $\langle \mathbb{R}, + \rangle$, even though $\mathbb{Q}^+$ is contained in $\mathbb{R}$ as a set. In this instance, $2 \cdot 3 = 6$ in $\langle \mathbb{Q}^+, \cdot \rangle$, while $2 + 3 = 5$ in $\langle \mathbb{R}, + \rangle$. We are requiring not only that the set of one group be a subset of the set of the other, but also that the group operation on the subset be the *induced operation* that assigns the same element to each ordered pair from this subset as is assigned by the group operation on the whole set.

5.1 Definition If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup of** G. We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G, and $H < G$ or $G > H$ shall mean $H \leq G$ but $H \neq G$. ■

Thus $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ but $\langle \mathbb{Q}^+, \cdot \rangle$ is *not* a subgroup of $\langle \mathbb{R}, + \rangle$, even though as sets, $\mathbb{Q}^+ \subset \mathbb{R}$. Every group G has as subgroups G itself and $\{e\}$, where e is the identity element of G.

5.2 Definition If G is a group, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups are **proper subgroups**. The subgroup $\{e\}$ is the **trivial subgroup** of G. All other subgroups are **nontrivial**. ■

We turn to some illustrations.

5.3 Example Let $\mathbb{R}^n$ be the additive group of all n-component row vectors with real number entries. The subset consisting of all of these vectors having 0 as entry in the first component is a subgroup of $\mathbb{R}^n$. ▲

5.4 Example $\mathbb{Q}^+$ under multiplication is a proper subgroup of $\mathbb{R}^+$ under multiplication. ▲

5.5 Example The n^{th} roots of unity in $\mathbb{C}$, U_n, form a subgroup of U, the complex numbers whose absolute value is 1, which in turn is a subgroup of $\mathbb{C}^*$, the nonzero complex numbers under multiplication. ▲

5.6 Example Recall that $S_{\mathbb{Z}_n}$ is the set of all one-to-one functions mapping $\mathbb{Z}_n$ onto $\mathbb{Z}_n$ and D_n is the set of all one-to-one functions ϕ mapping $\mathbb{Z}_n$ onto $\mathbb{Z}_n$ with the further property that the line segment between i and j is an edge of the regular n-gon P_n if and only if the line segment between $\phi(i)$ and $\phi(j)$ is an edge. $D_n \subseteq S_{\mathbb{Z}_n}$. Since both D_n and $S_{\mathbb{Z}_n}$ are groups under composition of functions, $D_n \leq S_{\mathbb{Z}_n}$. ▲

5.7 Example There are two different types of group structures of order 4 (see Exercise 20 of Section 2). We describe them by their group tables (Tables 5.8 and 5.9). The group V is the Klein 4-group.

The only nontrivial proper subgroup of $\mathbb{Z}_4$ is $\{0, 2\}$. Note that $\{0, 3\}$ is *not* a subgroup of $\mathbb{Z}_4$, since $\{0, 3\}$ is *not closed* under $+$. For example, $3 + 3 = 2$, and $2 \notin \{0, 3\}$. However, the group V has three nontrivial proper subgroups, $\{e, a\}$, $\{e, b\}$, and $\{e, c\}$. Here $\{e, a, b\}$ is *not* a subgroup, since $\{e, a, b\}$ is not closed under the operation of V because $ab = c$, and $c \notin \{e, a, b\}$. ▲

5.8 Table

$\mathbb{Z}_4$:

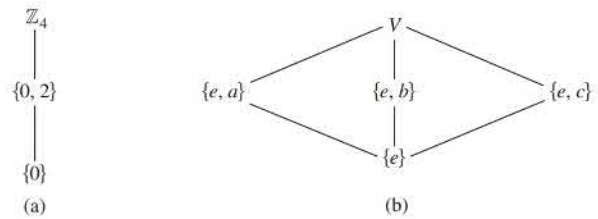
$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

5.9 Table

V:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It is often useful to draw a *subgroup diagram* of the subgroups of a group. In such a diagram, a line running downward from a group G to a group H means that H is a subgroup of G. Thus the larger group is placed nearer the top of the diagram. Figure 5.10 contains the subgroup diagrams for the groups $\mathbb{Z}_4$ and V of Example 5.7.



5.10 Figure (a) Subgroup diagram for $\mathbb{Z}_4$. (b) Subgroup diagram for V.

Note that if $H \leq G$ and $a \in H$, then by Theorem 2.17, the equation $ax = a$ must have a unique solution, namely the identity element of H. But this equation can also

be viewed as one in G, and we see that this unique solution must also be the identity element e of G. A similar argument then applied to the equation $ax = e$, viewed in both H and G, shows that the inverse a^{-1} of a in G is also the inverse of a in the subgroup H.

5.11 Example Let F be the group of all real-valued functions with domain $\mathbb{R}$ under addition. The subset of F consisting of those functions that are continuous is a subgroup of F, for the sum of continuous functions is continuous, the function f where $f(x) = 0$ for all x is continuous and is the additive identity element, and if f is continuous, then $-f$ is continuous. ▲

It is convenient to have routine steps for determining whether a subset of a group G is a subgroup of G. Example 5.11 indicates such a routine, and in the next theorem, we demonstrate carefully its validity.

5.12 Theorem A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G,
2. the identity element e of G is in H, and
3. for all $a \in H$, $a^{-1} \in H$ also.

Proof The fact that if $H \leq G$ then Conditions 1, 2, and 3 must hold follows at once from the definition of a subgroup and from the remarks preceding Example 5.11.

Conversely, suppose H is a subset of a group G such that Conditions 1, 2, and 3 hold. By 2 we have at once that $\mathscr{G}_2$ is satisfied. Also $\mathscr{G}_3$ is satisfied by 3. It remains to check the associative axiom, $\mathscr{G}_1$. But surely for all $a, b, c \in H$ it is true that $(ab)c = a(bc)$ in H, for we may actually view this as an equation in G, where the associative law holds. Hence $H \leq G$. ◆

5.13 Example Let F be as in Example 5.11. The subset of F consisting of those functions that are differentiable is a subgroup of F, for the sum of differentiable functions is differentiable, the constant function 0 is differentiable, and if f is differentiable, then $-f$ is differentiable. ▲

5.14 Example Recall from linear algebra that every square matrix A has associated with it a number $\det(A)$ called its determinant, and that A is invertible if and only if $\det(A) \neq 0$. If A and B are square matrices of the same size, then it can be shown that $\det(AB) = \det(A) \cdot \det(B)$. Let G be the multiplicative group of all invertible $n \times n$ matrices with entries in $\mathbb{C}$ and let T be the subset of G consisting of those matrices with determinant 1. The equation $\det(AB) = \det(A) \cdot \det(B)$ shows that T is closed under matrix multiplication. Recall that the identity matrix I_n has determinant 1. From the equation $\det(A) \cdot \det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1$, we see that if $\det(A) = 1$, then $\det(A^{-1}) = 1$. Theorem 5.12 then shows that T is a subgroup of G. ▲

Theorem 5.15 provides an alternate way of checking that a subset of a group is a subgroup.

5.15 Theorem A nonempty subset H of the group G is a subgroup of G if and only if for all $a, b \in G$, $ab^{-1} \in G$.

Proof We leave the proof as Exercise 51. ◆

On the surface Theorem 5.15 may seem simpler than Theorem 5.12 since we only need to show that H is not empty and one other condition. In practice, it is usually just as efficient to use Theorem 5.12. On the other hand, Theorem 5.16 can often be used efficiently.

5.16 Theorem Let H be a finite nonempty subset of the group G. Then H is a subgroup of G if and only if H is closed under the operation of G.

Proof We leave the proof as Exercise 57. ◆

5.17 Example Recall that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. We could use Theorem 5.16 to verify that U_n is a subgroup of C^* by noting that U_n has exactly n elements, so U_n is a finite nonempty subset of $\mathbb{C}^*$ and if $z_1, z_2 \in U_n$, then $(z_1 z_2)^n = 1$, which implies that U_n is closed under multiplication. ▲

5.18 Example We verify that the subset $H = \{\iota = \rho^0, \rho, \rho^2, \ldots, \rho^{n-1}\} \subset D_n$ is a subgroup of D_n. By Theorem 5.16, we only need to check that H is closed under the operation of D_n. Let $k, r \in \mathbb{Z}_n$. Then $\rho^k \rho^r = \rho^{k+_n r} \in H$. Therefore $H \leq D_n$. ▲

Cyclic Subgroups

Let us see how large a subgroup H of $\mathbb{Z}_{12}$ would have to be if it contains 3. It would have to contain the identity element 0 and $3 + 3$, which is 6. Then it has to contain $6 + 3$, which is 9. Note that the inverse of 3 is 9 and the inverse of 6 is 6. It is easily checked that $H = \{0, 3, 6, 9\}$ is a subgroup of $\mathbb{Z}_{12}$, and it is the smallest subgroup containing 3.

Let us imitate this reasoning in a general situation. As we remarked before, for a general argument we always use multiplicative notation. Let G be a group and let $a \in G$. A subgroup of G containing a must, by Theorem 5.12, contain a^n, the result of computing products of a and itself for n factors for every positive integer n. These positive integral powers of a do give a set closed under multiplication. It is possible, however, that the inverse of a is not in this set. Of course, a subgroup containing a must also contain a^{-1}, and, in general, it must contain a^{-m} for all $m \in \mathbb{Z}^+$. It must contain the identity element $e = a^0$. Summarizing, *a subgroup of G containing the element a must contain all elements* a^n *(or na for additive groups) for all* $n \in \mathbb{Z}$. That is, a subgroup containing a must contain $\{a^n | n \in \mathbb{Z}\}$. Observe that these powers a^n of a need not be distinct. For example, in the group V of Example 5.7,

$$a^2 = e, \quad a^3 = a, \quad a^4 = e, \quad a^{-1} = a, \qquad \text{and so on.}$$

We have almost proved the next theorem.

5.19 Theorem Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest† subgroup of G that contains a, that is, every subgroup containing a contains H.

Proof We check the three conditions given in Theorem 5.12 for a subset of a group to give a subgroup. Since $a^r a^s = a^{r+s}$ for $r, s \in \mathbb{Z}$, we see that the product in G of two elements of H is again in H. Thus H is closed under the group operation of G. Also $a^0 = e$, so $e \in H$, and for $a^r \in H, a^{-r} \in H$ and $a^{-r} a^r = e$. Hence all the conditions are satisfied, and $H \leq G$.

---

† We may find occasion to distinguish between the terms *minimal* and *smallest* as applied to subsets of a set S that have some property. A subset H of S is minimal with respect to the property if H has the property, and no subset $K \subset H, K \neq H$, has the property. If H has the property and $H \subseteq K$ for every subset K with the property, then H is the smallest subset with the property. There may be many minimal subsets, but there can be only one smallest subset. To illustrate, $\{e, a\}, \{e, b\}$, and $\{e, c\}$ are all minimal nontrivial subgroups of the group V. (See Fig. 5.10.) However, V contains no smallest nontrivial subgroup.

Our arguments prior to the statement of the theorem showed that any subgroup of G containing a must contain H, so H is the smallest subgroup of G containing a. ◆

5.20 Definition Let G be a group and let $a \in G$. Then the subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of G, characterized in Theorem 5.19, is called the **cyclic subgroup of G generated by a**, and denoted by $\langle a \rangle$. ■

5.21 Example Let us find two of the cyclic subgroups to D_{10}. We first consider $\langle \mu\rho^k \rangle$ for $k \in \mathbb{Z}_{10}$. Since $(\mu\rho^k)^2 = \iota$ and $(\mu\rho^k)^{-1} = \mu\rho^k$, for any integer r, $(\mu\rho^k)^r$ is either $\mu\rho^k$ or ι. Thus

$$\langle \mu\rho^k \rangle = \{\iota, \mu\rho^k\}.$$

Since $\rho^{-1} = \rho^9$, every negative power of ρ is also a positive power of ρ and $\rho^{10} = \iota$,

$$\langle \rho \rangle = \{\iota, \rho, \rho^2, \ldots, \rho^9\}.$$

▲

5.22 Definition An element a of a group G **generates** G and is a **generator for** G if $\langle a \rangle = G$. A group G is **cyclic** if there is some element a in G that generates G. ■

5.23 Example Let $\mathbb{Z}_4$ and V be the groups of Example 5.7. Then $\mathbb{Z}_4$ is cyclic and both 1 and 3 are generators, that is,

$$\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4.$$

However, V is *not* cyclic, for $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are proper subgroups of two elements. Of course, $\langle e \rangle$ is the trivial subgroup of one element. ▲

5.24 Example The group $\mathbb{Z}$ under addition is a cyclic group. Both 1 and -1 are generators for this group, and they are the only generators. Also, for $n \in \mathbb{Z}^+$, the group $\mathbb{Z}_n$ under addition modulo n is cyclic. If $n > 1$, then both 1 and $n - 1$ are generators, but there may be others. ▲

5.25 Example Consider the group $\mathbb{Z}$ under addition. Let us find $\langle 3 \rangle$. Here the notation is additive, and $\langle 3 \rangle$ must contain

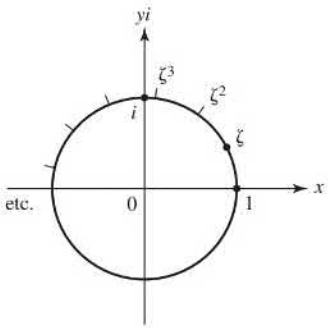
$$\begin{array}{llll} & 3, \quad 3+3=6, & 3+3+3=9, & \text{and so on,} \\ 0, \quad -3, & -3+-3=-6, & -3+-3+-3=-9, & \text{and so on.} \end{array}$$

In other words, the cyclic subgroup generated by 3 consists of all multiples of 3, positive, negative, and zero. We denote this subgroup by $3\mathbb{Z}$ as well as $\langle 3 \rangle$. In a similar way, we shall let $n\mathbb{Z}$ be the cyclic subgroup $\langle n \rangle$ of $\mathbb{Z}$. Note that $6\mathbb{Z} < 3\mathbb{Z}$. ▲

5.26 Example For each positive integer n, U_n is the multiplicative group of the nth roots of unity in $\mathbb{C}$. These elements of U_n can be represented geometrically by equally spaced points on a circle about the origin, as illustrated in Fig. 5.27. The point labeled represents the number

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

The geometric interpretation of multiplication of complex numbers, explained in Section 3, shows at once that as ζ is raised to powers, it works its way counterclockwise around the circle, landing on each of the elements of U_n in turn. Thus U_n under multiplication is a cyclic group, and ζ is a generator. The group U_n is the cyclic subgroup $\langle \zeta \rangle$ of the group U of all complex numbers z, where $|z| = 1$, under multiplication. ▲



5.27 Figure

EXERCISES 5

Computations

In Exercises 1 through 6, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. $\mathbb{R}$ **2.** $\mathbb{Q}^+$ **3.** $7\mathbb{Z}$

4. The set $i\mathbb{R}$ of pure imaginary numbers including 0

5. The set $\pi\mathbb{Q}$ of rational multiples of π **6.** The set $\{\pi^n \mid n \in \mathbb{Z}\}$

7. Which of the sets in Exercises 1 through 6 are subgroups of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication?

In Exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

8. The $n \times n$ matrices with determinant greater than or equal to 1

9. The diagonal $n \times n$ matrices with no zeros on the diagonal

10. The $n \times n$ matrices with determinant 2^k for some integer k

11. The $n \times n$ matrices with determinant -1

12. The $n \times n$ matrices with determinant -1 or 1

13. The set of all $n \times n$ matrices A such that $(A^T)A = I_n$. [These matrices are called **orthogonal.** Recall that A^T, the *transpose* of A, is the matrix whose jth column is the jth row of A for $1 \leq j \leq n$, and that the transpose operation has the property $(AB)^T = (B^T)(A^T)$.]

Let F be the set of all real-valued functions with domain $\mathbb{R}$ and let $\tilde{F}$ be the subset of F consisting of those functions that have a nonzero value at every point in $\mathbb{R}$. In Exercises 14 through 19, determine whether the given subset of F with the induced operation is (a) a subgroup of the group F under addition, (b) a subgroup of the group $\tilde{F}$ under multiplication.

14. The subset $\tilde{F}$

15. The subset of all $f \in F$ such that $f(1) = 0$

16. The subset of all $f \in \tilde{F}$ such that $f(1) = 1$

17. The subset of all $f \in \tilde{F}$ such that $f(0) = 1$

18. The subset of all $f \in \tilde{F}$ such that $f(0) = -1$

19. The subset of all constant functions in F.

20. Nine groups are given below. Give a *complete* list of all subgroup relations, of the form $G_i \leq G_j$, that exist between these given groups $G_1, G_2, \cdots, G_9$.

$G_1 = \mathbb{Z}$ under addition
$G_2 = 12\mathbb{Z}$ under addition
$G_3 = \mathbb{Q}^+$ under multiplication
$G_4 = \mathbb{R}$ under addition
$G_5 = \mathbb{R}^+$ under multiplication
$G_6 = \{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication
$G_7 = 3\mathbb{Z}$ under addition
$G_8 =$ the set of all integral multiples of 6 under addition
$G_9 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication

21. Write at least 5 elements of each of the following cyclic groups.

a. $25\mathbb{Z}$ under addition
b. $\{(\frac{1}{2})^n \mid n \in \mathbb{Z}\}$ under multiplication
c. $\{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication
d. $\langle \rho^3 \rangle$ in the group D_{18}
e. $\langle (1,2,3)(5,6) \rangle$ in the group S_6

In Exercises 22 through 25, describe all the elements in the cyclic subgroup of $GL(2, \mathbb{R})$ generated by the given 2×2 matrix.

22. $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ **23.** $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ **24.** $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ **25.** $\begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$

26. Which of the following groups are cyclic? For each cyclic group, list all the generators of the group.

$$G_1 = \langle \mathbb{Z}, + \rangle \quad G_2 = \langle \mathbb{Q}, + \rangle \quad G_3 = \langle \mathbb{Q}^+, \cdot \rangle \quad G_4 = \langle 6\mathbb{Z}, + \rangle$$
$$G_5 = \{6^n \mid n \in \mathbb{Z}\} \text{ under multiplication}$$
$$G_6 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ under addition}$$

In Exercises 27 through 35, find the order of the cyclic subgroup of the given group generated by the indicated element.

27. The subgroup of $\mathbb{Z}_4$ generated by 3

28. The subgroup of V generated by c (see Table 5.9)

29. The subgroup of U_6 generated by $\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$

30. The subgroup of $\mathbb{Z}_{10}$ generated by 8

31. The subgroup of $\mathbb{Z}_{16}$ generated by 12

32. The subgroup of the symmetric group S_8 generated by $(2,4,6,9)(3,5,7)$

33. The subgroup of the symmetric group S_{10} generated by $(1,10)(2,9)(3,8)(4,7)(5,6)$

34. The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

$$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

35. The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

36. **a.** Complete Table 5.28 to give the group $\mathbb{Z}_6$ of 6 elements.
b. Compute the subgroups $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, and $\langle 5 \rangle$ of the group $\mathbb{Z}_6$ given in part (a).

c. Which elements are generators for the group $\mathbb{Z}_6$ of part (a)?

d. Give the subgroup diagram for the part (b) subgroups of $\mathbb{Z}_6$. (We will see later that these are all the subgroups of $\mathbb{Z}_6$.)

5.28 Table

$\mathbb{Z}_6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2					
3	3					
4	4					
5	5					

Concepts

In Exercises 37 and 38, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

37. A *subgroup* of a group G is a subset H of G that contains the identity element e of G and also contains the inverse of each of its elements.

38. A group G is *cyclic* if and only if there exists $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$.

39. Determine whether each of the following is true or false.

a. The associative law holds in every group.

b. There may be a group in which the cancellation law fails.

c. Every group is a subgroup of itself.

d. Every group has exactly two improper subgroups.

e. In every cyclic group, every element is a generator.

f. A cyclic group has a unique generator.

g. Every set of numbers that is a group under addition is also a group under multiplication.

h. A subgroup may be defined as a subset of a group.

i. $\mathbb{Z}_4$ is a cyclic group.

j. Every subset of every group is a subgroup under the induced operation.

k. For any $n \geq 3$, the dihedral group D_n has at least $n + 2$ cyclic subgroups.

40. Show by means of an example that it is possible for the quadratic equation $x^2 = e$ to have more than two solutions in some group G with identity e.

In Exercises 41 through 44 let B be a subset of A, and let b be a particular element of B. Determine whether the given set is a subgroup of the symmetric group S_A under the induced operation. Here $\sigma[B] = \{\sigma(x) \mid x \in B\}$.

41. $\{\sigma \in S_A \mid \sigma(b) = b\}$

42. $\{\sigma \in S_A \mid \sigma(b) \in B\}$

43. $\{\sigma \in S_A \mid \sigma[B] \subseteq B\}$

44. $\{\sigma \in S_A \mid \sigma[B] = B\}$

Theory

In Exercises 45 and 46, let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Write out a proof to convince a skeptic of the intuitively clear statement.

45. If H is a subgroup of G, then $\phi[H] = \{\phi(h) \mid h \in H\}$ is a subgroup of G'. That is, an isomorphism carries subgroups into subgroups.

46. If there is an $a \in G$ such that $\langle a \rangle = G$, then G' is cyclic.

47. Show that if H and K are subgroups of an abelian group G, then

$$\{hk \mid h \in H \text{ and } k \in K\}$$

is a subgroup of G.

48. Find an example of a group G and two subgroups H and K such that the set in Exercise 47 is not a subgroup of G.

49. Prove that for any integer $n \geq 3$, S_n has a subgroup isomorphic with D_n.

50. Find the flaw in the following argument: "Condition 2 of Theorem 5.12 is redundant, since it can be derived from 1 and 3, for let $a \in H$. Then $a^{-1} \in H$ by 3, and by 1, $aa^{-1} = e$ is an element of H, proving 2."

51. Prove Theorem 5.15.

52. Prove that if G is a cyclic group and $|G| \geq 3$, then G has at least 2 generators.

53. Prove that if G is an abelian group, written multiplicatively, with identity element e, then all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

54. Repeat Exercise 53 for the general situation of the set H of all solutions x of the equation $x^n = e$ for a fixed integer $n \geq 1$ in an abelian group G with identity e.

55. Find a counterexample to Exercise 53 if the assumption of abelian is dropped.

56. Show that if $a \in G$, where G is a finite group with identity e, then there exists $n \in \mathbb{Z}^+$ such that $a^n = e$.

57. Prove Theorem 5.16.

58. Let G be a group and let a be one fixed element of G. Show that

$$H_a = \{x \in G \mid xa = ax\}$$

is a subgroup of G.

59. Generalizing Exercise 58, let S be any subset of a group G.

a. Show that $H_S = \{x \in G \mid xs = sx \text{ for all } s \in S\}$ is a subgroup of G.

b. In reference to part (a), the subgroup H_G is the **center of** G. Show that H_G is an abelian group.

60. Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

61. For sets H and K, we define the **intersection** $H \cap K$ by

$$H \cap K = \{x \mid x \in H \text{ and } x \in K\}.$$

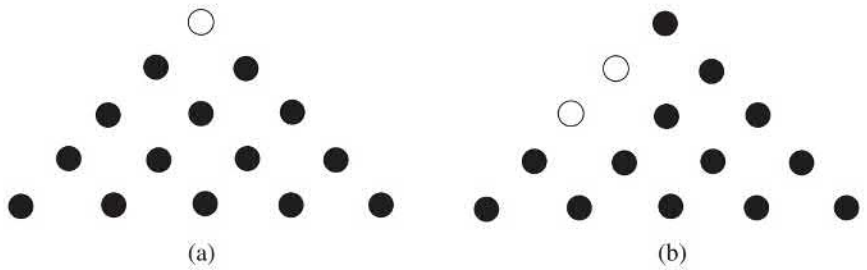
Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$. (Remember: $\leq$ denotes "is a subgroup of," not "is a subset of.")

62. Prove that every cyclic group is abelian.

63. Let G be a group and let $G_n = \{g^n \mid g \in G\}$. Under what hypothesis about G can we show that G_n is a subgroup of G?

64. Show that a group with no proper nontrivial subgroups is cyclic.

65. Cracker Barrel Restaurants place a puzzle called "Jump All But One Game" at each table. The puzzle starts with golf tees arranged in a triangle as in Figure 5.29a where the presence of a tee is noted with a solid dot and the absence is noted with a hollow dot. A move can be made if a tee can jump over one adjacent tee and land on an empty space. When a move is made, the tee that is jumped over is removed. A possible first move is shown in Figure 5.29b. The goal is to have just one remaining tee. Use the Klein 4-group to show that no matter what sequence of (legal) moves you make, the last remaining tee cannot be in a bottom corner position.



5.29 Figure

SECTION 6 CYCLIC GROUPS

Recall the following facts and notations from Section 5. If G is a group and $a \in G$, then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G (Theorem 5.19). This group is the **cyclic subgroup** $\langle a \rangle$ **of** G **generated by** a. Also, given a group G and an element a in G, if

$$G = \{a^n \mid n \in \mathbb{Z}\},$$

then a is a **generator of** G and the group $G = \langle a \rangle$ is **cyclic.** We introduce one new bit of terminology. Let a be an element of a group G. If the cyclic subgroup $\langle a \rangle$ of G is finite, then the **order of** a is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that a is of **infinite order.** We will see in this section that if $a \in G$ is of finite order m, then m is the smallest positive integer such that $a^m = e$.

The first goal of this section is to describe all cyclic groups and all subgroups of cyclic groups. This is not an idle exercise. We will see later that cyclic groups serve as building blocks for a significant class of abelian groups, in particular, for all finite abelian groups. Cyclic groups are fundamental to the understanding of groups.

Elementary Properties of Cyclic Groups

We start with a demonstration that cyclic groups are abelian.

6.1 Theorem Every cyclic group is abelian.

Proof Let G be a cyclic group and let a be a generator of G so that

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1,$$

so G is abelian. ◆

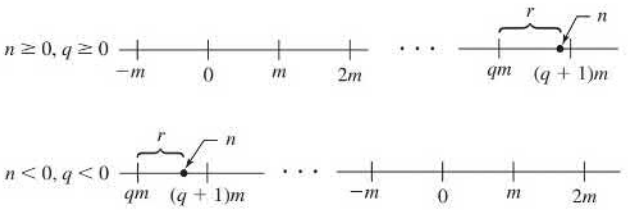
We shall continue to use multiplicative notation for our general work on cyclic groups, even though they are abelian.

The *division algorithm* that follows is well known and seems pretty simple. In fact, this algorithm is taught in elementary school. If you divide an integer n by a positive integer m, you get an integer quotient q with a remainder r where $0 \leq r < m$. You might write this as $n \div m = q \text{ R } r$, which of course means $\frac{n}{m} = q + \frac{r}{m}$. Multiplying both sides by m gives the form of the division algorithm that is a fundamental tool for the study of cyclic groups.

6.2 Division Algorithm for $\mathbb{Z}$ If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \qquad \text{and} \qquad 0 \leq r < m.$$

Proof We give an intuitive diagrammatic explanation, using Fig. 6.3. On the number line, mark off the multiples of m and the position of n. Now n falls either on a multiple qm of m and r can be taken as 0, or n falls between two multiples of m. If the latter is the case, let qm be the first multiple of m to the left of n. Then r is as shown in Fig. 6.3. Note that $0 \leq r < m$. Uniqueness of q and r follows since if n is not a multiple of m so that we can take $r = 0$, then there is a unique multiple qm of m to the left of n and at distance less than m from n, as illustrated in Fig. 6.3. ◆



6.3 Figure

In the notation of the division algorithm, we regard q as the **quotient** and r as the nonnegative **remainder** when n is divided by m.

6.4 Example Find the quotient q and remainder r when 38 is divided by 7 according to the division algorithm.

Solution The positive multiples of 7 are $7, 14, 21, 28, 35, 42, \cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$38 = 35 + 3 = 7(5) + 3$$

so the quotient is $q = 5$ and the remainder is $r = 3$. ▲

6.5 Example Find the quotient q and remainder r when -38 is divided by 7 according to the division algorithm.

Solution The negative multiples of 7 are $-7, -14, -21, -28, -35, -42, \cdots$. Choosing the multiple to leave a nonnegative remainder less than 7, we write

$$-38 = -42 + 4 = 7(-6) + 4$$

so the quotient is $q = -6$ and the remainder is $r = 4$. ▲

We will use the division algorithm to show that a subgroup H of a cyclic group G is also cyclic. Think for a moment what we will have to do to prove this. We will have to use the *definition* of a cyclic group since we have proved little about cyclic groups yet. That is, we will have to use the fact that G has a generating element a. We must then exhibit, in terms of this generator a, some generator $c = a^m$ for H in order to show that H is cyclic. There is really only one natural choice for the power m of a to try. Can you guess what it is before you read the proof of the theorem?

6.6 Theorem A subgroup of a cyclic group is cyclic.

Proof Let G be a cyclic group generated by a and let H be a subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. If $H \neq \{e\}$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$. Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$.

We claim that $c = a^m$ generates H; that is,

$$H = \langle a^m \rangle = \langle c \rangle.$$

We must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some n. Find q and r such that

$$n = mq + r \qquad \text{for} \qquad 0 \leq r < m$$

in accord with the division algorithm. Then

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

so

$$a^r = (a^m)^{-q} a^n.$$

Now since $a^n \in H, a^m \in H$, and H is a group, both $(a^m)^{-q}$ and a^n are in H. Thus

$$(a^m)^{-q} a^n \in H; \qquad \text{that is,} \qquad a^r \in H.$$

Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have $r = 0$. Thus $n = mq$ and

$$b = a^n = (a^m)^q = c^q,$$

so b is a power of c. ◆

As noted in Examples 5.24 and 5.25, $\mathbb{Z}$ under addition is cyclic and for a positive integer n, the set $n\mathbb{Z}$ of all multiples of n is a subgroup of $\mathbb{Z}$ under addition, the cyclic subgroup generated by n. Theorem 6.6 shows that these cyclic subgroups are the only subgroups of $\mathbb{Z}$ under addition. We state this as a corollary.

6.7 Corollary The subgroups of $\mathbb{Z}$ under addition are precisely the groups $n\mathbb{Z}$ under addition for $n \in \mathbb{Z}$. ◆

This corollary gives us an elegant way to define the *greatest common divisor* of two positive integers r and s. Exercise 54 shows that $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of the group $\mathbb{Z}$ under addition. Thus H must be cyclic and have a generator d, which we may choose to be positive.

6.8 Definition Let r be a positive integer and s be a non-negative integer. The positive generator d of the cyclic group

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor** (abbreviated gcd) of r and s. We write $d = \gcd(r, s)$. ■

Note that $d\mathbb{Z} = H$, $r = 1r + 0s \in H$, and $s = 0r + 1s \in H$. This implies that $r, s \in d\mathbb{Z}$, which says that d is a divisor of both r and s. Since $d \in H$, we can write

$$d = nr + ms$$

for some integers n and m. We see that every integer dividing both r and s divides the right-hand side of the equation, and hence must be a divisor of d also. Thus d must

be the largest number dividing both r and s; this accounts for the name given to d in Definition 6.8.

The fact that the greatest common divisor d of r and s can be written in the form $d = nr + ms$ for some integers n and m is called Bézout's identity. Bézout's identity is very useful in number theory, as we will see in studying cyclic groups.

6.9 Example Find the gcd of 42 and 72.

Solution The positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, and 42. The positive divisors of 72 are 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, and 72. The greatest common divisor is 6. Note that $6 = (3)(72) + (-5)(42)$. There is an algorithm for expressing the greatest common divisor d of r and s in the form $d = nr + ms$, but we will not need to make use of it here. The interested reader can find the algorithm by searching the Internet for the Euclidean algorithm and Bézout's identity. ▲

Two positive integers are **relatively prime** if their gcd is 1. For example, 12 and 25 are relatively prime. Note that they have no prime factors in common. In our discussion of subgroups of cyclic groups, we will need to know the following:

If r and s are relatively prime and if r divides sm, then r must divide m. (1)

Let's prove this. If r and s are relatively prime, then we may write

$$1 = ar + bs \qquad \text{for some} \qquad a, b \in \mathbb{Z}.$$

Multiplying by m, we obtain

$$m = arm + bsm.$$

Now r divides both arm and bsm since r divides sm. Thus r is a divisor of the right-hand side of this equation, so r must divide m.

The Structure of Cyclic Groups

We can now describe all cyclic groups, up to an isomorphism.

6.10 Theorem Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof **Case I** *For all positive integers m, $a^m \neq e$.* In this case we claim that no two distinct exponents h and k can give equal elements a^h and a^k of G. Suppose that $a^h = a^k$ and say $h > k$. Then

$$a^h a^{-k} = a^{h-k} = e,$$

contrary to our Case I assumption. Hence every element of G can be expressed as a^m for a unique $m \in \mathbb{Z}$. The map $\phi : G \to \mathbb{Z}$ given by $\phi(a^i) = i$ is thus well defined, one-to-one, and onto $\mathbb{Z}$. Also,

$$\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j),$$

so the homomorphism property is satisfied and ϕ is an isomorphism.

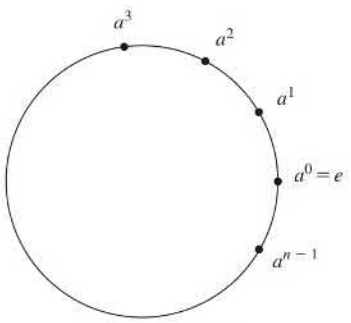
Case II *$a^m = e$ for some positive integer m.* Let n be the smallest positive integer such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. As in Case 1, if $0 \leq k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting our choice of n. Thus the elements

$$a^0 = e, a, a^2, a^3, \cdots, a^{n-1}$$

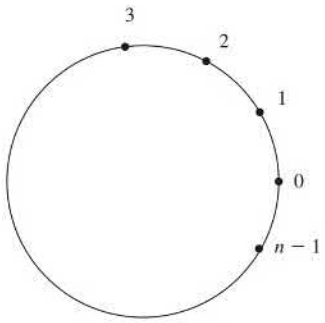
are all distinct and comprise all elements of G. The map $\psi : G \to \mathbb{Z}_n$ given by $\psi(a^i) = i$ for $i = 0, 1, 2, \cdots, n-1$ is thus well defined, one-to-one, and onto $\mathbb{Z}_n$. Because $a^n = e$, we see that $a^i a^j = a^k$ where $k = i +_n j$. Thus

$$\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j),$$

so the homomorphism property is satisfied and ψ is an isomorphism. ◆



6.11 Figure



6.12 Figure

6.13 Example Motivated by our work with U_n, it is nice to visualize the elements $e = a^0, a^1, a^2, \cdots, a^{n-1}$ of a cyclic group of order n as being distributed evenly on a circle (see Fig. 6.11). The element a^h is located h of these equal units counterclockwise along the circle, measured from the right where $e = a^0$ is located. To multiply a^h and a^k diagrammatically, we start from a^h and go k additional units around counterclockwise. To see arithmetically where we end up, find q and r such that

$$h + k = nq + r \qquad \text{for} \qquad 0 \leq r < n.$$

The nq takes us all the way around the circle q times, and we then wind up at a^r. ▲

Figure 6.12 is essentially the same as Fig. 6.11 but with the points labeled with the exponents on the generator. The operation on these exponents is *addition modulo n.*

This is simply the isomorphism between $\langle a \rangle$ and $\mathbb{Z}_n$. Of course this is the same isomorphism we saw when we defined $\mathbb{Z}_n$ from U_n, but using a instead of ζ.

As promised at the beginning of this section, we can see now that the order of an element a in a group G is simply the smallest positive number n such that $a^n = e$.

6.14 Example Let us find the order of the k-cycle, $\sigma = (a_1, a_2, a_3, \ldots, a_k)$, in the symmetric group. The order of σ is the smallest postive power of σ that is ι. Note that applying σ just maps each number to the next one in the cyclic order. So after k applications of σ, each number maps back to itself, but not before k applications of σ. Therefore, the order of a k-cycle is k. ▲

Subgroups of Finite Cyclic Groups

We have completed our description of cyclic groups and turn to their subgroups. Corollary 6.7 gives us complete information about subgroups of infinite cyclic groups. Let us give the basic theorem regarding generators of subgroups for the finite cyclic groups.

6.15 Theorem Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof That b generates a cyclic subgroup H of G is known from Theorem 5.19. We need show only that H has n/d elements. Following the argument of Case II of Theorem 6.10, we see that H has as many elements as the smallest positive power m of b that gives the identity. Now $b = a^s$, and $b^m = e$ if and only if $(a^s)^m = e$, or if and only if n divides ms. What is the smallest positive integer m such that n divides ms? Let d be the gcd of n and s. Then there exist integers u and v such that

$$d = un + vs.$$

Since d divides both n and s, we may write

$$1 = u(n/d) + v(s/d)$$

where both n/d and s/d are integers. This last equation shows that n/d and s/d are relatively prime, for any integer dividing both of them must also divide 1. We wish to find the smallest positive m such that

$$\frac{ms}{n} = \frac{m(s/d)}{(n/d)} \text{ is an integer.}$$

From the division property (1) following Example 6.9, we conclude that n/d must divide m, so the smallest such m is n/d. Thus the order of H is n/d.

Taking for the moment $\mathbb{Z}_n$ as a model for a cyclic group of order n, we see that if d is a divisor of n, then the cyclic subgroup $\langle d \rangle$ of $\mathbb{Z}_n$ has n/d elements, and contains all the positive integers m less than n such that $\gcd(m, n) = d$. Thus there is only one subgroup of $\mathbb{Z}_n$ of order n/d. Taken with the preceding paragraph, this shows at once that if a is a generator of the cyclic group G, then $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$. ◆

6.16 Example For an example using additive notation, consider $\mathbb{Z}_{12}$, with the generator $a = 1$. Since the greatest common divisor of 3 and 12 is 3, $3 = 3 \cdot 1$ generates a subgroup of $\frac{12}{3} = 4$ elements, namely

$$\langle 3 \rangle = \{0, 3, 6, 9\}.$$

Since the gcd of 8 and 12 is 4, 8 generates a subgroup of $\frac{12}{4} = 3$ elements, namely,

$$\langle 8 \rangle = \{0, 4, 8\}.$$

Since the gcd of 12 and 5 is 1, 5 generates a subgroup of $\frac{12}{1} = 12$ elements; that is, 5 is a generator of the whole group $\mathbb{Z}_{12}$. ▲

The following corollary follows immediately from Theorem 6.15.

6.17 Corollary If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.

6.18 Example Let us find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram. All subgroups are cyclic. By Corollary 6.17, the elements 1, 5, 7, 11, 13, and 17 are all generators of $\mathbb{Z}_{18}$. Starting with 2,

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}.$$

is of order 9 and has as generators elements of the form $h2$, where h is relatively prime to 9, namely, $h = 1, 2, 4, 5, 7$, and 8, so $h2 = 2, 4, 8, 10, 14$, and 16. The element 6 of $\langle 2 \rangle$ generates $\{0, 6, 12\}$, and 12 also is a generator of this subgroup.

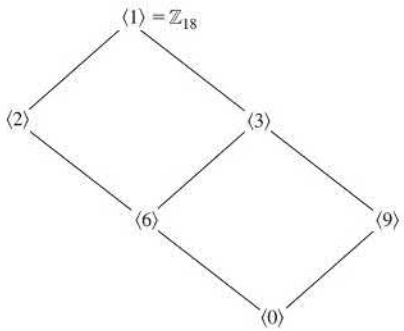
We have thus far found all subgroups generated by 0, 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, and 17. This leaves just 3, 9, and 15 to consider.

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\},$$

and 15 also generates this group of order 6, since $15 = 5 \cdot 3$, and the gcd of 5 and 6 is 1. Finally,

$$\langle 9 \rangle = \{0, 9\}.$$

The subgroup diagram for these subgroups of $\mathbb{Z}_{18}$ is given in Fig. 6.19.



6.19 Figure Subgroup diagram for $\mathbb{Z}_{18}$.

This example is straightforward; we are afraid we wrote it out in such detail that it may look complicated. The exercises give some practice along these lines. ▲

6.20 Corollary Let G be a finite cyclic group and $H \leq G$. Then $|H|$ divides $|G|$. That is, $|G|$ is a multiple of $|H|$.

Proof Let g be a generator for G and let $n = |G|$. By Theorem 6.6, H is cyclic, so there is an element in $h \in H$ such that h generates H. Since $h \in H \leq G$, $h = g^s$ for some s. Theorem 6.15 states that

$$|H| = \frac{n}{\gcd(n, s)}$$

which is a divisor of n. ◆

6.21 Example We find all orders of the subgroups of $\mathbb{Z}_{28}$. Factoring gives $28 = 2^2 \cdot 7$, so the possible orders of subgroups of the cyclic group $\mathbb{Z}_{28}$ are 1, 2, 4, 7, 14, and 28. We note that $|\langle 0 \rangle| = 1$, $|\langle 14 \rangle| = 2$, $|\langle 7 \rangle| = 4$, $|\langle 4 \rangle| = 7$, $|\langle 2 \rangle| = 14$, $|\langle 1 \rangle| = |\mathbb{Z}_{28}| = 28$. So there are subgroups of order 1, 2, 4, 7, 14, and 28. ▲

Actually, Corollary 6.20 can be strengthened considerably. The assumption that G is cyclic is completely unnecessary. As we will see in Section 10, Lagrange's Theorem states that for any finite group, the order of a subgroup divides the order of the group.

EXERCISES 6

Computations

In Exercises 1 through 4, find the quotient and remainder, according to the division algorithm, when n is divided by m.

1. $n = 42, m = 9$ **2.** $n = -42, m = 9$

3. $n = -37, m = 8$ **4.** $n = 37, m = 8$

In Exercises 5 through 7, find the greatest common divisor of the two integers.

5. 32 and 24 **6.** 48 and 88 **7.** 360 and 420

In Exercises 8 through 11, find the number of generators of a cyclic group having the given order.

8. 5 **9.** 8 **10.** 24 **11.** 84

An isomorphism of a group with itself is an **automorphism of the group.** In Exercises 12 through 16, find the number of automorphisms of the given group.
[*Hint:* You may use Exercise 53. What must be the image of a generator under an automorphism?]

12. $\mathbb{Z}_2$ **13.** $\mathbb{Z}_6$ **14.** $\mathbb{Z}_8$ **15.** $\mathbb{Z}$ **16.** $\mathbb{Z}_{84}$

In Exercises 17 through 23, find the number of elements in the indicated cyclic group.

17. The cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25

18. The cyclic subgroup of $\mathbb{Z}_{42}$ generated by 30

19. The cyclic subgroup $\langle i \rangle$ of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication

20. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $(1 + i)/\sqrt{2}$

21. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $1 + i$

22. The cyclic subgroup $\langle \rho^{10} \rangle$ of D_{24}

23. The cyclic subgoup $\langle \rho^{35} \rangle$ of D_{375}

24. Consider the group S_{10}

- **a.** What is the order of the cycle $(2, 4, 6, 7)$?
- **b.** What is the order of $(1, 4)(2, 3, 5)$? Of $(1, 3)(2, 4, 6, 7, 8)$?
- **c.** What is the order of $(1, 5, 9)(2, 6, 7)$? Of $(1, 3)(2, 5, 6, 8)$?
- **d.** What is the order of $(1, 2)(3, 4, 5, 6, 7, 8)$? Of $(1, 2, 3)(4, 5, 6, 7, 8, 9)$?
- **e.** State a theorem suggested by parts (c) and (d). [Hint: The important words you are looking for are *least common multiple*.]

In Exercises 25 through 30, find the maximum possibe order for an element of S_n for a given value of n.

25. $n = 5$ **26.** $n = 6$ **27.** $n = 7$

28. $n = 8$ **29.** $n = 10$ **30.** $n = 15$

In Exercises 31 through 33, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

31. $\mathbb{Z}_{12}$ **32.** $\mathbb{Z}_{36}$ **33.** $\mathbb{Z}_8$

In Exercises 34 through 38, find all orders of subgroups of the given group.

34. $\mathbb{Z}_6$ **35.** $\mathbb{Z}_8$ **36.** $\mathbb{Z}_{12}$ **37.** $\mathbb{Z}_{20}$ **38.** $\mathbb{Z}_{17}$

Concepts

In Exercises 39 and 40, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

39. An element a of a group G has *order* $n \in \mathbb{Z}^+$ if and only if $a^n = e$.

40. The *greatest common divisor* of two positive integers is the largest positive integer that divides both of them.

41. Determine whether each of the following is true or false.

a. Every cyclic group is abelian.
b. Every abelian group is cyclic.
c. $\mathbb{Q}$ under addition is a cyclic group.
d. Every element of every cyclic group generates the group.
e. There is at least one abelian group of every finite order >0.
f. Every group of order ≤ 4 is cyclic.
g. All generators of $\mathbb{Z}_{20}$ are prime numbers.
h. If G and G' are groups, then $G \cap G'$ is a group.
i. If H and K are subgroups of a group G, then $H \cap K$ is a group.
j. Every cyclic group of order >2 has at least two distinct generators.

In Exercises 42 through 46, either give an example of a group with the property described, or explain why no example exists.

42. A finite abelian group that is not cyclic

43. An infinite group that is not cyclic

44. A cyclic group having only one generator

45. An infinite cyclic group having four generators

46. A finite cyclic group having four generators

The generators of the cyclic multiplicative group U_n of all nth roots of unity in $\mathbb{C}$ are the **primitive** nth **roots of unity**. In Exercises 47 through 50, find the primitive nth roots of unity for the given value of n.

47. $n = 4$

48. $n = 6$

49. $n = 8$

50. $n = 12$

Proof Synopsis

51. Give a one-sentence synopsis of the proof of Theorem 6.1.

52. Give at most a three-sentence synopsis of the proof of Theorem 6.6.

Theory

53. Let G be a cyclic group with generator a, and let G' be a group isomorphic to G. If $\phi : G \to G'$ is an isomorphism, show that, for every $x \in G$, $\phi(x)$ is completely determined by the value $\phi(a)$. That is, if $\phi : G \to G'$ and $\psi : G \to G'$ are two isomophisms such that $\phi(a) = \psi(a)$, then $\phi(x) = \psi(x)$ for all $x \in G$.

54. Let r and s be integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

55. Prove that if G is a finite cyclic group, H and K are subgroups of G, and $H \neq K$, then $|H| \neq |K|$.

56. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

57. Let r and s be positive integers.

a. Define the **least common multiple** of r and s as a generator of a certain cyclic group.
b. Under what condition is the least common multiple of r and s their product, rs?
c. Generalizing part (b), show that the product of the greatest common divisor and of the least common multiple of r and s is rs.

58. Show that a group that has only a finite number of subgroups must be a finite group.

59. Show by a counterexample that the following "converse" of Theorem 6.6 is not a theorem: "If a group G is such that every proper subgroup is cyclic, then G is cyclic."

60. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Show that $ax = xa$ for all $x \in G$. [*Hint:* Consider $(xax^{-1})^2$.]

61. Prove that if G is a cyclic group with an odd number of generators, then G has two elements.

62. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

63. Let p be a prime number. Find the number of generators of the cyclic group $\mathbb{Z}_{p^r}$, where r is an integer ≥ 1.

64. Show that in a finite cyclic group G of order n, written multiplicatively, the equation $x^m = e$ has exactly m solutions x in G for each positive integer m that divides n.

65. With reference to Exercise 64, what is the situation if $1 < m < n$ and m does not divide n?

66. Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if p is a prime number.

67. Let G be an abelian group and let H and K be finite cyclic subgroups with $|H| = r$ and $|K| = s$.

a. Show that if r and s are relatively prime, then G contains a cyclic subgroup of order rs.

b. Generalizing part (a), show that G contains a cyclic subgroup of order the least common multiple of r and s.

SECTION 7 GENERATING SETS AND CAYLEY DIGRAPHS

Let G be a group, and let $a \in G$. We have described the cyclic subgroup $\langle a \rangle$ of G, which is the smallest subgroup of G that contains the element a. Suppose we want to find as small a subgroup as possible that contains both a and b for another element b in G. By Theorem 5.19, we see that any subgroup containing a and b must contain a^n and b^m for all $m, n \in \mathbb{Z}$, and consequently must contain all finite products of such powers of a and b. For example, such an expression might be $a^2b^4a^{-3}b^2a^5$. Note that we cannot "simplify" this expression by writing first all powers of a followed by the powers of b, since G may not be abelian. However, products of such expressions are again expressions of the same type. Furthermore, $e = a^0$ and the inverse of such an expression is again of the same type. For example, the inverse of $a^2b^4a^{-3}b^2a^5$ is $a^{-5}b^{-2}a^3b^{-4}a^{-2}$. By Theorem 5.12, this shows that all such products of integral powers of a and b form a subgroup of G, which surely must be the smallest subgroup containing both a and b. We call a and b **generators** of this subgroup. If this subgroup should be all of G, then we say that $\{a, b\}$ **generates** G. Of course, there is nothing sacred about taking just two elements $a, b \in G$. We could have made similar arguments for three, four, or any number of elements of G, as long as we take only finite products of their integral powers.

7.1 Example As we have seen, the dihedral group is generated by $\{\mu, \rho\}$ since every element in D_n can be written in the form ρ^k or $\mu\rho^k$ for $0 \leq k < n$. Also, $\{\mu, \mu\rho\}$ generates D_n since $\rho = \mu(\mu\rho)$, so any element in the dihedral group can also be written as a product of copies of μ and $\mu\rho$. It is interesting to note that both μ and $\mu\rho$ have order 2, while in the generating set $\{\mu, \rho\}$ one element has order 2, but the other has order n. ▲

7.2 Example The Klein 4-group $V = \{e, a, b, c\}$ of Example 5.7 is generated by $\{a, b\}$ since $ab = c$. It is also generated by $\{a, c\}$, $\{b, c\}$, and $\{a, b, c\}$. If a group G is generated by a subset S, then every subset of G containing S generates G. ▲

7.3 Example The group $\mathbb{Z}_6$ is generated by $\{1\}$ and $\{5\}$. It is also generated by $\{2, 3\}$ since $2 + 3 = 5$, so that any subgroup containing 2 and 3 must contain 5 and must therefore be $\mathbb{Z}_6$. It is also generated by $\{3, 4\}$, $\{2, 3, 4\}$, $\{1, 3\}$, and $\{3, 5\}$, but it is not generated by $\{2, 4\}$ since $\langle 2 \rangle = \{0, 2, 4\}$ contains 2 and 4. ▲

We have given an intuitive explanation of the subgroup of a group G generated by a subset of G. What follows is a detailed exposition of the same idea approached in another way, namely via intersections of subgroups. After we get an intuitive grasp of a concept, it is nice to try to write it up as neatly as possible. We give a set-theoretic definition and generalize a theorem that was in Exercise 61 of Section 5.

7.4 Definition Let $\{S_i \mid i \in I\}$ be a collection of sets. Here I may be any set of indices. The **intersection** $\cap_{i\in I} S_i$ **of the sets** S_i is the set of all elements that are in all the sets S_i; that is,

$$\bigcap_{i\in I} S_i = \{x \mid x \in S_i \text{ for all } i \in I\}.$$

If I is finite, $I = \{1, 2, \ldots, n\}$, we may denote $\cap_{i\in I} S_i$ by

$$S_1 \cap S_2 \cap \cdots \cap S_n.$$ ■

7.5 Theorem For any group G and any nonempty collection of subgroups $\{H_i \leq G \mid i \in I\}$, the intersection of all the subgroups H_i, $\cap_{i\in I} H_i$, is also a subgroup of G.

Proof Let us show closure. Let $a \in \cap_{i\in I} H_i$ and $b \in \cap_{i\in I} H_i$, so that $a \in H_i$ for all $i \in I$ and $b \in H_i$ for all $i \in I$. Then $ab \in H_i$ for all $i \in I$, since H_i is a group. Thus $ab \in \cap_{i\in I} H_i$.

Since H_i is a subgroup for all $i \in I$, we have $e \in H_i$ for all $i \in I$, and hence $e \in \cap_{i\in I} H_i$.

Finally, for $a \in \cap_{i\in I} H_i$, we have $a \in H_i$ for all $i \in I$, so $a^{-1} \in H_i$ for all $i \in I$, which implies that $a^{-1} \in \cap_{i\in I} H_i$. ◆

Let G be a group and let $a_i \in G$ for $i \in I$. There is at least one subgroup of G containing all the elements a_i for $i \in I$, namely G is itself. Theorem 7.5 assures us that if we take the intersection of all subgroups of G containing all a_i for $i \in I$, we will obtain a subgroup H of G. This subgroup H is the smallest subgroup of G containing all the a_i for $i \in I$.

7.6 Definition Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the **subgroup generated by** $\{a_i \mid i \in I\}$. If this subgroup is all of G, then $\{a_i \mid i \in I\}$ **generates** G and the a_i are **generators of** G. If there is a finite set $\{a_i \mid i \in I\}$ that generates G, then G is **finitely generated.** ■

Note that this definition is consistent with our previous definition of a generator for a cyclic group. Note also that the statement *a is a generator of G* may mean either that $G = \langle a \rangle$ or that a is a member of a subset of G that generates G. The context in which the statement is made should indicate which is intended. Our next theorem gives the structural insight into the subgroup of G generated by $\{a_i \mid i \in I\}$ that we discussed for two generators before Example 7.1.

7.7 Theorem If G is a group and $a_i \in G$ for $i \in I \neq \phi$, then the subgroup H of G generated by $\{a_i \mid i \in I\}$ has as elements precisely those elements of G that are finite products of integral powers of the a_i, where powers of a fixed a_i may occur several times in the product.

Proof Let K denote the set of all finite products of integral powers of the a_i. Then $K \subseteq H$. We need only observe that K is a subgroup and then, since H is the smallest subgroup containing a_i for $i \in I$, we will be done. Observe that a product of elements in K is again in K. Since $(a_i)^0 = e$, we have $e \in K$. For every element k in K, if we form from the product giving k a new product with the order of the a_i reversed and the opposite sign on all exponents, we have k^{-1}, which is thus in K. For example,

$$\left[(a_1)^3(a_2)^2(a_1)^{-7}\right]^{-1} = (a_1)^7(a_2)^{-2}(a_1)^{-3},$$

which is again in K. ◆

7.8 Example Recall that the dihedral group D_n consists of permutations of $\mathbb{Z}_n$ that map edges to edges in the regular n-gon P_n. In disjoint cycle notation, $\rho = (0, 1, 2, 3, \ldots, n-1)$ and $\mu = (1, n-1)(2, n-2)\cdots\left(\frac{n-1}{2}, \frac{n+1}{2}\right)$ if n is odd, and $\mu = (1, n-1)(2, n-2)\cdots\left(\frac{n-2}{2}, \frac{n+2}{2}\right)$ if n is even. Since $\mu^2 = \iota$ and $\rho^n = \iota$ any product of integer powers of μ and ρ can be rewritten to only have powers of 0 or 1 for μ and powers of $0, 1, 2, 3, \ldots n-1$ for ρ. Furthermore, the relation $\rho\mu = \mu\rho^{n-1}$ allows us to move all the powers of μ to the left and all the powers of ρ to the right, being careful to replace ρ with ρ^{n-1} each time we move a μ past a ρ. So in the case of $n = 6$,

$$\rho^8\mu^9 = \rho^2\mu = \rho\mu\rho^5 = \mu\rho^5\rho^5 = \mu\rho^4.$$

Thus the subgroup of $S_{\mathbb{Z}_n}$ generated by μ and ρ is the set

$$\{\iota, \rho, \rho^2, \ldots, \rho^{n-1}, \mu, \mu\rho, \mu\rho^2, \ldots, \mu\rho^{n-1}\}$$

which is the dihedral group. ▲

Cayley Digraphs

For each generating set S of a finite group G, there is a directed graph representing the group in terms of the generators in S. The term *directed graph* is usually abbreviated as *digraph*. These visual representations of groups were devised by Cayley, and are also referred to as *Cayley diagrams* in the literature.

Intuitively, a **digraph** consists of a finite number of points, called **vertices** of the digraph, and some **arcs** (each with a direction denoted by an arrowhead) joining vertices. In a digraph for a group G using a generating set S we have one vertex, represented by a dot, for each element of G. Each generator in S is denoted by one type of arc. We could use different colors for different arc types in pencil and paperwork. Since different colors are not available in our text, we use different style arcs, like solid, dashed, and dotted, to denote different generators. Thus if $S = \{a, b, c\}$ we might denote

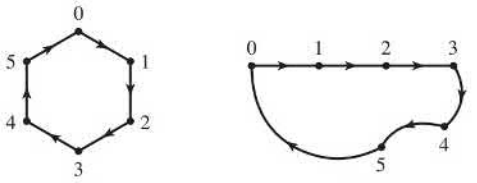
a by ——➤——, b by - - -➤- - -, and c by ·····➤·····.

With this notation, an occurrence of x •——➤——• y in a Cayley digraph means that $xa = y$. That is, traveling an arc in the direction of the arrow indicates that multiplication of the group element at the start of the arc *on the right* by the generator corresponding to that type of arc yields the group element at the end of the arc. Of course, since we are in a group, we know immediately that $ya^{-1} = x$. Thus traveling an arc in the direction opposite to the arrow corresponds to multiplication on the right by the inverse of the corresponding generator. If a generator in S is its own inverse, it is customary to denote this by omitting the arrowhead from the arc, rather than using a double arrow. For example, if $b^2 = e$, we might denote b by _ _ _ _ _ _ _ _.

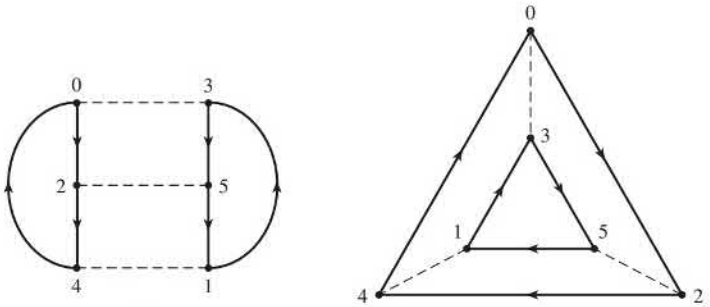
7.9 Example Both of the digraphs shown in Fig. 7.10 represent the group $\mathbb{Z}_6$ with generating set $S = \{1\}$. Neither the length and shape of an arc nor the angle between arcs has any significance. ▲

7.12 Example Both of the digraphs shown in Fig. 7.11 represent the group $\mathbb{Z}_6$ with generating set $S = \{2, 3\}$. Since 3 is its own inverse, there is no arrowhead on the dashed arcs representing 3. Notice how different these Cayley diagrams look from those in Fig. 7.10 for the same group. The difference is due to the different choice for the set of generators. ▲

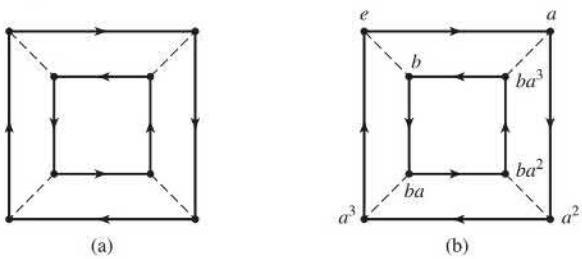
Every digraph for a group must satisfy these four properties for the reasons indicated.



7.10 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{1\}$ using $\xrightarrow[1]{}$.



7.11 Figure Two digraphs for $\mathbb{Z}_6$ with $S = \{2, 3\}$ using $\xrightarrow[2]{}$ and $\overset{3}{\text{- - - - - -}}$.



7.13 Figure

Property	***Reason***
1. The digraph is connected, that is, we can get from any vertex g to any vertex h by traveling along consecutive arcs, starting at g and ending at h.	Every equation $gx = h$ has a solution in a group.
2. At most one arc goes from a vertex g to a vertex h.	The solution of $gx = h$ is unique.
3. Each vertex g has exactly one arc of each type starting at g, and one of each type ending at g.	For $g \in G$ and each generator b we can compute gb, and $(gb^{-1})b = g$.
4. If two different sequences of arc types starting from vertex g lead to the same vertex h, then those same sequences of arc types starting from any vertex u will lead to the same vertex v.	If $gq = h$ and $gr = h$, then $uq = ug^{-1}h = ur$.

It can be shown that, conversely, every digraph satisfying these four properties is a Cayley digraph for some group. Due to the symmetry of such a digraph, we can choose labels like a, b, c for the various arc types, name any vertex e to represent the identity, and name each other vertex by a product of arc labels and their inverses that we can travel to attain that vertex starting from the one that we named e. Some finite groups were first constructed (found) using digraphs.

7.14 Example A digraph satisfying the four properties given above is shown in Fig. 7.13 (a). To obtain Fig. 7.13 (b), we selected the labels

$\xrightarrow[a]{}$ and $\underset{b}{\text{- - - - - - - -}}$,

named a vertex e, and then named the other vertices as shown. We have a group

$$\{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$$

of eight elements. From the diagram we could compute any product. For example, to compute ba^2ba^3 we start at the vertex labeled ba^2, follow a dotted edge, and then follow three solid edges to arrive at a. Note that the way we labeled the vertices is not unique. For example, the vertex labeled ba^3 could have been labeled ab simply by going along a different path starting at e. This says that $ab = ba^3$. We also see that $a^4 = e$ and $b^2 = e$. We hope that this example is starting to look familiar. In fact, Figure 7.13 is a Cayley digraph of the dihedral group D_4. We simply relabel a with ρ and b with μ! ▲

EXERCISES 7

Computations

In Exercises 1 through 8, list the elements of the subgroup generated by the given subset.

1. The subset $\{2, 3\}$ of $\mathbb{Z}_{12}$

2. The subset $\{4, 6\}$ of $\mathbb{Z}_{12}$

3. The subset $\{4, 6\}$ in $\mathbb{Z}_{25}$

4. The subset $\{12, 30\}$ of $\mathbb{Z}_{36}$

5. The subset $\{12, 42\}$ of $\mathbb{Z}$

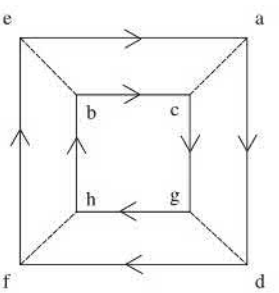
6. The subset $\{18, 24, 39\}$ of $\mathbb{Z}$

7. The subset $\{\mu, \mu\rho^2\}$ in D_8

8. The subset $\{\rho^8, \rho^{10}\}$ in D_{18}

9. Use the Cayley digraph in Figure 7.15 to compute these products. Note that the solid edges represent the generator a and the dashed lines represent b.

a. $(ba^2)a^3$ **b.** $(ba)(ba^3)$ **c.** $b(a^2b)$



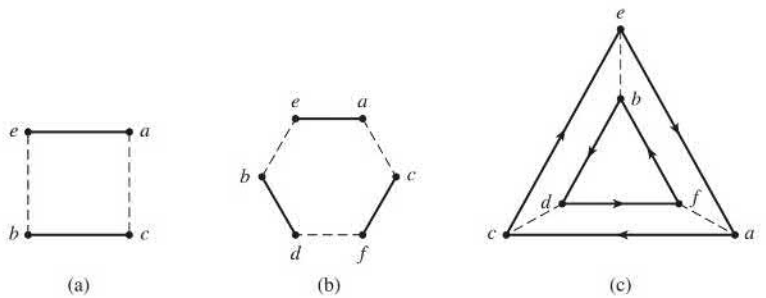
7.15 Figure

In Exercises 10 through 12, give the table for the group having the indicated digraph. In each digraph, take e as identity element. List the identity e first in your table, and list the remaining elements alphabetically, so that your answers will be easy to check.

10. The digraph in Fig. 7.16(a)

11. The digraph in Fig. 7.16(b)

12. The digraph in Fig. 7.16(c)



7.16 Figure

Concepts

13. How can we tell from a Cayley digraph whether or not the corresponding group is commutative?

14. Using the condition found in Exercise 13, show that the group corresponding to the Cayley digraph in Figure 7.13 is not commutative.

15. Is it obvious from a Cayley digraph of a group whether or not the group is cyclic? [*Hint:* Look at Fig. 7.9(b).]

16. The large outside triangle in Fig. 7.11(b) exhibits the cyclic subgroup {0, 2, 4} of $\mathbb{Z}_6$. Does the smaller inside triangle similarly exhibit a cyclic subgroup of $\mathbb{Z}_6$? Why or why not?

17. The generating set $S = \{1, 2\}$ for $\mathbb{Z}_6$ contains more generators than necessary, since 1 is a generator for the group. Nevertheless, we can draw a Cayley digraph for $\mathbb{Z}_6$ with this generating set S. Draw such a Cayley digraph.

18. Draw a Cayley digraph for $\mathbb{Z}_8$ with generating set $S = \{2, 5\}$.

19. A **relation** on a set S of generators of a group G is an equation that equates some product of generators and their inverses to the identity e of G. For example, if $S = \{a, b\}$ and G is commutative so that $ab = ba$, then one relation is $aba^{-1}b^{-1} = e$. If, moreover, b is its own inverse, then another relation is $b^2 = e$.

a. Explain how we can find some relations on S from a Cayley digraph of G.

b. Find three relations on the set $S = \{a, b\}$ of generators for the group described by Fig. 7.13(b).

20. Draw digraphs of the two possible structurally different groups of order 4, taking as small a generating set as possible in each case. You need not label vertices.

Theory

21. Use Cayley digraphs to show that for $n \geq 3$, there exists a nonabelian group with $2n$ elements that is generated by two elements of order 2.

22. Prove that there are at least three different abelian groups of order 8. [Hint: Find a Cayley digraph for a group of order 8 having one generator of order 4 and another of order 2. Find a second Cayley digraph for a group of order 8 having three generators each with order 2.]

This page is intentionally left blank

PART II

Structure of Groups

SECTION 8 GROUPS OF PERMUTATIONS

Let $\phi : G \to G'$ be a function mapping the group G to G'. Recall that the homomorphism property of an isomorphism states that for all $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$. Whenever a function has this property whether or not the function is one-to-one or onto, we say that ϕ is a **group homomorphism**. Of course any group isomorphism is a group homomorphism, but the reverse is not necessarily true.

8.1 Definition Let G and G' be groups with $\phi : G \to G'$. The map ϕ is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b)$$

holds for all $a, b \in G$. ■

8.2 Example Let $\phi : \mathbb{R} \to U$ (the circle group) be defined by the formula

$$\phi(x) = \cos(2\pi x) + i\sin(2\pi x) = e^{2\pi ix}.$$

Then

$$\phi(a+b) = \cos(2\pi(a+b)) + i\sin(2\pi(a+b)) = e^{2\pi i(a+b)}.$$

Using either the usual properties of the exponential function or the formulas from trigonometry involving the sum of two angles, we see that

$$\phi(a+b) = (\cos(2\pi a) + i\sin(2\pi a))(\cos(2\pi b) + i\sin(2\pi b)) = e^{2\pi ai}e^{2\pi bi},$$

so

$$\phi(a+b) = \phi(a)\phi(b),$$

which says that ϕ is a group homomorphism. Although ϕ maps onto U, it is not one-to-one, so ϕ is not an isomorphism.

The identity $0 \in \mathbb{R}$ maps to 1, the identity in U. Furthermore, for any $x \in \mathbb{R}$,

$$\phi(-x) = e^{-2\pi ix} = \frac{1}{e^{2\pi ix}} = (\phi(x))^{-1}.$$

▲

8.3 Example Recall that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Let $\phi : U_{28} \to U_4$ be given by $\phi(z) = z^7$. To check that ϕ is well defined, we see that if $z \in U_{28}$, then $z^{28} = 1$. Therefore, $(z^7)^4 = 1$, which implies that $z^7 \in U_4$. We check that ϕ is a homomorphism.

$$\phi(z_1 z_2) = (z_1 z_2)^7 = z_1^7 z_2^7 = \phi(z_1)\phi(z_2).$$

As in the previous example, ϕ maps the identity in U_{28}, in this case 1, to the identity 1 in U_4. Furthermore,

$$\phi(z^{-1}) = z^{-7} = (z^7)^{-1} = (\phi(z))^{-1}.$$ ▲

8.4 Definition Let $\phi : X \to Y$ and suppose that $A \subseteq X$ and $B \subseteq Y$. The set $\phi[A] = \{\phi(a) \mid a \in A\}$ is called the **image of A in Y under the mapping ϕ.** The set $\phi^{-1}[B] = \{a \in A \mid \phi(a) \in B\}$ is called the **inverse image of B under the mapping ϕ.** ■

The four properties of a homomorphism given in the theorem that follows are obvious in the case of an isomorphism since we think of an isomorphism as simply relabeling the elements of a group. However, it is not obvious that these properties hold for all homomorphisms whether or not they are one-to-one or onto maps. Consequently, we give careful proofs of all four properties.

8.5 Theorem Let ϕ be a homomorphism of a group G into a group G'.

1. If e is the identity element in G, then $\phi(e)$ is the identity element e' in G'.
2. If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$.
3. If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
4. If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Loosely speaking, ϕ preserves the identity element, inverses, and subgroups.

Proof Let ϕ be a homomorphism of G into G'. Then

$$\phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Multiplying on the left by $\phi(e)^{-1}$, we see that $e' = \phi(e)$. Thus $\phi(e)$ must be the identity element e' in G'. The equation

$$e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$$

shows that $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.

Turning to Statement (3), let H be a subgroup of G, and let $\phi(a)$ and $\phi(b)$ be any two elements in $\phi[H]$. Then $\phi(a)\phi(b) = \phi(ab)$, so we see that $\phi(a)\phi(b) \in \phi[H]$; thus, $\phi[H]$ is closed under the operation of G'. The fact that $e' = \phi(e)$ and $\phi(a^{-1}) = \phi(a)^{-1}$ completes the proof that $\phi[H]$ is a subgroup of G'.

Going the other way for Statement (4), let K' be a subgroup of G'. Suppose a and b are in $\phi^{-1}[K']$. Then $\phi(a)\phi(b) \in K'$ since K' is a subgroup. The equation $\phi(ab) = \phi(a)\phi(b)$ shows that $ab \in \phi^{-1}[K']$. Thus $\phi^{-1}[K']$ is closed under the binary operation in G. Also, K' must contain the identity element $e' = \phi(e)$, so $e \in \phi^{-1}[K']$. If $a \in \phi^{-1}[K']$, then $\phi(a) \in K'$, so $\phi(a)^{-1} \in K'$. But $\phi(a)^{-1} = \phi(a^{-1})$, so we must have $a^{-1} \in \phi^{-1}[K']$. Hence $\phi^{-1}[K']$ is a subgroup of G. ◆

Let $\phi : G \to G'$ be a homomorphism and let e' be the identity element of G'. Now $\{e'\}$ is a subgroup of G', so $\phi^{-1}[\{e'\}]$ is a subgroup H of G by Statement (4) in Theorem 8.5. This subgroup is critical to the study of homomorphisms.

8.6 Definition Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[\{e'\}] = \{x \in G \mid \phi(x) = e'\}$ is the **kernel of ϕ**, denoted by $\text{Ker}(\phi)$. ■

We will use the kernel of a homomorphism when we define the alternating group later in this section.

Another extreme is to let $H = G$ in Statement (3) of Theorem 8.5. In this case, the theorem says that $\phi[G]$ is a subgroup of G'. We use this in the proof of Cayley's Theorem.

8.7 Example In Example 8.2, the homomorphism $\phi : \mathbb{R} \to U$ is defined by $\phi(x) = \cos(2\pi x) + i\sin(2\pi x) = e^{2\pi ix}$. The kernel of ϕ is the set of integers since $\cos(2\pi x) + i\sin(2\pi x) = 1$ if and only if x is an integer.

Let n be a positive integer. Then $\left\langle \frac{1}{n} \right\rangle$ is a subgroup of $\mathbb{R}$ and

$$\begin{aligned}\phi\left[\left\langle \frac{1}{n} \right\rangle\right] &= \phi\left[\left\{ \frac{m}{n} \mid m \in \mathbb{Z} \right\}\right] \\ &= \{\cos(2\pi m/n + i\sin(2\pi m/n)) \mid m \in \mathbb{Z}\} \\ &= U_n.\end{aligned}$$

▲

8.8 Example Let $\phi : \mathbb{Z}_n \to D_n$ be given by $\phi(k) = \rho^k$. We check that ϕ is a homomorphism. Let $a, b \in \mathbb{Z}_n$. If $a + b < n$, then $a +_n b = a + b$, so $\phi(a +_n b) = \phi(a + b) = \rho^{a+b} = \rho^a\rho^b = \phi(a)\phi(b)$. If $a + b \geq n$, then $\phi(a +_n b) = \phi(a + b - n) = \rho^{a+b-n} = \rho^a\rho^b\rho^{-n} = \rho^a\rho^b = \phi(a)\phi(b)$. The image $\phi[\mathbb{Z}_n]$ is $\langle\rho\rangle$. ▲

Cayley's Theorem

Each of the groups we have seen so far is isomorphic to a subgroup of permutations on some set. For example, $\mathbb{Z}_n$ is isomorphic with the cyclic group $\langle(1, 2, 3, \ldots, n)\rangle \leq S_n$. The dihedral group D_n is defined to be the permutations in $S_{\mathbb{Z}_n}$ with the property that the line segment between vertices i and j is an edge in P_n, a regular n-gon, if and only if the line segment between the images of i and j is also an edge. The infinite group $\mathrm{GL}(n, \mathbb{R})$ can be thought of as invertible linear transformations of $\mathbb{R}^n$. Each element of $\mathrm{GL}(n, \mathbb{R})$ permutes the vectors in $\mathbb{R}^n$, which makes $\mathrm{GL}(n, \mathbb{R})$ isomorphic with a permutation group on vectors in $\mathbb{R}^n$. We refer to a subgroup of a permutation group as a **group of permutations**. Cayley's Theorem states that any group is isomorphic with a group of permutations.

At first Cayley's Theorem seems like a remarkable result that could be used to understand all groups. In fact, this is a nice and intriguing classic result. Unfortunately, approaching group theory by trying to determine all possible permutation groups is not feasible. On the other hand, Cayley's theorem does show the strength and generality of permutation groups and it deserves a special place in group theory for that reason. For example, if we wish to find a counterexample to a conjecture about groups, provided that there is one, it will occur in a permutation group.

It may seem a mystery how we could start with an arbitrary group and come up with a permutation group that is isomorphic with the given group. The key is to think about the group table. Each row contains each element of the group exactly once. So each row defines a permutation of the elements of the group by placing the table head as the top row in the two-row representation of a permutation and placing the row corresponding to an element a in the group as the bottom row. Table 8.9 is the group table for D_3. Note that the permutation obtained using the row $\mu\rho$ is

$$\begin{pmatrix} \iota & \rho & \rho^2 & \mu & \mu\rho & \mu\rho^2 \\ \mu\rho & \mu\rho^2 & \mu & \rho^2 & \iota & \rho \end{pmatrix}.$$

8.9 Table

D_3	ι	ρ	ρ^2	μ	$\mu\rho$	$\mu\rho^2$
ι	ι	ρ	ρ^2	μ	$\mu\rho$	$\mu\rho^2$
ρ	ρ	ρ^2	ι	$\mu\rho^2$	μ	$\mu\rho$
ρ^2	ρ^2	ι	ρ	$\mu\rho$	$\mu\rho^2$	μ
μ	μ	$\mu\rho$	$\mu\rho^2$	ι	ρ	ρ^2
$\mu\rho$	$\mu\rho$	$\mu\rho^2$	μ	ρ^2	ι	ρ
$\mu\rho^2$	$\mu\rho^2$	μ	$\mu\rho$	ρ	ρ^2	ι

All that remains to prove Cayley's Theorem, at least when the group is finite, is to check that the permutations obtained from the group table form a group isomorphism with the original group. Let λ_x be the permutation of the elements of G given by the x row of the table for G. Then for any $g \in G$, $\lambda_x(g)$ is the entry in the x row and g column of the group table. In other words, $\lambda_x(g) = xg$, which is perfectly valid in the case of an infinite as well as a finite group. We formalize this connection between G and permutations on G in Definition 8.10.

8.10 Definition Let G be a group. The function $\phi : G \to S_G$ given by $\phi(x) = \lambda_x$ where $\lambda_x(g) = xg$ for all $g \in G$ is called the **left regular representation** of G. ■

In order to be sure that λ_x is a permutation, it should be verified that λ_x is both one-to-one and onto. We see that λ_x is one-to-one since if $\lambda_x(a) = \lambda_x(b)$, $xa = xb$ and cancellation gives $a = b$. Also, λ_x maps onto G because for any $b \in G$, $\lambda_x(x^{-1}b)) = b$. We are now ready to prove Cayley's Theorem.

8.11 Theorem **(Cayley's Theorem)** Every group is isomorphic to a group of permutations.

Proof Let G be a group. The left regular representation provides a map $\phi : G \to S_G$ defined by $\phi(x) = \lambda_x$. We must verify that ϕ is a group homomorphism and that ϕ is one-to-one. Then $\phi[G]$ is a subgroup of S_G by Theorem 8.5 and $\phi : G \to \phi[G]$ is an isomorphism.

We first show that ϕ is one-to-one. Suppose that $a, b \in G$ and $\phi(a) = \phi(b)$. Then the permutations λ_a and λ_b are the same, so $\lambda_a(e) = \lambda_b(e)$. Thus $ae = be$ and $a = b$. So ϕ is one-to-one.

We now need to show that ϕ is a group homomorphism. Let $a, b \in G$. Then $\phi(ab) = \lambda_{ab}$ and $\phi_a\phi_b = \lambda_a\lambda_b$. We must show that the two permutations λ_{ab} and $\lambda_a\lambda_b$ are the same. Let $g \in G$.

$$\lambda_{ab}(g) = (ab)g = a(bg) = \lambda_a(bg) = \lambda_a(\lambda_b(g)) = (\lambda_a\lambda_b)(g).$$

Thus $\lambda_{ab} = \lambda_a\lambda_b$, which implies that $\phi(ab) = \phi(a)\phi(b)$. So ϕ is a one-to-one homomorphism, which completes the proof. ◆

8.12 Example The proof of Cayley's Theorem shows that any group G is isomorphic with a subgroup of S_G, but this is typically not the smallest symmetric group that has a subgroup isomorphic with G. For example, D_n is isomorphic with a subgroup of $S_{\mathbb{Z}_n}$ while the proof of Cayley's Theorem gives a subgroup of S_{D_n} and D_n has $2n$ elements while $\mathbb{Z}_n$ has only n elements. On the surface, it may seem that $\mathbb{Z}_6$ cannot be isomorphic with a subgroup of S_n for $n < 6$, but $(1, 2, 3)(4, 5) \in S_5$ generates a subgroup isomorphic with $\mathbb{Z}_6$. ▲

We defined the left regular representation in Definition 8.10. We now define the right regular representation. Instead of λ_x representing the row for x in the group table, we use σ_x to represent the column with head x. Instead of using ϕ for the function that sends x to λ_x, we use τ, which sends x to $\sigma_{x^{-1}}$.

HISTORICAL NOTE

Arthur Cayley (1821–1895) gave an abstract-sounding definition of a group in a paper of 1854: "A set of symbols, $1, \alpha, \beta, \cdots$, all of them different and such that the product of any two of them (no matter in what order) or the product of any one of them into itself, belongs to the set, is said to be a group." He then proceeded to define a group table and note that every line and column of the table "will contain all the symbols $1, \alpha, \beta, \cdots$." Cayley's symbols, however, always represented operations on sets; it does not seem that he was aware of any other kind of group. He noted, for instance, that the four matrix operations $1, \alpha =$ inversion, $\beta =$ transposition, and $\gamma = \alpha\beta$, form, abstractly, the non-cyclic group of four elements. In any case, his definition went unnoticed for a quarter of a century.

This paper of 1854 was one of about 300 written during the 14 years Cayley was practicing law, being unable to find a suitable teaching post. In 1863, he finally became a professor at Cambridge. In 1878, he returned to the theory of groups by publishing four papers, in one of which he stated Theorem 8.11 of this text; his "proof" was simply to notice from the group table that multiplication by any group element permuted the group elements. However, he wrote, "this does not in any wise show that the best or the easiest mode of treating the general problem [of finding all groups of a given order] is thus to regard it as a problem of [permutations]. It seems clear that the better course is to consider the general problem in itself."

The papers of 1878, unlike the earlier one, found a receptive audience; in fact, they were an important influence on Walther von Dyck's 1882 axiomatic definition of an abstract group, the definition that led to the development of abstract group theory.

8.13 Definition Let G be a group. The map $\tau : G \to S_G$ given by $\tau(x) = \sigma_{x^{-1}}$ where $\sigma_x(g) = gx$ is called the **right regular representation** of G. ■

We could have used the right regular representation to prove Cayley's Theorem instead of the left regular representation. Exercise 54 asks for the details of the proof.

Even and Odd Permutations

It seems reasonable that every reordering of the sequence $1, 2, \ldots, n$ can be achieved by repeated interchange of positions of pairs of numbers. We discuss this a bit more formally.

8.14 Definition A cycle of length 2 is a **transposition**. ■

Thus a transposition leaves all elements but two fixed, and maps each of these onto the other. A computation shows that

$$(a_1, a_2, \cdots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2).$$

Therefore any cycle of length n can be written as a product of $n - 1$ transpositions. Since any permutation of a finite set can be written as a product of cycles, we have the following.

8.15 Theorem Any permutation of a finite set containing at least two elements is a product of transpositions. ♦

Naively, this theorem just states that any rearrangement of n objects can be achieved by successively interchanging pairs of them.

8.16 Example Following the remarks prior to the theorem, we see that (1, 6) (2, 5, 3) is the product (1, 6) (2, 3) (2, 5) of transpositions. ▲

8.17 Example In S_n for $n \geq 2$, the identity permutation is the product (1, 2) (1, 2) of transpositions. ▲

We have seen that every permutation of a finite set with at least two elements is a product of transpositions. The transpositions may not be disjoint, and a representation of the permutation in this way is not unique. For example, we can always insert at the beginning the transposition (1, 2) twice, because (1, 2) (1, 2) is the identity permutation. What is true is that the number of transpositions used to represent a given permutation must either always be even or always be odd. This is an important fact. The proof involves counting orbits and was suggested by David M. Bloom.

Let $\sigma \in S_A$ and $a \in A$. We let the **orbit** of a be the set $\{\sigma^k(a) \mid k \in \mathbb{Z}\}$. In the case of $\sigma \in S_n$, a simple way to think of the orbit of a is to think of the elements in the cycle containing a in the disjoint cycle representation of σ.

8.18 Example Let $\sigma = (1,2,6)(3,5) \in S_6$. Then the orbit of 1 is the set $\{1,2,6\}$, which is also the orbit of 2 and the orbit of 6. The set $\{3,5\}$ is the orbit of 3 and the orbit of 5. What about the orbit of 4? Recall that if we include 1-cycles, $\sigma = (1,2,6)(3,5)(4)$, which says the orbit of 4 is $\{4\}$. ▲

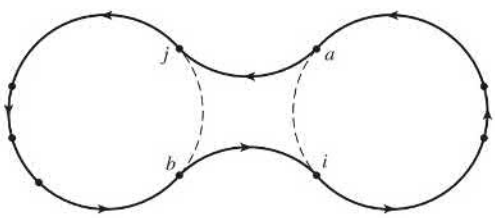
8.19 Theorem No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof Let $\sigma \in S_n$ and let $\tau = (i,j)$ be a transposition in S_n. We claim that the number of orbits of σ and of $\tau\sigma$ differ by 1.

Case I Suppose i and j are in different orbits of σ. Write σ as a product of disjoint cycles, the first of which contains j and the second of which contains i, symbolized by the two circles in Fig. 8.20. We may write the product of these two cycles symbolically as

$$(b,j,\times,\times,\times)(a,i,\times,\times)$$

where the symbols $\times$ denote possible other elements in these orbits.



8.20 Figure

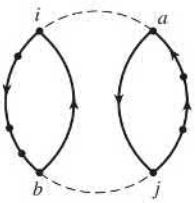
Computing the product of the first three cycles in $\tau\sigma = (i,j)\sigma$, we obtain

$$(i,j)(b,j,\times,\times,\times)(a,i,\times,\times) = (a,j,\times,\times,\times,b,i,\times,\times).$$

The original 2 orbits have been joined to form just one in $\tau\sigma$ as symbolized in Fig. 8.20. Exercise 42 asks us to repeat the computation to show that the same thing happens if either one or both of i and j should be the only element of their orbit in σ.

Case II Suppose i and j are in the same orbit of σ. We can then write σ as a product of disjoint cycles with the first cycle of the form

$$(a,i,\times,\times,\times,b,j,\times,\times)$$



8.21 Figure

shown symbolically by the circle in Fig. 8.20. Computing the product of the first two cycles in $\tau\sigma = (i,j)\sigma$, we obtain

$$(i,j)(a,i,\times,\times,\times,b,j,\times,\times) = (a,j,\times,\times)(b,i,\times,\times,\times).$$

The original single orbit has been split into two as symbolized in Fig. 8.21.

We have shown that the number of orbits of $\tau\sigma$ differs from the number of orbits of σ by 1. The identity permutation ι has n orbits, because each element is the only member of its orbit. Now the number of orbits of a given permutation $\sigma \in S_n$ differs from n by either an even or an odd number, but not both. Thus it is impossible to write

$$\sigma = \tau_1\tau_2\tau_3\cdots\tau_m\iota$$

where the τ_k are transpositions in two ways, once with m even and once with m odd. ◆

8.22 Definition A permutation of a finite set is **even** or **odd** according to whether it can be expressed as a product of an even number of transpositions or the product of an odd number of transpositions, respectively. ■

8.23 Example The identity permutation ι in S_n is an even permutation since we have $\iota = (1,2)(1,2)$. If $n = 1$ so that we cannot form this product, we define ι to be even. On the other hand, the permutation (1, 4, 5, 6) (2, 1, 5) in S_6 can be written as

$$(1,4,5,6)(2,1,5) = (1,6)(1,5)(1,4)(2,5)(2,1)$$

which has five transpositions, so this is an odd permutation. ▲

The Alternating Groups

We claim that for $n \geq 2$, the number of even permutations in S_n is the same as the number of odd permutations; that is, S_n is split equally and both numbers are $(n!)/2$. To show this, let A_n be the set of even permutations in S_n and let B_n be the set of odd permutations for $n \geq 2$. We proceed to define a one-to-one function from A_n onto B_n. This is exactly what is needed to show that A_n and B_n have the same number of elements.

Let τ be any fixed transposition in S_n; it exists since $n \geq 2$. We may as well suppose that $\tau = (1,2)$. We define a function

$$\lambda_\tau : A_n \to B_n$$

by

$$\lambda_\tau(\sigma) = \tau\sigma,$$

that is, $\sigma \in A_n$ is mapped into $(1,2)\sigma$ by λ_τ. Observe that since σ is even, the permutation $(1,2)\sigma$ can be expressed as a product of a (1 + even number), or odd number, of transpositions, so $(1,2)\sigma$ is indeed in B_n. If for σ and μ in A_n it is true that $\lambda_\tau(\sigma) = \lambda_\tau(\mu)$, then

$$(1,2)\sigma = (1,2)\mu,$$

and since S_n is a group, we have $\sigma = \mu$. Thus λ_τ is a one-to-one function. Finally,

$$\tau = (1,2) = \tau^{-1},$$

so if $\rho \in B_n$, then

$$\tau^{-1}\rho \in A_n,$$

and

$$\lambda_\tau(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho.$$

Thus λ_τ maps onto B_n. Hence the number of elements in A_n is the same as the number in B_n since there is a one-to-one correspondence between the elements of the sets.

Note that the product of two even permutations is again even. Also since $n \geq 2$, S_n has the transposition $(1, 2)$ and $\iota = (1, 2)(1, 2)$ is an even permutation. Finally, note that if σ is expressed as a product of transpositions, the product of the same transpositions taken in just the opposite order is σ^{-1}. Thus if σ is an even permutation, σ^{-1} must also be even. Referring to Theorem 5.12, we see that we have proved the following statement.

8.24 Theorem If $n \geq 2$, then the collection of all even permutations of $\{1, 2, 3, \cdots, n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n.

We can define a function called the **sign of a permutation**, $\text{sgn} : S_n \to \{1, -1\}$ by the formula

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

Thinking of $\{1, -1\}$ as a group under multiplication, it is easy to see that sgn is a homomorphism. Since 1 is the identity in the group $\{1, -1\}$, $\text{Ker}(\text{sgn}) = \text{sgn}^{-1}[\{1\}]$ is a subgroup of S_n consisting of all the even permutations. The homomorphism sgn is used in the standard way of defining the determinant of a square matrix. Exercise 52 asks you to prove some of the standard facts about determinants using this definition.

8.25 Definition The subgroup of S_n consisting of the even permutations of n letters is the **alternating group A_n on n letters**. ■

Both S_n and A_n are very important groups. Cayley's theorem shows that every finite group G is structurally identical to some subgroup of S_n for $n = |G|$. It can be shown that there are no formulas involving just radicals for solution of polynomial equations of degree n for $n \geq 5$. This fact is actually due to the structure of A_n, surprising as that may seem!

■ EXERCISES 8

Computations

In Exercises 1 through 10 determine whether the given map is a group homomorphism. [Hint: To verify that a map is a homomorphism, you must check the homomorphism property. To check that a map is not a homomorphism you could either find a and b such that $\phi(ab) \neq \phi(a)\phi(b)$, or else you could determine that any of the properties in Theorem 8.5 fail.]

1. Let $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder when x is divided by 2.
2. Let $\phi : \mathbb{Z}_9 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder when x is divided by 2.
3. Let $\phi : \mathbb{Q}^* \to \mathbb{Q}^*$ be given by $\phi(x) = |x|$.
4. Let $\phi : \mathbb{R} \to \mathbb{R}^+$ be given by $\phi(x) = 2^x$.
5. Let $\phi : D_4 \to \mathbb{Z}_4$ be given by $\phi(\rho^i) = \phi(\mu\rho^i) = i$ for $0 \leq i \leq 3$.

6. Let F be the additive group of all functions mapping $\mathbb{R}$ to $\mathbb{R}$. Let $\phi : F \to F$ be given by $\phi(f) = g$ where $g(x) = f(x) + x$.

7. Let F be as in Exercise 6 and $\phi : F \to F$ be defined by $\phi(f) = 5f$.

8. Let F be the additive group of all continuous functions mapping $\mathbb{R}$ to $\mathbb{R}$. Let $\phi : F \to \mathbb{R}$ be defined by $\phi(g) = \int_0^1 g(x)\,dx$.

9. Let M_n be the additive group of $n \times n$ matrices with real entries. Let $\phi : M_n \to \mathbb{R}$ be given by $\phi(A) = \det(A)$, the determinant of A.

10. Let M_n be as in Exercise 9 and $\phi : M_n \to \mathbb{R}$ be defined by $\phi(A) = \text{tr}(A)$ where $\text{tr}(A)$ is the trace of A, which is the sum of the entries on the diagonal.

In Exercises 11 through 16, compute the kernel for the given homomorphism ϕ.

11. $\phi : \mathbb{Z} \to \mathbb{Z}_8$ such that $\phi(1) = 6$.

12. $\phi : \mathbb{Z} \to \mathbb{Z}$ such that $\phi(1) = 12$.

13. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 3$ and $\phi(0, 1) = -5$.

14. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 6$ and $\phi(0, 1) = 9$.

15. $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(1, 0) = (2, 5)$ and $\phi(0, 1) = (-3, 2)$.

16. Let D be the additive group of all differentiable functions mapping $\mathbb{R}$ to $\mathbb{R}$ and F the additive group of all functions from $\mathbb{R}$ to $\mathbb{R}$. $\phi : D \to F$ is given by $\phi(f) = f'$, the derivative of f.

In Exercises 17 through 22, find all orbits of the given permutation.

17. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}$

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

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

20. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n + 1$

21. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n + 2$

22. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n - 3$

In Exercises 23 through 25, express the permutation of {1, 2, 3, 4, 5, 6, 7, 8} as a product of disjoint cycles, and then as a product of transpositions.

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

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

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

26. Figure 8.26 shows a Cayley digraph for the alternating group A_4 using the generating set $S = \{(1, 2, 3), (1, 2)(3, 4)\}$. Continue labeling the other nine vertices with the elements of A_4, expressed as a product of disjoint cycles.

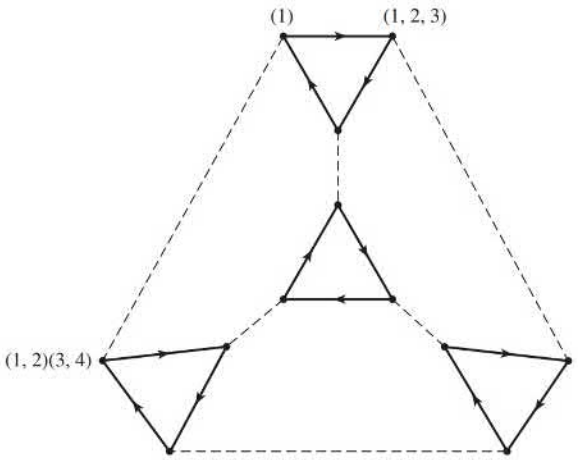
Concepts

In Exercises 27 through 29, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

27. For a permutation σ of a set A, an *orbit* of σ is a nonempty minimal subset of A that is mapped onto itself by σ.

28. The left regular representation of a group G is the map of G into S_G whose value at $g \in G$ is the permutation of G that carries each $x \in G$ into gx.

29. The *alternating group* is the group of all even permutations.



8.26 Figure

30. Before the proof of Cayley's Theorem, it is shown that λ_x is one-to-one. In the proof, one-to-one is shown again. Is it necessary to show one-to-one twice? Explain.

31. Determine whether each of the following is true or false.

a. Every permutation is a cycle.
b. Every cycle is a permutation.
c. The definition of even and odd permutations could have been given equally well before Theorem 8.19.
d. Every nontrivial subgroup H of S_9 containing some odd permutation contains a transposition.
e. A_5 has 120 elements.
f. S_n is not cyclic for any $n \geq 1$.
g. A_3 is a commutative group.
h. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 8 fixed.
i. S_7 is isomorphic to the subgroup of all those elements of S_8 that leave the number 5 fixed.
j. The odd permutations in S_8 form a subgroup of S_8.
k. Every group G is isomorphic with a subgroup of S_G.

32. The dihedral group is defined to be permutations with certain properties. Use the usual notation involving μ and ρ for elements in D_n.

a. Identify which elements in D_3 are even. Do the even elements form a cyclic group?
b. Identify which of elements of D_4 are even. Do the even elements form a cyclic group?
c. For which values of n do the even permutations of D_n form a cyclic group?

Proof Synopsis

33. Give a two-sentence synopsis of the proof of Cayley's Theorem.

34. Give a two-sentence synopsis of the proof of Theorem 8.19.

Theory

35. Suppose that $\phi : G \to G'$ is a group homomorphism and $a \in \text{Ker}\phi$. Show that for any $g \in G$, $gag^{-1} \in \text{Ker}\phi$.

36. Prove that a homomorphism $\phi : G \to G'$ is one-to-one if and only if $\text{Ker}(\phi)$ is the trivial subgroup of G.

37. Let $\phi : G \to G'$ be a group homomorphism. Show that $\phi(a) = \phi(b)$ if and only if $a^{-1}b \in \text{Ker}\phi$.

38. Use Exercise 37 to prove that if $\phi : G \to G'$ is a group homomorphism mapping onto G' and G is a finite group, then for any $b, c \in G'$, $|\phi^{-1}[\{b\}]| = |\phi^{-1}[\{c\}]|$. Conclude that if $|G|$ is a prime number, then either ϕ is an isomorphism or else G' is the trivial group.

39. Show that if $\phi : G \to G'$ and $\gamma : G' \to G''$ are group homomorphisms, then $\gamma \circ \phi : G \to G''$ is also a group homomorphism.

40. Let $\phi : G \to G'$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$ for all $x, y \in G$.

41. Prove the following about S_n if $n \geq 3$.

a. Every permutation in S_n can be written as a product of at most $n - 1$ transpositions.

b. Every permutation in S_n that is not a cycle can be written as a product of at most $n - 2$ transpositions.

c. Every odd permutation in S_n can be written as a product of $2n + 3$ transpositions, and every even permutation as a product of $2n + 8$ transpositions.

42. **a.** Draw a figure like Fig. 8.20 to illustrate that if i and j are in different orbits of σ and $\sigma(i) = i$, then the number of orbits of $(i, j)\sigma$ is one less than the number of orbits of σ.

b. Repeat part (a) if $\sigma(j) = j$ also.

43. Show that for every subgroup H of S_n for $n \geq 2$, either all the permutations in H are even or exactly half of them are even.

44. Let σ be a permutation of a set A. We shall say "σ **moves** $a \in A$" if $\sigma(a) \neq a$. If A is a finite set, how many elements are moved by a cycle $\sigma \in S_A$ of length n?

45. Let A be an infinite set. Let H be the set of all $\sigma \in S_A$ such that the number of elements moved by σ (see Exercise 44) is finite. Show that H is a subgroup of S_A.

46. Let A be an infinite set. Let K be the set of all $\sigma \in S_A$ that move (see Exercise 44) at most 50 elements of A. Is K a subgroup of S_A? Why?

47. Consider S_n for a fixed $n \geq 2$ and let σ be a fixed odd permutation. Show that every odd permutation in S_n is a product of σ and some permutation in A_n.

48. Show that if σ is a cycle of odd length, then σ^2 is a cycle.

49. Following the line of thought opened by Exercise 48, complete the following with a condition involving n and r so that the resulting statement is a theorem:

If σ is a cycle of length n, then σ^r is also a cycle if and only if . . .

50. Show that S_n is generated by $\{(1, 2), (1, 2, 3, \cdots, n)\}$. [*Hint:* Show that as r varies, $(1, 2, 3, \cdots, n)^r(1, 2)(1, 2, 3, \cdots, n)^{n-r}$ gives all the transpositions $(1, 2), (2, 3), (3, 4), \cdots, (n - 1, n), (n, 1)$. Then show that any transposition is a product of some of these transpositions and use Theorem 8.15.]

51. Let $\sigma \in S_n$ and define a relation on $\{1, 2, 3, \ldots, n\}$ by $i \sim j$ if and only if $j = \sigma^k(i)$ for some $k \in \mathbb{Z}$.

1. Prove that $\sim$ is an equivalence relation.

2. Prove that for any $1 \leq i \leq n$, the equivalence class of i is the orbit of i.

52. The usual definition for the determinant of an $n \times n$ matrix $A = (a_{i,j})$ is

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} a_{3,\sigma(3)} \cdots a_{n,\sigma(n)}$$

where $\text{sgn}(\sigma)$ is the sign of σ. Using this definition, prove the following properties of determinants.

a. If a row of matrix A has all zero entries, then $\det(A) = 0$.

b. If two different rows of A are switched to obtain B, then $\det(B) = -\det(A)$.

c. If r times one row of A is added to another row of A to obtain a matrix B, then $\det(A) = \det(B)$

d. If a row of A is multiplied by r to obtain the matrix B, then $\det(B) = r \det(A)$.

53. Prove that any finite group G is isomorphic with a subgroup of $\text{GL}(n, \mathbb{R})$ for some n. [Hint: For each $\sigma \in S_n$, find a matrix in $\text{GL}(n, \mathbb{R})$ that sends each basis vector e_i to $e_{\sigma(i)}$. Use this to show that S_n is isomorphic with a subgroup of $\text{GL}(n, \mathbb{R})$.]

54. Prove Cayley's Theorem using the right regular representation rather than the left regular representation.

55. Let $\sigma \in S_n$. An inversion is a pair (i, j) such that $i < j$ and $\sigma(i) > \sigma(j)$. Prove Theorem 8.19 by showing that multiplying a permutation by a transposition changes the number of inversions by an odd number.

56. The sixteen puzzle consists of 15 tiles numbered 1 through 15 arranged in a four-by-four grid with one position left blank. A move is sliding a tile adjacent to the blank position into the blank position. The goal is to arrange the numbers in order by a sequence of moves. Is it possible to start with the configuration pictured in Figure 8.27(a) and solve the puzzle as indicated in Figure 8.27(b)? Prove your answer by finding a sequence of moves to solve the puzzle or by proving that it is impossible to solve.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

a.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

b.

8.27 Figure

SECTION 9 FINITELY GENERATED ABELIAN GROUPS

Direct Products

Let us take a moment to review our present stockpile of groups. Starting with finite groups, we have the cyclic group $\mathbb{Z}_n$, the symmetric group S_n, and the alternating group A_n for each positive integer n. We also have the dihedral groups D_n and the Klein 4-group V. Of course we know that subgroups of these groups exist. Turning to infinite groups, we have groups consisting of sets of numbers under the usual addition or multiplication, as, for example, $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ under addition, and their nonzero elements under multiplication. We have the group U of complex numbers of magnitude 1 under multiplication, which is isomorphic to each of the groups $\mathbb{R}_c$ under addition modulo c, where $c \in \mathbb{R}^+$. We also have the group S_A of all permutations of an infinite set A, as well as various groups formed from matrices such as GL(n, $\mathbb{R}$).

One purpose of this section is to show a way to use known groups as building blocks to form more groups. The Klein 4-group will be recovered in this way from the cyclic groups. Employing this procedure with the cyclic groups gives us a large class of abelian groups that can be shown to include all possible structure types for a finite abelian group. We start by generalizing Definition 0.4.

9.1 Definition The **Cartesian product of sets** $B_1, B_2, \cdots, B_n$ is the set of all ordered n-tuples $(b_1, b_2, \cdots, b_n)$, where $b_i \in B_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$B_1 \times B_2 \times \cdots \times B_n$$

or by

$$\prod_{i=1}^{n} B_i.$$

■

We could also define the Cartesian product of an infinite number of sets, but the definition is considerably more sophisticated and we shall not need it.

Now let $G_1, G_2, \cdots, G_n$ be groups, and let us use multiplicative notation for all the group operations. Regarding the G_i as sets, we can form $\prod_{i=1}^{n} G_i$. Let us show that we can make $\prod_{i=1}^{n} G_i$ into a group by means of a binary operation of *multiplication by components*. Note again that we are being sloppy when we use the same notation for a group as for the set of elements of the group.

9.2 Theorem Let $G_1, G_2, \cdots, G_n$ be groups. For $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)$ to be the element $(a_1b_1, a_2b_2, \cdots, a_nb_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, the **direct product of the groups** G_i, under this binary operation.

Proof Note that since $a_i \in G_i, b_i \in G_i$, and G_i is a group, we have $a_ib_i \in G_i$. Thus the definition of the binary operation on $\prod_{i=1}^{n} G_i$ given in the statement of the theorem makes sense; that is, $\prod_{i=1}^{n} G_i$ is closed under the binary operation.

The associative law in $\prod_{i=1}^{n} G_i$ is thrown back onto the associative law in each component as follows:

$$\begin{aligned}
&(a_1, a_2, \cdots, a_n)[(b_1, b_2, \cdots, b_n)(c_1, c_2, \cdots, c_n)] \\
&\quad = (a_1, a_2, \cdots, a_n)(b_1c_1, b_2c_2, \cdots, b_nc_n) \\
&\quad = (a_1(b_1c_1), a_2(b_2c_2), \cdots, a_n(b_nc_n)) \\
&\quad = ((a_1b_1)c_1, (a_2b_2)c_2, \cdots, (a_nb_n)c_n) \\
&\quad = (a_1b_1, a_2b_2, \cdots, a_nb_n)(c_1, c_2, \cdots, c_n) \\
&\quad = [(a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n)](c_1, c_2, \cdots, c_n).
\end{aligned}$$

If e_i is the identity element in G_i, then clearly, with multiplication by components, $(e_1, e_2, \cdots, e_n)$ is an identity in $\prod_{i=1}^{n} G_i$. Finally, an inverse of $(a_1, a_2, \cdots, a_n)$ is $(a_1^{-1}, a_2^{-1}, \cdots, a_n^{-1})$; compute the product by components. Hence $\prod_{i=1}^{n} G_i$ is a group. ◆

In the event that the operation of each G_i is commutative, we sometimes use additive notation in $\prod_{i=1}^{n} G_i$ and refer to $\prod_{i=1}^{n} G_i$ as the **direct sum of the groups** G_i. The notation $\oplus_{i=1}^{n} G_i$ is sometimes used in this case in place of $\prod_{i=1}^{n} G_i$, especially with abelian groups with operation $+$. The direct sum of abelian groups $G_1, G_2, \cdots, G_n$ may be written $G_1 \oplus G_2 \oplus \cdots \oplus G_n$. We leave to Exercise 46 the proof that a direct product of abelian groups is again abelian.

It is quickly seen that if B_i has r_i elements for $i = 1, \cdots, n$, then $\prod_{i=1}^{n} B_i$ has $r_1r_2 \cdots r_n$ elements, for in an n-tuple, there are r_1 choices for the first component from B_1, and for each of these there are r_2 choices for the next component from B_2, and so on.

9.3 Example Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_3$, which has $2 \cdot 3 = 6$ elements, namely (0, 0), (0, 1), (0, 2), (1, 0), (1, 1), and (1, 2). We claim that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. It is only necessary to find a generator. Let us try (1, 1). Here the operations in $\mathbb{Z}_2$ and $\mathbb{Z}_3$ are written additively, so we do the same in the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$.

$$\begin{aligned}
(1,1) &= (1,1) \\
2(1,1) &= (1,1) + (1,1) = (0,2) \\
3(1,1) &= (1,1) + (1,1) + (1,1) = (1,0) \\
4(1,1) &= 3(1,1) + (1,1) = (1,0) + (1,1) = (0,1) \\
5(1,1) &= 4(1,1) + (1,1) = (0,1) + (1,1) = (1,2) \\
6(1,1) &= 5(1,1) + (1,1) = (1,2) + (1,1) = (0,0)
\end{aligned}$$

Thus (1, 1) generates all of $\mathbb{Z}_2 \times \mathbb{Z}_3$. Since there is, up to isomorphism, only one cyclic group structure of a given order, we see that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$. ▲

9.4 Example Consider $\mathbb{Z}_3 \times \mathbb{Z}_3$. This is a group of nine elements. We claim that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is *not* cyclic. Since the addition is by components, and since in $\mathbb{Z}_3$ every element added to itself three times gives the identity, the same is true in $\mathbb{Z}_3 \times \mathbb{Z}_3$. Thus no element can generate the group, for a generator added to itself successively could only give the identity after nine

summands. We have found another group structure of order 9. A similar argument shows that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic. Thus $\mathbb{Z}_2 \times \mathbb{Z}_2$ must be isomorphic to the Klein 4-group. ▲

The preceding examples illustrate the following theorem:

9.5 Theorem The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if m and n are relatively prime, that is, the gcd of m and n is 1.

Proof Consider the cyclic subgroup of $\mathbb{Z}_m \times \mathbb{Z}_n$ generated by (1, 1) as described by Theorem 5.19. As our previous work has shown, the order of this cyclic subgroup is the smallest power of (1, 1) that gives the identity (0, 0). Here taking a power of (1, 1) in our additive notation will involve adding (1, 1) to itself repeatedly. Under addition by components, the first component $1 \in \mathbb{Z}_m$ yields 0 only after m summands, $2m$ summands, and so on, and the second component $1 \in \mathbb{Z}_n$ yields 0 only after n summands, $2n$ summands, and so on. For them to yield 0 simultaneously, the number of summands must be a multiple of both m and n. The smallest number that is a multiple of both m and n will be mn if and only if the gcd of m and n is 1; in this case, (1, 1) generates a cyclic subgroup of order mn, which is the order of the whole group. This shows that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn, and hence isomorphic to $\mathbb{Z}_{mn}$ if m and n are relatively prime.

For the converse, suppose that the gcd of m and n is $d > 1$. Then mn/d is divisible by both m and n. Consequently, for any (r, s) in $\mathbb{Z}_m \times \mathbb{Z}_n$, we have

$$\underbrace{(r,s) + (r,s) + \cdots + (r,s)}_{mn/d \text{ summands}} = (0,0).$$

Hence no element (r, s) in $\mathbb{Z}_m \times \mathbb{Z}_n$ can generate the entire group, so $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic and therefore not isomorphic to $\mathbb{Z}_{mn}$. ◆

This theorem can be extended to a product of more than two factors by similar arguments. We state this as a corollary without going through the details of the proof.

9.6 Corollary The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, \cdots, n$ are such that the gcd of any two of them is 1.

9.7 Example The preceding corollary shows that if n is written as a product of powers of distinct prime numbers, as in

$$n = (p_1)^{n_1}(p_2)^{n_2} \cdots (p_r)^{n_r},$$

then $\mathbb{Z}_n$ is isomorphic to

$$\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \cdots \times \mathbb{Z}_{(p_r)^{n_r}}.$$

In particular, $\mathbb{Z}_{72}$ is isomorphic to $\mathbb{Z}_8 \times \mathbb{Z}_9$. ▲

We remark that changing the order of the factors in a direct product yields a group isomorphic to the original one. The names of elements have simply been changed via a permutation of the components in the n-tuples.

Exercise 57 of Section 6 asked you to define the least common multiple of two positive integers r and s as a generator of a certain cyclic group. It is straightforward to prove that the subset of $\mathbb{Z}$ consisting of all integers that are multiples of both r and s is a subgroup of $\mathbb{Z}$, and hence is a cyclic group. Likewise, the set of all common multiples of n positive integers $r_1, r_2, \cdots, r_n$ is a subgroup of $\mathbb{Z}$, and hence is cyclic.

9.8 Definition Let $r_1, r_2, \cdots, r_n$ be positive integers. Their **least common multiple** (abbreviated lcm) is the positive generator of the cyclic group of all common multiples of the r_i, that is, the cyclic group of all integers divisible by each r_i for $i = 1, 2, \cdots, n$. ■

From Definition 9.8 and our work on cyclic groups, we see that the lcm of $r_1, r_2, \cdots, r_n$ is the smallest positive integer that is a multiple of each r_i for $i = 1, 2, \cdots, n$, hence the name *least common multiple*.

9.9 Theorem Let $(a_1, a_2, \cdots, a_n) \in \prod_{i=1}^{n} G_i$. If a_i is of finite order r_i in G_i, then the order of $(a_1, a_2, \cdots, a_n)$ in $\prod_{i=1}^{n} G_i$ is equal to the least common multiple of all the r_i.

Proof This follows by a repetition of the argument used in the proof of Theorem 9.5. For a power of $(a_1, a_2, \cdots, a_n)$ to give $(e_1, e_2, \cdots, e_n)$, the power must simultaneously be a multiple of r_1 so that this power of the first component a_1 will yield e_1, a multiple of r_2, so that this power of the second component a_2 will yield e_2, and so on. ◆

9.10 Example Find the order of (8, 4, 10) in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

Solution Since the gcd of 8 and 12 is 4, we see that 8 is of order $\frac{12}{4} = 3$ in $\mathbb{Z}_{12}$. (See Theorem 6.15.) Similarly, we find that 4 is of order 15 in $\mathbb{Z}_{60}$ and 10 is of order 12 in $\mathbb{Z}_{24}$. The lcm of 3, 15, and 12 is $3 \cdot 5 \cdot 4 = 60$, so (8, 4, 10) is of order 60 in the group $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. ▲

9.11 Example The group $\mathbb{Z} \times \mathbb{Z}_2$ is generated by the elements (1, 0) and (0, 1). More generally, the direct product of n cyclic groups, each of which is either $\mathbb{Z}$ or $\mathbb{Z}_m$ for some positive integer m, is generated by the n n-tuples

$$(1, 0, 0, \cdots, 0), \quad (0, 1, 0, \cdots, 0), \quad (0, 0, 1, \cdots, 0), \quad \cdots, \quad (0, 0, 0, \cdots, 1).$$

Such a direct product might also be generated by fewer elements. For example, $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$ is generated by the single element (1, 1, 1). ▲

Note that if $\prod_{i=1}^{n} G_i$ is the direct product of groups G_i, then the subset

$$\bar{G}_i = \{(e_1, e_2, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \mid a_i \in G_i\},$$

that is, the set of all n-tuples with the identity elements in all places but the ith, is a subgroup of $\prod_{i=1}^{n} G_i$. It is also clear that this subgroup $\bar{G}_i$ is naturally isomorphic to G_i; just rename

$$(e_1, e_2, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \text{ by } a_i.$$

The group G_i is mirrored in the ith component of the elements of $\bar{G}_i$, and the e_j in the other components just ride along. We consider $\prod_{i=1}^{n} G_i$ to be the *internal direct product* of these subgroups $\bar{G}_i$. The direct product given by Theorem 9.2 is called the *external direct product* of the groups G_i. The terms *internal* and *external,* as applied to a direct product of groups, just reflect whether or not (respectively) we are regarding the component groups as subgroups of the product group. We shall usually omit the words *external* and *internal* and just say *direct product*. Which term we mean will be clear from the context.

The Structure of Finitely Generated Abelian Groups

Some theorems of abstract algebra are easy to understand and use, although their proofs may be quite technical and time-consuming to present. This is one section in the text where we explain the meaning and significance of a theorem but omit its proof. The

HISTORICAL NOTE

In his *Disquisitiones Arithmeticae,* Carl Gauss demonstrated various results in what is today the theory of abelian groups in the context of number theory. Not only did he deal extensively with equivalence classes of quadratic forms, but he also considered residue classes modulo a given integer. Although he noted that results in these two areas were similar, he did not attempt to develop an abstract theory of abelian groups.

In the 1840s, Ernst Kummer in dealing with ideal complex numbers noted that his results were in many respects analogous to those of Gauss. (See the Historical Note in Section 30.) But it was Kummer's student Leopold Kronecker (see the Historical Note in Section 39) who finally realized that an abstract theory could be developed out of the analogies. As he wrote in 1870, "these principles [from the work of Gauss and Kummer] belong to a more general, abstract realm of ideas. It is therefore appropriate to free their development from all unimportant restrictions, so that one can spare oneself from the necessity of repeating the same argument in different cases. This advantage already appears in the development itself, and the presentation gains in simplicity, if it is given in the most general admissible manner, since the most important features stand out with clarity." Kronecker then proceeded to develop the basic principles of the theory of finite abelian groups and was able to state and prove a version of Theorem 9.12 restricted to finite groups.

meaning of any theorem whose proof we omit is well within our understanding, and we feel we should be acquainted with it. It would be impossible for us to meet some of these fascinating facts in a one-semester course if we were to insist on wading through complete proofs of all theorems. The theorem that we now state gives us complete structural information about many abelian groups, in particular, about all finite abelian groups.

9.12 Theorem **(Primary Factor Version of the Fundamental Theorem of Finitely Generated Abelian Groups)** Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and the r_i are positive integers. The direct product is unique except for possible rearrangement of the factors; that is, the number (**Betti number** of G) of factors $\mathbb{Z}$ is unique and the prime powers $(p_i)^{r_i}$ are unique.

Proof The proof is omitted here. ◆

9.13 Example Find all abelian groups, up to isomorphism, of order 360. The phrase *up to isomorphism* signifies that any abelian group of order 360 should be structurally identical (isomorphic) to one of the groups of order 360 exhibited.

Solution We make use of Theorem 9.12. Since our groups are to be of the finite order 360, no factors $\mathbb{Z}$ will appear in the direct product shown in the statement of the theorem.

First we express 360 as a product of prime powers $2^3 3^2 5$. Then using Theorem 9.12, we get as possibilities

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
3. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Thus there are six different abelian groups (up to isomorphism) of order 360. ▲

There is another version of the Fundamental Theorem of Finitely Generated Abelian Groups. Each version can be proven from the other, so technically, if one version is used to prove something, the other version could also be used. However, it is sometimes more convenient to use one version rather than the other for a particular problem.

9.14 Theorem **(Invariant Factor Version of the Fundamental Theorem of Finitely Generated Abelian Groups)** Every finitely generated abelian group is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \mathbb{Z}_{d_3} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where each of the $d_i \geq 2$ is an integer and d_i divides d_{i+1} for $1 \leq i \leq k-1$. Furthermore, the representation is unique. ♦

The Betti number of a group is the number of factors of $\mathbb{Z}$ in both Theorem 9.12 and 9.14. The numbers d_i are called the **invariant factors** or the **torsion coefficients**. Theorem 9.12 implies Theorem 9.14 and the other way around. Here we show with an example how to start with a finite group that is in the form specified in Theorem 9.12 and find its representation in the form of Theorem 9.14.

9.15 Example Let us find the invariant factor form of the abelian group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times Z_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7$, which is in primary factor form. We make a table, one row for each prime number involved in G: 2, 3, and 7. We list the powers of each prime in the primary factor form starting with the highest power to the lowest power, filling the ends of the short rows with $1 = p^0$. Table 9.16 is the table for G. The group G is the direct product of cyclic groups of the orders listed in the table. The products of the entries in the columns give the invariant factors. For G, the invariant factors are $d_4 = 8 \cdot 9 \cdot 7 = 504$, $d_3 = 4 \cdot 3 \cdot 1 = 12$, $d_2 = 2 \cdot 1 \cdot 1 = 2$, and $d_1 = 2 \cdot 1 \cdot 1 = 2$. The construction of the table insures that d_1 divides d_2, d_2 divides d_3, d_3 divides d_4, and G is isomorphic with $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \mathbb{Z}_{d_3} \times \mathbb{Z}_{d_4} = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{504}$. ▲

9.16 Table

8	4	2	2
9	3	1	1
7	1	1	1

Example 9.15 shows how to create a table from a finitely generated abelian group that is in primary factor form. From the table we can find the invariant form of the group. This process can easily be reversed by factoring the invariants to find the primary factors.

Applications

Because of Theorems 9.12 and 9.14, there is a plethora of theorems regarding finitely generated abelian groups that are fairly easily proven. We present a few examples.

9.17 Definition A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is **indecomposable**. ■

9.18 Theorem The finite indecomposable abelian groups are exactly the cyclic groups with order a power of a prime.

Proof Let G be a finite indecomposable abelian group. Then by Theorem 9.12, G is isomorphic to a direct product of cyclic groups of prime power order. Since G is indecomposable, this direct product must consist of just one cyclic group whose order is a power of a prime number.

Conversely, let p be a prime. Then $\mathbb{Z}_{p^r}$ is indecomposable, for if $\mathbb{Z}_{p^r}$ were isomorphic to $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, where $i + j = r$, then every element would have an order at most $p^{\max(i,j)} < p^r$. ◆

9.19 Theorem If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof By Theorem 9.12, we can think of G as being

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}},$$

where not all primes p_i need be distinct. Since $(p_1)^{r_1}(p_2)^{r_2} \cdots (p_n)^{r_n}$ is the order of G, then m must be of the form $(p_1)^{s_1}(p_2)^{s_2} \cdots (p_n)^{s_n}$, where $0 \leq s_i \leq r_i$. By Theorem 6.15, $(p_i)^{r_i - s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order equal to the quotient of $(p_i)^{r_i}$ by the gcd of $(p_i)^{r_i}$ and $(p_i)^{r_i - s_i}$. But the gcd of $(p_i)^{r_i}$ and $(p_i)^{r_i - s_i}$ is $(p_i)^{r_i - s_i}$. Thus $(p_i)^{r_i - s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order

$$[(p_i)^{r_i}]/[(p_i)^{r_i - s_i}] = (p_i)^{s_i}.$$

Recalling that $\langle a \rangle$ denotes the cyclic subgroup generated by a, we see that

$$\langle (p_1)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \cdots \times \langle (p_n)^{r_n - s_n} \rangle$$

is the required subgroup of order m. ◆

9.20 Theorem If m is a square-free integer, that is, m is not divisible by the square of any integer $n \geq 2$ then every abelian group of order m is cyclic.

Proof Let G be a finite abelian group of square-free order m. Then by Theorem 9.14, G is isomorphic to

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k},$$

where each $d_i \geq 2$ divides d_{i+1} for $1 \leq i \leq k - 1$. The order of G is $m = d_1 \cdot d_2 \cdots d_k$. If $k \geq 2$, then d_1^2 divides m, which is a contradiction. Thus $k = 1$ and G is cyclic. ◆

EXERCISES 9

Computations

1. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$. Find the order of each of the elements. Is this group cyclic?

2. Repeat Exercise 1 for the group $\mathbb{Z}_3 \times \mathbb{Z}_4$.

In Exercises 3 through 7, find the order of the given element of the direct product.

3. $(2, 6)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12}$

4. $(3, 4)$ in $\mathbb{Z}_{21} \times \mathbb{Z}_{12}$

5. $(40, 12)$ in $\mathbb{Z}_{45} \times \mathbb{Z}_{18}$

6. $(3, 10, 9)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$

7. $(3, 6, 12, 16)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$

8. What is the largest order among the orders of all the cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_8$? of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$?

9. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

10. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

11. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ of order 4.

12. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ that are isomorphic to the Klein 4-group.

13. Disregarding the order of the factors, write direct products of two or more groups of the form $\mathbb{Z}_n$ so that the resulting product is isomorphic to $\mathbb{Z}_{60}$ in as many ways as possible.

14. Fill in the blanks.

a. The cyclic subgroup of $\mathbb{Z}_{24}$ generated by 18 has order____.

b. $\mathbb{Z}_3 \times \mathbb{Z}_4$ is of order____.

c. The element (4, 2) of $\mathbb{Z}_{12} \times \mathbb{Z}_8$ has order___.

d. The Klein 4-group is isomorphic to $\mathbb{Z}$___ $\times$ $\mathbb{Z}$___.

e. $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}_4$ has___elements of finite order.

15. Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

16. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic? Why or why not?

17. Find the maximum possible order for some element of $\mathbb{Z}_8 \times \mathbb{Z}_{28} \times \mathbb{Z}_{24}$.

18. Are the groups $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ and $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$ isomorphic? Why or why not?

19. Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$.

20. Are the groups $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10}$ isomorphic? Why or why not?

In Exercises 21 through 25, proceed as in Example 9.13 to find all abelian groups, up to isomorphism, of the given order. For each group, find the invariant factors and find an isomorphic group of the form indicated in Theorem 9.14.

21. Order 8

22. Order 16

23. Order 32

24. Order 720

25. Order 1089

26. How many abelian groups (up to isomorphism) are there of order 24? of order 25? of order (24)(25)?

27. Following the idea suggested in Exercise 26, let m and n be relatively prime positive integers. Show that if there are (up to isomorphism) r abelian groups of order m and s of order n, then there are (up to isomorphism) rs abelian groups of order mn.

28. Use Exercise 27 to determine the number of abelian groups (up to isomorphism) of order $(10)^5$.

29. **a.** Let p be a prime number. Fill in the second row of the table to give the number of abelian groups of order p^n, up to isomorphism.

n	2	3	4	5	6	7	8
number of groups							

b. Let p, q, and r be distinct prime numbers. Use the table you created to find the number of abelian groups, up to isomorphism, of the given order.

i. $p^3q^4r^7$ **ii.** $(qr)^7$ **iii.** $q^5r^4q^3$

30. Indicate schematically a Cayley digraph for $\mathbb{Z}_m \times \mathbb{Z}_n$ for the generating set $S = \{(1, 0), (0, 1)\}$.

31. Consider Cayley digraphs with two arc types, a solid one with an arrow and a dashed one with no arrow, and consisting of two regular n-gons, for $n \geq 3$, with solid arc sides, one inside the other, with dashed arcs joining the vertices of the outer n-gon to the inner one. Figure 7.11(b) shows such a Cayley digraph with $n = 3$, and Figure 7.13(b) shows one with $n = 4$. The arrows on the outer n-gon may have the same (clockwise or counterclockwise) direction as those on the inner n-gon, or they may have the opposite direction. Let G be a group with such a Cayley digraph.

a. Under what circumstances will G be abelian?

b. If G is abelian, to what familiar group is it isomorphic?

c. If G is abelian, under what circumstances is it cyclic?

d. If G is not abelian, to what group we have discussed is it isomorphic?

Concepts

32. Determine whether each of the following is true or false.

a. If G_1 and G_2 are any groups, then $G_1 \times G_2$ is always isomorphic to $G_2 \times G_1$.

b. Computation in an external direct product of groups is easy if you know how to compute in each component group.

c. Groups of finite order must be used to form an external direct product.

d. A group of prime order could not be the internal direct product of two proper nontrivial subgroups.

e. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_8$.
f. $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to S_8.
g. $\mathbb{Z}_3 \times \mathbb{Z}_8$ is isomorphic to S_4.
h. Every element in $\mathbb{Z}_4 \times \mathbb{Z}_8$ has order 8.
i. The order of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is 60.
j. $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements whether m and n are relatively prime or not.

33. Give an example illustrating that not every nontrivial abelian group is the internal direct product of two proper nontrivial subgroups.

34. **a.** How many subgroups of $\mathbb{Z}_5 \times \mathbb{Z}_6$ are isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_6$?
b. How many subgroups of $\mathbb{Z} \times \mathbb{Z}$ are isomorphic to $\mathbb{Z} \times \mathbb{Z}$?

35. Give an example of a nontrivial group that is not of prime order and is not the internal direct product of two nontrivial subgroups.

36. Determine whether each of the following is true or false.

a. Every abelian group of prime order is cyclic.
b. Every abelian group of prime power order is cyclic.
c. $\mathbb{Z}_8$ is generated by $\{4, 6\}$.
d. $\mathbb{Z}_8$ is generated by $\{4, 5, 6\}$.
e. All finite abelian groups are classified up to isomorphism by Theorem 9.12.
f. Any two finitely generated abelian groups with the same Betti number are isomorphic.
g. Every abelian group of order divisible by 5 contains a cyclic subgroup of order 5.
h. Every abelian group of order divisible by 4 contains a cyclic subgroup of order 4.
i. Every abelian group of order divisible by 6 contains a cyclic subgroup of order 6.
j. Every finite abelian group has a Betti number of 0.

37. Let p and q be distinct prime numbers. How does the number (up to isomorphism) of abelian groups of order p^r compare with the number (up to isomorphism) of abelian groups of order q^r?

38. Let G be an abelian group of order 72.

a. Can you say how many subgroups of order 8 G has? Why, or why not?
b. Can you say how many subgroups of order 4 G has? Why, or why not?

39. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

Exercises 40 through 43 deal with the concept of the torsion subgroup just defined.

40. Find the order of the torsion subgroup of $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$; of $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$.

41. Find the torsion subgroup of the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

42. Find the torsion subgroup T of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers.

43. An abelian group is **torsion free** if e is the only element of finite order. Use Theorem 9.12 to show that every finitely generated abelian group is the internal direct product of its torsion subgroup and of a torsion-free subgroup. (Note that $\{e\}$ may be the torsion subgroup, and is also torsion free.)

44. Find the torsion coefficients for each of the following groups.

a. $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$
b. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}$
c. $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{49} \times \mathbb{Z}_7$
d. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Proof Synopsis

45. Give a two-sentence synopsis of the proof of Theorem 9.5.

Theory

46. Prove that a direct product of abelian groups is abelian.

47. Let G be an abelian group. Let H be the subset of G consisting of the identity e together with all elements of G of order 2. Show that H is a subgroup of G.

48. Following up the idea of Exercise 47 determine whether H will always be a subgroup for every abelian group G if H consists of the identity e together with all elements of G of order 3; of order 4. For what positive integers n will H always be a subgroup for every abelian group G, if H consists of the identity e together with all elements of G of order n? Compare with Exercise 54 of Section 5.

49. Find a counterexample of Exercise 47 with the hypothesis that G is abelian omitted.

Let H and K be subgroups of a group G. Exercises 50 and 51 ask you to establish necessary and sufficient criteria for G to appear as the internal direct product of H and K.

50. Let H and K be groups and let $G = H \times K$. Recall that both H and K appear as subgroups of G in a natural way. Show that these subgroups H (actually $H \times \{e\}$) and K (actually $\{e\} \times K$) have the following properties.

a. Every element of G is of the form hk for some $h \in H$ and $k \in K$.

b. $hk = kh$ for all $h \in H$ and $k \in K$.

c. $H \cap K = \{e\}$.

51. Let H and K be subgroups of a group G satisfying the three properties listed in the preceding exercise. Show that for each $g \in G$, the expression $g = hk$ for $h \in H$ and $k \in K$ is unique. Then let each g be renamed (h, k). Show that, under this renaming, G becomes structurally identical (isomorphic) to $H \times K$.

52. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.

53. Prove that if a finite abelian group has order a power of a prime p, then the order of every element in the group is a power of p.

54. Let G, H, and K be finitely generated abelian groups. Show that if $G \times K$ is isomorphic to $H \times K$, then $G \simeq H$.

55. Using the notation of Theorem 9.14, prove that for any finite abelian group G, every cyclic subgroup of G has order no more than d_k, the largest invariant factor for G.

SECTION 10 COSETS AND THE THEOREM OF LAGRANGE

You may have noticed that the order of a subgroup H of a finite group G seems always to be a divisor of the order of G. This is the theorem of Lagrange. We shall prove it by exhibiting a partition of G into cells, all having the same size as H. Thus if there are r such cells, we will have

$$r(\text{order of } H) = (\text{order of } G)$$

from which the theorem follows immediately. The cells in the partition will be called *cosets of* H, and they are important in their own right. In Section 12, we will see that if H satisfies a certain property, then each coset can be regarded as an element of a group in a very natural way. We give some indication of such *coset groups* in this section to help you develop a feel for the topic.

Cosets

Let H be a subgroup of a group G, which may be of finite or infinite order. We exhibit a partition a G by defining an equivalence relation, $\sim_L$ on G.

10.1 Theorem Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \quad \text{if and only if} \quad a^{-1}b \in H.$$

Then $\sim_L$ is an equivalence relation on G.

Proof When reading the proof, notice how we must constantly make use of the fact that H is a *subgroup* of G.

Reflexive Let $a \in G$. Then $a^{-1}a = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_L a$.

Symmetric Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a subgroup, $(a^{-1}b)^{-1}$ is in H and $(a^{-1}b)^{-1} = b^{-1}a$, so $b^{-1}a$ is in H and $b \sim_L a$.

Transitive Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is a subgroup, $(a^{-1}b)(b^{-1}c) = a^{-1}c$ is in H, so $a \sim_L c$. ◆

The equivalence relation $\sim_L$ in Theorem 10.1 defines a partition of G, as described in Theorem 0.22. Let's see what the cells in this partition look like. Suppose $a \in G$. The cell containing a consists of all $x \in G$ such that $a \sim_L x$, which means all $x \in G$ such that $a^{-1}x \in H$. Now $a^{-1}x \in H$ if and only if $a^{-1}x = h$ for some $h \in H$, or equivalently, if and only if $x = ah$ for some $h \in H$. Therefore the cell containing a is $\{ah \mid h \in H\}$, which we denote by aH.

10.2 Definition Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ of G is the **left coset** of H containing a. ■

10.3 Example Exhibit the left coset of the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$.

Solution Our notation here is additive, so the left coset of $3\mathbb{Z}$ containing m is $m + 3\mathbb{Z}$. Taking $m = 0$, we see that

$$3\mathbb{Z} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$

is itself one of its left cosets, the coset containing 0. To find another left coset, we select an element of $\mathbb{Z}$ not in $3\mathbb{Z}$, say 1, and find the left coset containing it. We have

$$1 + 3\mathbb{Z} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}.$$

These two left cosets, $3\mathbb{Z}$ and $1 + 3\mathbb{Z}$, do not yet exhaust $\mathbb{Z}$. For example, 2 is in neither of them. The left coset containing 2 is

$$2 + 3\mathbb{Z} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}.$$

It is clear that these three left cosets we have found do exhaust $\mathbb{Z}$, so they constitute the partition of $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$. ▲

10.4 Example We find the partition of $\mathbb{Z}_{12}$ into left cosets of $H = \langle 3 \rangle$. One coset is always the subgroup itself, so $0 + H = \{0, 3, 6, 9\}$. We next find $1 + H = \{1, 4, 7, 10\}$. We are still not done since we have not included every element of $\mathbb{Z}_{12}$ in the two cosets we listed so far. Finally, $2 + H = \{2, 5, 8, 11\}$ and we have computed all the left cosets of H in $\mathbb{Z}_{12}$. ▲

10.5 Example We now list the left cosets of the subgroup $H = \langle \mu \rangle = \{\iota, \mu\}$ of the nonabelian group $D_4 = \{\iota, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}$.

$$\begin{aligned} \iota\{\iota, \mu\} &= \{\iota, \mu\} \\ \rho\{\iota, \mu\} &= \{\rho, \mu\rho^3\} \\ \rho^2\{\iota, \mu\} &= \{\rho^2, \mu\rho^2\} \\ \rho^3\{\iota, \mu\} &= \{\rho^3, \mu\rho\} \end{aligned}$$

We know this is a complete list of the left cosets since every element of D_4 appears in exactly one of the listed sets. ▲

The Theorem of Lagrange

In Example 10.4 each left coset of $\langle 3 \rangle \leq \mathbb{Z}_{12}$ has four elements. In Example 10.5, each left coset has two elements. From the computation of the left cosets, it is no surprise that all left cosets of a subgroup have the same number of elements. Theorem 10.6 confirms this is what happens in general.

10.6 Theorem Let H be a subgroup of G. Then for any $a \in G$, the coset aH has the same cardinality as H.

Proof Let $f : H \to aH$ be defined by the formula $f(h) = ah$. To show f is one-to-one, we suppose that $b, c \in H$ and $f(b) = f(c)$. Then $ab = ac$ and left cancellation gives $b = c$. So f is one-to-one. Now suppose that $y \in aH$. Then there is an $h \in H$ such that $y = ah$ by definition of the left coset aH. Thus $y = f(h)$ and f is surjective. Since there is a one-to-one function mapping H onto aH, H and aH have the same cardinality. ◆

In the case of a finite subgroup H, Theorem 10.6 says that H and aH have the same number of elements for any a in the group G. This is precisely what we were seeking in order to prove Lagrange's Theorem.

10.7 Theorem **(Theorem of Lagrange)** Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof Let n be the order of G, and let H have order m. Theorem 10.6 shows that every coset of H also has m elements. Let r be the number of cells in the partition of G into left cosets of H. Then $n = rm$, so m is indeed a divisor of n. ◆

Note that this elegant and important theorem comes from the simple counting of cosets and the number of elements in each coset. We continue to derive consequences of Theorem 10.7, which should be regarded as a counting theorem.

10.8 Corollary Every group of prime order is cyclic.

Proof Let G be of prime order p, and let a be an element of G different from the identity. Then the cyclic subgroup $\langle a \rangle$ of G generated by a has at least two elements, a and e. But by Theorem 10.7, the order $m \geq 2$ of $\langle a \rangle$ must divide the prime p. Thus we must have $m = p$ and $\langle a \rangle = G$, so G is cyclic. ◆

Since every cyclic group of order p is isomorphic to $\mathbb{Z}_p$, we see that *there is only one group structure, up to isomorphism, of a given prime order* ρ. Now doesn't this elegant result follow easily from the theorem of Lagrange, a *counting* theorem? *Never underestimate a theorem that counts something*. Proving the preceding corollary is a favorite examination question.

10.9 Theorem The order of an element of a finite group divides the order of the group.

Proof Remembering that the order of an element is the same as the order of the cyclic subgroup generated by the element, we see that this theorem follows directly from Lagrange's Theorem. ◆

10.10 Definition Let H be a subgroup of a group G. The number of left cosets of H in G is the **index** $(G : H)$ **of** H **in** G. ■

The index $(G : H)$ just defined may be finite or infinite. If G is finite, then obviously $(G : H)$ is finite and $(G : H) = |G|/|H|$, since every coset of H contains $|H|$ elements. We state a basic theorem concerning indices of subgroups, and leave the proof to the exercises (see Exercise 40).

10.11 Theorem Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose $(H:K)$ and $(G:H)$ are both finite. Then $(G:K)$ is finite, and $(G:K) = (G:H)(H:K)$.

Lagrange's Theorem says that for any subgroup H of a finite group G, the order of H divides the order of G. But if d is a divisor of the order of G, does G necessarily have a subgroup with exactly d elements? We will show in Section 13 that the answer is no for some groups. This suggests a new question: Under what conditions does G have a subgroup of every order d that is a divisor of G? We saw in Section 9 that for every divisor of the order of an abelian group, there is a subgroup of that order. The complete answer to this question is beyond the scope of this book, but we will come back to the question later.

Cosets Left and Right!

It is possible to do everything we have done in this section using right cosets instead of left cosets. All it takes is some minor and straightforward modifications to the definitions and proofs. We briefly give the corresponding definitions that lead to right cosets and point out some of their properties.

Let H be a subgroup of G. To start with, instead of $\sim_L$ we could have used $\sim_R$ defined by

$$a \sim_R b \quad \text{if and only if} \quad ab^{-1} \in H.$$

With this definition, $\sim_R$ is an equivalence relation and the equivalence classes are the **right cosets**. The right coset of H containing the element $a \in G$ is

$$Ha = \{ha \mid h \in H\}.$$

Just like left cosets, each right coset of a subgroup H has the same cardinality as H. So left cosets and right cosets have the same cardinality. In abelian groups, the right and left cosets are the same, but there is no reason to think they would be the same in general for nonabelian groups. If the right and left cosets are the same, we can drop left or right and just refer to cosets.

10.12 Example In Example 10.5 we computed the left cosets of the subgroup $H = \langle \mu \rangle = \{\iota, \mu\}$ of the group $D_4 = \{\iota, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}$. We now compute the right cosets.

$$\begin{aligned} \{\iota, \mu\}\iota &= \{\iota, \mu\} \\ \{\iota, \mu\}\rho &= \{\rho, \mu\rho\} \\ \{\iota, \mu\}\rho^2 &= \{\rho^2, \mu\rho^2\} \\ \{\iota, \mu\}\rho^3 &= \{\rho^3, \mu\rho^3\} \end{aligned}$$

The right cosets and the left cosets are not the same. For example, $\rho H = \{\rho, \mu\rho^3\}$ while $H\rho = \{\rho, \mu\rho\}$. ▲

If this were the whole story of left and right cosets, there would be no reason to even mention right cosets. We could just use left coset, prove Lagrange's Theorem, and call it a day. However, as we shall see in Part III, a curious thing happens when the left and right cosets are the same. We illustrate with an example.

10.13 Example The group $\mathbb{Z}_6$ is abelian. Find the partition of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0, 3\}$.

Solution One coset is $\{0, 3\}$ itself. The coset containing 1 is $1 + \{0, 3\} = \{1, 4\}$. The coset containing 2 is $2 + \{0, 3\} = \{2, 5\}$. Since $\{0, 3\}$, $\{1, 4\}$, and $\{2, 5\}$ exhaust all of $\mathbb{Z}_6$, these are all the cosets. ▲

We point out a fascinating thing that we will develop in detail in Section 12. Referring back to Example 10.13, Table 10.14 gives the binary operation for $\mathbb{Z}_6$ but with elements listed in the order they appear in the cosets $\{0, 3\}$, $\{1, 4\}$, $\{2, 5\}$. We shaded the table according to these cosets.

10.14 Table

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

10.15 Table

	LT	MD	DK
LT	LT	MD	DK
MD	MD	DK	LT
DK	DK	LT	MD

Suppose we denote these cosets by LT(light), MD(medium), and DK(dark) according to their shading. Table 10.14 then defines a binary operation on these shadings, as shown in Table 10.15. Note that if we replace LT by 0, MD by 1, and DK by 2 in Table 10.15, we obtain the table for $\mathbb{Z}_3$. Thus the table of shadings forms a group!

We will see in Section 12 that when left cosets and right cosets are the same, then the cosets form a group as in Example 10.13. If right and left cosets are different, the construction fails.

10.16 Example Let $H = \{\iota, \mu\} \leq D_3$. The group table for D_3 is given below with the elements arranged so that left cosets are together. The double lines divide the cosets.

	ι	μ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$
ι	ι	μ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$
μ	μ	ι	$\mu\rho$	ρ^2	$\mu\rho^2$	ρ
ρ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$	ι	μ
$\mu\rho^2$	$\mu\rho^2$	ρ	μ	ι	$\mu\rho$	ρ^2
ρ^2	ρ^2	$\mu\rho$	ι	μ	ρ	$\mu\rho^2$
$\mu\rho$	$\mu\rho$	ρ^2	$\mu\rho^2$	ρ	μ	ι

The situation here is much different from the situation in Example 10.13. In Table 10.14 the two-by-two blocks in the table each contain only elements of a left coset. In the present example, most blocks do not contain elements from only one left coset. Furthermore, even if we tried to use the two-by-two blocks of elements to form a three-by-three group table, the second row of blocks contains two blocks, both having the same elements, $\{\rho^2, \mu\rho, \mu, \iota\}$. So the table of blocks would have a row with the same element listed twice. In this case, there is no natural way of making the left cosets a group. ▲

If G is an abelian group, then the left and right cosets are the same. Theorem 10.17 gives another condition when left and right cosets are the same. Recall that if $\phi : G \to G'$ is a group homomorphism, then $\text{Ker}(\phi) = \phi^{-1}[\{e\}] \leq G$ is the kernel of ϕ.

10.17 Theorem Let $\phi : G \to G'$ be a group homomorphism. Then the left and right cosets of $\text{Ker}(\phi)$ are identical. Furthermore, $a, b \in G$ are in the same coset of $\text{Ker}(\phi)$ if and only if $\phi(a) = \phi(b)$.

Proof We first assume that a and b are in the same left cosets of $\text{Ker}(\phi)$ and show they are also in the same right cosets. Then $a^{-1}b \in \text{Ker}(\phi)$. So $\phi(a^{-1}b) = e$, the identity element. Because ϕ is a homomorphism, $\phi(a)^{-1}\phi(b) = e$, which implies that $\phi(a) = \phi(b)$. Therefore, $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \phi(a)\phi(a)^{-1} = e$. Thus $ab^{-1} \in \text{Ker}(\phi)$, which says that a and b are in the same right coset. Note that in the process we showed that if a and b are in the same left coset of $\text{Ker}(\phi)$, then $\phi(a) = \phi(b)$.

Now suppose that $\phi(a) = \phi(b)$. Then $\phi(b^{-1}a) = \phi(b)^{-1}\phi(a) = e$. Thus $b^{-1}a \in \text{Ker}(\phi)$, which implies that a and b are in the same left coset.

To complete the proof, we need to show that if a and b are in the same right coset, then they are also in the same left coset. The proof is essentially the same as above, so we leave this detail to the reader. ◆

10.18 Example Consider the determinant map $\det : \text{GL}(2, \mathbb{R}) \to \mathbb{R}^*$. In linear algebra you learn that $\det(AB) = \det(A)\det(B)$, so the determinant is a group homomorphism. The kernel of det is the set of all 2×2 matrices with determinant 1. Two matrices $A, B \in \text{GL}(2, \mathbb{R})$ are in the same left coset of Ker(det) if and only if they are in the same right coset of Ker(det) if and only if $\det(A) = \det(B)$. In particular, the two matrices

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 3 & 2 \\ 2 & 2 \end{bmatrix}$$

each have determinant 2, so they are in the same left (and right) cosets of Ker(det). ▲

10.19 Corollary A homomorphism $\phi : G \to G'$ is one-to-one if and only if $\text{Ker}(\phi)$ is the trivial subgroup of G.

Proof We first assume that $\text{Ker}(\phi) = \{e\}$. Every coset of $\text{Ker}(\phi)$ has only one element. Suppose that $\phi(a) = \phi(b)$. Then a and b are in the same coset of $\text{Ker}(\phi)$ by Theorem 10.17. Thus $a = b$.

Now suppose that ϕ is one-to-one. Then only the identity e is mapped to the identity in G'. So $\text{Ker}(\phi) = \{e\}$. ◆

Corollary 10.19 says that to check if a homomorphism $\phi : G \to G'$ is one-to-one one merely needs to check that $\text{Ker}(\phi)$ is the trivial subgroup. In other words, show that the only solution to $\phi(x) = e'$ is e, where e and e' are the identities in G and G', respectively.

10.20 Example Let $\phi : \mathbb{R} \to \mathbb{R}^+$ be defined by $\phi(x) = 2^x$. Since ϕ is a homomorphism, we can check that ϕ is one-to-one by solving $\phi(x) = 1$. The equation $2^x = \phi(x) = 1$ has only the solution 0 since for $x > 0$, $2^x > 1$ and for $x < 0$, $2^x < 1$. Thus ϕ is one-to-one. ▲

EXERCISES 10

Computations

1. Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.
2. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.
3. Find all cosets of the subgroup $\langle 3 \rangle$ in $\mathbb{Z}_{18}$.
4. Find all cosets of the subgroup $\langle 6 \rangle$ in $\mathbb{Z}_{18}$.
5. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.
6. Find all left cosets of $\langle \mu\rho \rangle$ in D_4.
7. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left cosets?

8. Are the left and right cosets the same for the subgroup $\{\iota, \rho^4, \mu, \mu\rho^4\}$ of D_8? If so, display the cosets. If not, find a left coset that is not the same as any right coset.

9. Find all the left cosets of $\langle \rho^2 \rangle \leq D_4$.

10. Repeat the previous exercise, but find the right cosets. Are the left and right cosets the same? If so, make the group table for D_4, ordering the elements so that the cosets are in blocks, see if the blocks form a group with four elements, and determine what group of order 4 the blocks form.

11. Find the index of $\langle \rho^2 \rangle$ in the group D_6.

12. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.

13. Find the index of $12\mathbb{Z}$ in $\mathbb{Z}$.

14. Find the index of $12\mathbb{Z}$ in $3\mathbb{Z}$.

15. Let $\sigma = (1, 2, 5, 4)(2, 3)$ in S_5. Find the index of $\langle \sigma \rangle$ in S_5.

16. Let $\mu = (1, 2, 4, 5)(3, 6)$ in S_6. Find the index of $\langle \mu \rangle$ in S_6.

Concepts

In Exercises 17 through 19, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

17. Let G be a group and let $H \subseteq G$. The *left coset of H containing a* is $aH = \{ah \mid h \in H\}$.

18. Let G be a group and let $H \leq G$. The *index of H in G* is the number of right cosets of H in G.

19. Let $\phi : G \to G'$. Then the *kernel* of ϕ is $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e\}$.

20. Determine whether each of the following is true or false.

- **a.** Every subgroup of every group has left cosets.
- **b.** The number of left cosets of a subgroup of a finite group divides the order of the group.
- **c.** Every group of prime order is abelian.
- **d.** One cannot have left cosets of a finite subgroup of an infinite group.
- **e.** A subgroup of a group is a left coset of itself.
- **f.** Only subgroups of finite groups can have left cosets.
- **g.** A_n is of index 2 in S_n for $n > 1$.
- **h.** The theorem of Lagrange is a nice result.
- **i.** Every finite group contains an element of every order that divides the order of the group.
- **j.** Every finite cyclic group contains an element of every order that divides the order of the group.
- **k.** The kernel of a homomorphism is a subgroup of the range of the homomorphism.
- **l.** Left cosets and right cosets of the kernel of a homomorphism are the same.

In Exercises 21 through 26, give an example of the desired subgroup and group if possible. If impossible, say why it is impossible.

21. A subgroup $H \leq G$ with G infinite and H having only a finite number of left cosets in G

22. A subgroup of an abelian group G whose left cosets and right cosets give different partitions of G

23. A subgroup of a group G whose left cosets give a partition of G into just one cell

24. A subgroup of a group of order 6 whose left cosets give a partition of the group into 6 cells

25. A subgroup of a group of order 6 whose left cosets give a partition of the group into 12 cells

26. A subgroup of a group of order 6 whose left cosets give a partition of the group into 4 cells

Proof Synopsis

27. Give a one-sentence synopsis of the proof of the Theorem of Lagrange.

Theory

28. Prove that the relation $\sim_R$ that is used to define right cosets is an equivalence relation.

29. Let H be a subgroup of a group G and let $g \in G$. Define a one-to-one map of H onto Hg. Prove that your map is one-to-one and is onto Hg.

30. Let H be a subgroup of a group G such that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. Show that every left coset gH is the same as the right coset Hg.

31. Let H be a subgroup of a group G. Prove that if the partition of G into left cosets of H is the same as the partition into right cosets of H, then $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. (Note that this is the converse of Exercise 30.)

Let H be a subgroup of a group G and let $a, b \in G$. In Exercises 32 through 35 prove the statement or give a counterexample.

32. If $aH = bH$, then $Ha = Hb$.

33. If $Ha = Hb$, then $b \in Ha$.

34. If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.

35. If $aH = bH$, then $a^2H = b^2H$.

36. Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

37. Show that there are the same number of left as right cosets of a subgroup H of a group G; that is, exhibit a one-to-one map of the collection of left cosets onto the collection of right cosets. (Note that this result is obvious by counting for finite groups. Your proof must hold for any group.)

38. Exercise 29 of Section 2 showed that every finite group of even order $2n$ contains an element of order 2. Using the theorem of Lagrange, show that if n is odd, then an abelian group of order $2n$ contains precisely one element of order 2.

39. Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order.

40. Prove Theorem 10.11 [*Hint:* Let $\{a_iH \mid i = 1, \cdots, r\}$ be the collection of distinct left cosets of H in G and $\{b_jK \mid j = 1, \cdots, s\}$ be the collection of distinct left cosets of K in H. Show that

$$\{(a_ib_j)K \mid i = 1, \cdots, r; j = 1, \cdots, s\}$$

is the collection of distinct left cosets of K in G.]

41. Show that if H is a subgroup of index 2 in a finite group G, then every left coset of H is also a right coset of H.

42. Show that if a group G with identity e has finite order n, then $a^n = e$ for all $a \in G$.

43. Show that every left coset of the subgroup $\mathbb{Z}$ of the additive group of real numbers contains exactly one element x such that $0 \leq x < 1$.

44. Show that the function *sine* assigns the same value to each element of any fixed left coset of the subgroup $\langle 2\pi \rangle$ of the additive group $\mathbb{R}$ of real numbers. (Thus *sine* induces a well-defined function on the set of cosets; the value of the function on a coset is obtained when we choose an element x of the coset and compute $\sin x$.)

45. Let H and K be subgroups of a group G. Define $\sim$ on G by $a \sim b$ if and only if $a = hbk$ for some $h \in H$ and some $k \in K$.

a. Prove that $\sim$ is an equivalence relation on G.

b. Describe the elements in the equivalence class containing $a \in G$. (These equivalence classes are called **double cosets.**)

46. Let S_A be the group of all permutations of the set A, and let c be one particular element of A.

a. Show that $\{\sigma \in S_A \mid \sigma(c) = c\}$ is a subgroup $S_{c,c}$ of S_A.

b. Let $d \neq c$ be another particular element of A. Is $S_{c,d} = \{\sigma \in S_A \mid \sigma(c) = d\}$ a subgroup of S_A? Why or why not?

c. Characterize the set $S_{c,d}$ of part (b) in terms of the subgroup $S_{c,c}$ of part (a).

47. Show that a finite cyclic group of order n has exactly one subgroup of each order d dividing n, and that these are all the subgroups it has.

48. The **Euler phi-function** is defined for positive integers n by $\varphi(n) = s$, where s is the number of positive integers less than or equal to n that are relatively prime to n. Use Exercise 47 to show that

$$n = \sum_{d \mid n} \varphi(d),$$

the sum being taken over all positive integers d dividing n. [*Hint:* Note that the number of generators of $\mathbb{Z}_d$ is $\varphi(d)$ by Corollary 6.17.]

49. Let G be a finite group. Show that if for each positive integer m the number of solutions x of the equation $x^m = e$ in G is at most m, then G is cyclic. [*Hint:* Use Theorem 10.9 and Exercise 48 to show that G must contain an element of order $n = |G|$.]

50. Show that a finite group cannot be written as the union of two of its proper subgroups. Does the statement remain true if "two" is replaced by "three"? (This was problem B-2 on the 1969 Putnam Exam.)

SECTION 11 †PLANE ISOMETRIES

Consider the Euclidean plane $\mathbb{R}^2$. An **isometry of** $\mathbb{R}^2$ is a permutation $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distance, so that the distance between points P and Q is the same as the distance between the points $\phi(P)$ and $\phi(Q)$ for all points P and Q in $\mathbb{R}^2$. If ψ is also an isometry of $\mathbb{R}^2$, then the distance between $\psi(\phi(P))$ and $\psi(\phi(Q))$ must be the same as the distance between $\phi(P)$ and $\phi(Q)$, which in turn is the distance between P and Q, showing that the composition of two isometries is again an isometry. Since the identity map is an isometry and the inverse of an isometry is an isometry, we see that the isometries of $\mathbb{R}^2$ form a subgroup of the group of all permutations of $\mathbb{R}^2$.

Given any subset S of $\mathbb{R}^2$, the isometries of $\mathbb{R}^2$ that carry S onto itself form a subgroup of the group of isometries. This subgroup is the **group of symmetries of** S **in** $\mathbb{R}^2$. Although we defined the dihedral group D_n as one-to-one maps from the vertices of a regular n-gon onto itself that preserves edges, we can extend each map in D_n to an isometry of the whole plane; μ is reflection across the x-axis and ρ is rotation about the origin by $\frac{2\pi}{n}$. So we can think of D_n as the group of isometries of a regular n-gon in $\mathbb{R}^2$.

Everything we have defined in the two preceding paragraphs could equally well have been done for n-dimensional Euclidean space $\mathbb{R}^n$, but we will concern ourselves chiefly with plane isometries here.

It can be proved that every isometry of the plane is one of just four types (see Artin [5]). We will list the types and show, for each type, a labeled figure that can be carried into itself by an isometry of that type. In each of Figs. 11.1, 11.3, and 11.4, consider the line with spikes shown to be extended infinitely to the left and to the right. We also give an example of each type in terms of coordinates.

translation τ: Slide every point the same distance in the same direction. See Fig. 11.1. (*Example:* $\tau(x, y) = (x, y) + (2, -3) = (x + 2, y - 3)$.)

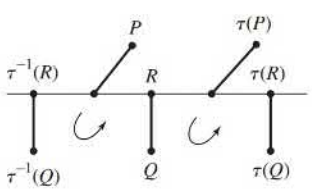
rotation ρ: Rotate the plane about a point P through an angle θ. See Fig. 11.2. (*Example:* $\rho(x, y) = (-y, x)$ is a rotation through 90° counterclockwise about the origin $(0, 0)$.)

reflection μ: Map each point into its mirror image (μ for mirror) across a line L, each point of which is left fixed by μ. See Fig. 11.3. The line L is the *axis of reflection*. (*Example:* $\mu(x, y) = (y, x)$ is a reflection across the line $y = x$.)

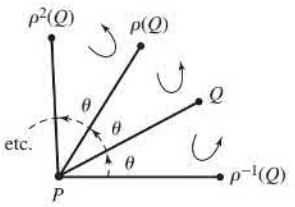
† This section is not used in the remainder of the text.

glide reflection γ: The product of a translation and a reflection across a line mapped into itself by the translation. See Fig. 11.4. (*Example:* $\gamma(x, y) = (x + 4, -y)$ is a glide reflection along the x-axis.)

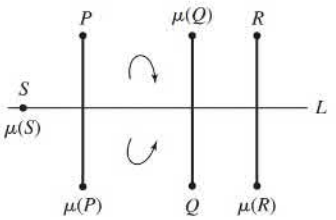
Notice the little curved arrow that is carried into another curved arrow in each of Figs. 11.1 through 11.4. For the translation and rotation, the counterclockwise directions of the curved arrows remain the same, but for the reflection and glide reflection, the counterclockwise arrow is mapped into a clockwise arrow. We say that translations and rotations *preserve orientation,* while the reflection and glide reflection *reverse orientation.* We do not classify the identity isometry as any definite one of the four types listed; it could equally well be considered to be a translation by the zero vector or a rotation about any point through an angle of 0°. We always consider a glide reflection to be the product of a reflection and a translation that is different from the identity isometry.



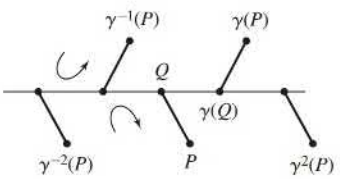
11.1 Figure Translation τ.



11.2 Figure Rotation ρ.



11.3 Figure Reflection μ.



11.4 Figure Glide reflection γ.

The theorem that follows describes the possible structures of finite subgroups of the full isometry group.

11.5 Theorem Every finite group G of isometries of the plane is isomorphic to either the Klein 4-group, $\mathbb{Z}_n$ for $n \geq 1$, or D_n for some $n \geq 3$.

Proof **(Outline)** First we show that there is a point in the plane that is fixed by every element of G. We let $G = \{\phi_1, \phi_2, \phi_3, \ldots, \phi_m\}$ and $(x_i, y_i) = \phi_i(0, 0)$. Then the point

$$P = (\overline{x}, \overline{y}) = \left(\frac{x_1 + x_2 + x_3 + \cdots + x_m}{m}, \frac{y_1 + y_1 + y_3 + \cdots + y_m}{m} \right)$$

is the center of mass of the set $S = \{(x_i, y_i) \mid 1 \leq i \leq m\}$ where each point is weighted by the number of ϕ_i that map $(0, 0)$ to that point. It is easy to see that the isometries in G permute the points in S since for each i and j, $\phi_i \circ \phi_j = \phi_k$ for some k. Thus $\phi_i(x_j, y_j) = (x_k, y_k)$. This implies the center of mass of $\phi(S)$ is the same as the center of mass of S. It can be shown that given the distances from the center of mass to the points of the set S, the center of mass is the only point having these distances from the points of S. This says that $(\overline{x}, \overline{y})$ is fixed by every isometry in G.

The orientation preserving isometries of G form a subgroup H of G which is either all of G or else of order $m/2$. You are asked to prove this in Exercise 22. Of course H consists of the identity and possibly rotations about the point $(\overline{x}, \overline{y})$. If H has only one element, then G has one or two elements and is therefore isomorphic with $\mathbb{Z}_1$ or $\mathbb{Z}_2$. If H has two elements, then G has two or four elements and is therefore isomorphic with either the Klein 4-group, $\mathbb{Z}_4$, or $\mathbb{Z}_2$. So we can assume that H has at least three elements.

If we choose a rotation ρ in H that rotates through the smallest positive angle θ among all the elements of H, ρ generates H. The proof of this fact is similar to the proof that a subgroup of a cyclic group is cyclic and you are asked to provide the details of the proof in Exercise 23. If $G = H$, then G is isomorphic with $\mathbb{Z}_m$. So we now assume that G contains a reflection, say μ. Then the coset μH contains only isometries of G that reverse orientation. Each coset H and μH contains half the elements of G, so $G = H \cup \mu H$.

Consider now a regular n-gon (recall that we are assuming that $n \geq 3$) with center the point $(\overline{x}, \overline{y})$ and having a vertex v_0 on the line fixed by μ. Each element of G permutes the vertices of the n-gon and preserves edges. Furthermore, no two elements of G permute the vertices in the same way. Thus G is isomorphic with a subgroup of the dihedral group D_n. Since $|G| = |D_n|$, G is isomorphic with D_n. ◆

In Theorem 11.5 the Klein 4-group, V, seems like an exception. However, V fits into the family of dihedral groups since V has two elements of order 2, a and b, with the property that $ab = ba^{-1}$. Sometimes V is denoted D_2 and considered a dihedral group. The isometries of the plane that map a line segment to itself are isomorphic with V.

The preceding theorem gives the complete story about finite plane isometry groups. We turn now to some infinite groups of plane isometries that arise naturally in decorating and art. Among these are the *discrete frieze groups*. A discrete frieze consists of a pattern of finite width and height that is repeated endlessly in both directions along its baseline to form a strip of infinite length but finite height; think of it as a decorative border strip that goes around a room next to the ceiling on wallpaper. We consider those isometries that carry each basic pattern onto itself or onto another instance of the pattern in the frieze. The set of all such isometries is called the **"frieze group."** All discrete frieze groups are infinite and have a subgroup isomorphic to $\mathbb{Z}$ generated by the translation that slides the frieze lengthwise until the basic pattern is superimposed on the position of its next neighbor pattern in that direction. As a simple example of a discrete frieze, consider integral signs spaced equal distances apart and continuing infinitely to the left and right, indicated schematically like this.

$$\cdots\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\int\cdots$$

Let us consider the integral signs to be one unit apart. The symmetry group of this frieze is generated by a translation τ sliding the plane one unit to the right, and by a rotation ρ of 180° about a point in the center of some integral sign. There are no horizontal or vertical reflections, and no glide reflections. This frieze group is nonabelian; we can check that $\tau\rho = \rho\tau^{-1}$. This relation between τ and ρ looks very familiar. The dihedral group D_n is also generated by two elements ρ and μ that satisfy the relation $\rho\mu = \mu\rho^{-1}$. If τ and ρ in the frieze group are replaced by ρ and μ, respectively, we have the same relation. In D_n, μ has order 2, as does ρ in the frieze group, but the element ρ in D_n has order n while τ has infinite order. Thus it is natural to use the notation D_∞ for this nonabelian frieze group.

As another example, consider the frieze given by an infinite string of D's.

$$\cdots \mathbf{D\,D\,D\,D\,D\,D\,D\,D\,D\,D\,D}\cdots$$

Its group is generated by a translation τ one step to the right and by a vertical reflection μ across a horizontal line cutting through the middle of all the D's. We can check that these group generators commute this time, that is, $\tau\mu = \mu\tau$, so this frieze group is abelian and is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$.

It can be shown that if we classify such discrete friezes only by whether or not their groups contain a

rotation	horizontal axis reflection
vertical axis reflection	nontrivial glide reflection

then there are a total of seven possibilities. A *nontrivial glide reflection* in a symmetry group is one that is not equal to a product of a translation in that group and a reflection in that group. The group for the string of D's above contains glide reflections across the horizontal line through the centers of the D's, but the translation component of each glide reflection is also in the group so they are all considered trivial glide reflections in that group. The frieze group for

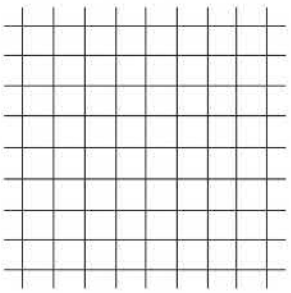
contains a nontrivial glide reflection whose translation component is not an element of the group. The exercises exhibit the seven possible cases, and ask you to tell, for each case, which of the four types of isometries displayed above appear in the symmetry group. We do not obtain seven different group structures. Each of the groups obtained can be shown to be isomorphic to one of

$$\mathbb{Z}, \quad D_\infty, \quad \mathbb{Z} \times \mathbb{Z}_2, \quad \text{or} \quad D_\infty \times \mathbb{Z}_2.$$

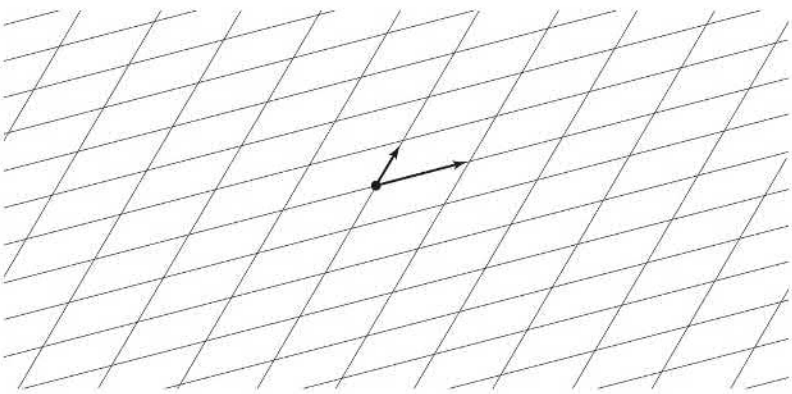
Equally interesting is the study of symmetries when a pattern in the shape of a square, parallelogram, rhombus, or hexagon is repeated by translations along *two nonparallel vector directions* to fill the entire plane, like patterns that appear on wallpaper. These groups are called the *wallpaper groups* or the *plane crystallographic groups*. While a frieze could not be carried into itself by a rotation through a positive angle less than 180°, it is possible to have rotations of 60°, 90°, 120°, and 180° for some of these plane-filling patterns. Figure 11.6 provides an illustration where the pattern consists of a square. We are interested in the group of plane isometries that carry this square onto itself or onto another square. Generators for this group are given by two translations (one sliding a square to the next neighbor to the right and one to the next above), by a rotation through 90° about the center of a square, and by a reflection in a vertical (or horizontal) line along the edges of the square. The one reflection is all that is needed to "turn the plane over"; a diagonal reflection can also be used. After being turned over, the translations and rotations can be used again. The isometry group for this *periodic pattern* in the plane surely contains a subgroup isomorphic to $\mathbb{Z} \times \mathbb{Z}$ generated by the unit translations to the right and upward, and a subgroup isomorphic to D_4 generated by those isometries that carry one square (it can be any square) into itself.

If we consider the plane to be filled with parallelograms as in Fig. 11.7, we do not get all the types of isometries that we did for Fig. 11.6. The symmetry group this time is generated by the translations indicated by the arrows and a rotation through 180° about any vertex of a parallelogram.

It can be shown that there are 17 different types of wallpaper patterns when they are classified according to the types of rotations, reflections, and nontrivial glide reflections that they admit. We refer you to Gallian [8] for pictures of these 17 possibilities and a chart to help you identify them. The exercises illustrate a few of them. The situation



11.6 Figure



11.7 Figure

in space is more complicated; it can be shown that there are 230 three-dimensional crystallographic groups. The final exercise we give involves rotations in space.

M. C. Escher (1898–1973) was an artist whose work included plane-filling patterns. In the exercises you are asked to analyze two of his works of this type.

EXERCISES 11

1. This exercise shows that the group of symmetries of a certain type of geometric figure may depend on the dimension of the space in which we consider the figure to lie.

a. Describe all symmetries of a point in the real line $\mathbb{R}$; that is, describe all isometries of $\mathbb{R}$ that leave one point fixed.

b. Describe all symmetries (translations, reflections, etc.) of a point in the plane $\mathbb{R}^2$.

c. Describe all symmetries of a line segment in $\mathbb{R}$.

d. Describe all symmetries of a line segment in $\mathbb{R}^2$.

e. Describe some symmetries of a line segment in $\mathbb{R}^3$.

2. Let P stand for an orientation preserving plane isometry and R for an orientation reversing one. Fill in the table with P or R to denote the orientation preserving or reversing property of a product.

	P	R
P		
R		

3. Fill in the table to give *all* possible types of plane isometries given by a product of two types as indicated in Tables 11.1 through 11.4. For example, a product of two rotations may be a rotation, or it may be another type. Fill in the box corresponding to $\rho\rho$ with both letters. Use your answer to Exercise 2 to eliminate some types. Eliminate the identity from consideration.

	τ	ρ	μ	γ
τ				
ρ				
μ				
γ				

4. Draw a plane figure that has a one-element group as its group of symmetries in $\mathbb{R}^2$.
5. Draw a plane figure that has a two-element group as its group of symmetries in $\mathbb{R}^2$.
6. Draw a plane figure that has a three-element group as its group of symmetries in $\mathbb{R}^2$.
7. Draw a plane figure that has a four-element group isomorphic to $\mathbb{Z}_4$ as its group of symmetries in $\mathbb{R}^2$.
8. Draw a plane figure that has a four-element group isomorphic to the Klein 4-group V as its group of symmetries in $\mathbb{R}^2$.
9. For each of the four types of plane isometries (other than the identity), give the possibilities for the order of an isometry of that type in the group of plane isometries.
10. A plane isometry ϕ has a *fixed point* if there exists a point P in the plane such that $\phi(P) = P$. Which of the four types of plane isometries (other than the identity) can have a fixed point?
11. Referring to Exercise 10, which types of plane isometries, if any, have exactly one fixed point?
12. Referring to Exercise 10, which types of plane isometries, if any, have exactly two fixed points?
13. Referring to Exercise 10, which types of plane isometries, if any, have an infinite number of fixed points?
14. Argue geometrically that a plane isometry that leaves three noncolinear points fixed must be the identity map.
15. Using Exercise 14, show algebraically that if two plane isometries ϕ and ψ agree on three noncolinear points, that is, if $\phi(P_i) = \psi(P_i)$ for noncolinear points P_1, P_2, and P_3, then ϕ and ψ are the same map.
16. Do the rotations, together with the identity map, form a subgroup of the group of plane isometries? Why or why not?
17. Do the translations, together with the identity map, form a subgroup of the group of plane isometries? Why or why not?
18. Do the rotations about one particular point P, together with the identity map, form a subgroup of the group of plane isometries? Why or why not?
19. Does the reflection across one particular line L, together with the identity map, form a subgroup of the group of plane isometries? Why or why not?
20. Do the glide reflections, together with the identity map, form a subgroup of the group of plane isometries? Why or why not?
21. Which of the four types of plane isometries can be elements of a *finite* subgroup of the group of plane isometries?
22. Completing a detail of the proof of Theorem 11.5, let G be a finite group of plane isometries. Show that the rotations in G, together with the identity isometry, form a subgroup H of G, and that either $H = G$ or $|G| = 2|H|$. [*Hint:* Use the same method that we used to show that $|S_n| = 2|A_n|$.]

23. Completing a detail in the proof of Theorem 11.5, let G be a finite group consisting of the identity isometry and rotations about one point P in the plane. Show that G is cyclic, generated by the rotation in G that turns the plane counterclockwise about P through the smallest angle $\theta > 0$. [*Hint:* Follow the idea of the proof that a subgroup of a cyclic group is cyclic.]

Exercises 24 through 30 illustrate the seven different types of friezes when they are classified according to their symmetries. Imagine the figure shown to be continued infinitely to the right and left. The symmetry group of a frieze always contains translations. For each of these exercises answer these questions about the symmetry group of the frieze.

a. Does the group contain a rotation?

b. Does the group contain a reflection across a horizontal line?

c. Does the group contain a reflection across a vertical line?

d. Does the group contain a nontrivial glide reflection?

e. To which of the possible groups $\mathbb{Z}, D_\infty, \mathbb{Z} \times \mathbb{Z}_2$, or $D_\infty \times \mathbb{Z}_2$ do you think the symmetry group of the frieze is isomorphic?

24. F F F F F F F F F F F F F F

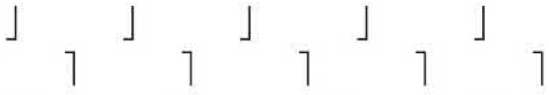
25. T T T T T T T T T T

26. E E E E E E E E E E E

27. Z Z Z Z Z Z Z Z Z Z Z

28. H H H H H H H H H H

29.



30.

Exercises 31 through 37 describe a pattern to be used to fill the plane by translation in the two directions given by the specified vectors. Answer these questions in each case.

a. Does the symmetry group contain any rotations? If so, through what possible angles θ where $0 < \theta \leq 180°$?

b. Does the symmetry group contain any reflections?

c. Does the symmetry group contain any nontrivial glide reflections?

31. A square with horizontal and vertical edges using translation directions given by vectors $(1, 0)$ and $(0, 1)$.

32. A square as in Exercise 31 using translation directions given by vectors $(1, 1/2)$ and $(0, 1)$.

33. A square as in Exercise 31 with the letter L at its center using translation directions given by vectors $(1, 0)$ and $(0, 1)$.

34. A square as in Exercise 31 with the letter E at its center using translation directions given by vectors $(1, 0)$ and $(0, 1)$.

35. A square as in Exercise 31 with the letter H at its center using translation directions given by vectors $(1, 0)$ and $(0, 1)$.

36. A regular hexagon with a vertex at the top using translation directions given by vectors $(1, 0)$ and $(1, \sqrt{3})$.

37. A regular hexagon with a vertex at the top containing an equilateral triangle with vertex at the top and centroid at the center of the hexagon, using translation directions given by vectors $(1, 0)$ and $(1, \sqrt{3})$.

Exercises 38 and 39 are concerned with art works of M. C. Escher. Find images of the indicated art by searching on the internet. Neglect the shading and colors in the figures and assume the markings in each human figure, reptile,

or horseman are the same, even though they may be invisible due to shading. Answer the same questions (a), (b), and (c) that were asked for Exercises 31 through 36, and also answer this part (d).

d. Assuming horizontal and vertical coordinate axes with equal scales as usual, give vectors in the two nonparallel directions of vectors that generate the translation subgroup. Do not concern yourself with the length of these vectors.

38. *The Study of Regular Division of the Plane with Horsemen.*

39. *The Study of Regular Division of the Plane with Reptiles.*

40. Let $\phi : \mathbb{R} \to U$ be given by $\phi(\theta) = \cos(\theta) + i\sin(\theta)$ and $S = \phi[\mathbb{Z}]$.

a. Show that any rotation mapping S to S is a rotation by an angle $n \in \mathbb{Z}$ where angles are measured in radians.

b. Show that reflection across the x-axis maps S to S.

c. What is the group of symmetries of S?

41. Show that the rotations of a cube in space form a group isomorphic to S_4. [*Hint:* A rotation of the cube permutes the diagonals through the center of the cube.]

PART III

Homomorphisms and Factor Groups

SECTION 12 FACTOR GROUPS

Recall from Section 10 that for some group tables we can arrange the head on top and on the left so that the elements are grouped into left cosets of a subgroup in such a way that the coset blocks form a group table. We start this section by looking more closely at why the cosets of $\{0, 3\} \leq \mathbb{Z}_6$ form a group and why the cosets of the subgroup $\{\iota, \mu\} \leq D_3$ do not. Table 12.1 is the group table for $\mathbb{Z}_6$ with the heads at the top and left sorted by cosets of $\{0, 3\}$.

12.1 Table

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

According to Table 12.1 the coset $\{1, 4\}$ plus the coset $\{2, 5\}$ is the coset $\{0, 3\}$. This means that if we add either 1 or 4 to either 2 or 5 in $\mathbb{Z}_6$, we should get either 0 or 3. This is easily checked by adding the four possibilities.

$$1 +_6 2 = 3$$
$$1 +_6 5 = 0$$
$$4 +_6 2 = 0$$
$$4 +_6 5 = 3$$

We observe that if we wish to break up a group into its left cosets so the group table shows an operation on the left cosets, we need to be sure that if a_1, a_2 are in the same

left coset and b_1, b_2 are in the same left coset, then a_1b_1 and a_2b_2 are in the same left coset. If this condition is satisfied for a subgroup $H \leq G$, we say that the operation on the left cosets of H is **induced** by the operation of G or that the operation of G **induces** an operation on the left cosets of H. In this case for any $a, b \in G$ we write

$$(aH)(bH) = (ab)H$$

to mean that the product of any element in aH multiplied by any element in bH must be in the left coset $(ab)H$.

12.2 Example We show that the operation $+$ in the group $\mathbb{Z}$ induces an operation on the cosets of $5\mathbb{Z} \leq \mathbb{Z}$. We first list the left cosets.

$$\begin{aligned} 5\mathbb{Z} &= \{\cdots -10, -5, 0, 5, 10, \ldots\} \\ 1 + 5\mathbb{Z} &= \{\cdots -9, -4, 1, 6, 11, \ldots\} \\ 2 + 5\mathbb{Z} &= \{\cdots -8, -3, 2, 7, 12, \ldots\} \\ 3 + 5\mathbb{Z} &= \{\cdots -7, -2, 3, 8, 13, \ldots\} \\ 4 + 5\mathbb{Z} &= \{\cdots -6, -1, 4, 9, 14, \ldots\} \end{aligned}$$

Let a_1 and a_2 be in the same left coset of $5\mathbb{Z}$. Then $a_2 = a_1 + 5r$ for some $r \in \mathbb{Z}$. We also let b_1, b_2 be in the same left coset of $5\mathbb{Z}$. Then $b_2 = b_1 + 5s$ for some $s \in \mathbb{Z}$. We compute $a_2 + b_2$.

$$\begin{aligned} a_2 + b_2 &= (a_1 + 5r) + (b_1 + 5s) \\ &= a_1 + 5r + b_1 + 5s \\ &= a_1 + b_1 + 5r + 5s && \textbf{(1)} \\ &= (a_1 + b_1) + 5(r + s) && \textbf{(2)} \\ &\in (a_1 + b_1) + 5\mathbb{Z} \end{aligned}$$

So $a_2 + b_2$ is in the same coset as $a_1 + b_1$, which says that addition in $\mathbb{Z}$ induces an operation on the five left cosets $5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}$. Looking back at the calculations, we see that only properties shared by all groups were used in each step except in line (1) where we used the fact that $\mathbb{Z}$ is abelian. Furthermore, line (2) is not necessary since $5\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ so we know that $5\mathbb{Z}$ is closed under addition. From this example, it appears that as long as G is an abelian group, the operation of G induces an operation on the left cosets of any subgroup of G. ▲

In Equation (1) of Example 12.2 we used the fact that $5r + b_1 = b_1 + 5r$. If we were doing the same computation in multiplicative notation and using any group G and subgroup H of G, this would correspond to $hb_1 = b_1h$. If the group G is not abelian, then this computation fails. However, we can weaken the abelian condition slightly and still get an induced operation on the left cosets. All we really need is that $hb_1 = b_1h'$ for some $h' \in H$. This happens when the left coset b_1H is the same set as the right coset Hb_1.

12.3 Definition Let H be a subgroup of G. We say that H is a **normal** subgroup of G if for all $g \in G$, $gH = Hg$. If H is a normal subgroup of G, we write $H \trianglelefteq G$. ■

Recall that Theorem 10.17 states that if $\phi : G \to G'$ is a group homomorphism and e' is the identity element in G', then $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e'\}$ has the property that left and right cosets of $\text{Ker}(\phi)$ are the same. So the kernel of any homomorphism is a normal subgroup.

12.4 Example The subgroup of even permutations $A_n \leq S_n$ is normal since A_n is the kernel of the homomorphism $\text{sgn} : S_n \to \{1, -1\}$. ▲

12.5 Example If $H \leq G$ and G is an abelian group, then H is a normal subgroup of G. ▲

12.6 Example Let $H = \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \det(A) = 1\}$. The determinant map satisfies $\det(AB) = \det(A)\det(B)$, which means that the determinant map is a homomorphism, $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$. Thus $H = \mathrm{Ker}(\det)$, which says that $H \trianglelefteq \mathrm{GL}(n, \mathbb{R})$. This subgroup H is called the **special linear group** and it is denoted by $\mathrm{SL}(n, \mathbb{R})$. ▲

12.7 Theorem Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Proof Suppose first that $(aH)(bH) = (ab)H$ does give a well-defined binary operation on left cosets. Let $a \in G$. We want to show that aH and Ha are the same set. We use the standard technique of showing that each is a subset of the other.

Let $x \in aH$. Choosing representatives $x \in aH$ and $a^{-1} \in a^{-1}H$, we have $(xH)(a^{-1}H) = (xa^{-1})H$. On the other hand, choosing representatives $a \in aH$ and $a^{-1} \in a^{-1}H$, we see that $(aH)(a^{-1}H) = eH = H$. Using our assumption that left coset multiplication by representatives is well defined, we must have $xa^{-1} = h \in H$. Then $x = ha$, so $x \in Ha$ and $aH \subseteq Ha$. We leave the symmetric proof that $Ha \subseteq aH$ to Exercise 26.

We turn now to the converse: If H is a normal subgroup, then left coset multiplication by representatives is well-defined. Due to our hypothesis, we can simply say *cosets,* omitting *left* and *right*. Suppose we wish to compute $(aH)(bH)$. Choosing $a \in aH$ and $b \in bH$, we obtain the coset $(ab)H$. Choosing different representatives $ah_1 \in aH$ and $bh_2 \in bH$, we obtain the coset ah_1bh_2H. We must show that these are the same cosets. Now $h_1b \in Hb = bH$, so $h_1b = bh_3$ for some $h_3 \in H$. Thus

$$(ah_1)(bh_2) = a(h_1b)h_2 = a(bh_3)h_2 = (ab)(h_3h_2)$$

and $(ab)(h_3h_2) \in (ab)H$. Therefore, ah_1bh_2 is in $(ab)H$. ◆

Theorem 12.7 shows that we have an operation on the left cosets of $H \leq G$ induced by the operation on G if and only if H is a normal subgroup of G. We next verify that this operation makes G/H, the cosets of H in G, a group.

12.8 Corollary Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH)(bH) = (ab)H$. ▲

Proof Computing, $(aH)[(bH)(cH)] = (aH)[(bc)H] = [a(bc)]H$, and similarly, we have $[(aH)(bH)](cH) = [(ab)c]H$, so associativity in G/H follows from associativity in G. Because $(aH)(eH) = (ae)H = aH = (ea)H = (eH)(aH)$, we see that $eH = H$ is the identity element in G/H. Finally, $(a^{-1}H)(aH) = (a^{-1}a)H = eH = (aa^{-1})H = (aH)(a^{-1}H)$ shows that $a^{-1}H = (aH)^{-1}$. ◆

12.9 Definition The group G/H in the preceding corollary is the **factor group** (or **quotient group**) of G by H. ■

12.10 Example Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Corollary 12.8 allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$. For any integer m, the division algorithm says that $m = nq + r$ for some $0 \leq r < n$. Therefore, $m \in r + n\mathbb{Z}$. So $\mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} \mid 0 \leq k < n\}$. Thus $\langle 1 + n\mathbb{Z} \rangle = \mathbb{Z}/n\mathbb{Z}$, which implies that $\mathbb{Z}/n\mathbb{Z}$ is cyclic and isomorphic with $\mathbb{Z}_n$. ▲

12.11 Example Consider the abelian group $\mathbb{R}$ under addition, and let $c \in \mathbb{R}^+$. The cyclic subgroup $\langle c \rangle$ of $\mathbb{R}$ contains as elements

$$\cdots -3c, -2c, -c, 0, c, 2c, 3c, \cdots .$$

Every coset of $\langle c \rangle$ contains just one element x such that $0 \leq x < c$. If we choose these elements as representatives of the cosets when computing in $\mathbb{R}/\langle c \rangle$, we find that we are computing their sum modulo c as discussed for the computation in $\mathbb{R}_c$ in Section 3. For example, if $c = 5.37$, then the sum of the cosets $4.65 + \langle 5.37 \rangle$ and $3.42 + \langle 5.37 \rangle$ is the coset $8.07 + \langle 5.37 \rangle$, which contains $8.07 - 5.37 = 2.7$, which is $4.65 +_{5.37} 3.42$. Working with these coset elements x where $0 \leq x < c$, we thus see that the group $\mathbb{R}_c$ of Section 3 is isomorphic to $\mathbb{R}/\langle c \rangle$ under an isomorphism ψ where $\psi(x) = x + \langle c \rangle$ for all $x \in \mathbb{R}_c$. Of course, $\mathbb{R}/\langle c \rangle$ is then also isomorphic to the circle group U of complex numbers of magnitude 1 under multiplication. ▲

We have seen that the group $\mathbb{Z}/\langle n \rangle$ is isomorphic to the group $\mathbb{Z}_n$, and as a set, $\mathbb{Z}_n = \{0, 1, 3, 4, \cdots, n-1\}$, the set of nonnegative integers less than n. Example 12.11 shows that the group $\mathbb{R}/\langle c \rangle$ is isomorphic to the group $\mathbb{R}_c$. In Section 3, we choose the notation $\mathbb{R}_c$ rather than the conventional $[0, c)$ for the half-open interval of nonnegative real numbers less than c. We did that to bring out now the comparison of these factor groups of $\mathbb{Z}$ with these factor groups of $\mathbb{R}$.

Homomorphisms and Factor Groups

We learned that the kernel of any homomorphism $\phi : G \to G'$ is a normal subgroup of G. Do all normal subgroups arise in this way? That is, for any normal subgroup $H \trianglelefteq G$, is there a group homomorphism $\phi : G \to G'$ for some group G' such that H is the kernel of G? The answer to the question is yes as we see in Theorem 12.12.

12.12 Theorem Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Proof Let $x, y \in G$. Then

$$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y),$$

so γ is a homomorphism. Since $xH = H$ if and only if $x \in H$, we see that the kernel of γ is indeed H. ◆

Since the kernel of any homomorphism $\phi : G \to G'$ is a normal subgroup, it is natural to ask how the factor group $G/\text{Ker}(\phi)$ is related to G'. Theorem 12.12 and the next example illustrate that there is a very strong connection.

12.13 Example **(Reduction Modulo n)** Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be defined by letting $\phi(m)$ be the remainder when m is divided by n. We check that ϕ is a group homomorphism. Let $m_1, m_2 \in \mathbb{Z}$ and suppose that the division algorithm gives us

$$m_1 = nq_1 + r_1 \qquad \text{and}$$
$$m_2 = nq_2 + r_2.$$

Then $m_1 + m_2 = n(q_1 + q_2) + r_1 + r_2$. If $r_1 + r_2 < n$, then

$$\phi(m_1 + m_2) = r_1 + r_2 = \phi(m_1) +_n \phi(m_2).$$

On the other hand, if $r_1 + r_2 \geq n$, then $m_1 + m_2 = n(q_1 + q_2 + 1) + (r_1 + r_2 - n)$ and $0 \leq r_1 + r_2 - n < n$, which implies

$$\phi(m_1 + m_2) = r_1 + r_2 - n = \phi(m_1) +_n \phi(m_2).$$

The kernel of ϕ is the set of all the multiples of n, $n\mathbb{Z}$. So $\mathbb{Z}/\text{Ker}(\phi) = \mathbb{Z}/n\mathbb{Z}$, which is isomorphic to $\mathbb{Z}_n$. ▲

The previous example is a special case of the Fundamental Homomorphism Theorem.

12.14 Theorem **(The Fundamental Homomorphism Theorem)** Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then $\phi[G]$ is a group, and $\mu : G/H \to \phi[G]$ given by $\mu(gH) = \phi(g)$ is an isomorphism. If $\gamma : G \to G/H$ is the homomorphism given by $\gamma(g) = gH$, then $\phi(g) = \mu \circ \gamma(g)$ for each $g \in G$.

Proof Theorem 8.5 says that $\phi[G]$ is a subgroup of G'. Theorem 10.17 shows that the map $\mu : G/H \to \phi[G]$ is well defined. We show μ is a homomorphism. Let $aH, bH \in G/H$. Then $\mu((aH)(bH)) = \mu((ab)H) = \phi(ab) = \phi(a)\phi(b) = \mu(aH)\mu(bH)$. Since ϕ maps G onto $\phi[G]$, μ maps G/H onto $\phi[G]$. To show that μ is one-to-one, we compute the kernel of μ. Since $\mu(aH) = \phi(a)$, the kernel of μ is $\{aH \mid \phi(a) = e'\}$. But $\phi(a) = e'$ if and only if $a \in \text{Ker}(\phi) = H$. So $\text{Ker}(\mu) = \{H\}$ which is the trivial subgroup of G/H. By Corollary 10.19 μ is one-to-one, which completes the proof that μ is an isomorphism.

We next turn to the final statement of the theorem. Let $g \in G$. Then

$$\phi(g) = \mu(gH) = \mu(\gamma(g)) = \mu \circ \gamma(g).$$

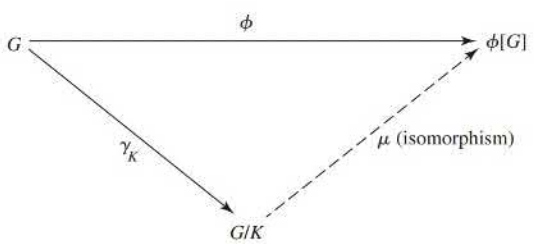
◆

The Fundamental Homomorphism Theorem is sometimes called the First Isomorphism Theorem. As the name suggests, there are other related theorems. In fact we will prove two others, the Second Isomorphism Theorem and the Third Isomorphism Theorem, in Section 16.

Theorem 12.14 states that $\phi(g) = \mu \circ \gamma(g)$. This can be visualized in Figure 12.15. If we start with an element $g \in G$, and map it to $\phi(g)$, we get the same result as first mapping g to $\gamma(g)$ and then mapping $\gamma(g)$ to $\mu \circ \gamma(g)$. When we have a situation like this, we say that the map ϕ can be *factored* as $\phi = \mu \circ \gamma$.

The isomorphism μ in Theorem 12.14 is referred to as a *natural* or *canonical* isomorphism, and the same adjectives are used to describe the homomorphism γ. There may be other isomorphisms and homomorphisms for these same groups, but the maps μ and γ have a special status with ϕ and are uniquely determined by Theorem 12.14.

In summary, every homomorphism with domain G gives rise to a factor group G/H, and every factor group G/H gives rise to a homomorphism mapping G into G/H. Homomorphisms and factor groups are closely related. We give an example indicating how useful this relationship can be.



12.15 Figure

12.16 Example Classify the group $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$ according to the fundamental theorem of finitely generated abelian groups (Theorem 9.12).

Solution The projection map $\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ given by $\pi_1(x, y) = x$ is a homomorphism of $\mathbb{Z}_4 \times \mathbb{Z}_2$ onto $\mathbb{Z}_4$ with kernel $\{0\} \times \mathbb{Z}_2$. By Theorem 12.14, we know that the given factor group is isomorphic to $\mathbb{Z}_4$. ▲

Normal Subgroups and Inner Automorphisms

We derive some alternative characterizations of normal subgroups, which often provide us with an easier way to check normality than finding both the left and the right coset decompositions.

Suppose that H is a subgroup of G such that $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. Then $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq H$ for all $g \in G$. We claim that actually $gHg^{-1} = H$. We must show that $H \subseteq gHg^{-1}$ for all $g \in G$. Let $h \in H$. Replacing g by g^{-1} in the relation $ghg^{-1} \in H$, we obtain $g^{-1}h(g^{-1})^{-1} = g^{-1}hg = h_1$ where $h_1 \in H$. Consequently, $h = gh_1g^{-1} \in gHg^{-1}$, and we are done.

Suppose that $gH = Hg$ for all $g \in G$. Then $gh = h_1g$, so $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. By the preceding paragraph, this means that $gHg^{-1} = H$ for all $g \in G$. Conversely, if $gHg^{-1} = H$ for all $g \in G$, then $ghg^{-1} = h_1$ so $gh = h_1g \in Hg$, and $gH \subseteq Hg$. But also, $g^{-1}Hg = H$ giving $g^{-1}hg = h_2$, so that $hg = gh_2$ and $Hg \subseteq gH$.

The comments after Definition 12.3 show that the kernel of any homomorphism is a normal subgroup of the domain. Also, Theorem 12.12 says that any normal subgroup is the kernel of some homomorphism.

We summarize our work as a theorem.

12.17 Theorem The following are four equivalent conditions for a subgroup H of a group G to be a *normal* subgroup of G.

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
2. $gHg^{-1} = H$ for all $g \in G$.
3. There is a group homomorphism $\phi : G \to G'$ such that $\text{Ker}(\phi) = H$.
4. $gH = Hg$ for all $g \in G$.

Condition (2) of Theorem 12.17 is often taken as the definition of a normal subgroup H of a group G. ◆

12.18 Example Every subgroup H of an abelian group G is normal. We need only note that $gh = hg$ for all $h \in H$ and all $g \in G$, so, of course, $ghg^{-1} = h \in H$ for all $g \in G$ and all $h \in H$. ▲

If G is a group and $g \in G$, then the map $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$ is a group homomorphism since $i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(x)$. We see that $gag^{-1} = gbg^{-1}$ if and only if $a = b$, so i_g is one-to-one. Since $g(g^{-1}yg)g^{-1} = y$, we see that i_g is onto G, so it is an isomorphism of G with itself.

12.19 Definition An isomorphism $\phi : G \to G$ of a group G with itself is an **automorphism** of G. The automorphism $i_g : G \to G$, where $i_g(x) = gxg^{-1}$ for all $x \in G$, is the **inner automorphism of G by g**. Performing i_g on x is called **conjugation of x by g**. ■

The equivalence of conditions (1) and (2) in Theorem 12.17 shows that $gH = Hg$ for all $g \in G$ if and only if $i_g[H] = H$ for all $g \in G$, that is, if and only if H is **invariant** under all inner automorphisms of G. It is important to realize that $i_g[H] = H$ is an

equation in *sets;* we need not have $i_g(h) = h$ for all $h \in H$. That is i_g may perform a nontrivial *permutation* of the set H. We see that the normal subgroups of a group G are precisely those that are invariant under all inner automorphisms. A subgroup K of G is a **conjugate subgroup** of H if $K = i_g[H] = gHg^{-1}$ for some $g \in G$.

EXERCISES 12

Computations

In Exercises 1 through 8, find the order of the given factor group.

1. $\mathbb{Z}_6/\langle 3\rangle$

2. $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle 2\rangle \times \langle 2\rangle)$

3. $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle (2,1)\rangle$

4. $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{0\} \times \mathbb{Z}_5)$

5. $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle (1,1)\rangle$

6. $(\mathbb{Z}_{50} \times \mathbb{Z}_{75})/\langle (15,15)\rangle$

7. $(\mathbb{Z}_{26} \times \mathbb{Z}_{15})/\langle (1,1)\rangle$

8. $(\mathbb{Z}_8 \times S_3)/\langle (2,(1,2,3))\rangle$

In Exercises 9 through 15, give the order of the element in the factor group.

9. $5 + \langle 4\rangle$ in $\mathbb{Z}_{12}/\langle 4\rangle$

10. $26 + \langle 12\rangle$ in $\mathbb{Z}_{60}/\langle 12\rangle$

11. $(2,1) + \langle (1,1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle (1,1)\rangle$

12. $(3,1) + \langle (1,1)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle (1,1)\rangle$

13. $(2,3) + \langle (0,3)\rangle$ in $(\mathbb{Z}_{10} \times \mathbb{Z}_4)/\langle (0,3)\rangle$

14. $(2,5) + \langle (1,2)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle (1,2)\rangle$

15. $(2,0) + \langle (4,4)\rangle$ in $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle (4,4)\rangle$

16. Compute $i_\rho[H]$ for the subgroup $H = \{\iota, \mu\}$ of the dihedral group D_3.

Concepts

In Exercises 17 through 19, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

17. A *normal subgroup* H of G is one satisfying $hG = Gh$ for all $h \in H$.

18. A *normal subgroup* H of G is one satisfying $g^{-1}hg \in H$ for all $h \in H$ and all $g \in G$.

19. An *automorphism* of a group G is a homomorphism mapping G into G.

20. What is the importance of a *normal* subgroup of a group G?

Students often write nonsense when first proving theorems about factor groups. The next two exercises are designed to call attention to one basic type of error.

21. A student is asked to show that if H is a normal subgroup of an abelian group G, then G/H is abelian. The student's proof starts as follows:

We must show that G/H is abelian. Let a and b be two elements of G/H.

a. Why does the instructor reading this proof expect to find nonsense from here on in the student's paper?

b. What should the student have written?

c. Complete the proof.

22. A **torsion group** is a group all of whose elements have finite order. A group is **torsion free** if the identity is the only element of finite order. A student is asked to prove that if G is a torsion group, then so is G/H for every normal subgroup H of G. The student writes

We must show that each element of G/H is of finite order. Let $x \in G/H$.

Answer the same questions as in Exercise 21.

23. Determine whether each of the following is true or false.

a. It makes sense to speak of the factor group G/N if and only if N is a normal subgroup of the group G.

b. Every subgroup of an abelian group G is a normal subgroup of G.

c. The only automorphism of an abelian group is the identity map.

d. Every factor group of a finite group is again of finite order.

e. Every factor group of a torsion group is a torsion group. (See Exercise 22.)

f. Every factor group of a torsion-free group is torsion free. (See Exercise 22.)

g. Every factor group of an abelian group is abelian.

h. Every factor group of a nonabelian group is nonabelian.

i. $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n.

j. $\mathbb{R}/n\mathbb{R}$ is cyclic of order n, where $n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$ and $\mathbb{R}$ is under addition.

Theory

24. Let G_1 and G_2 be groups and $\pi_1 : G_1 \times G_2 \to G_1$ be the function defined by $\pi_1(a, b) = a$. Prove that π_1 is a homomorphism, find $\text{Ker}(\pi_1)$, and prove $(G_1 \times G_2)/\text{Ker}(\pi_1)$ is isomorphic to G_1.

25. Let G_1 and G_2 be groups and $\phi : G_1 \times G_2 \to G_1 \times G_2$ be the function defined by $\phi(a, b) = (a, e_2)$ where e_2 is the identity in G_2. Prove that ϕ is a homomorphism, find $\text{Ker}(\phi)$, and prove $(G_1 \times G_2)/\text{Ker}(\phi)$ is isomorphic to G_1.

26. Complete the proof of Theorem 12.7 by showing that if H is a subgroup of a group G and if left coset multiplication $(aH)(bH) = (ab)H$ is well defined, then $Ha \subseteq aH$.

27. Prove that the torsion subgroup T of an abelian group G is a normal subgroup of G, and that G/T is torsion free. (See Exercise 22.)

28. A subgroup H is **conjugate to a subgroup** K of a group G if there exists an inner automorphism i_g of G such that $i_g[H] = K$. Show that conjugacy is an equivalence relation on the collection of subgroups of G.

29. Characterize the normal subgroups of a group G in terms of the cells where they appear in the partition given by the conjugacy relation in the preceding exercise.

30. Find all subgroups of D_3 that are conjugate to $H = \{\iota, \mu\}$. (See Exercise 28.)

31. **(Evaluation Homomorphism)** Let F be the set of all functions mapping the real numbers to the real numbers and let $c \in \mathbb{R}$. The sum of two functions $f + g$ is the function defined by $(f + g)(x) = f(x) + g(x)$. Function addition makes F a group. Let $\phi_c : F \to \mathbb{R}$ be defined by $\phi_c(f) = f(c)$.

a. Show that ϕ_c is a group homomorphism.

b. Find $\text{Ker}(\phi_c)$.

c. Identify the coset of $\text{Ker}(\phi_c)$ that contains the constant function $f(x) = 1$.

d. Find a well-known group that is isomorphic with $F/\text{Ker}(\phi_c)$. Use the Fundamental Homomorphism Theorem to prove your answer.

32. Let H be a normal subgroup of a group G, and let $m = (G : H)$. Show that $a^m \in H$ for every $a \in G$.

33. Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.

34. Given any subset S of a group G, show that it makes sense to speak of the smallest normal subgroup that contains S. [*Hint:* Use Exercise 33.]

35. Let G be a group. An element of G that can be expressed in the form $aba^{-1}b^{-1}$ for some $a, b \in G$ is a **commutator** in G. The preceding exercise shows that there is a smallest normal subgroup C of a group G containing all commutators in G; the subgroup C is the **commutator subgroup** of G. Show that G/C is an abelian group.

36. Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G.

37. Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

38. Let G be a group containing at least one subgroup of a fixed finite order s. Show that the intersection of all subgroups of G of order s is a normal subgroup of G. [*Hint:* Use the fact that if H has order s, then so does $x^{-1}Hx$ for all $x \in G$.]

39. **a.** Show that all automorphisms of a group G form a group under function composition.

b. Show that the inner automorphisms of a group G form a normal subgroup of the group of all automorphisms of G under function composition. [*Warning:* Be sure to show that the inner automorphisms do form a subgroup.]

40. Show that the set of all $g \in G$ such that $i_g : G \to G$ is the identity inner automorphism i_e is a normal subgroup of a group G.

41. Let G and G' be groups, and let H and H' be normal subgroups of G and G', respectively. Let ϕ be a homomorphism of G into G'. Show that ϕ induces a natural homomorphism $\phi_* : (G/H) \to (G'/H')$ if $\phi[H] \subseteq H'$. (This fact is used constantly in algebraic topology.)

42. Use the properties $\det(AB) = \det(A) \cdot \det(B)$ and $\det(I_n) = 1$ for $n \times n$ matrices to show the $n \times n$ matrices with determinant ± 1 form a normal subgroup of $\mathrm{GL}(n, \mathbb{R})$.

43. Let G be a group, and let $\mathscr{P}(G)$ be the set of all *subsets* of G. For any $A, B \in \mathscr{P}(G)$, let us define the product subset $AB = \{ab \mid a \in A, b \in B\}$.

a. Show that this multiplication of subsets is associative and has an identity element, but that $\mathscr{P}(G)$ is not a group under this operation.

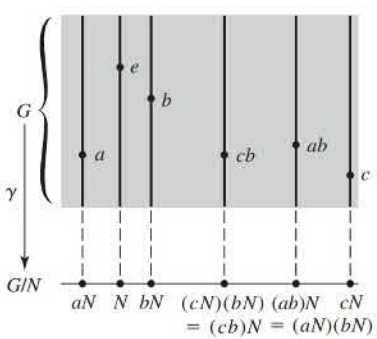
b. Show that if N is a normal subgroup of G, then the set of cosets of N is closed under the above operation on $\mathscr{P}(G)$, and that this operation agrees with the multiplication given by the formula in Corollary 12.8.

c. Show (without using Corollary 12.8) that the cosets of N in G form a group under the above operation. Is its identity element the same as the identity element of $\mathscr{P}(G)$?

SECTION 13 FACTOR-GROUP COMPUTATIONS AND SIMPLE GROUPS

Factor groups can be a tough topic for students to grasp. There is nothing like a bit of computation to strengthen understanding in mathematics. We start by attempting to improve our intuition concerning factor groups. Since we will be dealing with normal subgroups throughout this section, we often denote a subgroup of a group G by N rather than by H.

Let N be a normal subgroup of G. In the factor group G/N, the subgroup N acts as identity element. We may regard N as being *collapsed* to a single element, either to 0 in additive notation or to e in multiplicative notation. This collapsing of N together with the algebraic structure of G require that other subsets of G, namely, the cosets of N, also each collapse into a single element in the factor group. A visualization of this collapsing is provided by Fig. 13.1. Recall from Theorem 12.12 that $\gamma : G \to G/N$ defined by $\gamma(a) = aN$ for $a \in G$ is a homomorphism of G onto G/N. We can view the "line" G/N at the bottom of Figure 13.1 as obtained by collapsing to a point each coset of N in a copy of G. Each point of G/N thus corresponds to a whole vertical line



13.1 Figure

segment in the shaded portion, representing a coset of N in G. It is crucial to remember that multiplication of cosets in G/N can be computed by multiplying in G, using any representative elements of the cosets as shown in the figure.

Additively, two elements of G will collapse into the same element of G/N if they differ by an element of N. Multiplicatively, a and b collapse together if ab^{-1} is in N. The degree of collapsing can vary from nonexistent to catastrophic. We illustrate the two extreme cases by examples.

13.2 Example The trivial subgroup $N = \{0\}$ of $\mathbb{Z}$ is, of course, a normal subgroup. Compute $\mathbb{Z}/\{0\}$.

Solution Since $N = \{0\}$ has only one element, every coset of N has only one element. That is, the cosets are of the form $\{m\}$ for $m \in \mathbb{Z}$. There is no collapsing at all, and consequently, $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$. Each $m \in \mathbb{Z}$ is simply renamed $\{m\}$ in $\mathbb{Z}/\{0\}$. ▲

13.3 Example Let n be a positive integer. The set $n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$ is a subgroup of $\mathbb{R}$ under addition, and it is normal since $\mathbb{R}$ is abelian. Compute $\mathbb{R}/n\mathbb{R}$.

Solution A bit of thought shows that actually $n\mathbb{R} = \mathbb{R}$, because each $x \in \mathbb{R}$ is of the form $n(x/n)$ and $x/n \in \mathbb{R}$. Thus $\mathbb{R}/n\mathbb{R}$ has only one element, the subgroup $n\mathbb{R}$. The factor group is a trivial group consisting only of the identity element. ▲

As illustrated in Examples 13.2 and 13.3 for any group G, we have $G/\{e\} \simeq G$ and $G/G \simeq \{e\}$, where $\{e\}$ is the trivial group consisting only of the identity element e. These two extremes of factor groups are of little importance. We would like knowledge of a factor group G/N to give some information about the structure of G. If $N = \{e\}$, the factor group has the same structure as G and we might as well have tried to study G directly. If $N = G$, the factor group has no significant structure to supply information about G. If G is a finite group and $N \neq \{e\}$ is a normal subgroup of G, then G/N is a smaller group than G, and consequently may have a more simple structure than G. The multiplication of cosets in G/N reflects the multiplication in G, since products of cosets can be computed by multiplying in G representative elements of the cosets.

We give two examples showing that even when G/N has order 2, we may be able to deduce some useful results. If G is a finite group and G/N has just two elements, then we must have $|G| = 2|N|$. Note that every subgroup H containing just half the elements of a finite group G must be a normal subgroup, since for each element a in G but not in H, both the left coset aH and the right coset Ha must consist of all elements in G that are not in H. Thus the left and right cosets of H coincide and H is a normal subgroup of G.

13.4 Example Because $|S_n| = 2|A_n|$, we see that A_n is a normal subgroup of S_n, and S_n/A_n has order 2. Let σ be an odd permutation in S_n, so that $S_n/A_n = \{A_n, \sigma A_n\}$. Renaming the element A_n "even" and the element σA_n "odd," the multiplication in S_n/A_n shown in Table 13.5 becomes

13.5 Table

	A_n	σA_n
A_n	A_n	σA_n
σA_n	σA_n	A_n

$$\begin{array}{ll} (\text{even})(\text{even}) = \text{even} & (\text{odd})(\text{even}) = \text{odd} \\ (\text{even})(\text{odd}) = \text{odd} & (\text{odd})(\text{odd}) = \text{even}. \end{array}$$

Thus the factor group reflects these multiplicative properties for all the permutations in S_n. ▲

Example 13.4 illustrates that while knowing the product of two cosets in G/N does not tell us what the product of two elements of G is, it may tell us that the product in G of two *types* of elements is itself of a certain type.

13.6 Example **(The Converse of the Theorem of Lagrange is False)** Recall that the Theorem of Lagrange states that the order of a subgroup of a finite group G must divide the order of G. We are now in a position to demonstrate that although the group A_4 has 12 elements and 6 divides 12, A_4 has no subgroup of order 6.

Suppose that H were a subgroup of A_4 having order 6. As observed before in Example 13.4, it would follow that H would be a normal subgroup of A_4. Then A_4/H would have only two elements, H and σH for some $\sigma \in A_4$ not in H. Since in a group of order 2, the square of each element is the identity, we would have $HH = H$ and $(\sigma H)(\sigma H) = H$. Now computation in a factor group can be achieved by computing with representatives in the original group. Thus, computing in A_4, we find that for each $\alpha \in H$ we must have $\alpha^2 \in H$ and for each $\beta \in \sigma H$ we must have $\beta^2 \in H$. That is, the square of every element in A_4 must be in H. But in A_4, we have

$$(1,2,3) = (1,3,2)^2 \quad \text{and} \quad (1,3,2) = (1,2,3)^2$$

so (1, 2, 3) and (1, 3, 2) are in H. A similar computation shows that (1, 2, 4), (1, 4, 2), (1, 3, 4), (1, 4, 3), (2, 3, 4), and (2, 4, 3) are all in H. This shows that there must be at least 8 elements in H, contradicting the fact that H was supposed to have order 6. ▲

We now turn to several examples that *compute* factor groups. If the group we start with is finitely generated and abelian, then its factor group will be also. *Computing* such a factor group means classifying it according to the fundamental theorem (Theorem 9.12 or Theorem 9.14).

13.7 Example Let us compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle(0,1)\rangle$. Here $\langle(0,1)\rangle$ is the cyclic subgroup H of $\mathbb{Z}_4 \times \mathbb{Z}_6$ generated by (0, 1). Thus

$$H = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\}.$$

Since $\mathbb{Z}_4 \times \mathbb{Z}_6$ has 24 elements and H has 6 elements, all cosets of H must have 6 elements, and $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$ must have order 4. Since $\mathbb{Z}_4 \times \mathbb{Z}_6$ is abelian, so is $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$ (remember, we compute in a factor group by means of representatives from the original group). In additive notation, the cosets are

$$H = (0,0) + H, \qquad (1,0) + H, \qquad (2,0) + H, \qquad (3,0) + H.$$

Since we can compute by choosing the representatives (0, 0), (1, 0), (2, 0), and (3, 0), it is clear that $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$ is isomorphic to $\mathbb{Z}_4$. Note that this is what we would expect, since in a factor group modulo H, everything in H becomes the identity element; that is, we are essentially setting everything in H equal to zero. Thus the whole second factor $\mathbb{Z}_6$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is collapsed, leaving just the first factor $\mathbb{Z}_4$. ▲

Example 13.7 is a special case of a general theorem that we now state and prove. We should acquire an intuitive feeling for this theorem in terms of *collapsing one of the factors to the identity element.*

13.8 Theorem Let $G = H \times K$ be the direct product of groups H and K. Then $\bar{H} = \{(h,e) \mid h \in H\}$ is a normal subgroup of G. Also $G/\bar{H}$ is isomorphic to K in a natural way. Similarly, $G/\bar{K} \simeq H$ in a natural way.

Proof Consider the homomorphism $\pi_2 : H \times K \to K$, where $\pi_2(h,k) = k$. Because $\text{Ker}(\pi_2) = \bar{H}$, we see that $\bar{H}$ is a normal subgroup of $H \times K$. Because π_2 is onto K, Theorem 12.14 tells us that $(H \times K)/\bar{H} \simeq K$. ◆

We continue with additional computations of abelian factor groups. To illustrate how easy it is to compute in a factor group if we can compute in the whole group, we prove the following theorem.

13.9 Theorem If G is a cyclic group and N is a subgroup of G, then G/N is cyclic.

Proof Let G be a cyclic group, so $\langle a \rangle = G$ for some $a \in G$. Let N be any subgroup of G. Since G is abelian, N is a normal subgroup of G. We compute the cyclic subgroup of G/N generated by aN.

$$\langle aN \rangle = \{(aN)^n \mid n \in \mathbb{Z}\} = \{a^n N \mid n \in \mathbb{Z}\}$$

Since $\{a^n \mid n \in \mathbb{Z}\} = G$,

$$\{a^n N \mid n \in \mathbb{Z}\} = \{gN \mid g \in G\}.$$

So $\langle aN \rangle$ contains every coset of G and we see that G/N is cyclic with generator $\langle aN \rangle$. ◆

13.10 Example Let us compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (0,2) \rangle$. Now $(0, 2)$ generates the subgroup

$$H = \{(0,0), (0,2), (0,4)\}$$

of $\mathbb{Z}_4 \times \mathbb{Z}_6$ of order 3. Here the first factor $\mathbb{Z}_4$ of $\mathbb{Z}_4 \times \mathbb{Z}_6$ is left alone. The $\mathbb{Z}_6$ factor, on the other hand, is essentially collapsed by a subgroup of order 3, giving a factor group in the second factor of order 2 that must be isomorphic to $\mathbb{Z}_2$. Thus $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (0,2) \rangle$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$.

We can verify that $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (0,2) \rangle$ is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ by using Theorem 12.14. We need a homomorphism $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_4 \times \mathbb{Z}_2$ that is onto, with kernel $\langle (0,2) \rangle$. Defining ϕ by $\phi(a,b) = (0,r)$ where r is the remainder when b is divided by 2 does the trick. ▲

13.11 Example Let us compute the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (2,3) \rangle$. *Be careful*! There is a great temptation to say that we are setting the 2 of $\mathbb{Z}_4$ and the 3 of $\mathbb{Z}_6$ both equal to zero, so that $\mathbb{Z}_4$ is collapsed to a factor group isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_6$ to one isomorphic to $\mathbb{Z}_3$, giving a total factor group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. *This is wrong*! Note that

$$H = \langle (2,3) \rangle = \{(0,0), (2,3)\}$$

is of order 2, so $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (2,3) \rangle$ has order 12, not 6. Setting $(2, 3)$ equal to zero does not make $(2, 0)$ and $(0, 3)$ equal to zero individually, so the factors do not collapse separately.

The possible abelian groups of order 12 are $\mathbb{Z}_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, and we must decide to which one our factor group is isomorphic. These two groups are most easily distinguished in that $\mathbb{Z}_4 \times \mathbb{Z}_3$ has an element of order 4, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ does not. We claim that the coset $(1,0) + H$ is of order 4 in the factor group $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$. To find the smallest power of a coset giving the identity in a factor group modulo H, we must, by choosing representatives, find the smallest power of a representative that is in the subgroup H. Now,

$$4(1,0) = (1,0) + (1,0) + (1,0) + (1,0) = (0,0)$$

is the first time that $(1, 0)$ added to itself gives an element of H. Thus $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (2,3) \rangle$ has an element of order 4 and is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$ or $\mathbb{Z}_{12}$.

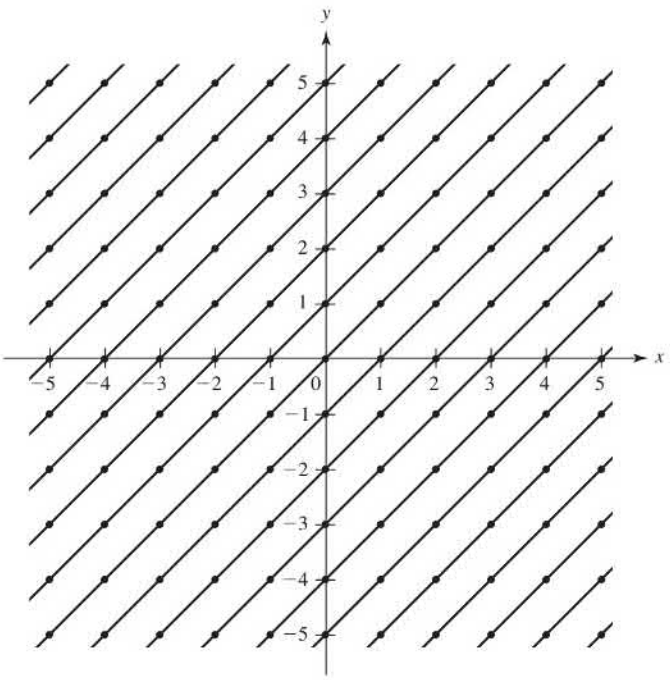
We can use Theorem 12.14 to verify that $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (2,3) \rangle$ is isomorphic to $\mathbb{Z}_{12}$, although it is a little challenging to see what the homomorphism $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_{12}$ should be. We define $\phi : \mathbb{Z}_4 \times \mathbb{Z}_6 \to \mathbb{Z}_{12}$ by setting $\phi(a,b) = 3a +_{12} (12 - 2b)$. Here we interpret $3a$ and $2b$ as integer multiplication, so $0 \leq 3a < 12$ and $0 \leq 2b < 12$. The map ϕ is a homomorphism, but this takes some checking, which we leave to the reader. Also, $\text{Ker}(\phi) = \{(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_6 \mid 3a = 2b\} = \{(0,0), (2,3)\} = \langle (2,3) \rangle$. We also see that $\phi(1,1) = 1$, which implies that ϕ maps onto $\mathbb{Z}_{12}$. By the Fundamental Homomorphism Theorem, $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (2,3) \rangle$ is isomorphic to $\mathbb{Z}_{12}$. ▲

13.12 Example Let us compute (that is, classify as in Theorem 9.12) the group $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$. We may visualize $\mathbb{Z} \times \mathbb{Z}$ as the points in the plane with both coordinates integers, as indicated by the dots in Fig. 13.13. The subgroup $\langle(1,1)\rangle$ consists of those points that lie on the 45° line through the origin, indicated in the figure. The coset $(1,0) + \langle(1,1)\rangle$ consists of those dots on the 45° line through the point $(1,0)$, also shown in the figure. Continuing, we see that each coset consists of those dots lying on one of the 45° lines in the figure. We may choose the representatives

$$\cdots, (-3,0), (-2,0), (-1,0), (0,0), (1,0), (2,0), (3,0), \cdots$$

of these cosets to compute in the factor group. Since these representatives correspond precisely to the points of $\mathbb{Z}$ on the x-axis, we see that the factor group $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$ is isomorphic to $\mathbb{Z}$.

Again, we can use the Fundamental Homomorphism Theorem as another method of computing this group. We let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $\phi(n,m) = n - m$. It is easy to verify that ϕ is a homomorphism, ϕ maps onto $\mathbb{Z}$, and $\text{Ker}(\phi) = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid n = m\} = \langle(1,1)\rangle$. So by the Fundamental Homomorphism Theorem, $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle$ is isomorphic to $\mathbb{Z}$. Furthermore, an isomorphism is given by $\mu((n,m) + \langle(1,1)\rangle) = n - m$. This is the same isomorphism that we saw above. ▲



13.13 Figure

13.14 Example We now compute $(\mathbb{Z} \times \mathbb{Z})/\langle(2,4)\rangle$. This is similar to Example 13.12, but there is a little twist to this one. In this example, we know that the factor group has an element with order 2, since $(1,2) \notin \langle(2,4)\rangle$, but $(1,2) + (1,2) \in \langle(2,4)\rangle$. Furthermore, $(\mathbb{Z} \times \mathbb{Z})/\langle(2,4)\rangle$ has an element $(1,0) + \langle(2,4)\rangle$ with infinite order since $(n,0) \notin \langle(2,4)\rangle$ for any $n \in \mathbb{Z}^+$. Figure 13.15 illustrates the situation. Along the line $y = 2x$ only every other lattice point is in $\langle(2,4)\rangle$. These points are filled dots in the figure. Each line with slope two contains

two cosets, one indicated with solid dots and one with hollow dots. Adding $(1, 2)$ moves the solid dot cosets to the hollow dot cosets and the hollow dot cosets to the solid dot cosets while staying on the same line. Adding $(0, 1)$ moves a coset from one line to the next. We may choose coset representatives

$$\ldots, (0, -3), (0, -2), (0, -1), (0, 0), (0, 1), (0, 2), (0, 3), \ldots$$

for the solid dot cosets and

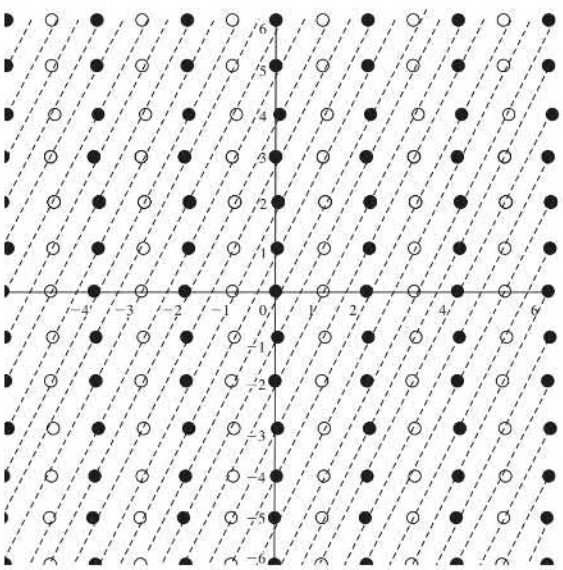
$$\ldots, (1, -3), (1, -2), (1, -1), (1, 0), (1, 1), (1, 2), (1, 3), \ldots$$

for the hollow dot cosets. So it seems that we have two copies of the integers, one with a zero in the first coordinate and one with a one in the first coordinate. This leads us to guess that $(\mathbb{Z} \times \mathbb{Z})/\langle(2, 4)\rangle$ is isomorphic with $\mathbb{Z}_2 \times \mathbb{Z}$.

To verify that our guess is correct, we seek a homomorphism $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_2 \times \mathbb{Z}$ that maps onto $\mathbb{Z}_2 \times \mathbb{Z}$ and whose kernel is $\langle(2, 4)\rangle$. We let $\phi(a, b) = (r, 2a - b)$ where r is the remainder when a is divided by 2. It is easy to check that ϕ is a homomorphism. Furthermore, $\phi(0, -1) = (0, 1)$ and $\phi(1, 2) = (1, 0)$, which implies that ϕ maps onto $\mathbb{Z} \times \mathbb{Z}_2$. It remains to compute $\text{Ker}(\phi)$.

$$\text{Ker}(\phi) = \{(a, b) \mid b = 2a \text{ and } a \text{ is even}\} = \{(2n, 4n) \mid n \in \mathbb{Z}\} = \langle(2, 4)\rangle.$$

Thus $(\mathbb{Z} \times \mathbb{Z})/\langle(2, 4)\rangle$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_2$ by the Fundamental Homomorphism Theorem. Furthermore, an isomorphism $\mu : (\mathbb{Z} \times \mathbb{Z})/\langle(2, 4)\rangle \to \mathbb{Z}_2 \times \mathbb{Z}$ is defined by the formula $\mu((a, b) + \langle(2, 4)\rangle) = (r, 2a - b)$ where r is the remainder when a is divided by 2. ▲



13.15 Figure

Simple Groups

As we mentioned in the preceding section, one feature of a factor group is that it gives crude information about the structure of the whole group. Of course, sometimes there may be no nontrivial proper normal subgroup. For example, Lagrange's Theorem shows that a group of prime order can have no nontrivial proper subgroup of any sort.

13.16 Definition A group is **simple** if it is nontrivial and has no proper nontrivial normal subgroup. ■

13.17 Theorem The alternating group A_n is simple for $n \geq 5$.

Proof See Exercise 41. ◆

There are many simple groups other than those given above. For example, A_5 is of order 60 and A_6 is of order 360, and there is a simple group of nonprime order, namely 168, between these orders.

The complete determination and classification of all finite simple groups is one of the mathematical triumphs of the twentieth century. Hundreds of mathematicians worked on this task from 1950 to 1980. It can be shown that a finite group has a sort of factorization into simple groups, where the factors are unique up to order. The situation is similar to the factorization of positive integers into primes. The knowledge of all finite simple groups can be used to solve some problems of finite group theory and combinatorics.

We have seen in this text that a finite simple abelian group is isomorphic to $\mathbb{Z}_p$ for some prime p. In 1963, Thompson and Feit [21] published their proof of a long-standing conjecture of Burnside, showing that every finite nonabelian simple group is of even order. Further great strides toward the complete classification were made by Aschbacher in the 1970s. Early in 1980, Griess announced that he had constructed a predicted "monster" simple group of order

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,$$
$$000,000,000.$$

Aschbacher added the final details of the classification in August 1980. The research papers contributing to the entire classification fill roughly 5000 journal pages.

We turn to the characterization of those normal subgroups N of a group G for which G/N is a simple group. First we state an addendum to Theorem 8.5 on properties of a group homomorphism. The proof is left to Exercises 37 and 38.

13.18 Theorem Let $\phi : G \to G'$ be a group homomorphism. If N is a normal subgroup of G, then $\phi[N]$ is a normal subgroup of $\phi[G]$. Also, if N' is a normal subgroup of $\phi[G]$, then $\phi^{-1}[N']$ is a normal subgroup of G. ◆

Theorem 13.18 should be viewed as saying that a homomorphism $\phi : G \to G'$ preserves normal subgroups between G and $\phi[G]$. It is important to note that $\phi[N]$ may not be normal in G', even though N is normal in G. For example, $\phi : \mathbb{Z}_2 \to S_3$, where $\phi(0) = \iota$ and $\phi(1) = (1,2)$ is a homomorphism, and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\iota, (1,2)\}$ is not a normal subgroup of S_3.

We can now characterize when G/N is a simple group.

13.19 Definition A **maximal normal subgroup of a group** G is a normal subgroup M not equal to G such that there is no proper normal subgroup N of G properly containing M. ■

13.20 Theorem M is a maximal normal subgroup of G if and only if G/M is simple.

Proof Let M be a maximal normal subgroup of G. Consider the canonical homomorphism $\gamma : G \to G/M$ given by Theorem 12.12. Now γ^{-1} of any nontrivial proper normal subgroup of G/M is a proper normal subgroup of G properly containing M. But M is maximal, so this cannot happen. Thus G/M is simple.

Conversely, Theorem 13.18 shows that if N is a normal subgroup of G properly containing M, then $\gamma[N]$ is normal in G/M. If also $N \neq G$, then

$$\gamma[N] \neq G/M \qquad \text{and} \qquad \gamma[N] \neq \{M\}.$$

Thus, if G/M is simple so that no such $\gamma[N]$ can exist, no such N can exist, and M is maximal. ◆

The Center and Commutator Subgroups

Every nonabelian group G has two important normal subgroups, the *center* $Z(G)$ of G and the *commutator subgroup* C of G. (The letter Z comes from the German word *zentrum,* meaning center.) The center $Z(G)$ is defined by

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}.$$

Exercise 59 of Section 5 shows that $Z(G)$ is an abelian subgroup of G. Since for each $g \in G$ and $z \in Z(G)$ we have $gzg^{-1} = zgg^{-1} = ze = z$, we see at once that $Z(G)$ is a normal subgroup of G. If G is abelian, then $Z(G) = G$; in this case, the center is not useful.

13.21 Example The center of a group G always contains the identity element e. It may be that $Z(G) = \{e\}$, in which case we say that **the center of G is trivial**. For example, examination of Table 4.15 for the group S_3 shows us that $Z(S_3) = \{\iota\}$, so the center of S_3 is trivial. (This is a special case of Exercise 40, which shows that the center of every nonabelian group of order pq for primes p and q is trivial.) Consequently, the center of $S_3 \times \mathbb{Z}_5$ must be $\{\iota\} \times \mathbb{Z}_5$, which is isomorphic to $\mathbb{Z}_5$. ▲

Turning to the commutator subgroup, recall that in forming a factor group of G modulo a normal subgroup N, we are essentially putting every element in G that is in N equal to e, for N forms our new identity in the factor group. This indicates another use for factor groups. Suppose, for example, that we are studying the structure of a nonabelian group G. Since Theorem 9.12 gives complete information about the structure of all finitely generated abelian groups, it might be of interest to try to form an abelian group as much like G as possible, an *abelianized version* of G, by starting with G and then requiring that $ab = ba$ for all a and b in our new group structure. To require that $ab = ba$ is to say that $aba^{-1}b^{-1} = e$ in our new group. An element $aba^{-1}b^{-1}$ in a group is a **commutator of the group.** Thus we wish to attempt to form an abelianized version of G by replacing every commutator of G by e. By the first observation of this paragraph, we should then attempt to form the factor group of G modulo the smallest normal subgroup we can find that contains all commutators of G.

13.22 Theorem Let G be a group. The set of all commutators $aba^{-1}b^{-1}$ for $a, b \in G$ generates a subgroup C (the **commutator subgroup**) of G. This subgroup C is a normal subgroup of G. Furthermore, if N is a normal subgroup of G, then G/N is abelian if and only if $C \leq N$.

Proof The commutators certainly generate a subgroup C; we must show that it is normal in G. Note that the inverse $(aba^{-1}b^{-1})^{-1}$ of a commutator is again a commutator, namely, $bab^{-1}a^{-1}$. Also $e = eee^{-1}e^{-1}$ is a commutator. Theorem 7.7 then shows that C consists precisely of all finite products of commutators. For $x \in C$, we must show that $g^{-1}xg \in C$ for all $g \in G$, or that if x is a product of commutators, so is $g^{-1}xg$ for all $g \in G$. By inserting $e = gg^{-1}$ between each product of commutators occurring in x, we see that it is sufficient to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C. But

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})(e)(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g], \end{aligned}$$

which is in C. Thus C is normal in G.

The rest of the theorem is obvious if we have acquired the proper feeling for factor groups. One doesn't visualize in this way, but writing out that G/C is abelian follows from

$$\begin{aligned}(aC)(bC) &= abC = ab(b^{-1}a^{-1}ba)C \\ &= (abb^{-1}a^{-1})baC = baC = (bC)(aC).\end{aligned}$$

Furthermore, if N is a normal subgroup of G and G/N is abelian, then $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$; that is, $aba^{-1}b^{-1}N = N$, so $aba^{-1}b^{-1} \in N$, and $C \leq N$. Finally, if $C \leq N$, then

$$\begin{aligned}(aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN).\end{aligned}$$

◆

13.23 Example Using cycle notation in the symmetric group S_3, one commutator is

$$(1,2,3)(2,3)(1,2,3)^{-1}(2,3)^{-1} = (1,2,3)(2,3)(1,3,2)(2,3) = (1,3,2).$$

So the commutator subgroup C contains $\langle(1,3,2)\rangle = A_3$, the alternating group. Since S_3/A_3 is abelian (isomorphic with $\mathbb{Z}_2$), Theorem 13.22 says that $C \leq A_3$. Therefore, A_3 is the commutator subgroup. ▲

EXERCISES 13

Computations

In Exercises 1 through 14, classify the given group according to the fundamental theorem of finitely generated abelian groups.

1. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,1)\rangle$

2. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0,2)\rangle$

3. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1,2)\rangle$

4. $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$

5. $(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2,4)\rangle$

6. $(\mathbb{Z} \times \mathbb{Z})/\langle(0,1)\rangle$

7. $(\mathbb{Z} \times \mathbb{Z})/\langle(0,2)\rangle$

8. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(1,1,1)\rangle$

9. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_4)/\langle(3,0,0)\rangle$

10. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle(0,4,0)\rangle$

11. $(\mathbb{Z} \times \mathbb{Z})/\langle(2,2)\rangle$

12. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(3,3,3)\rangle$

13. $(\mathbb{Z} \times \mathbb{Z})/\langle(2,6)\rangle$

14. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_2)/\langle(1,1,1)\rangle$

15. Find both the center and the commutator subgroup of D_4.

16. Find both the center and the commutator subgroup of $\mathbb{Z}_3 \times S_3$.

17. Find both the center and the commutator subgroup of $S_3 \times D_4$.

18. Describe all subgroups of order ≤ 4 of $\mathbb{Z}_4 \times \mathbb{Z}_4$, and in each case classify the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup by Theorem 9.12. That is, describe the subgroup and say that the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, or whatever the case may be. [*Hint:* $\mathbb{Z}_4 \times \mathbb{Z}_4$ has six different cyclic subgroups of order 4. Describe them by giving a generator, such as the subgroup $\langle(1,0)\rangle$. There is one subgroup of order 4 that is isomorphic to the Klein 4-group. There are three subgroups of order 2.]

Concepts

In Exercises 19 and 20, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

19. The *center* of a group G contains all elements of G that commute with every element of G.

20. The *commutator subgroup* of a group G is $\{a^{-1}b^{-1}ab \mid a, b \in G\}$.

21. Determine whether each of following is true or false.

a. Every factor group of a cyclic group is cyclic.

b. A factor group of a noncyclic group is again noncyclic.

c. $\mathbb{R}/\mathbb{Z}$ under addition has no element of order 3.

d. $\mathbb{R}/\mathbb{Q}$ under addition has no element of order 2.

e. $\mathbb{R}/\mathbb{Z}$ under addition has an infinite number of elements of order 4.

f. If the commutator subgroup C of a group G is $\{e\}$, then G is abelian.

g. If G/H is abelian, then the commutator subgroup C of G contains H.

h. The commutator subgroup of a simple group G must be G itself.

i. The commutator subgroup of a nonabelian simple group G must be G itself.

j. All nontrivial finite simple groups have prime order.

In Exercises 22 through 25, let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let F^* be the multiplicative group of all elements of F that do not assume the value 0 at any point of $\mathbb{R}$.

22. Let K be the subgroup of F consisting of the constant functions. Find a subgroup of F to which F/K is isomorphic.

23. Let K^* be the subgroup of F^* consisting of the nonzero constant functions. Find a subgroup of F^* to which F^*/K^* is isomorphic.

24. Let K be the subgroup of continuous functions in F. Can you find an element of F/K having order 2? Why or why not?

25. Let K^* be the subgroup of F^* consisting of the continuous functions in F^*. Can you find an element of F^*/K^* having order 2? Why or why not?

In Exercises 26 through 28, let U be the multiplicative group $\{z \in \mathbb{C} \mid |z| = 1\}$.

26. Let $z_0 \in U$. Show that $z_0U = \{z_0z \mid z \in U\}$ is a subgroup of U, and compute U/z_0U.

27. To what group we have mentioned in the text is $U/\langle -1\rangle$ isomorphic?

28. Let $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ where $n \in \mathbb{Z}^+$. To what group we have mentioned is $U/\langle\zeta_n\rangle$ isomorphic?

29. To what group mentioned in the text is the additive group $\mathbb{R}/\mathbb{Z}$ isomorphic?

30. Give an example of a group G having no elements of finite order greater than 1 and a normal subgroup $H \trianglelefteq G$, $H \neq G$, so that in G/H every element has finite order.

31. Let H and K be normal subgroups of a group G. Give an example showing that we may have $H \simeq K$ while G/H is not isomorphic to G/K.

32. Describe the center of every simple

a. abelian group

b. nonabelian group.

33. Describe the commutator subgroup of every simple

a. abelian group

b. nonabelian group.

Proof Synopsis

34. Give a one-sentence synopsis of the proof of Theorem 13.9.

35. Give at most a two-sentence synopsis of the proof of Theorem 13.20.

Theory

36. Show that if a finite group G contains a nontrivial subgroup of index 2 in G, then G is not simple.

37. Let $\phi : G \to G'$ be a group homomorphism, and let N be a normal subgroup of G. Show that $\phi[N]$ is a normal subgroup of $\phi[G]$.

38. Let $\phi : G \to G'$ be a group homomorphism, and let N' be a normal subgroup of G'. Show that $\phi^{-1}[N']$ is a normal subgroup of G.

39. Show that if G is nonabelian, then the factor group $G/Z(G)$ is not cyclic. [*Hint:* Show the equivalent contrapositive, namely, that if $G/Z(G)$ is cyclic then G is abelian (and hence $Z(G) = G$).]

40. Using Exercise 39, show that a nonabelian group G of order pq where p and q are primes has a trivial center.

41. Prove that A_n is simple for $n \geq 5$, following the steps and hints given.

a. Show A_n contains every 3-cycle if $n \geq 3$.

b. Show A_n is generated by the 3-cycles for $n \geq 3$. [*Hint:* Note that $(a, b)(c, d) = (a, c, b)(a, c, d)$ and $(a, c)(a, b) = (a, b, c)$.]

c. Let r and s be fixed elements of $\{1, 2, \cdots, n\}$ for $n \geq 3$. Show that A_n is generated by the n "special" 3-cycles of the form (r, s, i) for $1 \leq i \leq n$ [*Hint:* Show every 3-cycle is the product of "special" 3-cycles by computing

$$(r, s, i)^2, \quad (r, s, j)(r, s, i)^2, \quad (r, s, j)^2(r, s, i),$$

and

$$(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i).$$

Observe that these products give all possible types of 3-cycles.]

d. Let N be a normal subgroup of A_n for $n \geq 3$. Show that if N contains a 3-cycle, then $N = A_n$. [*Hint:* Show that $(r, s, i) \in N$ implies that $(r, s, j) \in N$ for $j = 1, 2, \cdots, n$ by computing

$$((r, s)(i, j))(r, s, i)^2((r, s)(i, j))^{-1}.]$$

e. Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Show that one of the following cases must hold, and conclude in each case that $N = A_n$.

Case I N contains a 3-cycle.

Case II N contains a product of disjoint cycles, at least one of which has length greater than 3. [*Hint:* Suppose N contains the disjoint product $\sigma = \mu(a_1, a_2, \cdots, a_r)$. Show $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it.]

Case III N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$. [*Hint:* Show $\sigma^{-1}(a_1, a_2, a_4)$ $\sigma(a_1, a_2, a_4)^{-1}$ is in N, and compute it.]

Case IV N contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where μ is a product of disjoint 2-cycles. [*Hint:* Show $\sigma^2 \in N$ and compute it.]

Case V N contains a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, where μ is a product of an even number of disjoint 2-cycles. [*Hint:* Show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it to deduce that $\alpha = (a_2, a_4)(a_1, a_3)$ is in N. Using $n \geq 5$ for the first time, find $i \neq a_1, a_2, a_3, a_4$ in $\{1, 2, \cdots, n\}$. Let $\beta = (a_1, a_3, i)$. Show that $\beta^{-1}\alpha\beta\alpha \in N$, and compute it.]

42. Let N be a normal subgroup of G and let H be any subgroup of G. Let $HN = \{hn \mid h \in H, n \in N\}$. Show that HN is a subgroup of G, and is the smallest subgroup containing both N and H.

43. With reference to the preceding exercise, let M also be a normal subgroup of G. Show that NM is again a normal subgroup of G.

44. Show that if H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. [*Hint:* Consider the commutator $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$.]

45. With reference to the three preceding exercises, let H and K be normal subgroups of a group G such that $HK = G$ and $H \cap K = \{e\}$. Prove that G is isomorphic with $H \times G$.

SECTION 14 †GROUP ACTION ON A SET

We have seen examples of how groups may *act on things*, like the group of symmetries of a triangle or of a square, the group of rotations of a cube, the general linear group acting on $\mathbb{R}^n$, and so on. In this section we give the general notion of group action and apply it to learn more about finite groups. The next section will give applications to counting.

The Notion of a Group Action

Definition 1.1 defines a binary operation $*$ on a set S to be a function mapping $S \times S$ into S. The function $*$ gives us a rule for "multiplying" an element s_1 in S and an element s_2 in S to yield an element $s_1 * s_2$ in S.

More generally, for any sets A, B, and C, we can view a map $* : A \times B \to C$ as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write $a * b = c$, or simply $ab = c$. In this section, we will be concerned with the case where X is a set, G is a group, and we have a map $* : G \times X \to X$. We shall write $*(g, x)$ as $g * x$ or gx.

14.1 Example Let $G = \mathrm{GL}(n, \mathbb{R})$ and X the set of all column vectors in $\mathbb{R}^n$. Then for any matrix $A \in G$ and vector $v \in X$, Av is a vector in X. So multiplying is an operation $* : G \times X \to X$. From linear algebra, we know that if B is also a matrix in G, then $(AB)v = A(Bv)$. Furthermore, for the identity matrix I, $Iv = v$. ▲

14.2 Example Let G be the dihedral group D_n. Then elements of D_n permute the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$. For example, $\rho(k) = k +_n 1$. Thus we have an operation $* : D_n \times \mathbb{Z}_n \to \mathbb{Z}_n$. Furthermore, if $\alpha, \gamma \in D_n$ and $k \in \mathbb{Z}_n$, then $(\alpha\gamma)(k) = \alpha(\gamma(k))$ and $\iota(k) = k$. ▲

The two previous examples share the same properties, which we formalize in Definition 14.3.

14.3 Definition Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.** ■

14.4 Example Let X be any set, and let H be a subgroup of the group S_X of all permutations of X. Then X is an H-set, where the action of $\sigma \in H$ on X is its action as an element of S_X, so that $\sigma x = \sigma(x)$ for all $x \in X$. Condition 2 is a consequence of the definition of permutation multiplication as function composition, and Condition 1 is immediate from the definition of the identity permutation as the identity function. Note that, in particular, $\{1, 2, 3, \cdots, n\}$ is an S_n-set. ▲

Our next theorem will show that for every G-set X and each $g \in G$, the map $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ is a permutation of X, and that there is a homomorphism $\phi : G \to S_X$ such that the action of G on X is essentially the Example 14.4 action of the image subgroup $H = \phi[G]$ of S_X on X. So actions of subgroups of S_X on X describe all possible group actions on X. When studying the set X, actions using subgroups of S_X suffice. However, sometimes a set X is used to study G via a group action of G on X. Thus we need the more general concept given by Definition 14.3.

† This section is a prerequisite only for Sections 15 and 17.

14.5 Theorem Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

Proof To show that σ_g is a permutation of X, we must show that σ_g is a one-to-one map of X onto itself. Suppose that $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$. Then $gx_1 = gx_2$. Consequently, $g^{-1}(gx_1) = g^{-1}(gx_2)$. Using Condition 2 in Definition 14.3, we see that $(g^{-1}g)x_1 = (g^{-1}g)x_2$, so $ex_1 = ex_2$. Condition 1 of the definition then yields $x_1 = x_2$, so σ_g is one-to-one. The two conditions of the definition show that for $x \in X$, we have $\sigma_g(g^{-1}x) = g(g^{-1})x = (gg^{-1})x = ex = x$, so σ_g maps X onto X. Thus σ_g is indeed a permutation.

To show that $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism, we must show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. We show the equality of these two permutations in S_X by showing they both carry an $x \in X$ into the same element. Using the two conditions in Definition 14.3 and the rule for function composition, we obtain

$$\begin{aligned}\phi(g_1g_2)(x) = \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x))\\ = (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) = (\phi(g_1)\phi(g_2))(x).\end{aligned}$$

Thus ϕ is a homomorphism. The stated property of ϕ follows at once since by our definitions, we have $\phi(g)(x) = \sigma_g(x) = gx$. ◆

It follows from the preceding theorem and Theorem 12.17 that if X is a G-set, then the subset of G leaving every element of X fixed is a normal subgroup N of G, and we can regard X as a G/N-set where the action of a coset gN on X is given by $(gN)x = gx$ for each $x \in X$. If $N = \{e\}$, then the identity element of G is the only element that leaves every $x \in X$ fixed; we then say that G **acts faithfully** on X. A group G is **transitive** on a G-set X if for each $x_1, x_2 \in X$, there exists $g \in G$ such that $gx_1 = x_2$.

We continue with more examples of G-sets.

14.6 Example Every group G is itself a G-set, where the action on $g_2 \in G$ by $g_1 \in G$ is given by left multiplication. That is, $*(g_1, g_2) = g_1g_2$. If H is a subgroup of G, we can also regard G as an H-set, where $*(h, g) = hg$. ▲

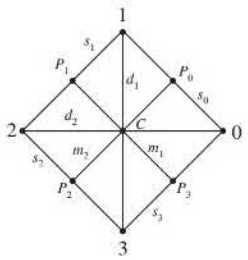
14.7 Example Let H be a subgroup of G. Then G is an H-set under conjugation where $*(h, g) = hgh^{-1}$ for $g \in G$ and $h \in H$. Condition 1 is obvious, and for Condition 2 note that

$$*(h_1h_2, g) = (h_1h_2)g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = *(h_1, *(h_2, g)).$$

We always write this action of H on G by conjugation as hgh^{-1}. The abbreviation hg described before the definition would cause terrible confusion with the group operation of G. ▲

14.8 Example Let H be a subgroup of G, and let L_H be the set of all left cosets of H. Then L_H is a G-set, where the action of $g \in G$ on the left coset xH is given by $g(xH) = (gx)H$. Observe that this action is well defined: if $yH = xH$, then $y = xh$ for some $h \in H$, and $g(yH) = (gy)H = (gxh)H = (gx)(hH) = (gx)H = g(xH)$. A series of exercises shows that every G-set is isomorphic to one that may be formed using these left coset G-sets as building blocks. (See Exercises 22 through 25.) ▲

14.9 Example Let us look closer at the the dihedral group D_4, which permutes the vertices of the square as labeled in Figure 14.10. As indicated in the figure, we label the vertices $0, 1, 2, 3$ as usual; the sides s_0, s_1, s_2, s_3; the midpoints of the sides P_0, P_1, P_2, P_3; the diagonals d_1, d_2; the lines joining opposite side midpoints m_1, m_2; and we label the intersection of the lines d_1, d_2, m_1, m_2 with C.



14.10 Figure

We can think of the set

$$X = \{0, 1, 2, 3, s_0, s_1, s_2, s_3, m_1, m_2, d_1, d_2, C, P_0, P_1, P_2, P_3\}$$

as a D_4-set in a natural way. Table 14.11 shows the action of D_4 on X. Recall that ι is the identity, ρ^k is rotation by $k\pi/2$, and μ is reflection across the line d_2. We can see from the table that $\mu\rho$ is reflection across the line m_1, $\mu\rho^2$ is reflection across the line d_1, and $\mu\rho^3$ is reflection across the line m_2. It is worthwhile to spend a little time to understand how Table 14.11 was constructed before continuing. ▲

14.11 Table

	0	1	2	3	s_0	s_1	s_2	s_3	m_1	m_2	d_1	d_2	C	P_0	P_1	P_2	P_3
ι	0	1	2	3	s_0	s_1	s_2	s_3	m_1	m_2	d_1	d_2	C	P_0	P_1	P_2	P_3
ρ	1	2	3	0	s_1	s_2	s_3	s_0	m_2	m_1	d_2	d_1	C	P_1	P_2	P_3	P_0
ρ^2	2	3	0	1	s_2	s_3	s_0	s_1	m_1	m_2	d_1	d_2	C	P_2	P_3	P_0	P_1
ρ^3	3	0	1	2	s_3	s_0	s_1	s_2	m_2	m_1	d_2	d_1	C	P_3	P_0	P_1	P_2
μ	0	3	2	1	s_3	s_2	s_1	s_0	m_2	m_1	d_1	d_2	C	P_3	P_2	P_1	P_0
$\mu\rho$	3	2	1	0	s_2	s_1	s_0	s_3	m_1	m_2	d_2	d_1	C	P_2	P_1	P_0	P_3
$\mu\rho^2$	2	1	0	3	s_1	s_0	s_3	s_2	m_2	m_1	d_1	d_2	C	P_1	P_0	P_3	P_2
$\mu\rho^3$	1	0	3	2	s_0	s_3	s_2	s_1	m_1	m_2	d_2	d_1	C	P_0	P_3	P_2	P_1

Isotropy Subgroups

Let X be a G-set. Let $x \in X$ and $g \in G$. It will be important to know when $gx = x$. We let

$$X_g = \{x \in X \mid gx = x\} \qquad \text{and} \qquad G_x = \{g \in G \mid gx = x\}.$$

14.12 Example For the D_4-set X in Example 14.9, we have

$$X_\iota = X, \qquad X_\rho = \{C\}, \qquad X_\mu = \{0, 2, d_1, d_2, C\}.$$

Also, using the same D_4 action on X,

$$G_0 = \{\iota, \mu\}, \qquad G_{s_2} = \{\iota, \mu\rho^3\}, \qquad G_{d_1} = \{\iota, \rho^2, \mu, \mu\rho^2\}.$$

We leave the computations of the other sets of the form X_σ and G_x to Exercises 1 and 2. ▲

Note that the subsets G_x given in the preceding example were, in each case, subgroups of G. This is true in general.

14.13 Theorem Let X be a G-set. Then G_x is a subgroup of G for each $x \in X$.

Proof Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x = x$ and $g_2x = x$. Consequently, $(g_1g_2)x = g_1(g_2x) = g_1x = x$, so $g_1g_2 \in G_x$, and G_x is closed under the induced operation of G. Of course, $ex = x$, so $e \in G_x$. If $g \in G_x$, then $gx = x$, so $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, and consequently $g^{-1} \in G_x$. Thus G_x is a subgroup of G. ◆

14.14 Definition Let X be a G-set and let $x \in X$. The subgroup G_x is the **isotropy subgroup of** x. ■

Orbits

For the D_4-set X of Example 14.9 with action table in Table 14.11, the elements in the subset {0, 1, 2, 3} are carried into elements of this same subset under action by D_4. Furthermore, each of the elements 0, 1, 2, and 3 is carried into all the other elements of the subset by the various elements of D_4. We proceed to show that every G-set X can be partitioned into subsets of this type.

14.15 Theorem Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Proof For each $x \in X$, we have $ex = x$, so $x \sim x$ and $\sim$ is reflexive.

Suppose $x_1 \sim x_2$, so $gx_1 = x_2$ for some $g \in G$. Then $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = ex_1 = x_1$, so $x_2 \sim x_1$, and $\sim$ is symmetric.

Finally, if $x_1 \sim x_2$ and $x_2 \sim x_3$, then $g_1x_1 = x_2$ and $g_2x_2 = x_3$ for some $g_1, g_2 \in G$. Then $(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive. ◆

14.16 Definition Let X be a G-set. Each cell in the partition of the equivalence relation described in Theorem 14.15 is an **orbit in** X **under** G. If $x \in X$, the cell containing x is the **orbit of** x. We let this cell be Gx. ■

The relationship between the orbits in X and the group structure of G lies at the heart of many applications. The following theorem gives this relationship. Recall that for a set X, we use $|X|$ for the number of elements in X, and $(G : H)$ is the index of a subgroup H in a group G.

14.17 Theorem Let X be a G-set and let $x \in X$. Then $|Gx| = (G : G_x)$. If $|G|$ is finite, then $|Gx|$ is a divisor of $|G|$.

Proof We define a one-to-one map ψ from Gx onto the collection of left cosets of G_x in G. Let $x_1 \in Gx$. Then there exists $g_1 \in G$ such that $g_1x = x_1$. We define $\psi(x_1)$ to be the left coset g_1G_x of G_x. We must show that this map ψ is well defined, independent of the choice of $g_1 \in G$ such that $g_1x = x_1$. Suppose also that $g_1'x = x_1$. Then, $g_1x = g_1'x$, so $g_1^{-1}(g_1x) = g_1^{-1}(g_1'x)$, from which we deduce $x = (g_1^{-1}g_1')x$. Therefore $g_1^{-1}g_1' \in G_x$, so $g_1' \in g_1G_x$, and $g_1G_x = g_1'G_x$. Thus the map ψ is well defined.

To show the map ψ is one-to-one, suppose $x_1, x_2 \in Gx$, and $\psi(x_1) = \psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $x_1 = g_1x, x_2 = g_2x$, and $g_2 \in g_1G_x$. Then $g_2 = g_1g$ for some $g \in G_x$, so $x_2 = g_2x = g_1(gx) = g_1x = x_1$. Thus ψ is one-to-one.

Finally, we show that each left coset of G_x in G is of the form $\psi(x_1)$ for some $x_1 \in Gx$. Let g_1G_x be a left coset. Then if $g_1x = x_1$, we have $g_1G_x = \psi(x_1)$. Thus ψ maps Gx one-to-one onto the collection of left cosets so $|Gx| = (G : G_x)$.

If $|G|$ is finite, then the equation $|G| = |G_x|(G : G_x)$ shows that $|Gx| = (G : G_x)$ is a divisor of $|G|$. ◆

14.18 Example Let X be the D_4-set in Example 14.9, with action table given by Table 14.11. With $G = D_4$, we have $G_0 = \{\iota, \mu\}$. Since $|G| = 8$, we have $|G0| = (G : G_0) = 4$. From Table 14.11, we see that $G0 = \{0, 1, 2, 3\}$, which indeed has four elements. ▲

We should remember not only the cardinality equation in Theorem 14.17 but also that the *elements of G carrying x into g_1x are precisely the elements of the left coset g_1G_x*. Namely, if $g \in G_x$, then $(g_1g)x = g_1(gx) = g_1x$. On the other hand, if $g_2x = g_1x$, then $g_1^{-1}(g_2x) = x$ so $(g_1^{-1}g_2)x = x$. Thus $g_1^{-1}g_2 \in G_x$ so $g_2 \in g_1G_x$.

Applications of G-Sets to Finite Groups

Theorem 14.17 is a very useful theorem in the study of finite groups. Suppose that X is a G-set for a finite group G and we pick out one element from each orbit of X to make the set $S = \{x_1, x_2, \ldots, x_r\}$ where we indexed the elements of X so that if $i \leq j$, then $|Gx_i| \geq |Gx_j|$. That is, we arrange by orbit size, largest first and smallest last. Every element in X is in precisely one orbit, so

$$|X| = \sum_{i=1}^{r} |Gx_i|. \tag{1}$$

We let $X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}$. That is, X_G is the set of all elements of X whose orbit size is 1. So by equation (1),

$$|X| = |X_G| + \sum_{i=1}^{s} |Gx_i| \tag{2}$$

where we simply place all the orbits with one element into X_G and we are left with s orbits each containing at least two elements. Although Equation (2) is simply saying that if you add up the sizes of all the orbits you account for all the elements of X, when coupled with Theorem 14.17, it gives some very interesting results. We give a few in the remainder of this section. In Section 17 we will use Equation 2 extensively to prove the Sylow Theorems.

For the remainder of this section, *we assume that p is a prime number.*

14.19 Theorem Let G be a group with p^n elements. If X is a G-set, then $|X| \equiv |X_G| \mod p$.

Proof Using Equation 2,

$$|X| = |X_G| + \sum_{i=1}^{s} |Gx_i|.$$

Since for each $i \leq s$, $|Gx_i| \geq 2$ and $|Gx_i| = (G : G_{x_i})$ is a divisor of $|G| = p^n$, by Theorem 14.17 p divides each term in the sum $\sum_{i=1}^{s} |Gx_i|$. Thus $|X| \equiv |X_G| \mod p$. ◆

Knowing that k divides the order of a group is not sufficient information to assume that the group has a subgroup of order k. For example, we saw that A_4 has no subgroup of order 6 and that in general, A_n has no subgroup of index 2 if $n \geq 4$. On the positive side, in Exercise 29 in Section 2, you were asked to show that if a group has an even number of elements, then it has an element of order two. Theorem 14.20 generalizes this result to show that if a prime number p divides the order of a group, then the group has an element of order p. The proof of this theorem relies on Theorem 14.19.

14.20 Theorem **(Cauchy's Theorem)** Let G be a group such that p divides the order of G. Then G has an element of order p and therefore a subgroup of order p.

Proof We let

$$X = \{(g_0, g_1, g_2, \ldots, g_{p-1}) \mid g_0, g_1, \ldots, g_{p-1} \in G \text{ and } g_0 g_1 g_2 \ldots g_{p-1} = e\}.$$

That is, X is the set of all p-tuples with entries in G so that when the entries are multiplied together (in order) their product is the identity e. Since the product is e, $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$ and given any $g_1, g_2, \ldots, g_{p-1} \in G$, by picking $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$ we have an element in X. Thus $|X| = |G|^{p-1}$ and in particular, p divides the order of X since p divides the order of G.

Suppose that $(g_0, g_1, g_2, \ldots, g_{p-1}) \in X$. Since $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$, it follows that $(g_1, g_2, \ldots g_{p-1}, g_0)$ is in X. Repeating this process, noting that $g_1 = (g_2 g_3 \ldots g_{p-1} g_0)^{-1}$ we conclude that $(g_2, g_3, g_4, \cdots, g_{p-1}, g_0, g_1) \in X$. Continuing in this manner we have that for any $k \in \mathbb{Z}_p$,

$$(g_k, g_{k+_p 1}, g_{k+_p 2}, \ldots, g_{k+_p (p-1)}) \in X.$$

We check that this gives a group action of $\mathbb{Z}_p$ on X. Let $k \in \mathbb{Z}_p$ and $(g_0, g_1, g_2, \ldots, g_{p-1}) \in X$. Then

$$k(g_0, g_1, g_2, \ldots, g_{p-1}) = (g_k, g_{k+_p 1}, g_{k+_p 2}, \ldots, g_{k+_p (p-1)}) \in X.$$

Since

$$0(g_0, g_1, g_2, \ldots, g_{p-1}) = (g_0, g_1, g_2, \ldots, g_{p-1}) \text{ and}$$

$$\begin{aligned} k(l(g_0, g_1, g_2, \ldots, g_{p-1})) &= k(g_l, g_{l+_p 1}, g_{l+_p 2}, \ldots, g_{l+_p (p-1)}) \\ &= (g_{k+_p l}, g_{k+_p l+_p 1}, \ldots, g_{k+_p l+_p (p-1)}) \\ &= (k +_p l)(g_0, g_1, g_2, \ldots, g_{p-1}) \end{aligned}$$

this is indeed a group action.

By Theorem 14.19, $0 \equiv |X| \equiv |X_{\mathbb{Z}_p}| \mod p$. The p-tuple $(e, e, e, \ldots, e)$ is in $X_{\mathbb{Z}_p}$ because rearranging the entries does not change the p-tuple. Since $X_{\mathbb{Z}_p}$ contains at least one element and p divides $|X_{\mathbb{Z}_p}|$, $X_{\mathbb{Z}_p}$ must contain at least one element other than $(e, e, e, \ldots, e)$. That element must have the form $(a, a, a, \ldots, a)$ with $a \neq e$ and $a^p = e$. So a has order p and the subgroup it generates is a subgroup of G with order p. ◆

14.21 Definition A p-group is a group such that each element in the group has order a power of p. A p-subgroup of a group is a subgroup that is a p-group. ■

14.22 Example The group D_{16} is a 2-group since the order of any element of D_{16} divides $|D_{16}| = 32$. ▲

14.23 Example Using the Fundamental Theorem of Finitely Generated Abelian Groups, a finite abelian group is a p-group if and only if it is isomorphic to

$$\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \mathbb{Z}_{p^{r_3}} \times \cdots \times \mathbb{Z}_{p^{r_n}}.$$

This is because if there were a factor of the form $\mathbb{Z}_{q^s}$ where $q \neq p$ is a prime number and $s \geq 1$, then there would be an element in G with order q^s which is not a power of p.

In Exercise 30, you are asked to show that for G a finite group, G is a p-group if and only if the order of G is a power of p.

The next theorem assures us that any finite p-group has a nontrivial normal subgroup, namely the center of the group. ▲

14.24 Theorem Let G be a finite p-group. Then the center of G, $Z(G)$, is not the trivial group.

Proof We let $X = G$ and we make X into a G-set using conjugation. That is, $*(g, a) = gag^{-1}$. Equation 2 states that $0 \equiv |X| \equiv |X_G| \mod p$. For all $g \in G$, $geg^{-1} = e$. So X_G has at

least one element, namely e. Since the number of elements in X_G must be at least p, there is an element $a \in X$ such that $a \neq e$ and $gag^{-1} = a$ for all $g \in G$. Thus $ga = ag$ for all $g \in G$, which says that $a \in Z(G)$. So $Z(G)$ is not the trivial subgroup. ◆

When studying p-groups, the fact that the center is nontrivial is often very helpful. We conclude this section with a theorem that illustrates the utility of Theorem 14.24.

14.25 Theorem Every group of order p^2 is abelian.

Proof Let G be a group of order p^2 with center $Z(G)$. By Theorem 14.24, $Z(G)$ is not the trivial group so it is either all of G or else it has order p. We wish to show that $Z(G) = G$ using proof by contradiction. So we assume that $Z(G)$ has p elements. Since $Z(G)$ is a normal subgroup of G, we can form $G/Z(G)$. The group $G/Z(G)$ also has p elements and so both $Z(G)$ and $G/Z(G)$ are cyclic. Let $\langle a \rangle = Z(G)$ and $\langle bZ(G) \rangle = G/Z(G)$. Let $x, y \in G$. Then $x = b^i a^j$ and $y = b^r a^s$ for some integers i, j, r, s since the cosets of $Z(G)$ partition G. Then

$$xy = b^i a^j b^r a^s = b^i b^r a^j a^s$$

since $\langle a \rangle$ is the center of G. So

$$xy = b^{i+r} a^{j+s} = b^r b^i a^s a^j = b^r a^s b^i a^j = yx.$$

Since every element in G commutes with every other element, $Z(G) = G$, which contradicts our assumption that the center has only p elements. So the center of G must be G, which means that G is abelian. ◆

14.26 Example Since every group of order p^2 is abelian, the Fundamental Homomorphism Theorem says that every group with p^2 elements is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. The two groups of order 4 are $\mathbb{Z}_4$ and the Klein 4-group. The two groups of order 9 are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. ▲

EXERCISES 14

Computations

In Exercises 1 through 3, let

$$X = \{0, 1, 2, 3, s_0, s_1, s_2, s_3, m_1, m_2, d_1, d_2, C, P_0, P_1, P_2, P_3\}$$

be the D_4-set of Example 14.9. Find the following, where $G = D_4$.

1. The fixed sets X_σ for each $\sigma \in D_4$.
2. The isotropy subgroups G_x for each $x \in X$, that is, $G_0, G_1, \cdots, G_{P_2}, G_{P_3}$.
3. The orbits in X under D_4.
4. Theorem 14.24 states that every p-group has nontrivial center. Find the center of D_8.
5. Find the center of D_7.
6. Let $G = X = S_3$ and make X a G-set using conjugation. That is, $*(\sigma, \tau) = \sigma\tau\sigma^{-1}$. Find all the orbits of X using this action. (Write permutations in disjoint cycle notation.)
7. Let $G = D_4$ and X be the set of all subgroups of D_4 with order two. The set X is a G-set using conjugation, $*(\sigma, H) = \sigma H \sigma^{-1}$. Find all the orbits of this group action.
8. Let $G = U = \{z \in \mathbb{C} \mid |z| = 1\}$ be the circle group. Then $X = \mathbb{C}$, the set of complex numbers, is a G-set with group action given by complex number multiplication. That is, if $z \in U$ and $w \in \mathbb{C}$, $*(z, w) = zw$. Find all the orbits of this action. Also, find X_G.

9. Let G be a group of order 3 and suppose that $|X| = 6$. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest. (Recall that the orbits partition the set X.)

10. Let G be a group of order 9 and suppose that $|X| = 10$. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest.

11. Let G be a group of order 8 and suppose that $|X| = 10$. For each possible way to make X a G-set the orbits partition X. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest.

Concepts

In Exercises 12 and 13, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

12. A group G *acts faithfully* on X if and only if $gx = x$ implies that $g = e$.

13. A group G is *transitive* on a G-set X if and only if, for some $g \in G$, gx can be every other x.

14. Let X be a G-set and let $S \subseteq X$. If $Gs \subseteq S$ for all $s \in S$, then S is a **sub-G-set.** Characterize a sub-G-set of a G-set X in terms of orbits in X under G.

15. Characterize a transitive G-set in terms of its orbits.

16. Determine whether each of the following is true or false.

- **a.** Every G-set is also a group.
- **b.** Each element of a G-set is fixed by the identity of G.
- **c.** If every element of a G-set is fixed by the same element g of G, then g must be the identity e.
- **d.** Let X be a G-set with $x_1, x_2 \in X$ and $g \in G$. If $gx_1 = gx_2$, then $x_1 = x_2$.
- **e.** Let X be a G-set with $x \in X$ and $g_1, g_2 \in G$. If $g_1x = g_2x$, then $g_1 = g_2$.
- **f.** Each orbit of a G-set X is a transitive sub-G-set. (See Exercise 14.)
- **g.** Let X be a G-set and let $H \leq G$. Then X can be regarded in a natural way as an H-set.
- **h.** With reference to (g), the orbits in X under H are the same as the orbits in X under G.
- **i.** If X is a G-set, then each element of G acts as a permutation of X.
- **j.** Let X be a G-set and let $x \in X$. If G is finite, then $|G| = |Gx| \cdot |G_x|$.

17. Let X and Y be G-sets with the *same* group G. An **isomorphism** between G-sets X and Y is a map $\phi : X \to Y$ that is one-to-one, onto Y, and satisfies $g\phi(x) = \phi(gx)$ for all $x \in X$ and $g \in G$. Two G-sets are **isomorphic** if such an isomorphism between them exists. Let X be the D_4-set of Example 14.9.

- **a.** Find two distinct orbits of X that are isomorphic sub-D_4-sets. (See Exercise 14.)
- **b.** Show that the orbits $\{0, 1, 2, 3\}$ and $\{s_0, s_1, s_2, s_3\}$ are not isomorphic sub-D_4-sets. [*Hint:* Find an element of G that acts in an essentially different fashion on the two orbits.]
- **c.** Are the orbits you gave for your answer to part (a) the only two different isomorphic sub-D_4-sets of X?

18. Let X be the D_4-set in Example 14.9.

- **a.** Does D_4 act faithfully on X?
- **b.** Find all orbits in X on which D_4 acts faithfully as a sub-D_4-set. (See Exercise 14.)

Theory

19. Let X be a G-set. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

20. Let X be a G-set and let $Y \subseteq X$. Let $G_Y = \{g \in G \mid gy = y \text{ for all } y \in Y\}$. Show G_Y is a subgroup of G, generalizing Theorem 14.13.

21. Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point other than the origin in the plane.

- **a.** Show $\mathbb{R}^2$ is a G-set.
- **b.** Describe geometrically the orbit containing P.
- **c.** Find the group G_P.

Exercises 22 through 25 show how all possible G-sets, up to isomorphism (see Exercise 17), can be formed from the group G.

22. Let $\{X_i \mid i \in I\}$ be a disjoint collection of sets, so $X_i \cap X_j = \varnothing$ for $i \neq j$. Let each X_i be a G-set for the same group G.

a. Show that $\bigcup_{i \in I} X_i$ can be viewed in a natural way as a G-set, the **union** of the G-sets X_i.

b. Show that every G-set X is the union of its orbits.

23. Let X be a transitive G-set, and let $x_0 \in X$. Show that X is isomorphic (see Exercise 17) to the G-set L of all left cosets of G_{x_0}, described in Example 14.8. [*Hint:* For $x \in X$, suppose $x = gx_0$, and define $\phi : X \to L$ by $\phi(x) = gG_{x_0}$. Be sure to show ϕ is well defined!]

24. Let X_i for $i \in I$ be G-sets for the same group G, and suppose the sets X_i are not necessarily disjoint. Let $X_i' = \{(x, i) \mid x \in X_i\}$ for each $i \in I$. Then the sets X_i' are disjoint, and each can still be regarded as a G-set in an obvious way. (The elements of X_i have simply been tagged by i to distinguish them from the elements of X_j for $i \neq j$.) The G-set $\bigcup_{i \in I} X_i'$ is the **disjoint union** of the G-sets X_i. Using Exercises 22 and 23, show that every G-set is isomorphic to a disjoint union of left coset G-sets, as described in Example 14.12.

25. The preceding exercises show that every G-set X is isomorphic to a disjoint union of left coset G-sets. The question then arises whether left coset G-sets of distinct subgroups H and K of G can themselves be isomorphic. Note that the map defined in the hint of Exercise 23 depends on the choice of x_0 as "base point." If x_0 is replaced by g_0x_0 and if $G_{x_0} \neq G_{g_0x_0}$, then the collections L_H of left cosets of $H = G_{x_0}$ and L_K of left cosets of $K = G_{g_0x_0}$ form distinct G-sets that must be isomorphic, since both L_H and L_K are isomorphic to X.

a. Let X be a transitive G-set and let $x_0 \in X$ and $g_0 \in G$. If $H = G_{x_0}$, describe $K = G_{g_0x_0}$ in terms of H and g_0.

b. Based on part (a), conjecture conditions on subgroups H and K of G such that the left coset G-sets of H and K are isomorphic.

c. Prove your conjecture in part (b).

26. Up to isomorphism, how many transitive $\mathbb{Z}_4$-sets X are there? (Use the preceding exercises.) Give an example of each isomorphism type, listing an action table of each as in Table 14.11. Take lowercase names a, b, c, and so on for the elements in the set X.

27. Repeat Exercise 26 for the group $\mathbb{Z}_6$.

28. Repeat Exercise 26 for the group S_3. List the elements of S_3 in the order ι, (1, 2, 3), (1, 3, 2), (2, 3), (1, 3), (1, 2).

29. Prove that if G is a group of order p^3, where p is a prime number, then $|Z(G)|$ is either p or p^3. Give an example where $|Z(G)| = p$ and an example where $|Z(G)| = p^3$.

30. Let p be a prime number. Prove that a finite group G is a p-group if and only if $|G| = p^n$ for some integer $n \geq 0$.

31. Let G be a group that acts on $X = \{H \mid H \leq G\}$ by conjugation. That is, $g * H = gHg^{-1}$. State and prove an equivalent condition for a subgroup $H \leq G$ to be a normal subgroup of G in terms of

a. G_H, the isotropy subgroup of H.

b. GH, the orbit of H.

SECTION 15 †APPLICATIONS OF G-SETS TO COUNTING

This section presents an application of our work with G-sets to counting. Suppose, for example, we wish to count how many distinguishable ways the six faces of a cube can be marked with from one to six dots to form a die. The standard die is marked so that when placed on a table with the 1 on the bottom and the 2 toward the front, the 6 is on top, the 3 on the left, the 4 on the right, and the 5 on the back. Of course, other ways of marking the cube to give a distinguishably different die are possible.

† This section is not used in the remainder of the text.

Let us distinguish between the faces of the cube for the moment and call them the bottom, top, left, right, front, and back. Then the bottom can have any one of six marks from one dot to six dots, the top any one of the five remaining marks, and so on. There are $6! = 720$ ways the cube faces can be marked in all. Some markings yield the same die as others, in the sense that one marking can be carried into another by a rotation of the marked cube. For example, if the standard die described above is rotated 90° counterclockwise as we look down on it, then 3 will be on the front face rather than 2, but it is the same die.

There are 24 possible positions of a cube on a table, for any one of six faces can be placed down, and then any one of four to the front, giving $6 \cdot 4 = 24$ possible positions. Any position can be achieved from any other by a rotation of the die. These rotations form a group G, which is isomorphic to a subgroup of S_8. We let X be the 720 possible ways of marking the cube and let G act on X by rotation of the cube. We consider two markings to give the same die if one can be carried into the other under action by an element of G, that is, by rotating the cube. In other words, we consider each *orbit* in X under G to correspond to a single die, and different orbits to give different dice. The determination of the number of distinguishable dice thus leads to the question of determining the number of orbits under G in a G-set X.

The following theorem gives a tool for determining the number of orbits in a G-set X under G. Recall that for each $g \in G$ we let X_g be the set of elements of X fixed by g, so that $X_g = \{x \in X \mid gx = x\}$. Recall also that for each $x \in X$, we let $G_x = \{g \in G \mid gx = x\}$, and Gx is the orbit of x under G.

15.1 Theorem **(Burnside's Formula)** Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G,

$$r \cdot |G| = \sum_{g \in G} |X_g|. \tag{1}$$

Proof We consider all pairs (g, x) where $gx = x$, and let N be the number of such pairs. For each $g \in G$ there are $|X_g|$ pairs having g as first member. Thus,

$$N = \sum_{g \in G} |X_g|. \tag{2}$$

On the other hand, for each $x \in X$ there are $|G_x|$ pairs having x as second member. Thus we also have

$$N = \sum_{x \in X} |G_x|.$$

By Theorem 14.17 we have $|Gx| = (G : G_x)$. But we know that $(G : G_x) = |G|/|G_x|$, so we obtain $|G_x| = |G|/|Gx|$. Then

$$N = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \left(\sum_{x \in X} \frac{1}{|Gx|} \right). \tag{3}$$

Now $1/|Gx|$ has the same value for all x in the same orbit, and if we let $\mathcal{O}$ be any orbit, then

$$\sum_{x \in \mathcal{O}} \frac{1}{|Gx|} = \sum_{x \in \mathcal{O}} \frac{1}{|\mathcal{O}|} = 1. \tag{4}$$

Substituting (4) in (3), we obtain

$$N = |G| \text{ (number of orbits in } X \text{ under } G) = |G| \cdot r. \tag{5}$$

Comparison of Eq. 2 and Eq. 5 gives Eq. 1. ◆

15.2 Corollary If G is a finite group and X is a finite G-set, then

$$(\text{number of orbits in } X \text{ under } G) = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Proof The proof of this corollary follows immediately from the preceding theorem. ◆

Let us continue our computation of the number of distinguishable dice as our first example.

15.3 Example We let X be the set of 720 different markings of faces of a cube using from one to six dots. Let G be the group of 24 rotations of the cube as discussed above. We saw that the number of distinguishable dice is the number of orbits in X under G. Now $|G| = 24$. For $g \in G$ where $g \neq e$, we have $|X_g| = 0$, because any rotation other than the identity element changes any one of the 720 markings into a different one. However, $|X_e| = 720$ since the identity element leaves all 720 markings fixed. Then by Corollary 15.2,

$$(\text{number of orbits}) = \frac{1}{24} \cdot 720 = 30,$$

so there are 30 distinguishable dice. ▲

Of course, the number of distinguishable dice could be counted without using the machinery of the preceding corollary, but by using elementary combinatorics as often taught in a freshman finite math course. In marking a cube to make a die, we can, by rotation if necessary, assume the face marked 1 is down. There are five choices for the top (opposite) face. By rotating the die as we look down on it, any one of the remaining four faces could be brought to the front position, so there are no different choices involved for the front face. But with respect to the number on the front face, there are $3 \cdot 2 \cdot 1$ possibilities for the remaining three side faces. Thus there are $5 \cdot 3 \cdot 2 \cdot 1 = 30$ possibilities in all.

The next two examples appear in some finite math texts and are easy to solve by elementary means. We use Corollary 15.2 so that we have more practice thinking in terms of orbits.

15.4 Example How many distinguishable ways can seven people be seated at a round table, where there is no distinguishable "head" to the table? Of course there are 7! ways to assign people to the different chairs. We take X to be the 7! possible assignments. A rotation of people achieved by asking each person to move one place to the right results in the same arrangement. Such a rotation generates a cyclic group G of order 7, which we consider to act on X in the obvious way. Again, only the identity e leaves any arrangement fixed, and it leaves all 7! arrangements fixed. By Corollary 15.2

$$(\text{number of orbits}) = \frac{1}{7} \cdot 7! = 6! = 720.$$ ▲

15.5 Example How many distinguishable necklaces (with no clasp) can be made using seven different-colored beads of the same size? Unlike the table in Example 15.4, the necklace can be turned over as well as rotated. Thus we consider the full dihedral group D_7 of order $2 \cdot 7 = 14$ as acting on the set X of 7! possibilities. Then the number of distinguishable necklaces is

$$(\text{number of orbits}) = \frac{1}{14} \cdot 7! = 360.$$ ▲

In using Corollary 15.2, we have to compute $|G|$ and $|X_g|$ for each $g \in G$. In the examples and the exercises, $|G|$ will pose no real problem. Let us give an example

where $|X_g|$ is not as trivial to compute as in the preceding examples. We will continue to assume knowledge of very elementary combinatorics.

15.6 Example Let us find the number of distinguishable ways the edges of an equilateral triangle can be painted if four different colors of paint are available, assuming only one color is used on each edge, and the same color may be used on different edges.

Of course there are $4^3 = 64$ ways of painting the edges in all, since each of the three edges may be any one of four colors. We consider X to be the set of these 64 possible painted triangles. The group G acting on X is the group of symmetries of the triangle, which is isomorphic to S_3 and which we consider to be S_3. We need to compute $|X_g|$ for each of the six elements g in S_3.

$\lvert X_\iota\rvert = 64$	Every painted triangle is fixed by i.
$\lvert X_{(1,2,3)}\rvert = 4$	To be invariant under (1,2,3) all edges must be the same color, and there are 4 possible colors.
$\lvert X_{(1,3,2)}\rvert = 4$	Same reason as for (1,2,3).
$\lvert X_{(1,2)}\rvert = 16$	The edges that are interchanged must be the same color (4 possibilities) and the other edge may also be any of the colors (times 4 possibilities).
$\lvert X_{(2,3)}\rvert = \lvert X_{(1,3)}\rvert = 16$	Same reason as for (1,2).

Then

$$\sum_{g \in S_3} |X_g| = 64 + 4 + 4 + 16 + 16 + 16 = 120.$$

Thus

$$\text{(number of orbits)} = \frac{1}{6} \cdot 120 = 20,$$

and there are 20 distinguishable painted triangles. ▲

15.7 Example We repeat Example 15.6 with the assumption that a different color is used on each edge. The number of possible ways of painting the edges is then $4 \cdot 3 \cdot 2 = 24$, and we let X be the set of 24 possible painted triangles. Again, the group acting on X can be considered to be S_3. Since all edges are a different color, we see $|X_\iota| = 24$ while $|X_g| = 0$ for $g \neq \iota$. Thus

$$\text{(number of orbits)} = \frac{1}{6} \cdot 24 = 4,$$

so there are four distinguishable triangles. ▲

We will use group actions in Section 17 to develop the Sylow Theorems, which give a tremendous amount of information about finite groups. In this section, we barely scratch the surface of how to count using Burnside's Formula. To explore this fascinating topic further, search the Internet using key words such as "cycle index" and "Pòlya's Enumeration Theorem." Given a group action on a set, the cycle index is a polynomial that can be computed by hand for small groups and by computer for larger groups. Pòlya's Enumeration Theorem then says that the number of different ways to color an object can be computed by simply substituting certain values into the polynomial. It is remarkable that counting the number of different colorings of geometric objects can be elegantly reduced to algebra!

EXERCISES 15

Computations

In each of the following exercises use Corollary 15.2, even though the answer might be obtained by more elementary methods.

1. Find the number of orbits in {1, 2, 3, 4, 5, 6, 7, 8} under the cyclic subgroup $\langle(1, 3, 5, 6)\rangle$ of S_8.

2. Find the number of orbits in {1, 2, 3, 4, 5, 6, 7, 8} under the subgroup of S_8 generated by $(1, 3)$ and $(2, 4, 7)$.

3. Find the number of distinguishable tetrahedral dice that can be made using one, two, three, and four dots on the faces of a regular tetrahedron, rather than a cube.

4. Wooden cubes of the same size are to be painted a different color on each face to make children's blocks. How many distinguishable blocks can be made if eight colors of paint are available?

5. Answer Exercise 4 if colors may be repeated on different faces at will. [*Hint:* The 24 rotations of a cube consist of the identity, 9 that leave a pair of opposite faces invariant, 8 that leave a pair of opposite vertices invariant, and 6 leaving a pair of opposite edges invariant.]

6. Each of the eight corners of a cube is to be tipped with one of four colors, each of which may be used on from one to all eight corners. Find the number of distinguishable markings possible. (See the hint in Exercise 5.)

7. Find the number of distinguishable ways the edges of a square of cardboard can be painted if six colors of paint are available and

a. no color is used more than once.

b. the same color can be used on any number of edges.

8. Consider six straight wires of equal lengths with ends soldered together to form edges of a regular tetrahedron. Either a 50-ohm or 100-ohm resistor is to be inserted in the middle of each wire. Assume there are at least six of each type of resistor available. How many essentially different wirings are possible?

9. A rectangular prism 2 ft long with 1-ft square ends is to have each of its six faces painted with one of six possible colors. How many distinguishable painted prisms are possible if

a. no color is to be repeated on different faces,

b. each color may be used on any number of faces?

PART V

Rings and Fields

SECTION 22 RINGS AND FIELDS

All our work thus far has been concerned with sets on which a single binary operation has been defined. Our years of work with the integers and real numbers show that a study of sets on which two binary operations have been defined should be of great importance. Algebraic structures of this type are introduced in this section. In one sense, this section seems more intuitive than those that precede it, for the structures studied are closely related to those we have worked with for many years. However, we will be continuing with our axiomatic approach. So, from another viewpoint this study is more complicated than group theory, for we now have two binary operations and more axioms to deal with.

Definitions and Basic Properties

The most general algebraic structure with two binary operations that we shall study is called a *ring*. As Example 22.2 following Definition 22.1 indicates, we have all worked with rings since elementary school.

22.1 Definition A **ring** $\langle R, +, \cdot \rangle$ is a set R together with two binary operations $+$ and $\cdot$, which we call *addition* and *multiplication*, defined on R such that the following axioms are satisfied:

$\mathscr{R}_1$. $\langle R, + \rangle$ is an abelian group.

$\mathscr{R}_2$. Multiplication is associative.

$\mathscr{R}_3$. For all $a, b, c \in R$, the **left distributive law**, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and the **right distributive law** $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ hold. ■

22.2 Example We are well aware that axioms $\mathscr{R}_1$, $\mathscr{R}_2$, and $\mathscr{R}_3$ for a ring hold in any subset of the complex numbers that is a group under addition and that is closed under multiplication. For example, $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, and $\langle \mathbb{C}, +, \cdot \rangle$ are rings. ▲

HISTORICAL NOTE

The theory of rings grew out of the study of two particular classes of rings, polynomial rings in n variables over the real or complex numbers (Section 27) and the "integers" of an algebraic number field. It was David Hilbert (1862–1943) who first introduced the term *ring,* in connection with the latter example, but it was not until the second decade of the twentieth century that a fully abstract definition appeared. The theory of commutative rings was given a firm axiomatic foundation by Emmy Noether (1882–1935) in her monumental paper "Ideal Theory in Rings," which appeared in 1921. A major concept of this paper is the ascending chain condition for ideals. Noether proved that in any ring in which every ascending chain of ideals has a maximal element, every ideal is finitely generated.

Emmy Noether received her doctorate from the University of Erlangen, Germany, in 1907. Hilbert invited her to Göttingen in 1915, but his efforts to secure her a paid position were blocked because of her sex. Hilbert complained, "I do not see that the sex of the candidate is an argument against her admission [to the faculty]. After all, we are a university, not a bathing establishment." Noether was, however, able to lecture under Hilbert's name. Ultimately, after the political changes accompanying the end of the First World War reached Göttingen, she was given in 1923 a paid position at the University. For the next decade, she was very influential in the development of the basic concepts of modern algebra. Along with other Jewish faculty members, however, she was forced to leave Göttingen in 1933. She spent the final two years of her life at Bryn Mawr College near Philadelphia.

It is customary to denote multiplication in a ring by juxtaposition, using ab in place of $a \cdot b$. We shall also observe the usual convention that multiplication is performed before addition in the absence of parentheses, so the left distributive law, for example, becomes

$$a(b + c) = ab + ac,$$

without the parentheses on the right side of the equation. Also, as a convenience analogous to our notation in group theory, we shall somewhat incorrectly refer to a *ring* R in place of a *ring* $\langle R, +, \cdot \rangle$, provided that no confusion will result. In particular, from now on $\mathbb{Z}$ will always be $\langle \mathbb{Z}, +, \cdot \rangle$, and $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ will also be the rings in Example 22.2. We may on occasion refer to $\langle R, + \rangle$ as *the additive group of the ring* R.

22.3 Example Let R be any ring and let $M_n(R)$ be the collection of all $n \times n$ matrices having elements of R as entries. The operations of addition and multiplication in R allow us to add and multiply matrices in the usual fashion, explained in the appendix. We can quickly check that $\langle M_n(R), + \rangle$ is an abelian group. The associativity of matrix multiplication and the two distributive laws in $M_n(R)$ are more tedious to demonstrate, but straightforward calculations indicate that they follow from the same properties in R. We will assume from now on that we know that $M_n(R)$ is a ring. In particular, we have the rings $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R})$, and $M_n(\mathbb{C})$. Note that multiplication is not a commutative operation in any of these rings for $n \geq 2$. ▲

22.4 Example Let F be the set of all functions $f : \mathbb{R} \to \mathbb{R}$. We know that $\langle F, + \rangle$ is an abelian group under the usual function addition,

$$(f + g)(x) = f(x) + g(x).$$

We define multiplication on F by

$$(fg)(x) = f(x)g(x).$$

That is, fg is the function whose value at x is $f(x)g(x)$. It is readily checked that F is a ring; we leave the demonstration to Exercise 36. We have used this juxtaposition

notation $\sigma\mu$ for the composite function $\sigma(\mu(x))$ when discussing permutation multiplication. If we were to use both function multiplication and function composition in F, we would use the notation $f \circ g$ for the composite function. However, we will use composition of functions almost exclusively with homomorphisms, which we will denote by Greek letters, and the usual product defined in this example chiefly when multiplying polynomial function's $f(x)g(x)$, so no confusion should result. ▲

22.5 Example Recall that in group theory, $n\mathbb{Z}$ is the cyclic subgroup of $\mathbb{Z}$ under addition consisting of all integer multiples of the integer n. Since $(nr)(ns) = n(nrs)$, we see that $n\mathbb{Z}$ is closed under multiplication. The associative and distributive laws that hold in $\mathbb{Z}$ then assure us that $\langle n\mathbb{Z}, +, \cdot\rangle$ is a ring. From now on in the text, we will consider $n\mathbb{Z}$ to be this ring. ▲

22.6 Example Consider the cyclic group $\langle \mathbb{Z}_n, +\rangle$. If we define for $a, b \in \mathbb{Z}_n$ the product ab as the remainder of the usual product of integers when divided by n, it can be shown that $\langle \mathbb{Z}_n, +, \cdot\rangle$ is a ring. We shall feel free to use this fact. For example, in $\mathbb{Z}_{10}$ we have $(3)(7) = 1$. This operation on $\mathbb{Z}_n$ is **multiplication modulo** n. We do not check the ring axioms here, for they will follow in Section 30 from some of the theory we develop there. From now on, $\mathbb{Z}_n$ will always be the ring $\langle \mathbb{Z}_n, +, \cdot\rangle$. ▲

22.7 Example If $R_1, R_2, \cdots, R_n$ are rings, we can form the set $R_1 \times R_2 \times \cdots \times R_n$ of all ordered n-tuples $(r_1, r_2, \cdots, r_n)$, where $r_i \in R_i$. Defining addition and multiplication of n-tuples by components (just as for groups), we see at once from the ring axioms in each component that the set of all these n-tuples forms a ring under addition and multiplication by components. The ring $R_1 \times R_2 \times \cdots \times R_n$ is the **direct product** of the rings R_i. ▲

Continuing matters of notation, we shall always let 0 be the additive identity of a ring. The additive inverse of an element a of a ring is $-a$. We shall frequently have occasion to refer to a sum

$$a + a + \cdots + a$$

having n summands. We shall let this sum be $n \cdot a$, always using the dot. However, $n \cdot a$ *is not to be interpreted as a multiplication of n and a in the ring, for the integer n may not be in the ring at all.* If $n < 0$, we let

$$n \cdot a = (-a) + (-a) + \cdots + (-a)$$

for $|n|$ summands. Finally, we define

$$0 \cdot a = 0$$

for $0 \in \mathbb{Z}$ on the left side of the equations and $0 \in R$ on the right side. Actually, the equation $0a = 0$ holds also for $0 \in R$ on both sides. The following theorem proves this and various other elementary but important facts. Note the strong use of the distributive laws in the proof of this theorem. Axiom $\mathscr{R}_1$ for a ring concerns only addition, and axiom $\mathscr{R}_2$ concerns only multiplication. This shows that in order to prove anything that gives a relationship between these two operations, we are going to have to use axiom $\mathscr{R}_3$. For example, the first thing that we will show in Theorem 22.8 is that $0a = 0$ for any element a in a ring R. Now this relation involves both addition and multiplication. The multiplication $0a$ stares us in the face, and 0 is an *additive* concept. Thus we will have to come up with an argument that uses a distributive law to prove this.

22.8 Theorem If R is a ring with additive identity 0, then for any $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

Proof For Property 1, note that by axioms $\mathscr{R}_1$ and $\mathscr{R}_2$,

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Then by the cancellation law for the additive group $\langle R, + \rangle$, we have $a0 = 0$. Likewise,

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a$$

implies that $0a = 0$. This proves Property 1.

In order to understand the proof of Property 2, we must remember that, by *definition*, $-(ab)$ is the element that when added to ab gives 0. Thus to show that $a(-b) = -(ab)$, we must show precisely that $a(-b) + ab = 0$. By the left distributive law,

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

since a0 = 0 by Property 1. Likewise,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

For Property 3, note that

$$(-a)(-b) = -(a(-b))$$

by Property 2. Again by Property 2,

$$-(a(-b)) = -(-(ab)),$$

and $-(-(ab))$ is the element that when added to $-(ab)$ gives 0. This is ab by definition of $-(ab)$ and by the uniqueness of an inverse in a group. Thus, $(-a)(-b) = ab$. ◆

Based on high school algebra it seems natural to begin a proof of Property 2 in Theorem 22.8 by writing $(-a)b = ((-1)a)b$. In Exercise 30 you will be asked to find an error in a "proof" of this sort.

It is important that you *understand* the preceding proof. The theorem allows us to use our usual rules for signs.

Homomorphisms and Isomorphisms

From our work in group theory, it is quite clear how a structure-relating map of a ring R into a ring R' should be defined.

22.9 Definition For rings R and R', a map $\phi : R \to R'$ is a **homomorphism** if the following two conditions are satisfied for all $a, b \in R$:

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$. ■

In the preceding definition, Condition 1 is the statement that ϕ is a group homomorphism mapping the abelian group $\langle R, + \rangle$ into $\langle R', + \rangle$. Condition 2 requires that ϕ relate the multiplicative structures of the rings R and R' in the same way. Since ϕ is also a group homomorphism, all the results concerning group homomorphisms are valid for the additive structure of the rings. In particular, ϕ is one-to-one if and only if its **kernel** $\text{Ker}(\phi) = \{a \in R \mid \phi(a) = 0'\}$ is just the subset $\{0\}$ of R. The homomorphism ϕ of the group $\langle R, + \rangle$ gives rise to a factor group. We expect that a ring homomorphism will give rise to a factor ring. This is indeed the case. We delay discussion of this to Section 30, where the treatment will parallel our treatment of factor groups in Section 12.

22.10 Example Let F be the ring of all functions mapping $\mathbb{R}$ into $\mathbb{R}$ defined in Example 22.4. For each $a \in \mathbb{R}$, we have the **evaluation homomorphism** $\phi_a : F \to \mathbb{R}$, where $\phi_a(f) = f(a)$ for $f \in F$. We will work a great deal with this homomorphism in the rest of this text, for finding a real solution of a polynomial equation $p(x) = 0$ amounts precisely to finding $a \in \mathbb{R}$ such that $\phi_a(p) = 0$. Much of the remainder of this text deals with solving polynomial equations. We leave the demonstration of the homomorphism properties for ϕ_a to Exercise 37. ▲

22.11 Example The map $\phi : \mathbb{Z} \to \mathbb{Z}_n$ where $\phi(a)$ is the remainder of a modulo n is a ring homomorphism for each positive integer n. We know $\phi(a + b) = \phi(a) + \phi(b)$ by group theory. To show the multiplicative property, write $a = q_1 n + r_1$ and $b = q_2 n + r_2$ according to the division algorithm. Then $ab = n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + r_1 r_2$. Thus $\phi(ab)$ is the remainder of $r_1 r_2$ when divided by n. Since $\phi(a) = r_1$ and $\phi(b) = r_2$, Example 22.6 indicates that $\phi(a)\phi(b)$ is also this same remainder, so $\phi(ab) = \phi(a)\phi(b)$. From group theory, we anticipate that the ring $\mathbb{Z}_n$ might be isomorphic to a factor ring $\mathbb{Z}/n\mathbb{Z}$. This is indeed the case; factor rings will be discussed in Section 30. ▲

We realize that in the study of any sort of mathematical structure, an idea of basic importance is the concept of two systems being *structurally identical*, that is, one being just like the other except for names. In algebra this concept is always called *isomorphism*. The concept of two things being just alike except for names of elements leads us, just as it did for groups, to the following definition.

22.12 Definition An **isomorphism** $\phi : R \to R'$ from a ring R to a ring R' is a homomorphism that is one-to-one and onto R'. The rings R and R' are then **isomorphic**. ■

From our work in group theory, we expect that isomorphism gives an equivalence relation on any collection of rings. We need to check that the multiplicative property of an isomorphism is satisfied for the inverse map $\phi^{-1} : R' \to R$ (to complete the symmetry argument). Similarly, we check that if $\mu : R' \to R''$ is also a ring isomorphism, then the multiplicative requirement holds for the composite map $\mu\phi : R \to R''$ (to complete the transitivity argument). We ask you to do this in Exercise 38.

22.13 Example As abelian groups, $\langle \mathbb{Z}, + \rangle$ and $\langle 2\mathbb{Z}, + \rangle$ are isomorphic under the map $\phi : \mathbb{Z} \to 2\mathbb{Z}$, with $\phi(x) = 2x$ for $x \in \mathbb{Z}$. Here ϕ is *not* a ring isomorphism, for $\phi(xy) = 2xy$, while $\phi(x)\phi(y) = 2x2y = 4xy$. ▲

Multiplicative Questions: Fields

Many of the rings we have mentioned, such as $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, have a multiplicative identity element 1. However, $2\mathbb{Z}$ does not have an identity element for multiplication. Note also that multiplication is not commutative in the matrix rings described in Example 22.3.

It is evident that $\{0\}$, with $0 + 0 = 0$ and $(0)(0) = 0$, gives a ring, the **zero ring.** Here 0 acts as multiplicative as well as additive identity element. By Theorem 22.8, this is the only case in which 0 could act as a multiplicative identity element, for from $0a = 0$, we can then deduce that $a = 0$. Theorem 1.15 shows that if a ring has a multiplicative identity element, it is unique. We denote a multiplicative identity element in a ring by 1.

22.14 Definition A ring in which the multiplication is commutative is a **commutative ring.** A ring with a multiplicative identity element is a **ring with unity;** the multiplicative identity element 1 is called "**unity.**" ■

In a ring with unity 1 the distributive laws show that

$$\underbrace{(1+1+\cdots+1)}_{n \text{ summands}}\underbrace{(1+1+\cdots+1)}_{m \text{ summands}} = \underbrace{(1+1+\cdots+1)}_{nm \text{ summands}},$$

that is, $(n \cdot 1)(m \cdot 1) = (nm) \cdot 1$. The next example gives an application of this observation.

22.15 Example We claim that for integers r and s where $\gcd(r, s) = 1$, the rings $\mathbb{Z}_{rs}$ and $\mathbb{Z}_r \times \mathbb{Z}_s$ are isomorphic. Additively, they are both cyclic abelian groups of order rs with generators 1 and (1, 1) respectively. Thus $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ defined by $\phi(n \cdot 1) = n \cdot (1, 1)$ is an additive group isomorphism. To check the multiplicative Condition 2 of Definition 22.9, we use the observation preceding this example for the unity (1, 1) in the ring $\mathbb{Z}_r \times \mathbb{Z}_s$, and compute.

$$\phi(nm) = (nm) \cdot (1, 1) = [n \cdot (1, 1)][m \cdot (1, 1)] = \phi(n)\phi(m). \quad \blacktriangle$$

Note that a direct product $R = R_1 \times R_2 \times \cdots \times R_n$ of rings is commutative if and and only if each ring R_i is commutative. Furthermore, R has a unity if and only if each R_i has a unity.

The set $\mathbb{R}^*$ of nonzero real numbers forms a group under multiplication. However, the nonzero integers do not form a group under multiplication since only the integers 1 and -1 have multiplicative inverses in $\mathbb{Z}$. In general, a **multiplicative inverse** of an element a in a ring R with unity $1 \neq 0$ is an element $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$. Precisely as for groups, a multiplicative inverse for an element a in R is unique, if it exists at all (see Exercise 45). Theorem 22.8 shows that it would be hopeless to have a multiplicative inverse for 0 except for the ring $\{0\}$, where $0 + 0 = 0$ and $(0)(0) = 0$, with 0 as both additive and multiplicative identity element. We are thus led to discuss the existence of multiplicative inverses for nonzero elements in a ring with nonzero unity. There is unavoidably a lot of terminology to be defined in this introductory section on rings. We are almost done.

22.16 Definition Let R be a ring with unity $1 \neq 0$. An element u in R is a **unit** of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a **division ring** (or **skew field**). A **field** is a commutative division ring. A noncommutative division ring is called a "**strictly skew field.**" ■

22.17 Example Let us find the units in $\mathbb{Z}_{14}$. Of course, 1 and $-1 = 13$ are units. Since $(3)(5) = 1$ we see that 3 and 5 are units; therefore $-3 = 11$ and $-5 = 9$ are also units. None of the remaining elements of $\mathbb{Z}_{14}$ can be units, since no multiple of 2, 4, 6, 7, 8, or 10 can be one more than a multiple of 14; they all have a common factor, either 2 or 7, with 14. Section 24 will show that the units in $\mathbb{Z}_n$ are precisely those $m \in \mathbb{Z}_n$ such that $\gcd(m, n) = 1$. ▲

22.18 Example $\mathbb{Z}$ is not a field, because 2, for example, has no multiplicative inverse, so 2 is not a unit in $\mathbb{Z}$. The only units in $\mathbb{Z}$ are 1 and -1. However, $\mathbb{Q}$ and $\mathbb{R}$ are fields. An example of a strictly skew field is given in Section 32. ▲

We have the natural concepts of a subring of a ring and a subfield of a field. A **subring of a ring** is a subset of the ring that is a ring under induced operations from the whole ring; a **subfield** is defined similarly for a subset of a field. In fact, let us say here once and for all that if we have a set, together with a certain specified type of *algebraic structure* (group, ring, field, integral domain, vector space, and so on), then any subset of this set, together with a natural induced algebraic structure *that yields an algebraic structure of the same type*, is a *substructure*. If K and L are both structures, we shall let $K \leq L$ denote that K is a substructure of L and $K < L$ denote that $K \leq L$ but $K \neq L$. Exercise 50 gives criteria for a subset S of a ring R to form a subring of R.

HISTORICAL NOTE

Although fields were implict in the early work on the solvability of equations by Abel and Galois, it was Leopold Kronecker (1823–1891) who in connection with his own work on this subject first published in 1881 a definition of what he called a "domain of rationality": "The domain of rationality $(R', R'', R''', \cdots)$ contains $\cdots$ every one of those quantities which are rational functions of the quantities $R', R'', R''', \cdots$ with integral coefficients." Kronecker, however, who insisted that any mathematical subject must be constructible in finitely many steps, did not view the domain of rationality as a complete entity, but merely as a region in which took place various operations on its elements.

Richard Dedekind (1831–1916), the inventor of the Dedekind cut definition of a real number, considered a field as a completed entity. In 1871, he published the following definition in his supplement to the second edition of Dirichlet's text on number theory: "By a field we mean any system of infinitely many real or complex numbers, which in itself is so closed and complete, that the addition, subtraction, multiplication, and division of any two numbers always produces a number of the same system." Both Kronecker and Dedekind had, however, dealt with their varying ideas of this notion as early as the 1850s in their university lectures.

A more abstract definition of a field, similar to the one in the text, was given by Heinrich Weber (1842–1913) in a paper of 1893. Weber's definition, unlike that of Dedekind, specifically included fields with finitely many elements as well as other fields, such as function fields, which were not subfields of the field of complex numbers.

Finally, be careful not to confuse our use of the words *unit* and *unity*. *Unity* is the multiplicative identity element, while a *unit* is any element having a multiplicative inverse. Thus the multiplicative identity element or unity is a unit, but not every unit is unity. For example, -1 is a unit in $\mathbb{Z}$, but -1 is not unity, that is, $-1 \neq 1$.

EXERCISES 22

Computations

In Exercises 1 through 6, compute the product in the given ring.

1. (12)(16) in $\mathbb{Z}_{24}$

2. (16)(3) in $\mathbb{Z}_{32}$

3. (11)(−4) in $\mathbb{Z}_{15}$

4. (20)(−8) in $\mathbb{Z}_{26}$

5. (2,3)(3,5) in $\mathbb{Z}_5 \times \mathbb{Z}_9$

6. (−3,5)(2,−4) in $\mathbb{Z}_4 \times \mathbb{Z}_{11}$

In Exercises 7 through 13, decide whether the indicated operations of addition and multiplication are defined (closed) on the set, and give a ring structure. If a ring is not formed, tell why this is the case. If a ring is formed, state whether the ring is commutative, whether it has unity, and whether it is a field.

7. $n\mathbb{Z}$ with the usual addition and multiplication

8. $\mathbb{Z}^+$ with the usual addition and multiplication

9. $\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components

10. $2\mathbb{Z} \times \mathbb{Z}$ with addition and multiplication by components

11. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ with the usual addition and multiplication

12. $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ with the usual addition and multiplication

13. The set of all pure imaginary complex numbers ri for $r \in \mathbb{R}$ with the usual addition and multiplication

In Exercises 14 through 19, describe all units in the given ring

14. $\mathbb{Z}$ **15.** $\mathbb{Z} \times \mathbb{Z}$ **16.** $\mathbb{Z}_5$

17. $\mathbb{Q}$ **18.** $\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}$ **19.** $\mathbb{Z}_4$

20. Consider the matrix ring $M_2(\mathbb{Z}_2)$.

a. Find the **order** of the ring, that is, the number of elements in it.

b. List all units in the ring.

21. If possible, give an example of a homomorphism $\phi : R \to R'$ where R and R' are rings with unity $1 \neq 0$ and $1' \neq 0'$, and where $\phi(1) \neq 0'$ and $\phi(1) \neq 1'$.

22. (Linear algebra) Consider the map det of $M_n(\mathbb{R})$ into $\mathbb{R}$ where $\det(A)$ is the determinant of the matrix A for $A \in M_n(\mathbb{R})$. Is det a ring homomorphism? Why or why not?

23. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z}$.

24. Describe all ring homomorphisms of $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$.

25. Describe all ring homomorphisms of $\mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$.

26. How many homomorphisms are there of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ into $\mathbb{Z}$?

27. Consider this solution of the equation $X^2 = I_3$ in the ring $M_3(\mathbb{R})$.

$X^2 = I_3$ implies $X^2 - I_3 = 0$, the zero matrix, so factoring, we have $(X - I_3)(X + I_3) = 0$

whence either $X = I_3$ or $X = -I_3$.

Is this reasoning correct? If not, point out the error, and if possible, give a counterexample to the conclusion.

28. Find all solutions of the equation $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{14}$ by factoring the quadratic polynomial. Compare with Exercise 27.

29. Find all solutions to the equations $x^2 + x - 6 = 0$ in the ring $\mathbb{Z}_{13}$ by factoring the quadratic polynomial. Why are there not the same number of solutions in Exercise 28?

30. What is wrong with the following attempt at a proof of Property 2 in Theorem 22.8?

$(-a)b = ((-1)a)b = (-1)(ab) = -(ab)$.

Concepts

In Exercises 31 and 32, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

31. A *field F* is a ring with nonzero unity such that the set of nonzero elements of F is a group under multiplication.

32. A *unit* in a ring is an element of magnitude 1.

33. Give an example of a ring having two elements a and b such that $ab = 0$ but neither a nor b is zero.

34. Give an example of a ring with unity $1 \neq 0$ that has a subring with nonzero unity $1' \neq 1$. [*Hint:* Consider a direct product, or a subring of $\mathbb{Z}_6$.]

35. Determine whether each of the following is true or false.

a. Every field is also a ring.

b. Every ring has a multiplicative identity.

c. Every ring with unity has at least two units.

d. Every ring with unity has at most two units.

e. It is possible for a subset of some field to be a ring but not a subfield, under the induced operations.

f. The distributive laws for a ring are not very important.

g. Multiplication in a field is commutative.

h. The nonzero elements of a field form a group under the multiplication in the field.

i. Addition in every ring is commutative.

j. Every element in a ring has an additive inverse.

Theory

36. Show that the multiplication defined on the set F of functions in Example 22.4 satisfies axioms $\mathscr{R}_2$ and $\mathscr{R}_3$ for a ring.

37. Show that the evaluation map ϕ_a of Example 22.10 is a ring homomorphism.

38. Complete the argument outlined after Definitions 22.12 to show that isomorphism gives an equivalence relation on a collection of rings.

39. Show that if U is the collection of all units in a ring $\langle R, +, \cdot \rangle$ with unity, then $\langle U, \cdot \rangle$ is a group. [*Warning:* Be sure to show that U is closed under multiplication.]

40. Show that $a^2 - b^2 = (a + b)(a - b)$ for all a and b in a ring R if and only if R is commutative.

41. Let $(R, +)$ be an abelian group. Show that $(R, +, \cdot)$ is a ring if we define $ab = 0$ for all $a, b \in R$.

42. Show that the rings $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic. Show that the fields $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

43. (Freshman exponentiation) Let p be a prime. Show that in the ring $\mathbb{Z}_p$ we have $(a + b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}_p$. [*Hint:* Observe that the usual binomial expansion for $(a + b)^n$ is valid in a *commutative* ring.]

44. Show that the unity element in a subfield of a field must be the unity of the whole field, in contrast to Exercise 34 for rings.

45. Show that the multiplicative inverse of a unit in a ring with unity is unique.

46. An element a of a ring R is **idempotent** if $a^2 = a$.

a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.

b. Find all idempotents in the ring $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

47. (Linear algebra) Recall that for an $m \times n$ matrix A, the *transpose* A^T of A is the matrix whose jth column is the jth row of A. Show that if A is an $m \times n$ matrix such that A^TA is invertible, then the *projection matrix* $P = A(A^TA)^{-1}A^T$ is an idempotent in the ring of $n \times n$ matrices.

48. An element a of a ring R is **nilpotent** if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that if a and b are nilpotent elements of a *commutative* ring, then $a + b$ is also nilpotent.

49. Show that a ring R has no nonzero nilpotent element if and only if 0 is the only solution of $x^2 = 0$ in R.

50. Show that a subset S of a ring R gives a subring of R if and only if the following hold:

$$0 \in S;$$
$$(a - b) \in S \text{ for all } a, b \in S;$$
$$ab \in S \text{ for all } a, b \in S.$$

51. **a.** Show that an intersection of subrings of a ring R is again a subring of R.

b. Show that an intersection of subfields of a field F is again a subfield of F.

52. Let R be a ring, and let a be a fixed element of R. Let $I_a = \{x \in R \mid ax = 0\}$. Show that I_a is a subring of R.

53. Let R be a ring, and let a be a fixed element of R. Let R_a be the subring of R that is the intersection of all subrings of R containing a (see Exercise 51). The ring R_a is the **subring of R generated by** a. Show that the abelian group $\langle R_a, + \rangle$ is generated (in the sense of Section 7) by $\{a^n \mid n \in \mathbb{Z}^+\}$.

54. (Chinese Remainder Theorem for two congruences) Let r and s be positive integers such that $\gcd(r, s) = 1$. Use the isomorphism in Example 22.15 to show that for $m, n \in \mathbb{Z}$, there exists an integer x such that $x \equiv m \pmod{r}$ and $x \equiv n \pmod{s}$.

55. **a.** State and prove the generalization of Example 22.15 for a direct product with n factors.

b. Prove the Chinese Remainder Theorem: Let $a_i, b_i \in \mathbb{Z}^+$ for $i = 1, 2, \cdots, n$ and let $\gcd(b_i, b_j) = 1$ for $i \neq j$. Then there exists $x \in \mathbb{Z}^+$ such that $x \equiv a_i \pmod{b_i}$ for $i = 1, 2, \cdots, n$.

56. Consider $\langle S, +, \cdot \rangle$, where S is a set and $+$ and $\cdot$ are binary operations on S such that

$\langle S, + \rangle$ is a group,

$\langle S^*, \cdot \rangle$ is a group where S^* consists of all elements of S except the additive identity element,

$a(b + c) = (ab) + (ac)$ and $(a + b)c = (ac) + (bc)$ for all $a, b, c \in S$.

Show that $\langle S, +, \cdot \rangle$ is a division ring. [*Hint:* Apply the distributive laws to $(1 + 1)(a + b)$ to prove the commutativity of addition.]

57. A ring R is a **Boolean ring** if $a^2 = a$ for all $a \in R$, so that every element is idempotent. Show that every Boolean ring is commutative.

58. (For students having some knowledge of the laws of set theory) For a set S, let $\mathscr{P}(S)$ be the collection of all subsets of S. Let binary operations $+$ and $\cdot$ on $\mathscr{P}(S)$ be defined by

$$A + B = (A \cup B) - (A \cap B) = \{x \mid x \in A \text{ or } x \in B \text{ but } x \notin (A \cap B)\}$$

and

$$A \cdot B = A \cap B$$

for $A, B \in \mathscr{P}(S)$.

a. Give the tables for $+$ and $\cdot$ for $\mathscr{P}(S)$, where $S = \{a, b\}$. [*Hint:* $\mathscr{P}(S)$ has four elements.]

b. Show that for *any* set S, $\langle \mathscr{P}(S), +, \cdot \rangle$ is a Boolean ring (see Exercise 57).

SECTION 23 INTEGRAL DOMAINS

While a careful treatment of polynomials is not given until Section 27, for purposes of motivation we shall make intuitive use of them in this section.

Divisors of Zero and Cancellation

One of the most important algebraic properties of our usual number system is that a product of two numbers can be 0 only if at least one of the factors is 0. We have used this fact many times in solving equations, perhaps without realizing that we were using it. Suppose, for example, we are asked to solve the equation

$$x^2 - 5x + 6 = 0.$$

The first thing we do is factor the left side:

$$x^2 - 5x + 6 = (x - 2)(x - 3).$$

Then we conclude that the only possible values for x are 2 and 3. Why? The reason is that if x is replaced by any number a, the product $(a - 2)(a - 3)$ of the resulting numbers is 0 if and only if either $a - 2 = 0$ or $a - 3 = 0$.

23.1 Example Solve the equation $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$.

Solution The factorization $x^2 - 5x + 6 = (x - 2)(x - 3)$ is still valid if we think of x as standing for any number in $\mathbb{Z}_{12}$. But in $\mathbb{Z}_{12}$, not only is $0a = a0 = 0$ for all $a \in \mathbb{Z}_{12}$, but also

$$\begin{aligned}(2)(6) = (6)(2) = (3)(4) = (4)(3) = (3)(8) = (8)(3)\\ = (4)(6) = (6)(4) = (4)(9) = (9)(4) = (6)(6) = (6)(8)\\ = (8)(6) = (6)(10) = (10)(6) = (8)(9) = (9)(8) = 0.\end{aligned}$$

We find, in fact, that our equation has not only 2 and 3 as solutions, but also 6 and 11, for $(6 - 2)(6 - 3) = (4)(3) = 0$ and $(11 - 2)(11 - 3) = (9)(8) = 0$ in $\mathbb{Z}_{12}$. ▲

These ideas are of such importance that we formalize them in a definition.

23.2 Definition If a and b are two nonzero elements of a ring R such that $ab = 0$, then a and b are **divisors of 0** (or **0 divisors**). ■

Example 23.1 shows that in $\mathbb{Z}_{12}$ the elements 2, 3, 4, 6, 8, 9, and 10 are divisors of 0. Note that these are exactly the numbers in $\mathbb{Z}_{12}$ that are not relatively prime to 12, that is, whose gcd with 12 is not 1.

If R is a ring with unity and a is a unit in R, then a is not a divisor of 0. To see this, note that if $ab = 0$, then $a^{-1}ab = 0$, so $b = 0$. Similarly, if $ba = 0$, then $baa^{-1} = 0$, so $b = 0$. Theorem 23.3 shows that in the ring $\mathbb{Z}_n$ every element is either 0, a unit, or a 0 divisor.

23.3 Theorem Let $m \in \mathbb{Z}_n$. Either $m = 0$, m is relatively prime to n, in which case m is a unit in $\mathbb{Z}_n$, or m is not relatively prime to n, in which case m is a 0 divisor in $\mathbb{Z}_n$.

Proof We first suppose that $m \neq 0$ and $\gcd(m, n) = d \neq 1$. Then, using integer multiplication

$$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n$$

is a multiple of n, so in $\mathbb{Z}_n$,

$$m\left(\frac{n}{d}\right) = 0 \in \mathbb{Z}_n.$$

Neither m nor n/d is 0 in $\mathbb{Z}_n$. Thus m is a divisor of 0.

Now suppose that $\gcd(m, n) = 1$. Then there are integers a and b such that $an + bm = 1$. By the division algorithm, there are integers q and r such that $0 \leq r \leq n - 1$ and $b = nq + r$. We can write

$$rm = (b - nq)m = bm - nqm = (1 - an) - nqm = 1 - n(a + qm).$$

So in $\mathbb{Z}_n$, $rm = mr = 1$ and m is a unit. ◆

23.4 Example Classify each nonzero element of $\mathbb{Z}_{20}$ as a unit or a 0 divisor.

Solution The greatest common divisor of m and 20 is 1 if $m = 1, 3, 7, 9, 11, 13, 17, 19$, so these are all units. For $m = 2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18$, $\gcd(m, 20) > 1$, so these are all 0 divisors. We see that

$$1 \cdot 1 = 3 \cdot 7 = 9 \cdot 9 = 11 \cdot 11 = 13 \cdot 17 = 19 \cdot 19 = 1 \in \mathbb{Z}_{20}$$

which verifies that each is a unit. We also see that

$$2 \cdot 10 = 4 \cdot 5 = 6 \cdot 10 = 8 \cdot 15 = 12 \cdot 5 = 14 \cdot 10 = 16 \cdot 5 = 18 \cdot 10 = 0 \in \mathbb{Z}_{20}$$

which verifies that each of these is a 0 divisor in $\mathbb{Z}_{20}$. ▲

23.5 Corollary If p is a prime number, then every nonzero element of $\mathbb{Z}_p$ is a unit, which means that $\mathbb{Z}_p$ is a field and it has no divisors of 0.

Proof For any $0 < m \leq p - 1$, $\gcd(m, p) = 1$. So m is a unit in $\mathbb{Z}_p$ by Theorem 23.3. ◆

The preceding corollary shows that when we consider the ring $M_n(\mathbb{Z}_p)$, we are talking about a ring of matrices over a *field*. In the typical undergraduate linear algebra course, only the field properties of the real or complex numbers are used in much of the work. Such notions as matrix reduction to solve linear systems, determinants, Cramer's rule, eigenvalues and eigenvectors, and similarity transformations to try to diagonalize a matrix are valid using matrices over any field; they depend only on the arithmetic properties of a field. Considerations of linear algebra involving notions of magnitude, such

as least-squares approximate solutions or orthonormal bases, make sense only when using fields where we have an idea of magnitude. The relation

$$p \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{p \text{ summands}} = 0$$

indicates that there can be no very natural notion of magnitude in the field $\mathbb{Z}_p$.

Another indication of the importance of the concept of 0 divisors is shown in the following theorem. Let R be a ring, and let $a, b, c \in R$. The **cancellation laws** hold in R if $ab = ac$ with $a \neq 0$ implies $b = c$, and $ba = ca$ with $a \neq 0$ implies $b = c$. These are multiplicative cancellation laws. Of course, the additive cancellation laws hold in R, since $\langle R, + \rangle$ is a group.

23.6 Theorem The cancellation laws hold in a ring R if and only if R has no divisors of 0.

Proof Let R be a ring in which the cancellation laws hold, and suppose $ab = 0$ for some $a, b \in R$. We must show that either a or b is 0. If $a \neq 0$, then $ab = a0$ implies that $b = 0$ by cancellation laws. Therefore, either $a = 0$ or $b = 0$.

Conversely, suppose that R has no divisors of 0, and suppose that $ab = ac$ with $a \neq 0$. Then

$$ab - ac = a(b - c) = 0.$$

Since $a \neq 0$, and since R has no divisors of 0, we must have $b - c = 0$, so $b = c$. A similar argument shows that $ba = ca$ with $a \neq 0$ implies $b = c$. ◆

Suppose that R is a ring with no divisors of 0. Then an equation $ax = b$, with $a \neq 0$, in R can have at most one solution x in R, for if $ax_1 = b$ and $ax_2 = b$, then $ax_1 = ax_2$, and by Theorem 23.6 $x_1 = x_2$, since R has no divisors of 0. If R has unity $1 \neq 0$ and a is a unit in R with multiplicative inverse a^{-1}, then the solution x of $ax = b$ is $a^{-1}b$. In the case that R is commutative, in particular if R is a field, it is customary to denote $a^{-1}b$ and ba^{-1} (they are equal by commutativity) by the formal quotient b/a. This quotient notation must not be used in the event that R is not commutative, for then we do not know whether b/a denotes $a^{-1}b$ or ba^{-1}. In particular, the multiplicative inverse a^{-1} of a nonzero element a of a field may be written $1/a$.

Integral Domains

The integers are really our most familiar number system. In terms of the algebraic properties we are discussing, $\mathbb{Z}$ is a commutative ring with unity and no divisors of 0. Surely this is responsible for the name that the next definition gives to such a structure.

23.7 Definition An **integral domain** D is a commutative ring with unity $1 \neq 0$ that contains no divisors of 0. ■

Thus, if the coefficients of a polynomial are from an integral domain, one can solve a polynomial equation in which the polynomial can be factored into linear factors in the usual fashion by setting each factor equal to 0.

In our hierarchy of algebraic structures, an integral domain belongs between a commutative ring with unity and a field, as we shall show. Theorem 23.6 shows that the cancellation laws for multiplication hold in an integral domain.

23.8 Example We have seen that $\mathbb{Z}$ and $\mathbb{Z}_p$ for any prime p are integral domains, but $\mathbb{Z}_n$ is not an integral domain if n is not prime. A moment of thought shows that the direct product $R \times S$ of two nonzero rings R and S is not an integral domain. Just observe that for $r \in R$ and $s \in S$ both nonzero, we have $(r, 0)(0, s) = (0, 0)$. ▲

23.9 Example Show that although $\mathbb{Z}_2$ is an integral domain, the matrix ring $M_2(\mathbb{Z}_2)$ has divisors of zero.

Solution We need only observe that

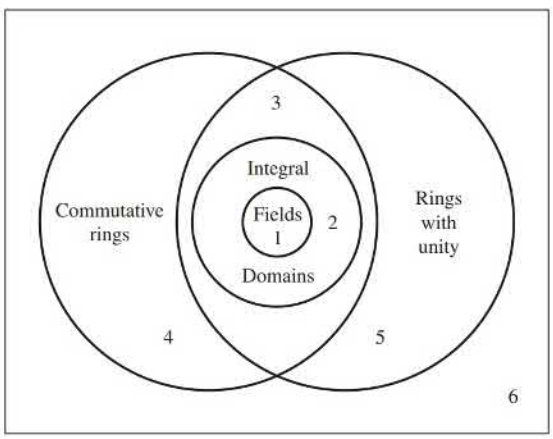
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

▲

In a field, every nonzero element is a unit. We saw that units cannot be divisors of 0, so in a field there are no divisors of 0. Since multiplication in a field is commutative, every field is an integral domain.

Figure 23.10 gives a Venn diagram view of containment for the algebraic structures having two binary operations with which we will be chiefly concerned. In Exercise 26 we ask you to redraw this figure to include strictly skew fields as well.

We have seen that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}_p$ for p a prime number are all fields. Theorem 23.3 implies that if $\mathbb{Z}_n$ is an integral domain, then $\mathbb{Z}_n$ is a field. In fact, the next theorem says that any finite integral domain is a field. The proof of this theorem is a personal favorite of both authors. It is done by counting, one of the most powerful techniques in mathematics.



23.10 Figure A collection of rings.

23.11 Theorem Every finite integral domain is a field.

Proof Let R be a finite integral domain and a a nonzero element of R. We wish to show there is an element $b \in R$ such that $ab = 1$. To this end, we define a function $f : R \to R$ by

$$f(x) = ax.$$

We first show that f is a one-to-one function. Suppose that $f(x_1) = f(x_2)$, then

$$ax_1 = ax_2$$

$$x_1 = x_2$$

since $a \neq 0$ and cancellation holds in an integral domain. Thus f is one-to-one. Since R is finite and $f : R \to R$ is one-to-one, f must also map onto R. Therefore, there is a $b \in R$ such that

$$1 = f(a) = ab = ba$$

which verifies that a is a unit. ◆

The finite condition in Theorem 23.11 is necessary since $\mathbb{Z}$ is an infinite integral domain, which is not a field. The counting argument fails in the case where the integral domain is infinite since there are one-to-one functions from an infinite set to itself that are not onto. For example, multiplication by 2 is a one-to-one function mapping $\mathbb{Z}$ to $\mathbb{Z}$, but 1 is not in the range of the function.

In Section 39 we will see that other than $\mathbb{Z}_p$ there are many finite integral domains and therefore fields.

The Characteristic of a Ring

Let R be any ring. We might ask whether there is a positive integer n such that $n \cdot a = 0$ for all $a \in R$, where $n \cdot a$ means $a + a + \cdots + a$ for n summands, as explained in Section 22. For example, the integer m has this property for the ring $\mathbb{Z}_m$.

23.12 Definition If for a ring R a positive integer n exists such that $n \cdot a = 0$ for all $a \in R$, then the least such positive integer is the **characteristic of the ring** R. If no such positive integer exists, then R is of **characteristic** 0. ■

We shall use the concept of a characteristic chiefly for fields. Exercise 35 asks us to show that the characteristic of an integral domain is either 0 or a prime p.

23.13 Example The ring $\mathbb{Z}_n$ is of characteristic n, while $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all have characteristic 0. ▲

At first glance, determination of the characteristic of a ring seems to be a tough job, unless the ring is obviously of characteristic 0. Do we have to examine *every* element a of the ring in accordance with Definition 23.12? Our final theorem of this section shows that if the ring has unity, it suffices to examine only $a = 1$.

23.14 Theorem Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{Z}^+$, then the smallest such integer n is the characteristic of R.

Proof If $n \cdot 1 \neq 0$ for all $n \in \mathbb{Z}^+$, then surely we cannot have $n \cdot a = 0$ for all $a \in R$ for some positive integer n, so by Definition 23.12, R has characteristic 0.

Suppose that n is a positive integer such that $n \cdot 1 = 0$. Then for any $a \in R$, we have

$$n \cdot a = a + a + \cdots + a = a(1 + 1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$$

Our theorem follows directly. ◆

EXERCISES 23

Computations

1. Find all solutions of the equation $x^3 - 2x^2 - 3x = 0$ in $\mathbb{Z}_{12}$.

2. Solve the equation $3x = 2$ in the field $\mathbb{Z}_7$; in the field $\mathbb{Z}_{23}$.

3. Find all solutions of the equation $x^2 + 2x + 2 = 0$ in $\mathbb{Z}_6$.

4. Find all solutions of $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$.

In Exercises 5 through 10, find the characteristic of the given ring.

5. $2\mathbb{Z}$

6. $\mathbb{Z} \times \mathbb{Z}$

7. $\mathbb{Z}_3 \times 3\mathbb{Z}$

8. $\mathbb{Z}_3 \times \mathbb{Z}_3$

9. $\mathbb{Z}_3 \times \mathbb{Z}_4$

10. $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

In Exercises 11 through 16, classify each nonzero element of the ring as a unit, a divisor of 0, or neither.

11. $\mathbb{Z}_6$ **12.** $\mathbb{Z}_8$ **13.** $\mathbb{Z}_{15}$

14. $\mathbb{Z}$ **15.** $\mathbb{Z}_3 \times \mathbb{Z}_3$ **16.** $\mathbb{Z}_4 \times \mathbb{Z}_5$

17. Let R be a commutative ring with unity of characteristic 4. Compute and simplify $(a + b)^4$ for $a, b \in R$.

18. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^9$ for $a, b \in R$.

19. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^6$ for $a, b \in R$.

20. Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.

Concepts

In Exercises 21 and 22, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

21. If $ab = 0$, then a and b are *divisors of zero*.

22. If $n \cdot a = 0$ for all elements a in a ring R, then n is the *characteristic of* R.

23. Determine whether each of the following is true or false.

- **a.** $n\mathbb{Z}$ has zero divisors if n is not prime.
- **b.** Every field is an integral domain.
- **c.** The characteristic of $n\mathbb{Z}$ is n.
- **d.** As a ring, $\mathbb{Z}$ is isomorphic to $n\mathbb{Z}$ for all $n \geq 1$.
- **e.** The cancellation law holds in any ring that is isomorphic to an integral domain.
- **f.** Every integral domain of characteristic 0 is infinite.
- **g.** The direct product of two integral domains is again an integral domain.
- **h.** A divisor of zero in a commutative ring with unity can have no multiplicative inverse.
- **i.** $n\mathbb{Z}$ is a subdomain of $\mathbb{Z}$.
- **j.** $\mathbb{Z}$ is a subfield of $\mathbb{Q}$.

24. Each of the six numbered regions in Fig. 23.10 corresponds to a certain type of a ring. Give an example of a ring in each of the six cells. For example, a ring in the region numbered 3 must be commutative (it is inside the commutative circle), have unity, but not be an integral domain.

25. (For students who have had a semester of linear algebra) Let F be a field. Give five different characterizations of the elements A of $M_n(F)$ that are divisors of 0.

26. Redraw Fig. 23.10 to include a subset corresponding to strictly skew fields.

Proof Synopsis

27. Give a one-sentence synopsis of the proof of the "if" part of Theorem 23.6.

28. Give a two-sentence synopsis of the proof of Theorem 23.11.

Theory

29. An element a of a ring R is **idempotent** if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

30. Show that an intersection of subdomains of an integral domain D is again a subdomain of D.

31. Show that a finite ring R with unity $1 \neq 0$ and no divisors of 0 is a division ring. (It is actually a field, although commutativity is not easy to prove. See Theorem 32.10.) [*Note:* In your proof, to show that $a \neq 0$ is a unit, you must show that a "left multiplicative inverse" of $a \neq 0$ in R is also a "right multiplicative inverse."]

32. Let R be a ring that contains at least two elements. Suppose for each nonzero $a \in R$, there exists a unique $b \in R$ such that $aba = a$.

a. Show that R has no divisors of 0.

b. Show that $bab = b$.

c. Show that R has unity.

d. Show that R is a division ring.

33. Show that the characteristic of a subdomain of an integral domain D is equal to the characteristic of D.

34. Show that if D is an integral domain, then $\{n \cdot 1 \mid n \in \mathbb{Z}\}$ is a subdomain of D contained in every subdomain of D.

35. Show that the characteristic of an integral domain D must be either 0 or a prime p. [*Hint:* If the characteristic of D is mn, consider $(m \cdot 1)(n \cdot 1)$ in D.]

36. This exercise shows that every ring R can be enlarged (if necessary) to a ring S with unity, having the same characteristic as R. Let $S = R \times \mathbb{Z}$ if R has characteristic 0, and $R \times \mathbb{Z}_n$ if R has characteristic n. Let addition in S be the usual addition by components, and let multiplication be defined by

$$(r_1, n_1)(r_2, n_2) = (r_1 r_2 + n_1 \cdot r_2 + n_2 \cdot r_1, n_1 n_2)$$

where $n \cdot r$ has the meaning explained in Section 22.

a. Show that S is a ring.

b. Show that S has unity.

c. Show that S and R have the same characteristic.

d. Show that the map $\phi : R \to S$ given by $\phi(r) = (r, 0)$ for $r \in R$ maps R isomorphically onto a subring of S.

SECTION 24 FERMAT'S AND EULER'S THEOREMS

Fermat's Theorem

We know that as additive groups, $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ are naturally isomorphic, with the coset $a + n\mathbb{Z}$ corresponding to a for each $a \in \mathbb{Z}_n$. Furthermore, addition of cosets in $\mathbb{Z}/n\mathbb{Z}$ may be performed by choosing any representatives, adding them in $\mathbb{Z}$, and finding the coset of $n\mathbb{Z}$ containing their sum. It is easy to see that $\mathbb{Z}/n\mathbb{Z}$ can be made into a ring by multiplying cosets in the same fashion, that is, by multiplying any chosen representatives. While we will be showing this later in a more general situation, we do this special case now. We need only show that such coset multiplication is well defined, because the associativity of multiplication and the distributive laws will follow immediately from those properties of the chosen representatives in $\mathbb{Z}$. To this end, choose representatives $a + rn$ and $b + sn$, rather than a and b, from the cosets $a + n\mathbb{Z}$ and $b + n\mathbb{Z}$. Then

$$(a + rn)(b + sn) = ab + (as + rb + rsn)n,$$

which is also an element of $ab + n\mathbb{Z}$. Thus the multiplication is well-defined, and our cosets form a ring isomorphic to the ring $\mathbb{Z}_n$.

Exercise 39 in Section 22 asks us to show that the units in a ring form a group under the multiplication operation of the ring. This is a very useful fact that we will use to provide simple proofs for both Fermat's Little Theorem and Euler's generalization. We start with Fermat's Theorem.

24.1 Theorem **(Little Theorem of Fermat)** If $a \in \mathbb{Z}$ and p is a prime not dividing a, then p divides $a^{p-1} - 1$, that is, $a^{p-1} \equiv 1 \pmod{p}$ for $a \not\equiv 0 \pmod{p}$.

Proof The ring $\mathbb{Z}_p$ is a field, which implies that all the nonzero elements are units. Thus $\langle \mathbb{Z}_p^*, \cdot \rangle$ is a group with $p - 1$ elements. Any b in the group $\mathbb{Z}_p^*$ has order a divisor of $|\mathbb{Z}_p^*| = p - 1$. Therefore

$$b^{p-1} = 1 \in \mathbb{Z}_p.$$

The rings $\mathbb{Z}_p$ and $\mathbb{Z}/p\mathbb{Z}$ are isomorphic where the element $b \in \mathbb{Z}_p$ corresponds to the coset $b + p\mathbb{Z}$. For any integer a that is not a multiple of p, $a + p\mathbb{Z} = b + p\mathbb{Z}$ for some $0 \leq b \leq p - 1$. Thus

$$(a + p\mathbb{Z})^{p-1} = (b + p\mathbb{Z})^{p-1} = 1 + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}.$$

In other words,

$$a^{p-1} \equiv 1 \pmod{p}. \quad \blacklozenge$$

24.2 Corollary If $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$ for any prime p.

Proof The corollary follows from Theorem 24.1 if $a \not\equiv 0 \pmod{p}$. If $a \equiv 0 \pmod{p}$, then both sides reduce to 0 modulo p. $\blacklozenge$

24.3 Example Let us compute the remainder of 8^{103} when divided by 13. Using Fermat's theorem, we have

$$\begin{aligned} 8^{103} &\equiv (8^{12})^8(8^7) \equiv (1^8)(8^7) \equiv 8^7 \equiv (-5)^7 \\ &\equiv (25)^3(-5) \equiv (-1)^3(-5) \equiv 5 \pmod{13}. \end{aligned}$$ $\blacktriangle$

HISTORICAL NOTE

The statement of Theorem 24.1 occurs in a letter from Pierre de Fermat (1601–1665) to Bernard Frenicle de Bessy, dated 18 October 1640. Fermat's version of the theorem was that for any prime p and any geometric progression $a, a^2, \cdots, a^t, \cdots$, there is a least number a^T of the progression such that p divides $a^T - 1$. Furthermore, T divides $p - 1$ and p also divides all numbers of the form $a^{KT} - 1$. (It is curious that Fermat failed to note the condition that p not divide a; perhaps he felt that it was obvious that the result fails in that case.)

Fermat did not in the letter or elsewhere indicate a proof of the result and, in fact, never mentioned it again. But we can infer from other parts of this correspondence that Fermat's interest in this result came from his study of perfect numbers. (A perfect number is a positive integer m that is the sum of all of its divisors less than m; for example, $6 = 1 + 2 + 3$ is a perfect number.) Euclid had shown that $2^{n-1}(2^n - 1)$ is perfect if $2^n - 1$ is prime. The question then was to find methods for determining whether $2^n - 1$ was prime. Fermat noted that $2^n - 1$ was composite if n is composite, and then derived from his theorem the result that if n is prime, the only possible divisors of $2^n - 1$ are those of the form $2kn + 1$. From this result he was able quickly to show, for example, that $2^{37} - 1$ was divisible by $223 = 2 \cdot 3 \cdot 37 + 1$.

24.4 Example Show that $2^{11,213} - 1$ is not divisible by 11.

Solution By Fermat's theorem, $2^{10} \equiv 1 \pmod{11}$, so

$$\begin{aligned} 2^{11,213} - 1 &\equiv [(2^{10})^{1,121} \cdot 2^3] - 1 \equiv [1^{1,121} \cdot 2^3] - 1 \\ &\equiv 2^3 - 1 \equiv 8 - 1 \equiv 7 \pmod{11}. \end{aligned}$$

Thus the remainder of $2^{11,213} - 1$ when divided by 11 is 7, not 0. (The number 11,213 is prime, and it has been shown that $2^{11,213} - 1$ is a prime number. Primes of the form $2^p - 1$ where p is prime are known as **Mersenne primes.**) $\blacktriangle$

24.5 Example Show that for every integer n, the number $n^{33} - n$ is divisible by 15.

Solution This seems like an incredible result. It means that 15 divides $2^{33} - 2, 3^{33} - 3, 4^{33} - 4$, etc.

Now $15 = 3 \cdot 5$, and we shall use Fermat's theorem to show that $n^{33} - n$ is divisible by both 3 and 5 for every n. Note that $n^{33} - n = n(n^{32} - 1)$.

If 3 divides n, then surely 3 divides $n(n^{32} - 1)$. If 3 does not divide n, then by Fermat's theorem, $n^2 \equiv 1 \pmod 3$ so

$$n^{32} - 1 \equiv (n^2)^{16} - 1 \equiv 1^{16} - 1 \equiv 0 \pmod 3,$$

and hence 3 divides $n^{32} - 1$.

If $n \equiv 0 \pmod 5$, then $n^{33} - n \equiv 0 \pmod 5$. If $n \not\equiv 0 \pmod 5$, then by Fermat's theorem, $n^4 \equiv 1 \pmod 5$, so

$$n^{32} - 1 \equiv (n^4)^8 - 1 \equiv 1^8 - 1 \equiv 0 \pmod 5.$$

Thus $n^{33} - n \equiv 0 \pmod 5$ for every n also. ▲

Euler's Generalization

Theorem 23.3 classifies all the elements in $\mathbb{Z}_n$ into three categories. An element k in $\mathbb{Z}_n$ is either 0, a unit if the $\gcd(n, k) = 1$, or else a divisor of 0 if $\gcd(n, k) > 1$. Exercise 39 in Section 22 shows that the units in a ring form a group under multiplication. Therefore, the set of nonzero elements in $\mathbb{Z}_n$, which are relatively prime to n, form a multiplicative group. Euler's generalization of Fermat's theorem is based on the number of units in $\mathbb{Z}_n$.

Let n be a positive integer. Let $\varphi(n)$ be defined as the number of positive integers less than or equal to n and relatively prime to n. Note that $\varphi(1) = 1$.

24.6 Example Let $n = 12$. The positive integers less than or equal to 12 and relatively prime to 12 are 1, 5, 7, and 11, so $\varphi(12) = 4$. ▲

By Theorem 23.3, $\varphi(n)$ is the number of nonzero elements of $\mathbb{Z}_n$ that are not divisors of 0. This function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is the **Euler phi-function.** We can now describe Euler's generalization of Fermat's theorem.

24.7 Theorem **(Euler's Theorem)** If a is an integer relatively prime to n, then $a^{\varphi(n)} - 1$ is divisible by n, that is, $a^{\varphi(n)} \equiv 1 \pmod n$.

Proof If a is relatively prime to n, then the coset $a + n\mathbb{Z}$ of $n\mathbb{Z}$ containing a contains an integer $b < n$ and relatively prime to n. Using the fact that multiplication of these cosets by multiplication modulo n of representatives is well-defined, we have

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod n.$$

But by Theorem 23.3, b can be viewed as an element of the multiplicative group G_n of order $\varphi(n)$ consisting of the $\varphi(n)$ elements of $\mathbb{Z}_n$ relatively prime to n. Thus

$$b^{\varphi(n)} \equiv 1 \pmod n,$$

and our theorem follows. ◆

24.8 Example Let $n = 12$. We saw in Example 24.6 that $\varphi(12) = 4$. Thus if we take any integer a relatively prime to 12, then $a^4 \equiv 1 \pmod{12}$. For example, with $a = 7$, we have $7^4 = (49)^2 = 2,401 = 12(200) + 1$, so $7^4 \equiv 1 \pmod{12}$. Of course, the easy way to compute $7^4 \pmod{12}$, without using Euler's theorem, is to compute it in $\mathbb{Z}_{12}$. In $\mathbb{Z}_{12}$, we have $7 = -5$ so

$$7^2 = (-5)^2 = (5)^2 = 1 \qquad \text{and} \qquad 7^4 = 1^2 = 1.$$ ▲

Application to $ax \equiv b \pmod{m}$

We can find all solutions of a linear congruence $ax \equiv b \pmod{m}$. We prefer to work with an equation in $\mathbb{Z}_m$ and interpret the results for congruences.

24.9 Theorem Let m be a positive integer and let $a \in \mathbb{Z}_m$ be relatively prime to m. For each $b \in \mathbb{Z}_m$, the equation $ax = b$ has a unique solution in $\mathbb{Z}_m$.

Proof By Theorem 23.3, a is a unit in $\mathbb{Z}_m$ and $s = a^{-1}b$ is certainly a solution of the equation. Multiplying both sides of $ax = b$ on the left by a^{-1}, we see this is the only solution. ◆

Interpreting this theorem for congruences, we obtain at once the following corollary.

24.10 Corollary If a and m are relatively prime integers, then for any integer b, the congruence $ax \equiv b \pmod{m}$ has as solutions all integers in precisely one residue class modulo m. ♦

Theorem 24.9 serves as a lemma for the general case.

24.11 Theorem Let m be a positive integer and let $a, b \in \mathbb{Z}_m$. Let d be the gcd of a and m. The equation $ax = b$ has a solution in $\mathbb{Z}_m$ if and only if d divides b. When d divides b, the equation has exactly d solutions in $\mathbb{Z}_m$.

Proof First we show there is no solution of $ax = b$ in $\mathbb{Z}_m$ unless d divides b. Suppose $s \in \mathbb{Z}_m$ is a solution. Then $as - b = qm$ in $\mathbb{Z}$, so $b = as - qm$. Since d divides both a and m, we see that d divides the right-hand side of the equation $b = as - qm$, and hence divides b. Thus a solution s can exist only if d divides b.

Suppose now that d does divide b. Let

$$a = a_1 d, \quad b = b_1 d, \quad \text{and} \quad m = m_1 d.$$

Then the equation $as - b = qm$ in $\mathbb{Z}$ can be rewritten as $d(a_1 s - b_1) = dqm_1$. We see that $as - b$ is a multiple of m if and only if $a_1 s - b_1$ is a multiple of m_1. Thus the solutions s of $ax = b$ in $\mathbb{Z}_m$ are precisely the elements that, read modulo m_1, yield solutions of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$. Now let $s \in \mathbb{Z}_{m_1}$ be the unique solution of $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$ given by Theorem 24.9. The numbers in $\mathbb{Z}_m$ that reduce to s modulo m_1 are precisely those that can be computed in $\mathbb{Z}_m$ as

$$s, s + m_1, s + 2m_1, s + 3m_1, \cdots, s + (d-1)m_1.$$

Thus there are exactly d solutions of the equation in $\mathbb{Z}_m$. ◆

Theorem 24.11 gives us at once this classical result on the solutions of a linear congruence.

24.12 Corollary Let d be the gcd of positive integers a and m. The congruence $ax \equiv b \pmod{m}$ has a solution if and only if d divides b. When this is the case, the solutions are the integers in exactly d distinct residue classes modulo m. ♦

Actually, our proof of Theorem 24.11 shows a bit more about the solutions of $ax \equiv b \pmod{m}$ than we stated in this corollary; namely, it shows that if any solution s is found, then the solutions are precisely all elements of the residue classes $(s + km_1) + (m\mathbb{Z})$ where $m_1 = m/d$ and k runs through the integers from 0 to $d - 1$. It also tells us that we can find such an s by finding $a_1 = a/d$ and $b_1 = b/d$, and solving $a_1 x \equiv b_1 \pmod{m_1}$. To solve this congruence, we may consider a_1 and b_1 to be replaced by their remainders modulo m_1 and solve the equation $a_1 x = b_1$ in $\mathbb{Z}_{m_1}$.

24.13 Example Find all solutions of the congruence $12x \equiv 27 \pmod{18}$.

Solution The gcd of 12 and 18 is 6, and 6 is not a divisor of 27. Thus by the preceding corollary, there are no solutions. ▲

24.14 Example Find all solutions of the congruence $15x \equiv 27 \pmod{18}$.

Solution The gcd of 15 and 18 is 3, and 3 does divide 27. Proceeding as explained before Example 24.13, we divide everything by 3 and consider the congruence $5x \equiv 9 \pmod{6}$, which amounts to solving the equation $5x = 3$ in $\mathbb{Z}_6$. Now the units in $\mathbb{Z}_6$ are 1 and 5, and 5 is clearly its own inverse in this group of units. Thus the solution in $\mathbb{Z}_6$ is $x = (5^{-1})(3) = (5)(3) = 3$. Consequently, the solutions of $15x \equiv 27 \pmod{18}$ are the integers in the three residue classes

$$3 + 18\mathbb{Z} = \{\cdots, -33, -15, 3, 21, 39, \cdots\},$$
$$9 + 18\mathbb{Z} = \{\cdots, -27, -9, 9, 27, 45, \cdots\}.$$
$$15 + 18\mathbb{Z} = \{\cdots, -21, -3, 15, 33, 51, \cdots\},$$

illustrating Corollary 24.12. Note the $d = 3$ solutions 3, 9, and 15 in $\mathbb{Z}_{18}$. All the solutions in the three displayed residue classes modulo 18 can be collected in the one residue class $3 + 6\mathbb{Z}$ modulo 6, for they came from the solution $x = 3$ of $5x = 3$ in $\mathbb{Z}_6$. ▲

EXERCISES 24

Computations

We will see later that the multiplicative group of nonzero elements of a finite field is cyclic. Illustrate this by finding a generator for this group for the given finite field.

1. $\mathbb{Z}_7$ **2.** $\mathbb{Z}_{11}$ **3.** $\mathbb{Z}_{17}$

4. Using Fermat's theorem, find the remainder of 3^{47} when it is divided by 23.

5. Use Fermat's theorem to find the remainder of 37^{49} when it is divided by 7.

6. Compute the remainder of $2^{(2^{17})} + 1$ when divided by 19. [*Hint:* You will need to compute the remainder of 2^{17} modulo 18.]

7. Make a table of values of $\varphi(n)$ for $n \leq 30$.

8. Compute $\varphi(p^2)$ where p is a prime.

9. Compute $\varphi(pq)$ where both p and q are primes.

10. Use Euler's generalization of Fermat's theorem to find the remainder of 7^{1000} when divided by 24.

In Exercises 11 through 18, describe all solutions of the given congruence, as we did in Examples 24.13 and 24.14.

11. $2x \equiv 6 \pmod{4}$ **12.** $22x \equiv 5 \pmod{15}$

13. $36x \equiv 15 \pmod{24}$ **14.** $45x \equiv 15 \pmod{24}$

15. $39x \equiv 125 \pmod{9}$ **16.** $41x \equiv 125 \pmod{9}$

17. $155x \equiv 75 \pmod{65}$ **18.** $39x \equiv 52 \pmod{130}$

19. Let p be a prime ≥ 3. Use Exercise 28 below to find the remainder of $(p-2)!$ modulo p.

20. Using Exercise 28 below, find the remainder of 34! modulo 37.

21. Using Exercise 28 below, find the remainder of 49! modulo 53.

22. Using Exercise 28 below, find the remainder of 24! modulo 29.

Concepts

23. Determine whether each of the following is true or false.

a. $a^{p-1} \equiv 1 \pmod{p}$ for all integers a and primes p.

b. $a^{p-1} \equiv 1 \pmod{p}$ for all integers a such that $a \not\equiv 0 \pmod{p}$ for a prime p.

c. $\varphi(n) \leq n$ for all $n \in \mathbb{Z}^+$.

d. $\varphi(n) \leq n - 1$ for all $n \in \mathbb{Z}^+$.

e. The units in $\mathbb{Z}_n$ are the positive integers less than n and relatively prime to n.

f. The product of two units in $\mathbb{Z}_n$ is always a unit.

g. The product of two nonunits in $\mathbb{Z}_n$ may be a unit.

h. The product of a unit and a nonunit in $\mathbb{Z}_n$ is never a unit.

i. Every congruence $ax \equiv b \pmod{p}$, where p is a prime, has a solution.

j. Let d be the gcd of positive integers a and m. If d divides b, then the congruence $ax \equiv b \pmod{m}$ has exactly d incongruent solutions.

24. Give the group multiplication table for the multiplicative group of units in $\mathbb{Z}_{12}$. To which group of order 4 is it isomorphic?

Proof Synopsis

25. Give a one-sentence synopsis of the proof of Theorem 24.1.

26. Give a one-sentence synopsis of the proof of Theorem 24.7.

Theory

27. Show that 1 and $p - 1$ are the only elements of the field $\mathbb{Z}_p$ that are their own multiplicative inverse. [*Hint:* Consider the equation $x^2 - 1 = 0$.]

28. Using Exercise 27, deduce the half of *Wilson's theorem* that states that if p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$. [The other half states that if n is an integer >1 such that $(n - 1)! \equiv -1 \pmod{n}$, then n is a prime. Just think what the remainder of $(n - 1)!$ would be modulo n if n is not a prime.]

29. Use Fermat's theorem to show that for any positive integer n, the integer $n^{37} - n$ is divisible by 383838. [*Hint:* $383838 = (37)(19)(13)(7)(3)(2)$.]

30. Referring to Exercise 29, find a number larger than 383838 that divides $n^{37} - n$ for all positive integers n.

SECTION 25 ENCRYPTION

An encryption scheme is a method to disguise a message so that it is extremely difficult for anyone other than the intended receiver to read. The sender **encrypts** the message and the receiver **decrypts** the message. One method, called cypher encryption, requires the sender to use a permutation of the letters in the alphabet to replace each letter with a different letter. The receiver then uses the inverse of the permutation to recover the original message. This method has two major weaknesses. First, both the sender and the receiver need to know the permutation, but no one else should know the permutation or else the message is not secure. It would be difficult to implement a cypher for a transaction when a company wishes to receive many orders each day, each using a different permutation that only the customer and the company know. Furthermore, cyphers are generally not difficult to crack. In fact, some newspapers carry a daily puzzle, which is essentially decrypting an encrypted message.

Researchers in the second half of the twentieth century sought a method that allows the receiver to publish public information that any sender could use to encrypt a message, yet only the receiver could decrypt it. This means that knowing how a message was encrypted is little help in decryption. This method relies on a function that is easy for computers to compute, but whose inverse is virtually impossible to compute without

more information. Functions of this type are called **trap door functions**. Most commercial online transactions are communicated with trap door functions. This allows anyone to make a secure credit card purchase with little risk of a third party gaining private information.

RSA Public and Private Keys

Euler's generalization of Fermat's Theorem is the basis of a very common trap door encryption scheme referred to as **RSA encryption**. RSA comes from the names of the three inventors of the system, Ron Rivest, Adi Shamir, and Leonard Adleman. The trap door function relies on the fact that it is easy to multiply two large prime numbers, but if you are only given their product, it is very difficult to factor the number to recover the two prime numbers. The following theorem is the key to this encryption scheme.

25.1 Theorem Let $n = pq$ where p and q are distinct prime numbers. If $a \in \mathbb{Z}$ with $\gcd(a, pq) = 1$ and $w \equiv 1 \pmod{(p-1)(q-1)}$, then $a^w \equiv a \pmod{n}$.

Proof Since $w \equiv 1 \pmod{(p-1)(q-1)}$, we can write

$$w = k(p-1)(q-1) + 1$$

for some integer k. Recall that the Euler phi-function $\phi(n)$ counts the number of positive integers less than or equal to n that are relatively prime to n. Since $n = pq$, we can compute $\phi(pq)$ by subtracting the number of integers less than n that are divisible by either p or q from $n - 1$. There are $p - 1$ multiples of q and $q - 1$ multiples of p that are less than pq. Furthermore, the least common multiple of p and q is pq since p and q are distinct primes. Thus

$$\begin{aligned}\phi(pq) &= (pq-1) - (p-1) - (q-1)\\ &= pq - p - q + 1\\ &= (p-1)(q-1).\end{aligned}$$

By Euler's Theorem (Theorem 24.7),

$$\begin{aligned}a^w &= a^{k(p-1)(q-1)+1}\\ &= a\left(a^{(p-1)(q-1)}\right)^k\\ &= a\left(a^{\phi(n)}\right)^k\\ &\equiv a(1^k)\\ &\equiv a \pmod{n}.\end{aligned}$$

◆

The RSA encryption scheme requires two sets of positive integers called the **private key** and the **public key**. The private key is known only by the person who will receive the message, and the public key is available to anyone who wishes to send a message to the receiver.

The private key consists of

- Two prime numbers p and q with $p \neq q$.
- The product $n = pq$.
- An integer $1 < r < (p-1)(q-1) - 1$ that is relatively prime to $(p-1)(q-1)$.

We know that r has an inverse in $\mathbb{Z}_{(p-1)(q-1)}$ since r is relatively prime to $(p-1)(q-1)$.

The public key consists of

- The integer s where $1 < s < (p-1)(q-1)$ and s is the inverse of r in $\mathbb{Z}_{(p-1)(q-1)}$.
- The product $n = pq$.

The public key does not include p, q, r, or $(p-1)(q-1)$. Knowing any of these numbers and the numbers in the public key would make it relatively easy to decrypt any encrypted message.

We can now give the encryption and decryption algorithms. The sender wishes to send a message to the receiver. We will assume the message is simply a number between 2 and $n-1$. To send a text message, the sender would use a standard way of representing the text as a number, such as the ASCII code. A long text would be broken up into smaller texts so that each would be coded as a number in the allowable range 2 to $n-1$ and each would be sent separately. Let $2 \leq m \leq n-1$ be the message to be sent.

Encryption Using the public key, the sender encrypts the message as a number $0 \leq y \leq n-1$ to be sent to the receiver where

$$y \equiv m^s \pmod{n}.$$

That is, the sender computes y to be the remainder when m^s is divided by n and sends y to the receiver.

Decryption Using the private key, the receiver decrypts y, the message received from the sender, by computing

$$y^r \pmod{n},$$

the remainder when y^r is divided by n. Since $rs \equiv 1 \pmod{(p-1)(q-1)}$, Theorem 25.1 says,

$$y^r = (m^s)^r = m^{rs} \equiv m \pmod{n}.$$

Thus the receiver reconstructs the original message m.

Of course, in practice the prime numbers p and q are very large. As of the writing of this book it is thought that prime numbers requiring 4096 bits or approximately 1200 digits are sufficient to make the RSA scheme secure. To illustrate how the process works, we will use small primes.

25.2 Example Let $p = 17$ and $q = 11$. The private key consists of

- $p = 17, q = 11$,
- $n = pq = 187$ and
- a number r relatively prime to $(p-1)(q-1) = 160$. For this example we take $r = 23$.

The public key consists of

- $n = 187$ and
- $s = 7$. A little calculation shows that $23 \cdot 7 = 161 = 160 + 1 \equiv 1 \pmod{160}$, which implies that $s = 7$. Since the public key consists of only n and s, $(p-1)(q-1)$ is unknown to all but the receiver. Without knowing $(p-1)(q-1)$, the value of r cannot be determined from the value of s.

Suppose the sender wishes to send the message $m = 2$ to the the receiver. The message is encrypted by computing

$$y = 2^7 \equiv 128 \pmod{187}.$$

The receiver recovers the original message by computing

$$128^{23} \equiv 2 \pmod{187}. \qquad \blacktriangle$$

In Example 25.2 some of the computations would be long and tedious without the use of a computer. For large primes p and q, it is essential to have an efficient algorithm to compute $m^s \pmod{n}$ and $y^r \pmod{n}$. This can be accomplished by using base 2. We illustrate with the following example.

25.3 Example In Example 25.2 we needed to compute $128^{23} \pmod{187}$. We can compute this value by expressing 23 in base 2, $23 = 16 + 4 + 2 + 1$, and then computing the following:

$$\begin{aligned}
128^1 &= 128 \\
128^2 &= 1638 \equiv 115 \pmod{187} \\
128^4 &= (128^2)^2 \equiv 115^2 \equiv 135 \pmod{187} \\
128^8 &= (128^4)^2 \equiv 135^2 \equiv 86 \pmod{187} \\
128^{16} &= (128^8)^2 \equiv 86^2 \equiv 103 \pmod{187},
\end{aligned}$$

Thus

$$\begin{aligned}
128^{23} &\equiv 128^{16+4+2+1} \\
&\equiv (128^{16}128^4)(128^2128^1) \\
&\equiv (103 \cdot 135)(115 \cdot 128) \\
&\equiv 67 \cdot 134 \\
&\equiv 2 \pmod{187}. \qquad \blacktriangle
\end{aligned}$$

As illustrated in the above example, this method gives a more efficient computation of $a^k \pmod{n}$.

The Euclidean algorithm is a simple and efficient way to compute the inverse of a unit in $\mathbb{Z}_{(p-1)(q-1)}$. It involves the repeated use of the division algorithm. However, we will not discuss the Euclidean algorithm here.

The reader may have noticed a potential flaw in the RSA encryption scheme. It is possible that m is a multiple of either p or q. In that case, $m^{(p-1)(q-1)} \not\equiv 1 \pmod{n}$, which means that m^{rs} may not be equivalent to m modulo n. In this case RSA encryption fails. However, when using large prime numbers the probability that the message is a multiple of p or q is extremely low. If one is concerned about this issue, the algorithm could be modified slightly to be sure that the message is smaller than both p and q.

How are the large prime numbers p and q in RSA encryption found? Basically, the process is to guess a value and check that it is prime. Unfortunately, there is no known fast method to test for primality, but it is possible to do a fast probabilistic test. One simple probabilistic test uses Fermat's Theorem (Theorem 24.1). The idea is to generate a random positive integer less than p and check if $a^{p-1} \equiv 1 \pmod{p}$. If p is prime, then $a^{p-1} \equiv 1 \pmod{p}$, so if $a^{p-1} \not\equiv 1 \pmod{p}$, then p is not a prime number and the number p is rejected. On the other hand, if $a^{p-1} \equiv 1 \pmod{p}$, then p passes the test and p could be a prime. If p passes the test, we repeat the process for a different random value of a. The probability that a composite number p is picked given that p passes the test several times is low enough to safely assume that p is prime.

EXERCISES 25

In Exercises 1 through 8, the notation is consistent with the notation used in the text for RSA encryption. It may be helpful to use a calculator or computer.

1. Let $p = 3$ and $q = 5$. Find n, and all possible pairs (r, s).

2. Let $p = 3$ and $q = 7$. Find n and all possible pairs (r, s).

3. Let $p = 3$ and $q = 11$. Find n and all possible pairs (r, s).

4. Let $p = 5$ and $q = 7$. Find n and all possible pairs (r, s).

5. Let $p = 13$, $q = 17$, and $r = 5$. Find the value of s.

6. For RSA encryption it is assumed that the message m is at least 2. Why should m not be 1?

7. The public key is $n = 143$ and $s = 37$.

a. Compute the value of y if the message is $m = 25$.

b. Find r. (Computer Algebra Systems have built-in functions to compute in $\mathbb{Z}_m$.)

c. Use your answers to parts a) and b) to decrypt y.

8. The public key is $n = 1457$ and $s = 239$.

a. Compute the value of y if the message is $m = 999$.

b. Find r. (Computer Algebra Systems have built-in functions to compute in $\mathbb{Z}_m$.)

c. Use your answers to parts a) and b) to decrypt y.

9. For $p = 257$, $q = 359$, and $r = 1493$ identify the private and public keys.