Pearson New International Edition

A First Course in Abstract Algebra
John B. Fraleigh
Seventh Edition

PEARSON

Table of Contents

Chapter 0. Sets and Relations
John B. Fraleigh **1**

Chapter 1. Groups and Subgroups
John B. Fraleigh **11**

Chapter 2. Permutations, Cosets, and Direct Products
John B. Fraleigh **75**

Chapter 3. Homomorphisms and Factor Groups
John B. Fraleigh **125**

Chapter 4. Rings and Fields
John B. Fraleigh **167**

Chapter 5. Ideals and Factor Rings
John B. Fraleigh **237**

Chapter 6. Ectension Fields
John B. Fraleigh **265**

Chapter 7. Advanced Group Theory
John B. Fraleigh **307**

Chapter 9. Factorization
John B. Fraleigh **355**

Chapter 10. Automorphisms and Galois Theory
John B. Fraleigh **381**

Appendix: Matrix Algebra
John B. Fraleigh **443**

Notations
John B. Fraleigh **449**

Index **453**

PART I

Groups and Subgroups

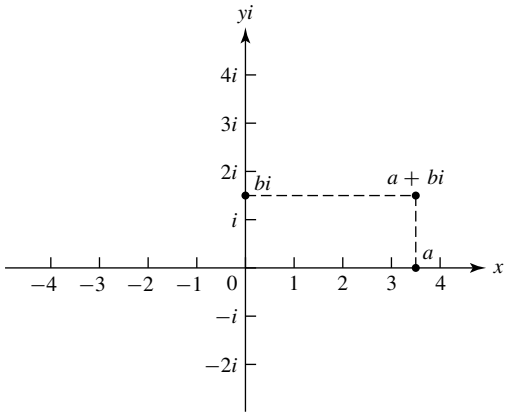
Section 1 Introduction and Examples
Section 2 Binary Operations
Section 3 Isomorphic Binary Structures
Section 4 Groups
Section 5 Subgroups
Section 6 Cyclic Groups
Section 7 Generating Sets and Cayley Digraphs

SECTION 1 Introduction and Examples

In this section, we attempt to give you a little idea of the nature of abstract algebra. We are all familiar with addition and multiplication of real numbers. Both addition and multiplication combine two numbers to obtain one number. For example, addition combines 2 and 3 to obtain 5. We consider addition and multiplication to be *binary operations*. In this text, we abstract this notion, and examine sets in which we have one or more binary operations. We think of a binary operation on a set as giving an algebra on the set, and we are interested in the *structural properties* of that algebra. To illustrate what we mean by a structural property with our familiar set $\mathbb{R}$ of real numbers, note that the equation $x + x = a$ has a solution x in $\mathbb{R}$ for each $a \in \mathbb{R}$, namely, $x = a/2$. However, the corresponding multiplicative equation $x \cdot x = a$ does not have a solution in $\mathbb{R}$ if $a < 0$. Thus, $\mathbb{R}$ with addition has a different algebraic structure than $\mathbb{R}$ with multiplication.

Sometimes two different sets with what we naturally regard as very different binary operations turn out to have the same algebraic structure. For example, we will see in Section 3 that the set $\mathbb{R}$ with addition has the same algebraic structure as the set $\mathbb{R}^+$ of positive real numbers with multiplication!

This section is designed to get you thinking about such things informally. We will make everything precise in Sections 2 and 3. We now turn to some examples. Multiplication of complex numbers of magnitude 1 provides us with several examples that will be useful and illuminating in our work. We start with a review of complex numbers and their multiplication.



1.1 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. 1.1. 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. 1.1. 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 $1, 3, \pi, -\sqrt{3}$, 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 $z_1 z_2 = z_2 z_1$, $z_1(z_2 z_3) = (z_1 z_2)z_3$ and $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$ all hold for all $z_1, z_2, z_3 \in \mathbb{C}$.

1.2 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. 1.1. We can now describe a complex number z in the polar-coordinate form

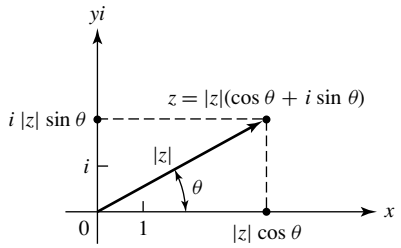
$$z = |z|(\cos\theta + i\sin\theta), \tag{4}$$

where θ is the angle measured counterclockwise from the x-axis to the vector from 0 to z, as shown in Fig. 1.3. A famous formula due to Leonard Euler states that

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

Euler's Formula

We ask you to derive Euler's formula formally from the power series expansions for e^θ, $\cos\theta$ and $\sin\theta$ in Exercise 41. Using this formula, we can express z in Eq. (4) as



1.3 Figure

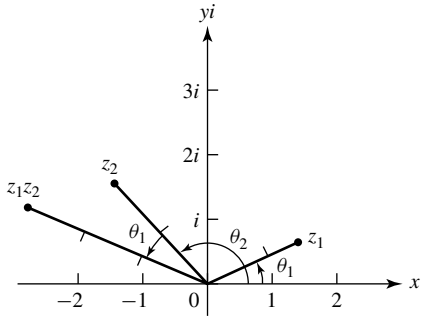
$z = |z|e^{i\theta}$. Let us set

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

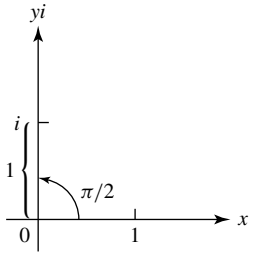
and compute their product in this form, assuming that the usual laws of exponentiation hold with complex number exponents. We obtain

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

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. 1.4. Exercise 39 indicates how this can be derived via trigonometric identities without recourse to Euler's formula and assumptions about complex exponentiation.



1.4 Figure



1.5 Figure

Note that i has polar angle $\pi/2$ and absolute value 1, as shown in Fig. 1.5. Thus i^2 has polar angle $2(\pi/2) = \pi$ and $|1 \cdot 1| = 1$, so that $i^2 = -1$.

1.6 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

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

or

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

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

Solution As in Example 1.6 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

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

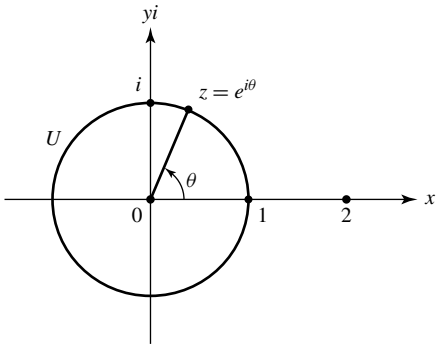
and division of $a + bi$ by nonzero $c + di$ can be performed using the device

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

Algebra on Circles

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. 1.8. The relation $|z_1 z_2| = |z_1||z_2|$ shows that the product of two numbers in U is again a number in U; we say that U is *closed* under multiplication. Thus, we can view multiplication in U as providing algebra on the circle in Fig. 1.8.

As illustrated in Fig. 1.8, we associate with each $z = \cos\theta + i \sin\theta$ in U a real number $\theta \in \mathbb{R}$ that lies in the half-open interval where $0 \le \theta < 2\pi$. This half-open interval is usually denoted by $[0, 2\pi)$, but we prefer to denote it by $\mathbb{R}_{2\pi}$ for reasons that will be apparent later. Recall that the angle associated with the product $z_1 z_2$ of two complex numbers is the sum $\theta_1 + \theta_2$ of the associated angles. Of course if $\theta_1 + \theta_2 \ge 2\pi$



1.8 Figure

then the angle in $\mathbb{R}_{2\pi}$ associated with $z_1 z_2$ is $\theta_1 + \theta_2 - 2\pi$. This gives us an **addition modulo 2π** on $\mathbb{R}_{2\pi}$. We denote this addition here by $+_{2\pi}$.

1.9 Example In $\mathbb{R}_{2\pi}$, we have $\frac{3\pi}{2} +_{2\pi} \frac{5\pi}{4} = \frac{11\pi}{4} - 2\pi = \frac{3\pi}{4}$. ▲

There was nothing special about the number 2π that enabled us to define addition on the half-open interval $\mathbb{R}_{2\pi}$. We can use any half-open interval $\mathbb{R}_c = \{x \in \mathbb{R} \mid 0 \leq x < c\}$.

1.10 Example In $\mathbb{R}_{23}$, we have $16 +_{23} 19 = 35 - 23 = 12$. In $\mathbb{R}_{8.5}$, we have $6 +_{8.5} 8 = 14 - 8.5 = 5.5$. ▲

Now complex number multiplication on the circle U where $|z| = 1$ and addition modulo 2π on $\mathbb{R}_{2\pi}$ have the same *algebraic properties*. We have the natural one-to-one correspondence $z \leftrightarrow \theta$ between $z \in U$ and $\theta \in \mathbb{R}_{2\pi}$ indicated in Fig. 1.8. Moreover, we deliberately defined $+_{2\pi}$ so that

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

isomorphism

The relation (8) shows that if we rename each $z \in U$ by its corresponding angle θ shown in Fig. 1.8, then the product of two elements in U is renamed by the sum of the angles for those two elements. Thus U with complex number multiplication and $\mathbb{R}_{2\pi}$ with addition modulo 2π must have the same algebraic properties. They differ only in the names of the elements and the names of the operations. Such a one-to-one correspondence satisfying the relation (8) is called an *isomorphism*. Names of elements and names of binary operations are not important in abstract algebra; we are interested in algebraic

properties. We illustrate what we mean by saying that the algebraic properties of U and of $\mathbb{R}_{2\pi}$ are the same.

1.11 Example In U there is exactly one element e such that $e \cdot z = z$ for all $z \in U$, namely, $e = 1$. The element 0 in $\mathbb{R}_{2\pi}$ that corresponds to $1 \in U$ is the only element e in $\mathbb{R}_{2\pi}$ such that $e +_{2\pi} x = x$ for all $x \in \mathbb{R}_{2\pi}$. ▲

1.12 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. ▲

Because our circle U has radius 1, it has circumference 2π and the radian measure of an angle θ is equal to the length of the arc the angle subtends. If we pick up our half-open interval $\mathbb{R}_{2\pi}$, put the 0 in the interval down on the 1 on the x-axis and wind it around the circle U counterclockwise, it will reach all the way back to 1. Moreover, each number in the interval will fall on the point of the circle having that number as the value of the central angle θ shown in Fig. 1.8. This shows that we could also think of addition on $\mathbb{R}_{2\pi}$ as being computed by adding lengths of subtended arcs counterclockwise, starting at $z = 1$, and subtracting 2π if the sum of the lengths is 2π or greater.

If we think of addition on a circle in terms of adding lengths of arcs from a starting point P on the circle and proceeding counterclockwise, we can use a circle of radius 2, which has circumference 4π, just as well as a circle of radius 1. We can take our half-open interval $\mathbb{R}_{4\pi}$ and wrap it around counterclockwise, starting at P; it will just cover the whole circle. Addition of arcs lengths gives us a notion of algebra for points on this circle of radius 2, which is surely isomorphic to $\mathbb{R}_{4\pi}$ with addition $+_{4\pi}$. However, if we take as the circle $|z| = 2$ in Fig. 1.8, multiplication of complex numbers does not give us an algebra on this circle. The relation $|z_1 z_2| = |z_1||z_2|$ shows that the product of two such complex numbers has absolute value 4 rather than 2. Thus complex number multiplication is *not closed* on this circle.

The preceding paragraphs indicate that a little geometry can sometimes be of help in abstract algebra. We can use geometry to convince ourselves that $\mathbb{R}_{2\pi}$ and $\mathbb{R}_{4\pi}$ are isomorphic. Simply stretch out the interval $\mathbb{R}_{2\pi}$ uniformly to cover the interval $\mathbb{R}_{4\pi}$, or, if you prefer, use a magnifier of power 2. Thus we set up the one-to-one correspondence $a \leftrightarrow 2a$ between $a \in \mathbb{R}_{2\pi}$ and $2a \in \mathbb{R}_{4\pi}$. The relation (8) for isomorphism becomes

$$\text{if} \quad a \leftrightarrow 2a \quad \text{and} \quad b \leftrightarrow 2b \quad \text{then} \quad (a +_{2\pi} b) \leftrightarrow (2a +_{4\pi} 2b). \tag{9}$$

isomorphism

This is obvious if $a + b \leq 2\pi$. If $a + b = 2\pi + c$, then $2a + 2b = 4\pi + 2c$, and the final pairing in the displayed relation becomes $c \leftrightarrow 2c$, which is true.

1.13 Example $x +_{4\pi} x +_{4\pi} x +_{4\pi} x = 0$ in $\mathbb{R}_{4\pi}$ has exactly four solutions, namely, $0, \pi, 2\pi$, and 3π, which are two times the solutions found for the analogous equation in $\mathbb{R}_{2\pi}$ in Example 1.12. ▲

There is nothing special about the numbers 2π and 4π in the previous argument. Surely, $\mathbb{R}_c$ with $+_c$ is isomorphic to $\mathbb{R}_d$ with $+_d$ for all $c, d \in \mathbb{R}^+$. We need only pair $x \in \mathbb{R}_c$ with $(d/c)x \in \mathbb{R}_d$.

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.** Using the technique of Examples 1.6 and 1.7, we see that the elements of this set are the numbers

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

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

$$1 = \zeta^0, \zeta^1, \zeta^2, \zeta^3, \cdots, \zeta^{n-1}. \tag{10}$$

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 $\mathbb{R}_n$.

Let $\mathbb{Z}_n = \{0, 1, 2, 3, \cdots, n-1\}$. We see that $\mathbb{Z}_n \subset \mathbb{R}_n$ and clearly addition modulo n is closed on $\mathbb{Z}_n$.

1.14 Example The solution of the equation $x + 5 = 3$ in $\mathbb{Z}_8$ is $x = 6$, because $5 +_8 6 = 11 - 8 = 3$. ▲

If we rename each of the n^{th} roots of unity in (10) by its exponent, we use for names all the elements of $\mathbb{Z}_n$. This gives a one-to-one correspondence between U_n and $\mathbb{Z}_n$. Clearly,

$$\text{if} \quad \zeta^i \leftrightarrow i \quad \text{and} \quad \zeta^j \leftrightarrow j, \quad \text{then} \quad (\zeta^i \cdot \zeta^j) \leftrightarrow (i +_n j). \tag{11}$$

isomorphism

Thus U_n with complex number multiplication and $\mathbb{Z}_n$ with addition $+_n$ have the same algebraic properties.

1.15 Example It can be shown that there is an isomorphism of U_8 with $\mathbb{Z}_8$ in which $\zeta = e^{i2\pi/8} \leftrightarrow 5$. Under this isomorphism, we must then have $\zeta^2 = \zeta \cdot \zeta \leftrightarrow 5 +_8 5 = 2$. ▲

Exercise 35 asks you to continue the computation in Example 1.15, finding the elements of $\mathbb{Z}_8$ to which each of the remaining six elements of U_8 correspond.

EXERCISES 1

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^{23}

4. $(-i)^{35}$ **5.** $(4 - i)(5 + 3i)$ **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 $|3 - 4i|$. **11.** Find $|6 + 4i|$.

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.** $z^3 = -8$ **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.** $8 +_{10} 6$ **24.** $20.5 +_{25} 19.3$

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. $x +_{15} 7 = 3$ in $\mathbb{Z}_{15}$ **30.** $x +_{2\pi} \frac{3\pi}{2} = \frac{3\pi}{4}$ in $\mathbb{R}_{2\pi}$

31. $x +_7 x = 3$ in $\mathbb{Z}_7$ **32.** $x +_7 x +_7 x = 5$ in $\mathbb{Z}_7$

33. $x +_{12} x = 2$ in $\mathbb{Z}_{12}$ **34.** $x +_4 x +_4 x +_4 x = 0$ in $\mathbb{Z}_4$

35. Example 1.15 asserts that 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.

36. 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.

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

38. 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 $e^{ia}e^{ib}$.

39. 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 38 to derive $z_1 z_2 = |z_1||z_2|[\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)]$.

40. **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 32.)

41. 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.

SECTION 2 Binary Operations

Suppose that we are visitors to a strange civilization in a strange world and are observing one of the creatures of this world drilling a class of fellow creatures in addition of numbers. Suppose also that we have not been told that the class is learning to add, but were just placed as observers in the room where this was going on. We are asked to give a report on exactly what happens. The teacher makes noises that sound to us approximately like *gloop, poyt.* The class responds with *bimt*. The teacher then gives *ompt, gaft,* and the class responds with *poyt*. What are they doing? We cannot report that they are adding numbers, for we do not even know that the sounds are representing numbers. Of course, we do realize that there is communication going on. All we can say with any certainty is that these creatures know some rule, so that when certain pairs of things are designated in their language, one after another, like *gloop, poyt,* they are able to agree on a response, *bimt*. This same procedure goes on in addition drill in our first grade classes where a teacher may say *four, seven,* and the class responds with *eleven*.

In our attempt to analyze addition and multiplication of numbers, we are thus led to the idea that addition is basically just a rule that people learn, enabling them to associate, with two numbers in a given order, some number as the answer. Multiplication is also such a rule, but a different rule. Note finally that in playing this game with students, teachers have to be a little careful of what two things they give to the class. If a first grade teacher suddenly inserts *ten, sky,* the class will be very confused. The rule is only defined for pairs of things from some specified set.

Definitions and Examples

As mathematicians, let us attempt to collect the core of these basic ideas in a useful definition, generalizing the notions of addition and multiplication of numbers. As we remarked in Section 0, we do not attempt to define a set. However, we can attempt to be somewhat mathematically precise, and we describe our generalizations as *functions* (see Definition 0.10 and Example 0.11) rather than as *rules*. Recall from Definition 0.4 that for any set S, the set $S \times S$ consists of all ordered pairs (a, b) for elements a and b of S.

2.1 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. We proceed with examples.

2.2 Example Our usual addition $+$ is a binary operation on the set $\mathbb{R}$. Our usual multiplication $\cdot$ is a different binary 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 a binary operation on a set S to be defined for *every* ordered pair (a, b) of elements from S.

2.3 Example Let $M(\mathbb{R})$ be the set of all matrices[†] with real entries. The usual matrix addition $+$ is *not* a binary 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 a binary operation on S provides a binary operation on a subset H of S also. We make a formal definition.

2.4 Definition Let $*$ be a binary 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 binary operation on H given by restricting $*$ to H is the **induced operation** of $*$ on H. ■

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

2.5 Example Our usual addition $+$ on the set $\mathbb{R}$ of real numbers does not induce a binary 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 have trouble here. Be sure you understand the next example.

2.6 Example Let $+$ and $\cdot$ be the usual binary 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. ▲

[†] 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.

2.7 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 binary operations $+$, $-$, $\cdot$, and $\circ$ on F. Namely, for each ordered pair (f, g) of functions in F, we define for each $x \in \mathbb{R}$

$$\begin{array}{ll} f + g \text{ by } (f + g)(x) = f(x) + g(x) & \text{addition,} \\ f - g \text{ by } (f - g)(x) = f(x) - g(x) & \text{subtraction,} \\ f \cdot g \text{ by } (f \cdot g)(x) = f(x)g(x) & \text{multiplication,} \end{array}$$

and

$$f \circ g \text{ by } (f \circ g)(x) = f(g(x)) \qquad \text{composition.}$$

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 binary 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 emphasize this concept of *abstraction* from the familiar, we should illustrate these structural concepts with unfamiliar examples. We presented the binary operations of complex number multiplication on U and U_n, addition $+_n$ on $\mathbb{Z}_n$, and addition $+_c$ on $\mathbb{R}_c$ in Section 1.

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.

2.8 Example On $\mathbb{Z}^+$, we define a binary 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 $3 * 3 = 3$. ▲

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

2.10 Example On $\mathbb{Z}^+$, we define a binary operation $*''$ by $a *'' b = (a * b) + 2$, where $*$ is defined in Example 2.8. Thus $4 *'' 7 = 6; 25 *'' 9 = 11$; and $6 *'' 6 = 8$. ▲

It may seem that these examples are of no importance, but consider for a moment. Suppose we go into a store to buy a large, delicious chocolate bar. Suppose we see two identical bars side by side, the wrapper of one stamped \$1.67 and the wrapper of the other stamped \$1.79. Of course we pick up the one stamped \$1.67. Our knowledge of which one we want depends on the fact that at some time we learned the binary operation $*$ of Example 2.8. It is a *very important operation*. Likewise, the binary operation $*'$ of Example 2.9 is defined using our ability to distinguish order. Think what a problem we would have if we tried to put on our shoes first, and then our socks! Thus we should not be hasty about dismissing some binary operation as being of little significance. Of course, our usual operations of addition and multiplication of numbers have a practical importance well known to us.

Examples 2.8 and 2.9 were chosen to demonstrate that a binary operation may or may not depend on the order of the given pair. Thus in Example 2.8, $a * b = b * a$ for all $a, b \in \mathbb{Z}^+$, and in Example 2.9 this is not the case, for $5 *' 7 = 5$ but $7 *' 5 = 7$.

2.11 Definition A binary 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 2.8, $(2 * 5) * 9$ 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 2.10,

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

while

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

Thus $(a *'' b) *'' c$ need not equal $a *'' (b *'' c)$, and an expression $a *'' b *'' c$ may be ambiguous.

2.12 Definition A binary 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 2.7. 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 this composition is always associative whenever it is defined.

2.13 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 2.13 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 binary 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 2.13.

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.

2.14 Example Table 2.15 defines the binary operation $*$ on $S = \{a, b, c\}$ by the following rule:

(ith *entry on the left*) $*$ (jth *entry on the top*)
= (*entry in the* ith *row and* jth *column of the table body*).

2.15 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.*

2.16 Example Complete Table 2.17 so that $*$ is a commutative binary operation on the set $S = \{a, b, c, d\}$.

Solution From Table 2.17, 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 2.18 from the square defining $b * a$. We obtain the rest of Table 2.18 in this fashion to give our solution. ▲

2.17 Table

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

2.18 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

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** $*$.

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

2.19 Example On $\mathbb{Q}$, let $a * b = a/b$. Here $*$ is *not everywhere defined* on $\mathbb{Q}$, for no rational number is assigned by this rule to the pair (2, 0). ▲

2.20 Example On $\mathbb{Q}^+$, let $a * b = a/b$. Here both Conditions 1 and 2 are satisfied, and $*$ is a binary operation on $\mathbb{Q}^+$. ▲

2.21 Example On $\mathbb{Z}^+$, let $a * b = a/b$. Here Condition 2 fails, for $1 * 3$ is not in $\mathbb{Z}^+$. Thus $*$ is not a binary operation on $\mathbb{Z}^+$, since $\mathbb{Z}^+$ is *not closed under* $*$. ▲

2.22 Example Let F be the set of all real-valued functions with domain $\mathbb{R}$ as in Example 2.7. 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 were to be 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 $h \notin F$. ▲

2.23 Example Let F be as in Example 2.22 and let $f * g = h$, where h is the function greater than both f and g. This "definition" is completely worthless. 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*. ▲

2.24 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. ▲

2.25 Example Let S be as in Example 2.24 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 2

Computations

Exercises 1 through 4 concern the binary operation $*$ defined on $S = \{a, b, c, d, e\}$ by means of Table 2.26.

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 computations whether $*$ is associative?

3. Compute $(b * d) * c$ and $b * (d * c)$. Can you say on the basis of this computation whether $*$ is associative?

2.26 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

2.27 Table

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

2.28 Table

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

4. Is $*$ commutative? Why?

5. Complete Table 2.27 so as to define a commutative binary operation $*$ on $S = \{a, b, c, d\}$.

6. Table 2.28 can be completed to define an associative binary operation $*$ on $S = \{a, b, c, d\}$. Assume this is possible and compute the missing entries.

In Exercises 7 through 11, determine whether the binary operation $*$ defined is commutative and whether $*$ is associative.

7. $*$ defined on $\mathbb{Z}$ by letting $a * b = a - b$

8. $*$ defined on $\mathbb{Q}$ by letting $a * b = ab + 1$

9. $*$ defined on $\mathbb{Q}$ by letting $a * b = ab/2$

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?

Concepts

In Exercises 14 through 16, 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.

14. A binary operation $*$ is *commutative* if and only if $a * b = b * a$.

15. A binary operation $*$ on a set S is *associative* if and only if, for all $a, b, c \in S$, we have $(b * c) * a = b * (c * a)$.

16. 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 $a, b \in S$.

In Exercises 17 through 22, 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 of these conditions on page 24 are violated.

17. On $\mathbb{Z}^+$, define $*$ by letting $a * b = a - b$.

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

19. On $\mathbb{R}$, define $*$ by letting $a * b = a - b$.

20. On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$, where c is the smallest integer greater than both a and b.

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

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

23. 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?

24. Mark each of the following 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.

25. 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

26. 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 27 and 28, either prove the statement or give a counterexample.

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

28. 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 2.7 defined the binary operations $+$, $-$, $\cdot$, and $\circ$ on F. In Exercises 29 through 35, either prove the given statement or give a counterexample.

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

30. Function subtraction $-$ on F is commutative

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

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

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

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

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

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

36. 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.)

37. 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 $*$.)

SECTION 3 Isomorphic Binary Structures

Compare Table 3.1 for the binary operation $*$ on the set $S = \{a, b, c\}$ with Table 3.2 for the binary operation $*'$ on the set $T = \{\#, \$, \&\}$.

Notice that if, in Table 3.1, we replace all occurrences of a by #, every b by \$, and every c by & using the one-to-one correspondence

$$a \leftrightarrow \# \qquad b \leftrightarrow \$ \qquad c \leftrightarrow \&$$

we obtain precisely Table 3.2. The two tables differ only in the symbols (or names) denoting the elements and the symbols $*$ and $*'$ for the operations. If we rewrite Table 3.3 with elements in the order y, x, z, we obtain Table 3.4. (Here we did not set up any one-one-correpondence; we just listed the same elements in different order outside the heavy bars of the table.) Replacing, in Table 3.1, all occurrences of a by y, every b by x, and every c by z using the one-to-one correspondence

$$a \leftrightarrow y \qquad b \leftrightarrow x \qquad c \leftrightarrow z$$

we obtain Table 3.4. We think of Tables 3.1, 3.2, 3.3, and 3.4 as being *structurally alike*. These four tables differ only in the names (or symbols) for their elements and in the order that those elements are listed as heads in the tables. However, Table 3.5 for binary operation $\bar{*}$ and Table 3.6 for binary operation $\hat{*}$ on the set $S = \{a, b, c\}$ are *structurally different* from each other and from Table 3.1. In Table 3.1, each element appears three times in the body of the table, while the body of Table 3.5 contains the single element b. In Table 3.6, for all $s \in S$ we get the same value c for $s \,\hat{*}\, s$ along the upper-left to lower-right diagonal, while we get three different values in Table 3.1. Thus Tables 3.1 through 3.6 give just three structurally different binary operations on a set of three elements, provided we disregard the names of the elements and the order in which they appear as heads in the tables.

The situation we have just discussed is somewhat akin to children in France and in Germany learning the operation of addition on the set $\mathbb{Z}^+$. The children have different

3.1 Table

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

3.2 Table

$*'$	#	\$	&
#	&	#	\$
\$	#	\$	&
&	\$	&	#

3.3 Table

$*''$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

3.4 Table

$*''$	y	x	z
y	z	y	x
x	y	x	z
z	x	z	y

3.5 Table

$\bar{*}$	a	b	c
a	b	b	b
b	b	b	b
c	b	b	b

3.6 Table

$\hat{*}$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

names (un, deux, trois, $\cdots$ versus eins, zwei, drei $\cdots$) for the numbers, but they are learning the same binary structure. (In this case, they are also using the same symbols for the numbers, so their addition tables would appear the same if they list the numbers in the same order.)

We are interested in studying the different types of *structures* that binary operations can provide on sets having the same number of elements, as typified by Tables 3.4, 3.5, and 3.6. Let us consider a **binary algebraic structure**[†] $\langle S, * \rangle$ to be a set S together with a binary operation $*$ on S. In order for two such binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ to be structurally alike in the sense we have described, we would have to have a one-to-one correspondence between the elements x of S and the elements x' of S' such that

$$\text{if} \quad x \leftrightarrow x' \quad \text{and} \quad y \leftrightarrow y', \quad \text{then} \quad x * y \leftrightarrow x' *' y'. \tag{1}$$

A one-to-one correspondence exists if the sets S and S' have the same number of elements. It is customary to describe a one-to-one correspondence by giving a *one-to-one* function ϕ mapping S *onto* S' (see Definition 0.12). For such a function ϕ, we regard the equation $\phi(x) = x'$ as reading the one-to-one pairing $x \leftrightarrow x'$ in left-to-right order. In terms of ϕ, the final $\leftrightarrow$ correspondence in (1), which asserts the algebraic structure in S' is the same as in S, can be expressed as

$$\phi(x * y) = \phi(x) *' \phi(y).$$

Such a function showing that two algebraic systems are structurally alike is known as an *isomorphism*. We give a formal definition.

3.7 Definition Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An **isomorphism of** S with S' is a one-to-one function ϕ mapping S onto S' such that

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S. \tag{2}$$
$$\textit{homomorphism property}$$

[†] Remember that boldface type indicates that a term is being defined.

If such a map ϕ exists, then S and S' are **isomorphic binary structures**, which we denote by $S \simeq S'$, omitting the $*$ and $*'$ from the notation. ■

You may wonder why we labeled the displayed condition in Definition 3.7 the *homomorphism property* rather than the *isomorphism property*. The notion of isomorphism includes the idea of one-to-one correspondence, which appeared in the definition via the words *one-to-one* and *onto* before the display. In Chapter 13, we will discuss the relation between S and S' when $\phi : S \to S'$ satisfies the displayed homomorphism property, but ϕ is not necessarily one to one; ϕ is then called a *homomorphism* rather than an *isomorphism*.

It is apparent that in Section 1, we showed that the binary structures $\langle U, \cdot \rangle$ and $\langle \mathbb{R}_c, +_c \rangle$ are isomorphic for all $c \in \mathbb{R}^+$. Also, $\langle U_n, \cdot \rangle$ and $\langle \mathbb{Z}_n, +_n \rangle$ are isomorphic for each $n \in \mathbb{Z}^+$.

Exercise 28 asks us to show that for a collection of binary algebraic structures, the relation $\simeq$ in Definition 3.7 is an equivalence relation on the collection. Our discussion leading to the preceding definition shows that the binary structures defined by Tables 3.1 through 3.4 are in the same equivalence class, while those given by Tables 3.5 and 3.6 are in different equivalence classes. We proceed to discuss how to try to determine whether binary structures are isomorphic.

How to Show That Binary Structures Are Isomorphic

We now give an outline showing how to proceed from Definition 3.7 to show that two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are isomorphic.

Step 1 *Define the function ϕ that gives the isomorphism of S with S'.* Now this means that we have to describe, in some fashion, what $\phi(s)$ is to be for every $s \in S$.

Step 2 *Show that ϕ is a one-to-one function.* That is, suppose that $\phi(x) = \phi(y)$ in S' and deduce from this that $x = y$ in S.

Step 3 *Show that ϕ is onto S'.* That is, suppose that $s' \in S'$ is given and show that there does exist $s \in S$ such that $\phi(s) = s'$.

Step 4 *Show that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$.* This is just a question of computation. Compute both sides of the equation and see whether they are the same.

3.8 Example Let us show that the binary structure $\langle \mathbb{R}, + \rangle$ with operation the usual addition is isomorphic to the structure $\langle \mathbb{R}^+, \cdot \rangle$ where $\cdot$ is the usual multiplication.

Step 1 We have to somehow convert an operation of addition to multiplication. Recall from $a^{b+c} = (a^b)(a^c)$ that addition of exponents corresponds to multiplication of two quantities. Thus we try defining $\phi : \mathbb{R} \to \mathbb{R}^+$ by $\phi(x) = e^x$ for $x \in \mathbb{R}$. Note that $e^x > 0$ for all $x \in \mathbb{R}$, so indeed, $\phi(x) \in \mathbb{R}^+$.

Step 2 If $\phi(x) = \phi(y)$, then $e^x = e^y$. Taking the natural logarithm, we see that $x = y$, so ϕ is indeed one to one.

Step 3 If $r \in \mathbb{R}^+$, then $\ln(r) \in \mathbb{R}$ and $\phi(\ln r) = e^{\ln r} = r$. Thus ϕ is onto $\mathbb{R}^+$.

Step 4 For $x, y \in \mathbb{R}$, we have $\phi(x + y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$. Thus we see that ϕ is indeed an isomorphism. ▲

3.9 Example Let $2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}$, so that $2\mathbb{Z}$ is the set of all even integers, positive, negative, and zero. We claim that $\langle \mathbb{Z}, + \rangle$ is isomorphic to $\langle 2\mathbb{Z}, + \rangle$, where $+$ is the usual addition. This will give an example of a binary structure $\langle \mathbb{Z}, + \rangle$ that is actually isomorphic to a structure consisting of a proper subset under the *induced* operation, in contrast to Example 3.8, where the operations were totally different.

Step 1 The obvious function $\phi : \mathbb{Z} \to 2\mathbb{Z}$ to try is given by $\phi(n) = 2n$ for $n \in \mathbb{Z}$.

Step 2 If $\phi(m) = \phi(n)$, then $2m = 2n$ so $m = n$. Thus ϕ is one to one.

Step 3 If $n \in 2\mathbb{Z}$, then n is even so $n = 2m$ for $m = n/2 \in \mathbb{Z}$. Hence $\phi(m) = 2(n/2) = n$ so ϕ is onto $2\mathbb{Z}$.

Step 4 Let $m, n \in \mathbb{Z}$. The equation

$$\phi(m + n) = 2(m + n) = 2m + 2n = \phi(m) + \phi(n)$$

then shows that ϕ is an isomorphism. ▲

How to Show That Binary Structures Are Not Isomorphic

We now turn to the reverse question, namely:

> *How do we demonstrate that two binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ are not isomorphic, if this is the case*?

This would mean that there is no one-to-one function ϕ from S onto S' with the property $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$. In general, it is clearly not feasible to try every possible one-to-one function mapping S onto S' and test whether it has this property, except in the case where there are *no* such functions. This is the case precisely when S and S' do not have the same cardinality. (See Definition 0.13.)

3.10 Example The binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{R}, + \rangle$ are not isomorphic because $\mathbb{Q}$ has cardinality $\aleph_0$ while $|\mathbb{R}| \neq \aleph_0$. (See the discussion following Example 0.13.) Note that it is not enough to say that $\mathbb{Q}$ is a proper subset of $\mathbb{R}$. Example 3.9 shows that a proper subset with the induced operation can indeed be isomorphic to the entire binary structure. ▲

A **structural property** of a binary structure is one that must be shared by any isomorphic structure. It is not concerned with names or some other nonstructural characteristics of the elements. For example, the binary structures defined by Tables 3.1 and 3.2 are isomorphic, although the elements are totally different. Also, a structural property is not concerned with what we consider to be the "name" of the binary operation. Example 3.8 showed that a binary structure whose operation is our usual addition can be isomorphic to one whose operation is our usual multiplication. The number of elements in the set S is a structural property of $\langle S, * \rangle$.

3.1 Table

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

3.2 Table

$*'$	#	\$	&
#	&	#	\$
\$	#	\$	&
&	\$	&	#

3.3 Table

$*''$	x	y	z
x	x	y	z
y	y	z	x
z	z	x	y

3.4 Table

$*''$	y	x	z
y	z	y	x
x	y	x	z
z	x	z	y

3.5 Table

$\bar{*}$	a	b	c
a	b	b	b
b	b	b	b
c	b	b	b

3.6 Table

$\hat{*}$	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

names (un, deux, trois, $\cdots$ versus ein, zwei, drei $\cdots$) for the numbers, but they are learning the same binary structure. (In this case, they are also using the same symbols for the numbers, so their addition tables would appear the same if they list the numbers in the same order.)

We are interested in studying the different types of *structures* that binary operations can provide on sets having the same number of elements, as typified by Tables 3.4, 3.5, and 3.6. Let us consider a **binary algebraic structure**[†] $\langle S, * \rangle$ to be a set S together with a binary operation $*$ on S. In order for two such binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$ to be structurally alike in the sense we have described, we would have to have a one-to-one correspondence between the elements x of S and the elements x' of S' such that

$$\text{if} \quad x \leftrightarrow x' \quad \text{and} \quad y \leftrightarrow y', \quad \text{then} \quad x * y \leftrightarrow x' *' y'. \tag{1}$$

A one-to-one correspondence exists if the sets S and S' have the same number of elements. It is customary to describe a one-to-one correspondence by giving a *one-to-one* function ϕ mapping S *onto* S' (see Definition 0.12). For such a function ϕ, we regard the equation $\phi(x) = x'$ as reading the one-to-one pairing $x \leftrightarrow x$ in left-to-right order. In terms of ϕ, the final $\leftrightarrow$ correspondence in (1), which asserts the algebraic structure in S' is the same as in S, can be expressed as

$$\phi(x * y) = \phi(x) *' \phi(y).$$

Such, a function showing that two algebraic systems are structurally alike is known as an *isomorphism*. We give a formal definition.

3.7 Definition Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures. An **isomorphism of** S with S' is a one-to-one function ϕ mapping S onto S' such that

$$\phi(x * y) = \phi(x) *' \phi(y) \text{ for all } x, y \in S. \tag{2}$$
$$\textit{homomorphism property}$$

[†] Remember that boldface type indicates that a term is being defined.

If you now have a good grasp of the notion of isomorphic binary structures, it should be evident that having an identity element for $*$ is indeed a structural property of a structure $\langle S, * \rangle$. However, we know from experience that many readers will be unable to see the forest because of all the trees that have appeared. For them, we now supply a careful proof, skipping along to touch those trees that are involved.

3.14 Theorem Suppose $\langle S, * \rangle$ has an identity element e for $*$. If $\phi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then $\phi(e)$ is an identity element for the binary operation $*'$ on S'.

Proof Let $s' \in S'$. We must show that $\phi(e) *' s' = s' *' \phi(e) = s'$. Because ϕ is an isomorphism, it is a one-to-one map of S onto S'. In particular, there exists $s \in S$ such that $\phi(s) = s'$. Now e is an identity element for $*$ so that we know that $e * s = s * e = s$. Because ϕ is a function, we then obtain

$$\phi(e * s) = \phi(s * e) = \phi(s).$$

Using Definition 3.7 of an isomorphism, we can rewrite this as

$$\phi(e) *' \phi(s) = \phi(s) *' \phi(e) = \phi(s).$$

Remembering that we chose $s \in S$ such that $\phi(s) = s'$, we obtain the desired relation $\phi(e) *' s' = s' *' \phi(e) = s'$. ◆

We conclude with three more examples showing via structural properties that certain binary structures are not isomorphic. In the exercises we ask you to show, as in Theorem 3.14, that the properties we use to distinguish the structures in these examples are indeed structural. That is, they must be shared by any isomorphic structure.

3.15 Example We show that the binary structures $\langle \mathbb{Q}, + \rangle$ and $\langle \mathbb{Z}, + \rangle$ under the usual addition are not isomorphic. (Both $\mathbb{Q}$ and $\mathbb{Z}$ have cardinality $\aleph_0$, so there are lots of one-to-one functions mapping $\mathbb{Q}$ onto $\mathbb{Z}$.) The equation $x + x = c$ has a solution x for all $c \in \mathbb{Q}$, but this is not the case in $\mathbb{Z}$. For example, the equation $x + x = 3$ has no solution in $\mathbb{Z}$. We have exhibited a structural property that *distinguishes* these two structures. ▲

3.16 Example The binary structures $\langle \mathbb{C}, \cdot \rangle$ and $\langle \mathbb{R}, \cdot \rangle$ under the usual multiplication are not isomorphic. (It can be shown that $\mathbb{C}$ and $\mathbb{R}$ have the same cardinality.) The equation $x \cdot x = c$ has a solution x for all $c \in \mathbb{C}$, but $x \cdot x = -1$ has no solution in $\mathbb{R}$. ▲

3.17 Example The binary structure $\langle M_2(\mathbb{R}), \cdot \rangle$ of 2×2 real matrices with the usual matrix multiplication is not isomorphic to $\langle \mathbb{R}, \cdot \rangle$ with the usual number multiplication. (It can be shown that both sets have cardinality $|\mathbb{R}|$.) Multiplication of numbers is commutative, but multiplication of matrices is not. ▲

EXERCISES 3

In all the exercises, $+$ is the usual addition on the set where it is specified, and $\cdot$ is the usual multiplication.

Computations

1. What three things must we check to determine whether a function $\phi: S \to S'$ is an isomorphism of a binary structure $\langle S, * \rangle$ with $\langle S', *' \rangle$?

In Exercises 2 through 10, determine whether the given map ϕ is an isomorphism of the first binary structure with the second. (See Exercise 1.) If it is not an isomorphism, why not?

2. $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\phi(n) = -n$ for $n \in \mathbb{Z}$

3. $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\phi(n) = 2n$ for $n \in \mathbb{Z}$

4. $\langle \mathbb{Z}, + \rangle$ with $\langle \mathbb{Z}, + \rangle$ where $\phi(n) = n + 1$ for $n \in \mathbb{Z}$

5. $\langle \mathbb{Q}, + \rangle$ with $\langle \mathbb{Q}, + \rangle$ where $\phi(x) = x/2$ for $x \in \mathbb{Q}$

6. $\langle \mathbb{Q}, \cdot \rangle$ with $\langle \mathbb{Q}, \cdot \rangle$ where $\phi(x) = x^2$ for $x \in \mathbb{Q}$

7. $\langle \mathbb{R}, \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(x) = x^3$ for $x \in \mathbb{R}$

8. $\langle M_2(\mathbb{R}), \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(A)$ is the determinant of matrix A

9. $\langle M_1(\mathbb{R}), \cdot \rangle$ with $\langle \mathbb{R}, \cdot \rangle$ where $\phi(A)$ is the determinant of matrix A

10. $\langle \mathbb{R}, + \rangle$ with $\langle \mathbb{R}^+, \cdot \rangle$ where $\phi(r) = 0.5^r$ for $r \in \mathbb{R}$

In Exercises 11 through 15, let F be the set of all functions f mapping $\mathbb{R}$ into $\mathbb{R}$ that have derivatives of all orders. Follow the instructions for Exercises 2 through 10.

11. $\langle F, + \rangle$ with $\langle F, + \rangle$ where $\phi(f) = f'$, the derivative of f

12. $\langle F, + \rangle$ with $\langle \mathbb{R}, + \rangle$ where $\phi(f) = f'(0)$

13. $\langle F, + \rangle$ with $\langle F, + \rangle$ where $\phi(f)(x) = \int_0^x f(t)dt$

14. $\langle F, + \rangle$ with $\langle F, + \rangle$ where $\phi(f)(x) = \frac{d}{dx}[\int_0^x f(t)dt]$

15. $\langle F, \cdot \rangle$ with $\langle F, \cdot \rangle$ where $\phi(f)(x) = x \cdot f(x)$

16. The map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = n + 1$ for $n \in \mathbb{Z}$ is one to one and onto $\mathbb{Z}$. Give the definition of a binary operation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphism mapping

a. $\langle \mathbb{Z}, + \rangle$ onto $\langle \mathbb{Z}, * \rangle$, **b.** $\langle \mathbb{Z}, * \rangle$ onto $\langle \mathbb{Z}, + \rangle$.

In each case, give the identity element for $*$ on $\mathbb{Z}$.

17. The map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = n + 1$ for $n \in \mathbb{Z}$ is one to one and onto $\mathbb{Z}$. Give the definition of a binary operation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphism mapping

a. $\langle \mathbb{Z}, \cdot \rangle$ onto $\langle \mathbb{Z}, * \rangle$, **b.** $\langle \mathbb{Z}, * \rangle$ onto $\langle \mathbb{Z}, \cdot \rangle$.

In each case, give the identity element for $*$ on $\mathbb{Z}$.

18. The map $\phi : \mathbb{Q} \to \mathbb{Q}$ defined by $\phi(x) = 3x - 1$ for $x \in \mathbb{Q}$ is one to one and onto $\mathbb{Q}$. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphism mapping

a. $\langle \mathbb{Q}, + \rangle$ onto $\langle \mathbb{Q}, * \rangle$, **b.** $\langle \mathbb{Q}, * \rangle$ onto $\langle \mathbb{Q}, + \rangle$.

In each case, give the identity element for $*$ on $\mathbb{Q}$.

19. The map $\phi : \mathbb{Q} \to \mathbb{Q}$ defined by $\phi(x) = 3x - 1$ for $x \in \mathbb{Q}$ is one to one and onto $\mathbb{Q}$. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphism mapping

a. $\langle \mathbb{Q}, \cdot \rangle$ onto $\langle \mathbb{Q}, * \rangle$, **b.** $\langle \mathbb{Q}, * \rangle$ onto $\langle \mathbb{Q}, \cdot \rangle$.

In each case, give the identity element for $*$ on $\mathbb{Q}$.

Concepts

20. The displayed homomorphism condition for an isomorphism ϕ in Definition 3.7 is sometimes summarized by saying, "ϕ must commute with the binary operation(s)." Explain how that condition can be viewed in this manner.

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. A function $\phi : S \to S'$ is an *isomorphism* if and only if $\phi(a * b) = \phi(a) *' \phi(b)$.

22. Let $*$ be a binary operation on a set S. An element e of S with the property $s * e = s = e * s$ is an *identity element for* $*$ for all $s \in S$.

Proof Synopsis

A good test of your understanding of a proof is your ability to give a one or two sentence synopsis of it, explaining the idea of the proof without all the details and computations. Note that we said "sentence" and not "equation." From now on, some of our exercise sets may contain one or two problems asking for a synopsis of a proof in the text. It should rarely exceed three sentences. We should illustrate for you what we mean by a synopsis. Here is our one-sentence synopsis of Theorem 3.14. Read the statement of the theorem now, and then our synopsis.

> Representing an element of S' as $\phi(s)$ for some $s \in S$, use the homomorphism property of ϕ to carry the computation of $\phi(e) *' \phi(s)$ back to a computation in S.

That is the kind of explanation that one mathematician might give another if asked, "How does the proof go?" We did not make the computation or explain why we could represent an element of S' as $\phi(s)$. To supply every detail would result in a completely written proof. We just gave the guts of the argument in our synopsis.

23. Give a proof synopsis of Theorem 3.13.

Theory

24. An identity element for a binary operation $*$ as described by Definition 3.12 is sometimes referred to as "a two-sided identity element." Using complete sentences, give analogous definitions for

a. a *left identity element* e_L for $*$, and **b.** a *right identity element* e_R for $*$.

Theorem 3.13 shows that if a two-sided identity element for $*$ exists, it is unique. Is the same true for a one-sided identity element you just defined? If so, prove it. If not, give a counterexample $\langle S, * \rangle$ for a finite set S and find the first place where the proof of Theorem 3.13 breaks down.

25. Continuing the ideas of Exercise 24 can a binary structure have a left identity element e_L and a right identity element e_R where $e_L \neq e_R$? If so, give an example, using an operation on a finite set S. If not, prove that it is impossible.

26. Recall that if $f : A \to B$ is a one-to-one function mapping A onto B, then $f^{-1}(b)$ is the unique $a \in A$ such that $f(a) = b$. Prove that if $\phi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$, then ϕ^{-1} is an isomorphism of $\langle S', *' \rangle$ with $\langle S, * \rangle$.

27. Prove that if $\phi : S \to S'$ is an isomorphism of $\langle S, * \rangle$ with $\langle S', *' \rangle$ and $\psi : S' \to S''$ is an isomorphism of $\langle S', *' \rangle$ with $\langle S'', *'' \rangle$, then the composite function $\psi \circ \phi$ is an isomorphism of $\langle S, * \rangle$ with $\langle S'', *'' \rangle$.

28. Prove that the relation $\simeq$ of being isomorphic, described in Definition 3.7, is an equivalence relation on any set of binary structures. You may simply quote the results you were asked to prove in the preceding two exercises at appropriate places in your proof.

In Exercises 29 through 32, give a careful proof for a skeptic that the indicated property of a binary structure $\langle S, * \rangle$ is indeed a structural property. (In Theorem 3.14, we did this for the property, "There is an identity element for $*$.")

29. The operation $*$ is commutative.

30. The operation $*$ is associative.

31. For each $c \in S$, the equation $x * x = c$ has a solution x in S.

32. There exists an element b in S such that $b * b = b$.

33. 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 $a, b \in \mathbb{R}$. Exercise 23 of Section 2 shows that H is closed under both matrix addition and matrix multiplication.

a. Show that $\langle \mathbb{C}, + \rangle$ is isomorphic to $\langle H, + \rangle$.

b. Show that $\langle \mathbb{C}, \cdot \rangle$ is isomorphic to $\langle H, \cdot \rangle$.

(We say that H is a *matrix representation* of the complex numbers $\mathbb{C}$.)

34. There are 16 possible binary structures on the set $\{a, b\}$ of two elements. How many nonisomorphic (that is, structurally different) structures are there among these 16? Phrased more precisely in terms of the isomorphism equivalence relation $\simeq$ on this set of 16 structures, how many equivalence classes are there? Write down one structure from each equivalence class. [*Hint:* Interchanging a and b everywhere in a table and then rewriting the table with elements listed in the original order does not always yield a table different from the one we started with.]

SECTION 4 GROUPS

Let us continue the analysis of our past experience with algebra. Once we had mastered the computational problems of addition and multiplication of numbers, we were ready to apply these binary operations to the solution of problems. Often problems lead to equations involving some unknown number x, which is to be determined. The simplest equations are the linear ones of the forms $a + x = b$ for the operation of addition, and $ax = b$ for multiplication. The additive linear equation always has a numerical solution, and so has the multiplicative one, provided $a \neq 0$. Indeed, the need for solutions of additive linear equations such as $5 + x = 2$ is a very good motivation for the negative numbers. Similarly, the need for rational numbers is shown by equations such as $2x = 3$.

It is desirable for us to be able to solve linear equations involving our binary operations. This is not possible for every binary operation, however. For example, the equation $a * x = a$ has no solution in $S = \{a, b, c\}$ for the operation $*$ of Example 2.14. Let us abstract from familiar algebra those properties of addition that enable us to solve the equation $5 + x = 2$ in $\mathbb{Z}$. We must not refer to subtraction, for we are concerned with the solution phrased in terms of a single binary operation, in this case addition. The steps in

the solution are as follows:

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

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:

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

We can now see what properties a set S and a binary operation $*$ on S would have to have to permit imitation of this procedure for an equation $a*x=b$ for $a, b \in S$. Basic to the procedure is the existence of an element e in S with the property that $e*x=x$ for all $x \in S$. For our additive example, 0 played the role of e, and 1 played the role for our multiplicative example. Then we need an element a' in S that has the property that $a'*a=e$. For our additive example with $a=5$, -5 played the role of a', and $\frac{1}{2}$ played the role for our multiplicative example with $a=2$. Finally we need the associative law. The remainder is just computation. A similar analysis shows that in order to solve the equation $x*a=b$ (remember that $a*x$ need not equal $x*a$), we would like to have an element e in S such that $x*e=x$ for all $x \in S$ and an a' in S such that $a*a'=e$. With all of these properties of $*$ on S, we could be sure of being able to solve linear equations. Thus we need an associative binary structure $\langle S, * \rangle$ with an identity element e such that for each $a \in S$, there exists $a' \in S$ such that $a*a'=a'*a=e$. This is precisely the notion of a *group*, which we now define.

Definition and Examples

Rather than describe a *group* using terms defined in Sections 2 and 3 as we did at the end of the preceding paragraph, we give a self-contained definition. This enables a person who picks up this text to discover what a group is without having to look up more terms.

4.1 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

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

4.2 Example We easily see that $\langle U, \cdot \rangle$ and $\langle U_n, \cdot \rangle$ are groups. Multiplication of complex numbers is associative and both U and U_n contain 1, which is an identity for multiplication. For $e^{i\theta} \in U$, the computation

$$e^{i\theta} \cdot e^{i(2\pi - \theta)} = e^{2\pi i} = 1$$

shows that every element of U has an inverse. For $z \in U_n$, the computation

$$z \cdot z^{n-1} = z^n = 1$$

shows that every element of U_n has an inverse. Thus $\langle U, \cdot \rangle$ and $\langle U_n, \cdot \rangle$ are groups. Because $\langle \mathbb{R}_c, +_c \rangle$ is isomorphic to $\langle U, \cdot \rangle$, we see that $\langle \mathbb{R}_c, +_c \rangle$ is a group for all $c \in \mathbb{R}^+$. Similarly, the fact that $\langle \mathbb{Z}_n, +_n \rangle$ is isomorphic to $\langle U_n, \cdot \rangle$ shows that $\langle \mathbb{Z}_n, +_n \rangle$ is a group for all $n \in \mathbb{Z}^+$. ▲

We point out now that we will sometimes be sloppy in notation. Rather than use the binary structure notation $\langle G, * \rangle$ constantly, we often refer to a group G, with the understanding that there is of course a binary operation on the set G. In the event that clarity demands that we specify an operation $*$ on G, we use the phrase "the group G

■ 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.

under $*$." For example, we may refer to the *groups* $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ *under addition* rather than write the more tedious $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, and $\langle \mathbb{R}, + \rangle$. However, we feel free to refer to the group $\mathbb{Z}_8$ without specifying the operation.

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

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.

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

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

4.5 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. ▲

4.6 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. ▲

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

4.8 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. ▲

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

4.10 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. ▲

4.11 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. ▲

4.12 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. ▲

4.13 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. It is our first example of a *nonabelian group*. ▲

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 $GL(\mathbb{R}^n)$. Of course, $GL(n, \mathbb{R}) \simeq GL(\mathbb{R}^n)$.

4.14 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 4.1, which is the only thing we know about groups at the moment. The proof of a second theorem can employ both Definition 4.1 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 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.

4.15 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 4.15. 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.

4.16 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 4.15, $y_1 = y_2$. 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 is a special type of binary structure, we know from Theorem 3.13 that the identity e in a group is unique. We state this again as part of the next theorem for easy reference.

4.17 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 3.13 shows that an identity element for any binary structure is unique. No use of the 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 4.15,

$$a'' = a',$$

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 4.17 show that $b' * a'$ is the unique inverse of $a * b$. That is, $(a * b)' = b' * a'$. We state this as a corollary.

4.18 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.

Finite Groups and Group Tables

All our examples after Example 4.2 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.

Let us try to put a group structure on a set of two elements. Since one of the elements must play the role of identity element, we may as well let the set be $\{e, a\}$. Let us attempt to find a table for a binary operation $*$ on $\{e, a\}$ that gives a group structure on $\{e, a\}$. When giving a table for a group operation, we shall always list the identity first, as in the following table.

$*$	e	a
e		
a		

Since e is to be the identity, so

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

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

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

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 follows:

$*$	e	a
e	e	a
a	a	e

All the group axioms are now satisfied, except possibly the associative property. Checking associativity on a case-by-case basis from a table defining an operation can be a very tedious process. However, we know that $\mathbb{Z}_2 = \{0, 1\}$ under addition modulo 2 is a group, and by our arguments, its table must be the one above with e replaced by 0 and a by 1. Thus the associative property must be satisfied for our table containing e and a.

With this example 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 4.16, not only 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.

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 shown in Table 4.19. 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 4.20. This leaves four places to be filled in. You can quickly see that Table 4.20 must be completed as shown in Table 4.21 if each row and each column are to contain each element exactly once. Because there was only one way to complete the table and $\mathbb{Z}_3 = \{0, 1, 2\}$ under addition modulo 3 is a group, the associative property must hold for our table containing e, a, and b.

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 in Section 3, this renaming gives an isomorphism of the group G' with the group G. Definition 3.7 defined the notion of *isomorphism* and of *isomorphic binary structures*. Groups are just certain types of binary structures, so the same definition pertains to them. 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 using the equivalence relation $\simeq$. Thus we may say, "There is only one group of three elements, up to isomorphism."

4.19 Table

$*$	e	a
e	e	a
a	a	e

4.20 Table

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

4.21 Table

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

EXERCISES 4

Computations

In Exercises 1 through 6, 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 4.1 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. Give an example of an abelian group G where G has exactly 1000 elements.

8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4(7) + 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.

9. Show that the group $\langle U, \cdot \rangle$ is not isomorphic to either $\langle \mathbb{R}, + \rangle$ or $\langle \mathbb{R}^*, \cdot \rangle$. (All three groups have cardinality $|\mathbb{R}|$.)

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. All $n \times n$ matrices with determinant either 1 or -1 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 4.22. 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 renaming function which is an isomorphism.

a. Are all groups of 4 elements commutative?

b. Which table gives a group isomorphic to the group U_4, so that we know the binary operation defined by the table is associative?

c. Show that the group given by one of the other tables is structurally the same as the group in Exercise 14 for one particular value of n, so that we know that the operation defined by that table is associative also.

21. According to Exercise 12 of Section 2, 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.)

4.22 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 for a binary operation on the set $\{e, a, b\}$ of three elements satisfying axioms $\mathscr{G}_2$ and $\mathscr{G}_3$ for a group but not axiom $\mathscr{G}_1$.

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 4.15." 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 4.15.

27. Give at most a two-sentence synopsis of the proof in Theorem 4.16 that an equation $ax = b$ has a unique solution in a group.

Theory

28. From our intuitive grasp of the notion of isomorphic groups, it should be clear that if $\phi : G \to G'$ is a group isomorphism, then $\phi(e)$ is the identity e' of G'. Recall that Theorem 3.14 gave a proof of this for isomorphic binary structures $\langle S, * \rangle$ and $\langle S', *' \rangle$. Of course, this covers the case of groups.

It should also be intuitively clear that if a and a' are inverse pairs in G, then $\phi(a)$ and $\phi(a')$ are inverse pairs in G', that is, that $\phi(a)' = \phi(a')$. Give a careful proof of this for a skeptic who can't see the forest for all the trees.

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. 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.]

35. 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.

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

37. 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.

38. Prove that a set G, together with a binary operation $*$ on G satisfying the left axioms 1, 2, and 3 given on page 43, is a group.

39. 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 38.]

40. Let $\langle G, \cdot \rangle$ be a group. Consider the binary operation $*$ on the set G defined by

$$a * b = b \cdot a$$

for $a, b \in G$. Show that $\langle G, * \rangle$ is a group and that $\langle G, * \rangle$ is actually isomorphic to $\langle G, \cdot \rangle$. [*Hint:* Consider the map ϕ with $\phi(a) = a'$ for $a \in G$.]

41. Let G be a group and let g be one fixed element of G. Show that the map i_g, such that $i_g(x) = gxg'$ for $x \in G$, is an isomorphism of G with itself.

SECTION 5 SUBGROUPS

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 5.1 or, since such a group is commutative, the table might look like Table 5.2. In general situations we shall continue to use e to denote the identity element of a group.

5.1 Table

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	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 be using 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:

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

5.2 Table

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

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.

Let us explain one more term that is used so often it merits a special definition.

5.3 Definition If G is a group, then the **order** $|G|$ of G is the number of elements in G. (Recall from Section 0 that, for any set S, $|S|$ is the cardinality of S.) ■

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.

5.4 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.

5.5 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.

5.6 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 $\mathbb{R}^n$. ▲

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

5.8 Example The nth roots of unity in $\mathbb{C}$ form a subgroup U_n of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication. ▲

5.9 Example There are two different types of group structures of order 4 (see Exercise 20 of Section 4). We describe them by their group tables (Tables 5.10 and 5.11). The group V is the **Klein 4-group,** and the notation V comes from the German word *Vier* for four. The group $\mathbb{Z}_4$ is isomorphic to the group $U_4 = \{1, i, -1, -i\}$ of fourth roots of unity under multiplication.

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 $c \notin \{e, a, b\}$. ▲

5.10 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

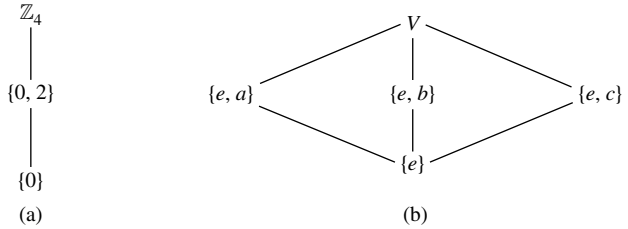
5.11 Table

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 5.12 contains the subgroup diagrams for the groups $\mathbb{Z}_4$ and V of Example 5.9.

Note that if $H \leq G$ and $a \in H$, then by Theorem 4.16, 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.



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

5.13 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 5.13 indicates such a routine, and in the next theorem, we demonstrate carefully its validity. While more compact criteria are available, involving only one condition, we prefer this more transparent theorem for a first course.

5.14 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,
3. for all $a \in H$ it is true that $a^{-1} \in H$ 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 5.13.

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 $H \leq G$. ◆

5.15 Example Let F be as in Example 5.13. 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. ▲

5.16 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 5.14 then shows that T is a subgroup of G. ▲

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 5.14, 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 5.9,

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

We have almost proved the next theorem.

5.17 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.

[†] 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. 5.12.) However, V contains no smallest nontrivial subgroup.

Proof We check the three conditions given in Theorem 5.14 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 $H \leq G$.

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. ◆

5.18 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 5.17, is called the **cyclic subgroup of G generated by a**, and denoted by $\langle a \rangle$. ■

5.19 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. ■

5.20 Example Let $\mathbb{Z}_4$ and V be the groups of Example 5.9. 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. ▲

5.21 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. ▲

5.22 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

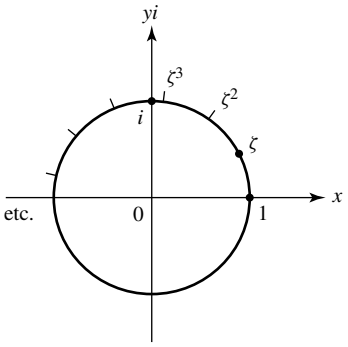
$$\begin{array}{llll} & 3, \quad 3+3=6, & 3+3+3=9, & \text{and so on,} \\ 0, \quad -3, & -3+-3=-6, & -3+-3+-3=-9, & \text{and so on.} \end{array}$$

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 $6\mathbb{Z} < 3\mathbb{Z}$. ▲

5.23 Example For each positive integer n, let U_n be 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. 5.24. The heavy point 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 1, 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. ▲



5.24 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 2

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

10. The upper-triangular $n \times n$ matrices with no zeros on the diagonal

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

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 5.11)

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

30. The subgroup of U_5 generated by $\cos \frac{4\pi}{5} + i \sin \frac{4\pi}{5}$

31. The subgroup of U_8 generated by $\cos \frac{3\pi}{2} + i \sin \frac{3\pi}{2}$

32. The subgroup of U_8 generated by $\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}$

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

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

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 5.25 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 $\mathbb{Z}_6$.)

5.25 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. Mark each of the following 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.

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.

Theory

In Exercises 41 and 42, 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.

41. 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.

42. If G is cyclic, then G' is cyclic.

43. 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.

44. Find the flaw in the following argument: "Condition 2 of Theorem 5.14 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."

45. Show that a nonempty subset H of a group G is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$. (This is one of the *more compact criteria* referred to prior to Theorem 5.14)

46. Prove that a cyclic group with only one generator can have at most 2 elements.

47. 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.

48. Repeat Exercise 47 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.

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

50. Let a nonempty finite subset H of a group G be closed under the binary operation of G. Show that H is a subgroup of G.

51. 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.

52. Generalizing Exercise 51, 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.

53. 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.

54. 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.")

55. Prove that every cyclic group is abelian.

56. 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?

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

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 5.17). 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 all sufficiently small 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

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

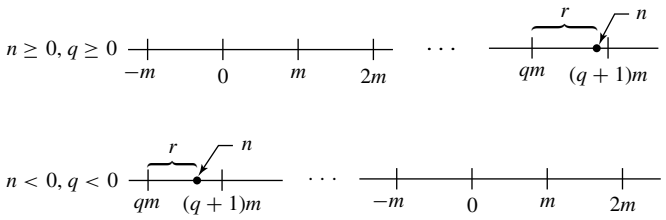
If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

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

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 a seemingly trivial, but very fundamental tool for the study of cyclic groups.



6.2 Figure

6.3 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. 6.2. On the real x-axis of analytic geometry, 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. 6.2. 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. 6.2. ◆

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 $n = qm$ and

$$b = a^n = (a^m)^q = c^q,$$

so b is a power of c. ◆

As noted in Examples 5.21 and 5.22, $\mathbb{Z}$ 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 45 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 and s be two positive integers. 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 from the definition that d is a divisor of both r and s since both $r = 1r + 0s$ and $s = 0r + 1s$ are in H. 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.

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. ▲

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.

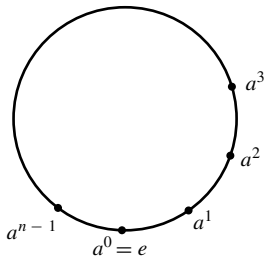
Case II *$a^m = e$ for some positive integer m.* Let n be the smallest positive integer such that $a^n = e$. If $s \in \mathbb{Z}$ and $s = nq + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$. As in Case 1, if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$, contradicting our choice of n. Thus the elements

$$a^0 = e, a, a^2, a^3, \cdots, a^{n-1}$$

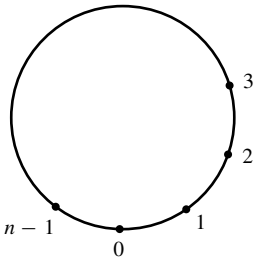
are all distinct and comprise all elements of G. The map $\psi : G \to \mathbb{Z}_n$ given by $\psi(a^i) = i$ for $i = 0, 1, 2, \cdots, n-1$ is thus well defined, one to one, and onto $\mathbb{Z}_n$. Because $a^n = e$, we see that $a^i a^j = a^k$ where $k = i +_n j$. Thus

$$\psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j),$$

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 bottom 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*.

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.

6.14 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 5.17. 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 exists 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 boxed division property (1), 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 $\mathbb{Z}_n$ had 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 $\gcd(s, n) = \gcd(t, n)$. ◆

6.15 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 6.14.

6.16 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.

6.17 Example Let us find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram. All subgroups are cyclic. By Corollary 6.16, 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.

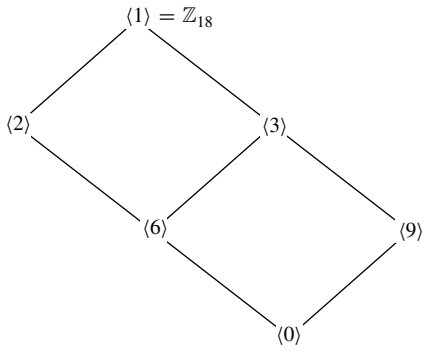
We have thus far found all subgroups generated by 0, 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, and 17. This leaves just 3, 9, and 15 to consider.

$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\},$$

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. 6.18.



6.18 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. ▲

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. $n = -50, m = 8$

4. $n = 50, m = 8$

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. 12

11. 60

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:* Make use of Exercise 44. 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.** $\mathbb{Z}_{12}$

In Exercises 17 through 21, 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 $1 + i$

In Exercises 22 through 24, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

22. $\mathbb{Z}_{12}$

23. $\mathbb{Z}_{36}$

24. $\mathbb{Z}_8$

In Exercises 25 through 29, find all orders of subgroups of the given group.

25. $\mathbb{Z}_6$ **26.** $\mathbb{Z}_8$ **27.** $\mathbb{Z}_{12}$ **28.** $\mathbb{Z}_{20}$ **29.** $\mathbb{Z}_{17}$

Concepts

In Exercises 30 and 31, 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.

30. An element a of a group G has *order* $n \in \mathbb{Z}^+$ if and only if $a^n = e$.

31. The *greatest common divisor* of two positive integers is the largest positive integer that divides both of them.

32. Mark each of the following 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 33 through 37, either give an example of a group with the property described, or explain why no example exists.

33. A finite group that is not cyclic

34. An infinite group that is not cyclic

35. A cyclic group having only one generator

36. An infinite cyclic group having four generators

37. 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 38 through 41, find the primitive nth roots of unity for the given value of n.

38. $n = 4$

39. $n = 6$

40. $n = 8$

41. $n = 12$

Proof Synopsis

42. Give a one-sentence synopsis of the proof of Theorem 6.1.

43. Give at most a three-sentence synopsis of the proof of Theorem 6.6.

Theory

44. 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 $x \in G$.

45. Let r and s be positive integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

46. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

47. 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.

48. Show that a group that has only a finite number of subgroups must be a finite group.

49. 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."

50. 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 $(xax^{-1})^2$.]

51. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

52. 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.

53. 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.

54. With reference to Exercise 53, what is the situation if $1 < m < n$ and m does not divide n?

55. Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if p is a prime number.

56. 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 5.17, 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 5.14, 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 The Klein 4-group $V = \{e, a, b, c\}$ of Example 5.9 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. ▲

7.2 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 54 of Section 5.

PART II

Permutations, Cosets, and Direct Products

Section 8 Groups of Permutations
Section 9 Orbits, Cycles, and the Alternating Groups
Section 10 Cosets and the Theorem of Lagrange
Section 11 Direct Products and Finitely Generated Abelian Groups
Section 12 †Plane Isometries

SECTION 8 Groups of 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. We shall show that any finite group is structurally the same as some group of permutations. Unfortunately, this result, which sounds very powerful, does not turn out to be particularly useful to us.

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. 8.1, resulting in the new arrangement $\{4, 2, 5, 3, 1\}$. Let us think of this schematic diagram in Fig. 8.1 as a function mapping of 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. 8.2 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.

† Section 12 is not used in the remainder of the text.

1→4	1→3
2→2	2→2
3→5	3→4
4→3	4→5
5→1	5→3

8.1 Figure **8.2 Figure**

8.3 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 $\sigma\tau$, as we have done for general groups. 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.

8.4 Example Suppose that

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

and that σ is the permutation given by Fig. 8.1. We write σ in a more standard notation, changing the columns to rows in parentheses and omitting the arrows, as

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

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.

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,

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

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

8.5 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 2, 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 $\mathcal{G}_3$ 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 51 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 $\{1, 2, 3, \cdots, \mathrm{n}\}$ to be a prototype for a finite set A of n elements.

8.6 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

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

Two Important Examples

8.7 Example An interesting example for us is the group S_3 of $3! = 6$ elements. Let the set A be $\{1, 2, 3\}$. We list the permutations of A and assign to each a subscripted Greek letter for a name.

The reasons for the choice of names will be clear later. Let

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

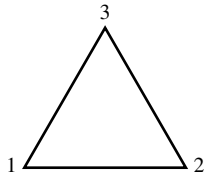
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

8.8 Table

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

The multiplication table for S_3 is shown in Table 8.8. Note that this group is not abelian! We have seen that any group of at most 4 elements is abelian. Later we will see that a group of 5 elements is also abelian. Thus S_3 has minimum order for any nonabelian group. ▲



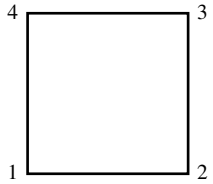
8.9 Figure

There is a natural correspondence between the elements of S_3 in Example 8.7 and the ways in which two copies of an equilateral triangle with vertices 1, 2, and 3 (see Fig. 8.9 can be placed, one covering the other with vertices on top of vertices. For this reason, S_3 is also the **group D_3 of symmetries of an equilateral triangle**. Naively, we used ρ_i for *rotations* and μ_i for *mirror images* in bisectors of angles. The notation D_3 stands for the third dihedral group. The ***n*th dihedral group** D_n is the group of symmetries of the regular n-gon. See Exercise 44.[†]

Note that we can consider the elements of S_3 to *act* on the triangle in Fig. 8.9. See the discussion at the start of this section.

8.10 Example Let us form the dihedral group D_4 of permutations corresponding to the ways that two copies of a square with vertices 1, 2, 3, and 4 can be placed, one covering the other with vertices on top of vertices (see Fig. 8.11). D_4 will then be the **group of symmetries of the square**. It is also called the **octic group**. Again, we choose seemingly arbitrary

[†] Many people denote the nth dihedral group by D_{2n} rather than by D_n since the order of the group is $2n$.



8.11 Figure

notation that we shall explain later. Naively, we are using ρ_i for *rotations*, μ_i for *mirror images* in perpendicular bisectors of sides, and δ_i for *diagonal flips*. There are eight permutations involved here. Let

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

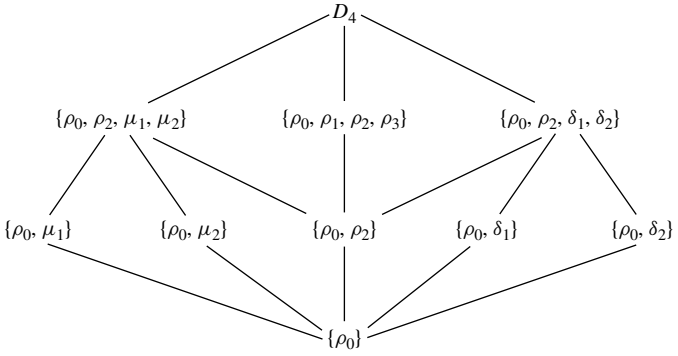
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \qquad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \qquad \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \qquad \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

8.12 Table

	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0



8.13 Figure Subgroup diagram for D_4.

The table for D_4 is given in Table 8.12. Note that D_4 is again nonabelian. This group is simply beautiful. It will provide us with nice examples for many concepts we will introduce in group theory. Look at the lovely symmetries in that table! Finally, we give in Fig. 8.13 the subgroup diagram for the subgroups of D_4. Look at the lovely symmetries in that diagram! ▲

Cayley's Theorem

Look at any group table in the text. Note how each row of the table gives a permutation of the set of elements of the group, as listed at the top of the table. Similarly, each column of the table gives a permutation of the group set, as listed at the left of the table. In view of these observations, it is not surprising that at least every finite group G is isomorphic to a subgroup of the group S_G of all permutations of G. The same is true for infinite groups; Cayley's theorem states that *every* group is isomorphic to some group consisting of permutations under permutation multiplication. This is a nice and intriguing result, and is a classic of group theory. At first glance, the theorem might seem to be a tool to answer *all* questions about groups. What it really shows is the generality of groups of permutations. Examining subgroups of all permutation groups S_A for sets A of all sizes would be a tremendous task. Cayley's theorem does show that if a counterexample exists to some conjecture we have made about groups, then some group of permutations will provide the counterexample.

We now proceed to the proof of Cayley's theorem, starting with a definition and then a lemma that is important in its own right.

■ 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 8.16 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.

8.14 Definition Let $f : A \to B$ be a function and let H be a subset of A. The **image of H under f** is $\{f(h) \mid h \in H\}$ and is denoted by $f[H]$. ■

8.15 Lemma Let G and G' be groups and let $\phi : G \to G'$ be a one-to-one function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Proof We show the conditions for a subgroup given in Theorem 5.14 are satisfied by $\phi[G]$. Let $x', y' \in \phi[G]$. Then there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By hypothesis, $\phi(xy) = \phi(x)\phi(y) = x'y'$, showing that $x'y' \in \phi[G]$. We have shown that $\phi[G]$ is closed under the operation of G'.

Let e' be the identity of G'. Then

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Cancellation in G' shows that $e' = \phi(e)$ so $e' \in \phi[G]$.

For $x' \in \phi[G]$ where $x' = \phi(x)$, we have

$$e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1}),$$

which shows that $x'^{-1} = \phi(x^{-1}) \in \phi[G]$. This completes the demonstration that $\phi[G]$ is a subgroup of G'.

That ϕ provides an isomorphism of G with $\phi[G]$ now follows at once because ϕ provides a one-to-one map of G *onto* $\phi[G]$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. ◆

8.16 Theorem **(Cayley's Theorem)** Every group is isomorphic to a group of permutations.

Proof Let G be a group. We show that G is isomorphic to a subgroup of S_G. By Lemma 8.15, we need only to define a one-to-one function $\phi : G \to S_G$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. For $x \in G$, let $\lambda_x : G \to G$ be defined by $\lambda_x(g) = xg$ for all $g \in G$. (We think of λ_x as performing *left multiplication* by x.) The equation $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$ for all $c \in G$ shows that λ_x maps G onto G. If $\lambda_x(a) = \lambda_x(b)$, then $xa = xb$ so $a = b$ by cancellation. Thus λ_x is also one to one, and is a permutation of G. We now define $\phi : G \to S_G$ by defining $\phi(x) = \lambda_x$ for all $x \in G$.

To show that ϕ is one to one, suppose that $\phi(x) = \phi(y)$. Then $\lambda_x = \lambda_y$ as functions mapping G into G. In particular $\lambda_x(e) = \lambda_y(e)$, so $xe = ye$ and $x = y$. Thus ϕ is one to one. It only remains to show that $\phi(xy) = \phi(x)\phi(y)$, that is, that $\lambda_{xy} = \lambda_x\lambda_y$. Now for any $g \in G$, we have $\lambda_{xy}(g) = (xy)g$. Permutation multiplication is function composition, so $(\lambda_x\lambda_y)(g) = \lambda_x(\lambda_y(g)) = \lambda_x(yg) = x(yg)$. Thus by associativity, $\lambda_{xy} = \lambda_x\lambda_y$. ◆

For the proof of the theorem, we could have considered equally well the permutations ρ_x of G defined by

$$\rho_x(g) = gx$$

for $g \in G$. (We can think of ρ_x as meaning *right multiplication* by x.) Exercise 52 shows that these permutations form a subgroup of S_G, again isomorphic to G, but provided by

a map $\mu : G \to S_G$ defined by

$$\mu(x) = \rho_{x^{-1}}.$$

8.17 Definition The map ϕ in the proof of Theorem 8.16 is the **left regular representation** of G, and the map μ in the preceding comment is the **right regular representation** of G. ■

8.18 Example Let us compute the left regular representation of the group given by the group table, Table 8.19. By "compute" we mean give the elements for the left regular representation and the group table. Here the elements are

$$\lambda_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}, \qquad \lambda_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}, \qquad \text{and} \qquad \lambda_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}.$$

The table for this representation is just like the original table with x renamed λ_x, as seen in Table 8.20. For example,

$$\lambda_a\lambda_b = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}\begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix} = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix} = \lambda_e. \qquad ▲$$

8.19 Table

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

8.20 Table

	λ_e	λ_a	λ_b
λ_e	λ_e	λ_a	λ_b
λ_a	λ_a	λ_b	λ_e
λ_b	λ_b	λ_e	λ_a

For a finite group given by a group table, ρ_a is the permutation of the elements corresponding to their order in the column under a at the very top, and λ_a is the permutation corresponding to the order of the elements in the row opposite a at the extreme left. The notations ρ_a and λ_a were chosen to suggest right and left multiplication by a, respectively.

EXERCISES 8

Computation

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

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

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. $|\langle\sigma\rangle|$ **7.** $|\langle\tau^2\rangle|$ **8.** σ^{100} **9.** μ^{100}

10. Partition the following collection of groups into subcollections of isomorphic groups. Here a * superscript means all nonzero elements of the set.

$\mathbb{Z}$ under addition	S_2
$\mathbb{Z}_6$	$\mathbb{R}^*$ under multiplication
$\mathbb{Z}_2$	$\mathbb{R}^+$ under multiplication
S_6	$\mathbb{Q}^*$ under multiplication
$17\mathbb{Z}$ under addition	$\mathbb{C}^*$ under multiplication
$\mathbb{Q}$ under addition	The subgroup $\langle \pi \rangle$ of $\mathbb{R}^*$ under multiplication
$3\mathbb{Z}$ under addition	The subgroup G of S_5 generated by $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$
$\mathbb{R}$ under addition	

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 11 through 13, find the orbit of 1 under the permutation defined prior to Exercise 1.

11. σ **12.** τ **13.** μ

14. In Table 8.8, we used ρ_0, ρ_1, ρ_2, μ_1, μ_2, μ_3 as the names of the 6 elements of S_3. Some authors use the notations ϵ, ρ, ρ^2, ϕ, $\rho\phi$, $\rho^2\phi$ for these elements, where their ϵ is our identity ρ_0, their ρ is our ρ_1, and their ϕ is our μ_1. Verify *geometrically* that their six expressions do give all of S_3.

15. With reference to Exercise 14, give a similar alternative labeling for the 8 elements of D_4 in Table 8.12.

16. Find the number of elements in the set $\{\sigma \in S_4 \mid \sigma(3) = 3\}$.

17. Find the number of elements in the set $\{\sigma \in S_5 \mid \sigma(2) = 5\}$.

18. Consider the group S_3 of Example 8.7

a. Find the cyclic subgroups $\langle \rho_1 \rangle$, $\langle \rho_2 \rangle$, and $\langle \mu_1 \rangle$ of S_3.

b. Find *all* subgroups, proper and improper, of S_3 and give the subgroup diagram for them.

19. Verify that the subgroup diagram for D_4 shown in Fig. 8.13 is correct by finding all (cyclic) subgroups generated by one element, then all subgroups generated by two elements, etc.

20. Give the multiplication table for the cyclic subgroup of S_5 generated by

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

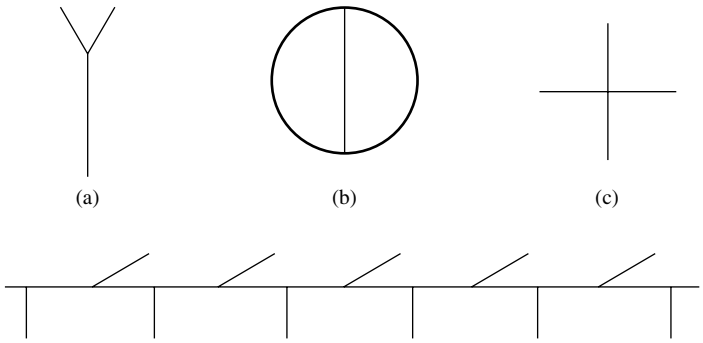
There will be six elements. Let them be ρ, ρ^2, ρ^3, ρ^4, ρ^5, and $\rho^0 = \rho^6$. Is this group isomorphic to S_3?

21. **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 $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ 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?



8.21 Figure

22. After working Exercise 21, write down eight matrices that form a group under matrix multiplication that is isomorphic to D_4.

In this section we discussed the group of symmetries of an equilateral triangle and of a square. In Exercises 23 through 26, give a group that we have discussed in the text that is isomorphic to the group of symmetries of the indicated figure. You may want to label some special points on the figure, write some permutations corresponding to symmetries, and compute some products of permutations.

23. The figure in Fig. 8.21 (a)

24. The figure in Fig. 8.21 (b)

25. The figure in Fig. 8.21 (c)

26. The figure in Fig. 8.21 (d)

27. Compute the left regular representation of $\mathbb{Z}_4$. Compute the right regular representation of S_3 using the notation of Example 8.7.

Concepts

In Exercises 28 and 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.

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

29. 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.

In Exercises 30 through 34, determine whether the given function is a permutation of $\mathbb{R}$.

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

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

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

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

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

35. Mark each of the following 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 group G is isomorphic to a subgroup of S_G.

_____ **e.** Every subgroup of an abelian group is abelian.

_____ **f.** Every element of a group generates a cyclic subgroup of the group.

_____ **g.** The symmetric group S_{10} has 10 elements.

_____ **h.** The symmetric group S_3 is cyclic.

_____ **i.** S_n is not cyclic for any n.

_____ **j.** Every group is isomorphic to some group of permutations.

36. Show by an example that every proper subgroup of a nonabelian group may be abelian.

37. Let A be a nonempty set. What type of algebraic structure mentioned previously in the text is given by the set of *all* functions mapping A into itself under function composition?

38. Indicate schematically a Cayley digraph for D_n using a generating set consisting of a rotation through $2\pi/n$ radians and a reflection (mirror image). See Exercise 44.

Proof Synopsis

39. Give a two-sentence synopsis of the proof of Cayley's theorem.

Theory

In Exercises 40 through 43, let A be a set, B a subset of A, and let b be one particular element of B. Determine whether the given set is sure to be a subgroup of S_A under the induced operation. Here $\sigma[B] = \{\sigma(x) \mid x \in B\}$.

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

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

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

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

44. In analogy with Examples 8.7 and 8.10, consider a regular plane n-gon for $n \geq 3$. Each way that two copies of such an n-gon can be placed, with one covering the other, corresponds to a certain permutation of the vertices. The set of these permutations is a group, the **nth dihedral group** D_n, under permutation multiplication. Find the order of this group D_n. Argue *geometrically* that this group has a subgroup having just half as many elements as the whole group has.

45. Consider a cube that exactly fills a certain cubical box. As in Examples 8.7 and 8.10, the ways in which the cube can be placed into the box correspond to a certain group of permutations of the vertices of the cube. This group is the **group of rigid motions** (or **rotations) of the cube**. (It should not be confused with the *group of symmetries of the figure*, which will be discussed in the exercises of Section 12.) How many elements does this group have? Argue *geometrically* that this group has at least three different subgroups of order 4 and at least four different subgroups of order 3.

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

47. Strengthening Exercise 46, 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.

48. Orbits were defined before Exercise 11. 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 $\mathcal{O}_{a,\sigma} = \mathcal{O}_{b,\sigma}$.

49. If A is a set, then a subgroup H of S_A is **transitive on** A if for each $a, b \in A$ there exists $\sigma \in H$ such that $\sigma(a) = b$. Show that if A is a nonempty finite set, then there exists a finite cyclic subgroup H of S_A with $|H| = |A|$ that is transitive on A.

50. Referring to the definition before Exercise 11 and to Exercise 49, show that for $\sigma \in S_A$, $\langle\sigma\rangle$ is transitive on A if and only if $\mathcal{O}_{a,\sigma} = A$ for some $a \in A$.

51. (See the warning on page 78). 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 class room 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 $*'$.

52. Let G be a group. Prove that the permutations $\rho_a : G \to G$, where $\rho_a(x) = xa$ for $a \in G$ and $x \in G$, do form a group isomorphic to G.

53. A **permutation matrix** is one that can be obtained from an identity matrix by reordering its rows. If P is an $n \times n$ permutation matrix and A is any $n \times n$ matrix and $C = PA$, then C can be obtained from A by making precisely the same reordering of the rows of A as the reordering of the rows which produced P from I_n.

a. Show that every finite group of order n is isomorphic to a group consisting of $n \times n$ permutation matrices under matrix multiplication.

b. For each of the four elements $e, a, b,$ and c in the Table 5.11 for the group V, give a specific 4×4 matrix that corresponds to it under such an isomorphism.

SECTION 9 Orbits, Cycles, and the Alternating Groups

Orbits

Each permutation σ of a set A determines a natural partition of A into cells with the property that $a, b \in A$ are in the same cell if and only if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. We establish this partition using an appropriate equivalence relation:

$$\text{For } a, b \in A, \text{ let } a \sim b \text{ if and only if } b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}. \qquad \textbf{(1)}$$

We now check that $\sim$ defined by Condition (1) is indeed an equivalence relation.

Reflexive Clearly $a \sim a$ since $a = \iota(a) = \sigma^0(a)$.

Symmetric If $a \sim b$, then $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. But then $a = \sigma^{-n}(b)$ and $-n \in \mathbb{Z}$, so $b \sim a$.

Transitive Suppose $a \sim b$ and $b \sim c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $n, m \in \mathbb{Z}$. Substituting, we find that $c = \sigma^m(\sigma^n(a)) = \sigma^{n+m}(a)$, so $a \sim c$.

9.1 Definition Let σ be a permutation of a set A. The equivalence classes in A determined by the equivalence relation (1) are the **orbits of** σ. ■

9.2 Example Since the identity permutation ι of A leaves each element of A fixed, the orbits of ι are the one-element subsets of A. ▲

9.3 Example Find the orbits of the permutation

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

in S_8.

Solution To find the orbit containing 1, we apply σ repeatedly, obtaining symbolically

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} \cdots.$$

Since σ^{-1} would simply reverse the directions of the arrows in this chain, we see that the orbit containing 1 is $\{1, 3, 6\}$. We now choose an integer from 1 to 8 not in $\{1, 3, 6\}$, say 2, and similarly find that the orbit containing 2 is $\{2, 8\}$. Finally, we find that the orbit containing 4 is $\{4, 7, 5\}$. Since these three orbits include all integers from 1 to 8, we see that the complete list of orbits of σ is

$$\{1, 3, 6\}, \quad \{2, 8\}, \quad \{4, 5, 7\}. \qquad \blacktriangle$$

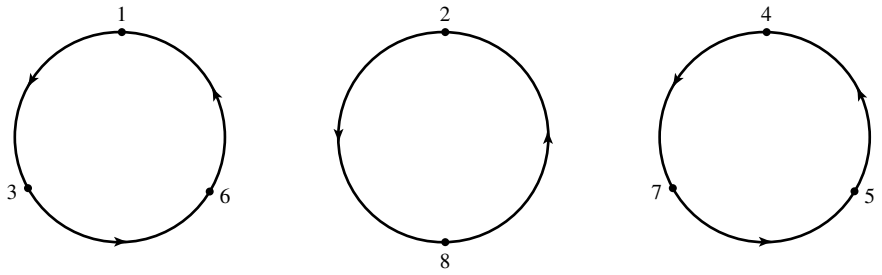
Cycles

For the remainder of this section, we consider just permutations of a finite set A of n elements. We may as well suppose that $A = \{1, 2, 3, \cdots, n\}$ and that we are dealing with elements of the symmetric group S_n.

Refer back to Example 9.3. The orbits of

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

are indicated graphically in Fig. 9.4. That is, σ acts on each integer from 1 to 8 on one of the circles by carrying it into the next integer on the circle traveled counterclockwise, in the direction of the arrows. For example, the leftmost circle indicates that $\sigma(1) = 3$, $\sigma(3) = 6$, and $\sigma(6) = 1$. Figure 9.4 is a nice way to visualize the structure of the permutation σ.

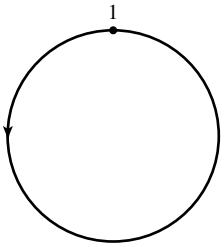


9.4 Figure

Each individual circle in Fig. 9.4 also defines, by itself, a permutation in S_8. For example, the leftmost circle corresponds to the permutation

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix} \tag{3}$$

that acts on 1, 3, and 6 just as σ does, but leaves the remaining integers 2, 4, 5, 7, and 8 fixed. In summary, μ has one three-element orbit $\{1, 3, 6\}$ and five one-element orbits $\{2\}, \{4\}, \{5\}, \{7\}$, and $\{8\}$. Such a permutation, described graphically by a single circle, is called a *cycle* (for circle). We consider the identity permutation to be a cycle since it can be represented by a circle having only the integer 1, as shown in Fig. 9.5. We now define the term *cycle* in a mathematically precise way.



9.5 Figure

9.6 Definition A permutation $\sigma \in S_n$ is a **cycle** if it has at most one orbit containing more than one element. The **length** of a cycle is the number of elements in its largest orbit. ■

To avoid the cumbersome notation, as in Eq. (3), for a cycle, we introduce a single-row *cyclic notation*. In cyclic notation, the cycle in Eq. (3) becomes

$$\mu = (1, 3, 6).$$

We understand by this notation that μ carries the first number 1 into the second number 3, the second number 3 into the next number 6, etc., until finally the last number 6 is carried into the first number 1. An integer not appearing in this notation for μ is understood to be left fixed by μ. Of course, the set on which μ acts, which is $\{1, 2, 3, 4, 5, 6, 7, 8\}$ in our example, must be made clear by the context.

9.7 Example Working within S_5, we see that

$$(1, 3, 5, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

Observe that

$$(1, 3, 5, 4) = (3, 5, 4, 1) = (5, 4, 1, 3) = (4, 1, 3, 5).$$ ▲

Of course, since cycles are special types of permutations, they can be multiplied just as any two permutations. The product of two cycles need not again be a cycle, however.

Using cyclic notation, we see that the permutation σ in Eq. (2) can be written as a product of cycles:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1, 3, 6)(2, 8)(4, 7, 5). \quad \textbf{(4)}$$

These cycles are **disjoint**, meaning that any integer is moved by at most one of these cycles; thus no one number appears in the notations of two different cycles. Equation (4) exhibits σ in terms of its orbits, and is a one-line description of Fig. 9.4. Every permutation in S_n can be expressed in a similar fashion as a product of the disjoint cycles corresponding to its orbits. We state this as a theorem and write out the proof.

9.8 Theorem Every permutation σ of a finite set is a product of disjoint cycles.

Proof Let $B_1, B_2, \cdots, B_r$ be the orbits of σ, and let μ_i be the cycle defined by

$$\mu_i(x) = \begin{cases} \sigma(x) & \text{for } x \in B_i \\ x & \text{otherwise.} \end{cases}$$

Clearly $\sigma = \mu_1\mu_2 \cdots \mu_r$. Since the equivalence-class orbits $B_1, B_2, \cdots, B$, being distinct equivalence classes, are disjoint, the cycles $\mu_1, \mu_2, \cdots, \mu_r$ are disjoint also. ◆

While permutation multiplication in general is not commutative, it is readily seen that *multiplication of disjoint cycles is commutative*. Since the orbits of a permutation are unique, the representation of a permutation as a product of disjoint cycles, none of which is the identity permutation, is unique up to the order of the factors.

9.9 Example Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

Let us write it as a product of disjoint cycles. First, 1 is moved to 6 and then 6 to 1, giving the cycle (1, 6). Then 2 is moved to 5, which is moved to 3, which is moved to 2, or (2, 5, 3). This takes care of all elements but 4, which is left fixed. Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1, 6)(2, 5, 3).$$

Multiplication of *disjoint* cycles is commutative, so the order of the factors (1, 6) and (2, 5, 3) is not important. ▲

You should practice multiplying permutations in cyclic notation where the cycles may or may not be disjoint. We give an example and provide further practice in Exercises 7 through 9.

9.10 Example Consider the cycles (1,4,5,6) and (2,1,5) in S_6. Multiplying, we find that

$$(1, 4, 5, 6)(2, 1, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$

and

$$(2, 1, 5)(1, 4, 5, 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}.$$

Neither of these permutations is a cycle. ▲

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.

9.11 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 is a product of transpositions. We then have the following as a corollary to Theorem 9.8.

9.12 Corollary Any permutation of a finite set of at least two elements is a product of transpositions.

Naively, this corollary just states that any rearrangement of n objects can be achieved by successively interchanging pairs of them.

9.13 Example Following the remarks prior to the corollary, we see that (1, 6) (2, 5, 3) is the product (1, 6) (2, 3) (2, 5) of transpositions. ▲

9.14 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. We will give two proofs. The first uses a property of determinants from linear algebra. The second involves counting orbits and was suggested by David M. Bloom.

9.15 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.

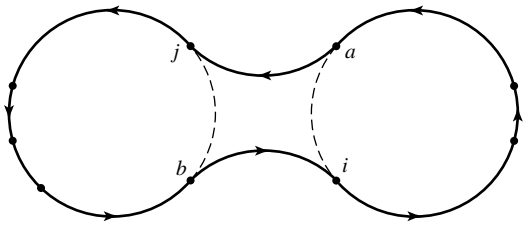
Proof 1 (From linear algebra) We remarked in Section 8 that $S_A \simeq S_B$ if A and B have the same cardinality. We work with permutations of the n rows of the $n \times n$ identity matrix I_n, rather than of the numbers $1, 2, \ldots, n$. The identity matrix has determinant 1. Interchanging any two rows of a square matrix changes the sign of the determinant. Let C be a matrix obtained by a permutation σ of the rows of I_n. If C could be obtained from I_n by both an even number and an odd number of transpositions of rows, its determinant would have to be both 1 and -1, which is impossible. Thus σ cannot be expressed both as a product of an even number and an odd number of transpositions.

Proof 2 (Counting orbits) 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. 9.16. 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.



9.16 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. 9.16. Exercise 28 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.

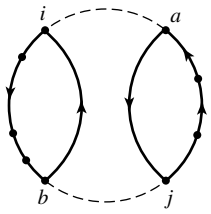
Case II Suppose i and j are in the same orbit of σ. We can then write σ as a product of disjoint cycles with the first cycle of the form

$$(a, i, \times, \times, \times, b, j, \times, \times)$$

shown symbolically by the circle in Fig. 9.17. 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. 9.17.



9.17 Figure

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. ◆

9.18 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. ■

9.19 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 permutation; 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 is 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 5.14, we see that we have proved the following statement.

9.20 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.

9.21 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 9

Computations

In Exercises 1 through 6, find all orbits of the given permutation.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 6 & 2 & 4 \end{pmatrix}$

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

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

4. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n + 1$

5. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n + 2$

6. $\sigma : \mathbb{Z} \to \mathbb{Z}$ where $\sigma(n) = n - 3$

In Exercises 7 through 9, compute the indicated product of cycles that are permutations of $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

7. $(1, 4, 5)(7, 8)(2, 5, 7)$

8. $(1, 3, 2, 7)(4, 8, 6)$

9. $(1, 2)(4, 7, 8)(2, 1)(7, 2, 8, 1, 5)$

In Exercises 10 through 12, 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.

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

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

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

13. Recall that element a of a group G with identity element e has order $r > 0$ if $a^r = e$ and no smaller positive power of a is the identity. Consider the group S_8.

- **a.** What is the order of the cycle $(1, 4, 5, 7)$?
- **b.** State a theorem suggested by part (a).
- **c.** What is the order of $\sigma = (4, 5)(2, 3, 7)$? of $\tau = (1, 4)(3, 5, 7, 8)$?
- **d.** Find the order of each of the permutations given in Exercises 10 through 12 by looking at its decomposition into a product of disjoint cycles.
- **e.** State a theorem suggested by parts (c) and (d). [*Hint:* The important words you are looking for are *least common multiple*.]

In Exercises 14 through 18, find the maximum possible order for an element of S_n for the given value of n.

14. $n = 5$ **15.** $n = 6$ **16.** $n = 7$ **17.** $n = 10$ **18.** $n = 15$

19. Figure 9.22 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.

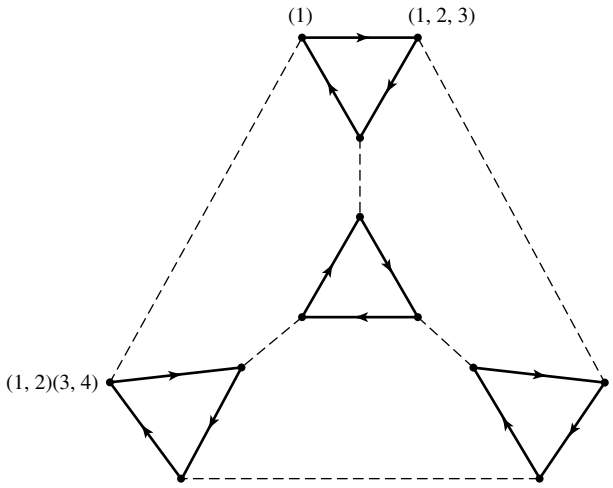
Concepts

In Exercises 20 through 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.

20. 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.

21. A *cycle* is a permutation having only one orbit.

22. The *alternating group* is the group of all even permutations.



9.22 Figure

23. Mark each of the following 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 9.15.
_____ **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.

24. Which of the permutations in S_3 of Example 8.7 are even permutations? Give the table for the alternating group A_3.

Proof Synopsis

25. Give a one-sentence synopsis of Proof 1 of Theorem 9.15.

26. Give a two-sentence synopsis of Proof 2 of Theorem 9.15.

Theory

27. 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.

28. **a.** Draw a figure like Fig. 9.16 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.

29. 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.

30. 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?

31. 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 30) is finite. Show that H is a subgroup of S_A.

32. Let A be an infinite set. Let K be the set of all $\sigma \in S_A$ that move (see Exercise 30) at most 50 elements of A. Is K a subgroup of S_A? Why?

33. 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.

34. Show that if σ is a cycle of odd length, then σ^2 is a cycle.

35. Following the line of thought opened by Exercise 34, 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 . . .

36. Let G be a group and let a be a fixed element of G. Show that the map $\lambda_a : G \to G$, given by $\lambda_a(g) = ag$ for $g \in G$, is a permutation of the set G.

37. Referring to Exercise 36, show that $H = \{\lambda_a \mid a \in G\}$ is a subgroup of S_G, the group of all permutations of G.

38. Referring to Exercise 49 of Section 8, show that H of Exercise 37 is transitive on the set G. [*Hint:* This is an immediate corollary of one of the theorems in Section 4.]

39. 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 Corollary 9.12]

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 14, 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 two partitions of G by defining two equivalence relations, $\sim_L$ and $\sim_R$ on G.

10.1 Theorem Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \qquad \text{if and only if} \qquad a^{-1}b \in H.$$

Let $\sim_R$ be defined by

$$a \sim_R b \qquad \text{if and only if} \qquad ab^{-1} \in H.$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof We show that $\sim_L$ is an equivalence relation, and leave the proof for $\sim_R$ to Exercise 26. 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. If we go through the same reasoning for the equivalence relation $\sim_R$ defined by H, we find the cell in this partition containing $a \in G$ is $Ha = \{ha \mid h \in H\}$. Since G need not be abelian, we have no reason to expect aH and Ha to be the same subset of G. We give a formal definition.

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, while the subset $Ha = \{ha \mid h \in H\}$ is the **right coset** of H containing a. ■

10.3 Example Exhibit the left cosets and the right cosets 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 $3\mathbb{Z}$.

Since $\mathbb{Z}$ is abelian, the left coset $m + 3\mathbb{Z}$ and the right coset $3\mathbb{Z} + m$ are the same, so the partition of $\mathbb{Z}$ into right cosets is the same. ▲

We observe two things from Example 10.3.

> For a subgroup H of an abelian group G, the partition of G into left cosets of H and the partition into right cosets are the same.

Also, looking back at Examples 0.17 and 0.20, we see that the equivalence relation $\sim_R$ for the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is the same as the relation of congruence modulo n. Recall that $h \equiv k \pmod{n}$ in $\mathbb{Z}$ if $h - k$ is divisible by n. This is the same as saying that $h + (-k)$ is in $n\mathbb{Z}$, which is relation $\sim_R$ of Theorem 10.1 in additive notation. Thus the partition of $\mathbb{Z}$ into cosets of $n\mathbb{Z}$ is the partition of $\mathbb{Z}$ into residue classes modulo n. For that reason, we often refer to the cells of this partition as *cosets modulo* $n\mathbb{Z}$. Note that we do not have to specify *left* or *right* cosets since they are the same for this abelian group $\mathbb{Z}$.

10.4 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 14. Referring back to Example 10.4, Table 10.5 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.

Suppose we denote these cosets by LT(light), MD(medium), and DK(dark) according to their shading. Table 10.5 then defines a binary operation on these shadings, as shown in Table 10.6. Note that if we replace LT by 0, MD by 1, and DK by 2 in Table 10.6, we obtain the table for $\mathbb{Z}_3$. Thus the table of shadings forms a group! We will see in

10.5 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

10.6 Table

	LT	MD	DK
LT	LT	MD	DK
MD	MD	DK	LT
DK	DK	LT	MD

Section 14 that for a partition of an *abelian* group into cosets of a subgroup, reordering the group table according to the elements in the cosets always gives rise to such a *coset group*.

10.7 Example Table 10.8 again shows Table 8.8 for the symmetric group S_3 on three letters. Let H be the subgroup $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$ of S_3. Find the partitions of S_3 into left cosets of H, and the partition into right cosets of H.

Solution For the partition into left cosets, we have

$$\begin{aligned} H &= \{\rho_0, \mu_1\}, \\ \rho_1 H &= \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\}, \\ \rho_2 H &= \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}. \end{aligned}$$

The partition into right cosets is

$$\begin{aligned} H &= \{\rho_0, \mu_1\}, \\ H\rho_1 &= \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\}, \\ H\rho_2 &= \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}. \end{aligned}$$

The partition into left cosets of H is different from the partition into right cosets. For example, the left coset containing ρ_1 is $\{\rho_1, \mu_3\}$, while the right coset containing ρ_1 is $\{\rho_1, \mu_2\}$. This does not surprise us since the group S_3 is not abelian. ▲

Referring to Example 10.7, Table 10.9 gives permutation multiplication in S_3. The elements are listed in the order they appear in the left cosets $\{\rho_0, \mu_1\}$, $\{\rho_1, \mu_3\}$, $\{\rho_2, \mu_2\}$ found in that example. Again, we have shaded the table light, medium, and dark according to the coset to which the element belongs. Note the difference between this table and Table 10.5. This time, the body of the table does not split up into 2×2 blocks opposite and under the shaded cosets at the left and the top, as in Table 10.5 and we don't get a coset group. The product of a light element and a dark one may be either dark or medium.

Table 10.8 is shaded according to the two left cosets of the subgroup $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$ of S_3. These are also the two right cosets, even though S_3 is not abelian.

10.8 Table

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

10.9 Table

	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
ρ_0	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
μ_1	μ_1	ρ_0	μ_2	ρ_2	μ_3	ρ_1
ρ_1	ρ_1	μ_3	ρ_2	μ_2	ρ_0	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_0	μ_2	ρ_2
ρ_2	ρ_2	μ_2	ρ_0	μ_1	ρ_1	μ_3
μ_2	μ_2	ρ_2	μ_3	ρ_1	μ_1	ρ_0

From Table 10.8 it is clear that we do have a coset group isomorphic to $\mathbb{Z}_2$ in this case. We will see in Section 14 that the left cosets of a subgroup H of a group G give rise to a coset group precisely when the partition of G into left cosets of H is the same as the partition into right cosets of H. In such a case, we may simply speak of the *cosets of* H, omitting the adjective left or right. We discuss coset groups in detail in Section 14, but we think it will be easier for you to understand them then if you experiment a bit with them now. Some of the exercises in this section are designed for such experimentation.

The Theorem of Lagrange

Let H be a subgroup of a group G. We claim that every left coset and every right coset of H have the same number of elements as H. We show this by exhibiting a *one-to-one* map of H *onto* a left coset gH of H for a fixed element g of G. If H is of finite order, this will show that gH has the same number of elements as H. If H is infinite, the existence of such a map is taken as the *definition* for equality of the size of H and the size of gH. (See Definition 0.13.)

Our choice for a one-to-one map $\phi : H \to gH$ is the natural one. Let $\phi(h) = gh$ for each $h \in H$. This map is onto gH by the definition of gH as $\{gh \mid h \in H\}$. To show that it is one to one, suppose that $\phi(h_1) = \phi(h_2)$ for h_1 and h_2 in H. Then $gh_1 = gh_2$ and by the cancellation law in the group G, we have $h_1 = h_2$. Thus ϕ is one to one.

Of course, a similar one-to-one map of H onto the right coset Hg can be constructed. (See Exercise 27.) We summarize as follows:

> Every coset (left or right) of a subgroup H of a group G has the same number of elements as H.

We can now prove the theorem of Lagrange.

10.10 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. The preceding boxed statement 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. *Never underestimate results that count something*! We continue to derive consequences of Theorem 10.10, which should be regarded as a counting theorem.

10.11 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 10.10, 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.

10.12 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 Theorem 10.10. ◆

10.13 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. Exercise 35 shows the index $(G : H)$ could be equally well defined as the number of right cosets of H in G. We state a basic theorem concerning indices of subgroups, and leave the proof to the exercises (see Exercise 38).

10.14 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 $(G : K) = (G : H)(H : K)$.

Theorem 10.10 shows that if there is a subgroup H of a finite group G, then the order of H divides the order of G. Is the converse true? That is, if G is a group of order n, and m divides n, is there always a subgroup of order m? We will see in the next section that this is true for abelian groups. However, A_4 can be shown to have no subgroup of order 6, which gives a counterexample for nonabelian groups.

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 $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.

4. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

5. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.

6. Find all left cosets of the subgroup $\{\rho_0, \mu_2\}$ of the group D_4 given by Table 8.12.

7. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left cosets?

8. Rewrite Table 8.12 in the order exhibited by the left cosets in Exercise 6. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group V?

9. Repeat Exercise 6 for the subgroup $\{\rho_0, \rho_2\}$ of D_4.

10. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left coset?

11. Rewrite Table 8.12 in the order exhibited by the left cosets in Exercise 9. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group V?

12. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.

13. Find the index of $\langle \mu_1 \rangle$ in the group S_3, using the notation of Example 10.7

14. Find the index of $\langle \mu_2 \rangle$ in the group D_4 given in Table 8.12

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 and 18, 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. Mark each of the following 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.

In Exercises 20 through 24, give an example of the desired subgroup and group if possible. If impossible, say why it is impossible.

20. A subgroup of an abelian group G whose left cosets and right cosets give different partitions of G

21. A subgroup of a group G whose left cosets give a partition of G into just one cell

22. A subgroup of a group of order 6 whose left cosets give a partition of the group into 6 cells

23. A subgroup of a group of order 6 whose left cosets give a partition of the group into 12 cells

24. A subgroup of a group of order 6 whose left cosets give a partition of the group into 4 cells

Proof Synopsis

25. Give a one-sentence synopsis of the proof of Theorem 10.10.

Theory

26. Prove that the relation $\sim_R$ of Theorem 10.1 is an equivalence relation.

27. 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.

28. 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.

29. 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 28.)

Let H be a subgroup of a group G and let $a, b \in G$. In Exercises 30 through 33 prove the statement or give a counterexample.

30. If $aH = bH$, then $Ha = Hb$.

31. If $Ha = Hb$, then $b \in Ha$.

32. If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.

33. If $aH = bH$, then $a^2H = b^2H$.

34. Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

35. 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.)

36. Exercise 29 of Section 4 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.

37. Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order.

38. Prove Theorem 10.14 [*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.]

39. 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.

40. Show that if a group G with identity e has finite order n, then $a^n = e$ for all $a \in G$.

41. Show that every left coset of the subgroup $\mathbb{Z}$ of the additive group of real numbers contains exactly one element x such that $0 \leq x < 1$.

42. 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 $\sin x$.)

43. 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.**)

44. 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).

45. 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.

46. 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 45 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 6.16.]

47. 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 10.12 and Exercise 46 to show that G must contain an element of order $n = |G|$.]

SECTION 11 Direct Products and 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 of Section 8, 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.

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.

11.1 Definition The **Cartesian product of sets** $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \cdots \times S_n$$

or by

$$\prod_{i=1}^{n} S_i. \qquad \blacksquare$$

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*

45. 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.

46. 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 45 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 6.16.]

47. 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 10.12 and Exercise 46 to show that G must contain an element of order $n = |G|$.]

SECTION 11 Direct Products and 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 of Section 8, 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.

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.

11.1 Definition The **Cartesian product of sets** $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \cdots \times S_n$$

or by

$$\prod_{i=1}^{n} S_i. \qquad \blacksquare$$

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.

11.2 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 the S_i has r_i elements for $i = 1, \cdots, n$, then $\prod_{i=1}^{n} S_i$ has $r_1r_2 \cdots r_n$ elements, for in an n-tuple, there are r_1 choices for the first component from S_1, and for each of these there are r_2 choices for the next component from S_2, and so on.

11.3 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 $\mathbb{Z}_6$. ▲

11.4 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:

11.5 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 5.17. 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.

11.6 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.

11.7 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 47 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.

11.8 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 11.8 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*.

11.9 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 11.5. 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. ◆

11.10 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 6.14.) 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 $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. ▲

11.11 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

$$\overline{G}_i = \{(e_1, e_2, \cdots, e_{i-1}, a_i, e_{i+1}, \cdots, e_n) \mid a_i \in G_i\},$$

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 $\overline{G}_i$ 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 $\overline{G}_i$, 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 $\overline{G}_i$. The direct product given by Theorem 11.2 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.

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 26.) But it was Kummer's student Leopold Kronecker (see the Historical Note in Section 29) 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 11.12 restricted to finite groups.

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 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 all sufficiently small abelian groups, in particular, about all finite abelian groups.

11.12 Theorem **(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. ◆

11.13 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 11.12. 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 11.12, 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. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
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. ▲

Applications

We conclude this section with a sampling of the many theorems we could now prove regarding abelian groups.

11.14 Definition A group G is **decomposable** if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is **indecomposable**. ■

11.15 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 11.12, 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 $p^{\max(i,j)} < p^r$. ◆

11.16 Theorem If m divides the order of a finite abelian group G, then G has a subgroup of order m.

Proof By Theorem 11.12, 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 $0 \le s_i \le r_i$. By Theorem 6.14, $(p_i)^{r_i-s_i}$ 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. ◆

11.17 Theorem If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.

Proof Let G be an abelian group of square free order m. Then by Theorem 11.12, G is isomorphic to

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}},$$

where $m = (p_1)^{r_1}(p_2)^{r_2}\cdots(p_n)^{r_n}$. Since m is square free, we must have all $r_i = 1$ and all p_i distinct primes. Corollary 11.6 then shows that G is isomorphic to $\mathbb{Z}_{p_1p_2\cdots p_n}$, so G is cyclic. ◆

EXERCISES 11

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. (2, 3) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

5. (8, 10) in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

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 $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$.

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 11.13 to find all abelian groups, up to isomorphism, of the given order.

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 7.9(b) shows such a Cayley digraph with $n = 3$, and Figure 7.11(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. Mark each of the following 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. Mark each of the following 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 11.12.

_____ **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 11.12 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. The part of the decomposition of G in Theorem 11.12 corresponding to the subgroups of prime-power order can also be written in the form $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, where m_i divides m_{i+1} for $i = 1, 2, \cdots, r-1$. The numbers m_i can be shown to be unique, and are the **torsion coefficients** of G.

a. Find the torsion coefficients of $\mathbb{Z}_4 \times \mathbb{Z}_9$.

b. Find the torsion coefficients of $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20}$.

c. Describe an algorithm to find the torsion coefficients of a direct product of cyclic groups.

Proof Synopsis

45. Give a two-sentence synopsis of the proof of Theorem 11.5.

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 48 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. Can the hypothesis of commutativity be dropped? Why, or why not?

54. Let G, H, and K be finitely generated abelian groups. Show that if $G \times K$ is isomorphic to $H \times K$, then $G \simeq H$.

PART III

Homomorphisms and Factor Groups

Section 13 Homomorphisms
Section 14 Factor Groups
Section 15 Factor-Group Computations and Simple Groups
Section 16 ‡Group Action on a Set
Section 17 †Applications of G-Sets to Counting

SECTION 13 HOMOMORPHISMS

Structure-Relating Maps

Let G and G' be groups. We are interested in maps from G to G' that relate the group structure of G to the group structure of G'. Such a map often gives us information about one of the groups from known structural properties of the other. An isomorphism $\phi : G \to G'$, if one exists, is an example of such a structure-relating map. If we know all about the group G and know that ϕ is an isomorphism, we immediately know all about the group structure of G', for it is structurally just a copy of G. We now consider more general structure-relating maps, weakening the conditions from those of an isomorphism by no longer requiring that the maps be one to one and onto. You see, those conditions are the purely *set-theoretic portion* of our definition of an isomorphism, and have nothing to do with the binary operations of G and of G'. The binary operations are what give us the *algebra* which is the focus of our study in this text. We keep just the homomorphism property of an isomorphism related to the binary operations for the definition we now make.

13.1 Definition A map ϕ of a group G into a group G' is a **homomorphism** if the homomorphism property

$$\phi(ab) = \phi(a)\phi(b) \tag{1}$$

holds for all $a, b \in G$. ■

‡ Section 16 is a prerequisite only for Sections 17 and 36.

† Section 17 is not required for the remainder of the text.

Let us now examine the idea behind the requirement (1) for a homomorphism $\phi : G \to G'$. In Eq. (1), the product ab on the left-hand side takes place in G, while the product $\phi(a)\phi(b)$ on the right-hand side takes place in G'. Thus Eq. (1) gives a relation between these binary operations, and hence between the two group structures.

For any groups G and G', there is always at least one homomorphism $\phi : G \to G'$, namely the **trivial homomorphism** defined by $\phi(g) = e'$ for all $g \in G$, where e' is the identity in G'. Equation (1) then reduces to the true equation $e' = e'e'$. No information about the structure of G or G' can be gained from the other group using this trivial homomorphism. We give an example illustrating how a homomorphism ϕ mapping G onto G' may give structural information about G'.

13.2 Example Let $\phi : G \to G'$ be a group homomorphism of G *onto* G'. We claim that if G is abelian, then G' must be abelian. Let $a', b' \in G'$. We must show that $a'b' = b'a'$. Since ϕ is onto G', there exist $a, b \in G$ such that $\phi(a) = a'$ and $\phi(b) = b'$. Since G is abelian, we have $ab = ba$. Using property (1), we have $a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'$, so G' is indeed abelian. ▲

Example 13.16 will give an illustration showing how information about G' may give information about G via a homomorphism $\phi : G \to G'$. We now give examples of homomorphisms for specific groups.

13.3 Example Let S_n be the symmetric group on n letters, and let $\phi : S_n \to \mathbb{Z}_2$ be defined by

$$\phi(\sigma) = \begin{cases} 0 & \text{if } \sigma \text{ is an even permutation,} \\ 1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Show that ϕ is a homomorphism.

Solution We must show that $\phi(\sigma\mu) = \phi(\sigma) + \phi(\mu)$ for all choices of $\sigma, \mu \in S_n$. Note that the operation on the right-hand side of this equation is written additively since it takes place in the group $\mathbb{Z}_2$. Verifying this equation amounts to checking just four cases:

σ odd and μ odd,

σ odd and μ even,

σ even and μ odd,

σ even and μ even.

Checking the first case, if σ and μ can both be written as a product of an odd number of transpositions, then $\sigma\mu$ can be written as the product of an even number of transpositions. Thus $\phi(\sigma\mu) = 0$ and $\phi(\sigma) + \phi(\mu) = 1 + 1 = 0$ in $\mathbb{Z}_2$. The other cases can be checked similarly. ▲

13.4 Example **(Evaluation Homomorphism)** Let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, let $\mathbb{R}$ be the additive group of real numbers, and let c be any real number. Let $\phi_c : F \to \mathbb{R}$ be the **evaluation homomorphism** defined by $\phi_c(f) = f(c)$ for $f \in F$. Recall that, by definition, the sum of two functions f and g is the function $f + g$ whose value at x is $f(x) + g(x)$. Thus we have

$$\phi_c(f + g) = (f + g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g),$$

and Eq. (1) is satisfied, so we have a homomorphism. ▲

13.5 Example Let $\mathbb{R}^n$ be the additive group of column vectors with n real-number components. (This group is of course isomorphic to the direct product of $\mathbb{R}$ under addition with itself for n factors.) Let A be an $m \times n$ matrix of real numbers. Let $\phi : \mathbb{R}^n \to \mathbb{R}^m$ be defined by $\phi(\mathbf{v}) = A\mathbf{v}$ for each column vector $\mathbf{v} \in \mathbb{R}^n$. Then ϕ is a homomorphism, since for $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, matrix algebra shows that $\phi(\mathbf{v} + \mathbf{w}) = A(\mathbf{v} + \mathbf{w}) = A\mathbf{v} + A\mathbf{w} = \phi(\mathbf{v}) + \phi(\mathbf{w})$. In linear algebra, such a map computed by multiplying a column vector on the left by a matrix A is known as a **linear transformation**. ▲

13.6 Example Let $GL(n, \mathbb{R})$ be the multiplicative group of all invertible $n \times n$ matrices. Recall that a matrix A is invertible if and only if its determinant, $\det(A)$, is nonzero. Recall also that for matrices $A, B \in GL(n, \mathbb{R})$ we have

$$\det(AB) = \det(A)\det(B).$$

This means that det is a homomorphism mapping $GL(n, \mathbb{R})$ into the multiplicative group $\mathbb{R}^*$ of nonzero real numbers. ▲

Homomorphisms of a group G into itself are often useful for studying the structure of G. Our next example gives a nontrivial homomorphism of a group into itself.

13.7 Example Let $r \in \mathbb{Z}$ and let $\phi_r : \mathbb{Z} \to \mathbb{Z}$ be defined by $\phi_r(n) = rn$ for all $n \in \mathbb{Z}$. For all $m, n \in \mathbb{Z}$, we have $\phi_r(m + n) = r(m + n) = rm + rn = \phi_r(m) + \phi_r(n)$ so ϕ_r is a homomorphism. Note that ϕ_0 is the trivial homomorphism, ϕ_1 is the identity map, and ϕ_{-1} maps $\mathbb{Z}$ *onto* $\mathbb{Z}$. For all other r in $\mathbb{Z}$, the map ϕ_r is not onto $\mathbb{Z}$. ▲

13.8 Example Let $G = G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_n$ be a direct product of groups. The **projection map** $\pi_i : G \to G_i$ where $\pi_i(g_1, g_2, \cdots, g_i, \cdots, g_n) = g_i$ is a homomorphism for each $i = 1, 2, \cdots, n$. This follows immediately from the fact that the binary operation of G coincides in the ith component with the binary operation in G_i. ▲

13.9 Example Let F be the additive group of continuous functions with domain $[0, 1]$ and let $\mathbb{R}$ be the additive group of real numbers. The map $\sigma : F \to \mathbb{R}$ defined by $\sigma(f) = \int_0^1 f(x)dx$ for $f \in F$ is a homomorphism, for

$$\begin{aligned}\sigma(f + g) &= \int_0^1 (f + g)(x)dx = \int_0^1 [f(x) + g(x)]dx \\ &= \int_0^1 f(x)dx + \int_0^1 g(x)dx = \sigma(f) + \sigma(g)\end{aligned}$$

for all $f, g \in F$. ▲

13.10 Example **(Reduction Modulo *n*)** Let γ be the natural map of $\mathbb{Z}$ into $\mathbb{Z}_n$ given by $\gamma(m) = r$, where r is the remainder given by the division algorithm when m is divided by n. Show that γ is a homomorphism.

Solution We need to show that

$$\gamma(s + t) = \gamma(s) + \gamma(t)$$

for $s, t \in \mathbb{Z}$. Using the division algorithm, we let

$$s = q_1 n + r_1 \qquad \textbf{(2)}$$

and

$$t = q_2 n + r_2 \tag{3}$$

where $0 \leq r_i < n$ for $i = 1, 2$. If

$$r_1 + r_2 = q_3 n + r_3 \tag{4}$$

for $0 \leq r_3 < n$, then adding Eqs. (2) and (3) we see that

$$s + t = (q_1 + q_2 + q_3)n + r_3,$$

so that $\gamma(s + t) = r_3$.

From Eqs. (2) and (3) we see that $\gamma(s) = r_1$ and $\gamma(t) = r_2$. Equation (4) shows that the sum $r_1 + r_2$ in $\mathbb{Z}_n$ is equal to r_3 also.

Consequently $\gamma(s + t) = \gamma(s) + \gamma(t)$, so we do indeed have a homomorphism. ▲

Each of the homomorphisms in the preceding three examples is a many-to-one map. That is, different points of the domain of the map may be carried into the same point. Consider, for illustration, the homomorphism $\pi_1 : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2$ in Example 13.8 We have

$$\pi_1(0, 0) = \pi_1(0, 1) = \pi_1(0, 2) = \pi_1(0, 3) = 0,$$

so four elements in $\mathbb{Z}_2 \times \mathbb{Z}_4$ are mapped into 0 in $\mathbb{Z}_2$ by π_1.

Composition of group homomorphisms is again a group homomorphism. That is, if $\phi : G \to G'$ and $\gamma : G' \to G''$ are both group homomorphisms then their composition $(\gamma \circ \phi) : G \to G''$, where $(\gamma \circ \phi)(g) = \gamma(\phi(g))$ for $g \in G$, is also a homomorphism. (See Exercise 49.)

Properties of Homomorphisms

We turn to some structural features of G and G' that are *preserved* by a homomorphism $\phi : G \to G'$. First we review set-theoretic definitions. Note the use of *square brackets* when we apply a function to a *subset* of its domain.

13.11 Definition Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The **image** $\phi[A]$ **of** A **in** Y **under** ϕ is $\{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the **range of** ϕ. The **inverse image** $\phi^{-1}[B]$ **of** B **in** X is $\{x \in X \mid \phi(x) \in B\}$. ■

The first three properties of a homomorphism stated in the theorem that follows have already been encountered for the special case of an isomorphism; namely, in Theorem 3.14, Exercise 28 of Section 4, and Exercise 41 of Section 5. There they were really obvious because the structures of G and G' were identical. We will now see that they hold for structure-relating maps of groups, even if the maps are not one to one and onto. We do not consider them obvious in this new context.

13.12 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 $G' \cap \phi[G]$, 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

$$\phi(a) = \phi(ae) = \phi(a)\phi(e).$$

Multiplying on the left by $\phi(a)^{-1}$, 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 $\phi(a^{-1}) = \phi(a)^{-1}$.

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'.

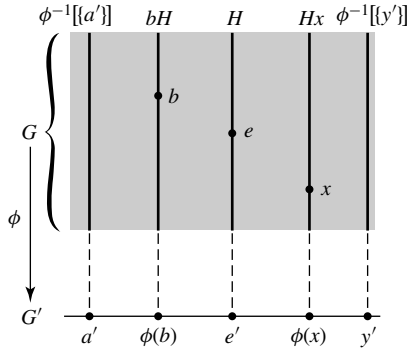
Going the other way for Statement (4), let K' be a subgroup of G'. Suppose a and b are in $\phi^{-1}[K']$. Then $\phi(a)\phi(b) \in K'$ since K' is a subgroup. The equation $\phi(ab) = \phi(a)\phi(b)$ shows that $ab \in \phi^{-1}[K']$. Thus $\phi^{-1}[K']$ is closed under the binary operation in G. Also, 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 13.12. This subgroup is critical to the study of homomorphisms.

13.13 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 $\text{Ker}(\phi)$. ■

Example 13.5 discussed the homomorphism $\phi : \mathbb{R}^n \to \mathbb{R}^m$ given by $\phi(\mathbf{v}) = A\mathbf{v}$ where A is an $m \times n$ matrix. In this context, $\text{Ker}(\phi)$ is called the *null space* of A. It consists of all $\mathbf{v} \in \mathbb{R}^n$ such that $A\mathbf{v} = \mathbf{0}$, the zero vector.

Let $H = \text{Ker}(\phi)$ for a homomorphism $\phi : G \to G'$. We think of ϕ as "collapsing" H down onto e'. Theorem 13.15 that follows shows that for $g \in G$, the cosets gH and Hg are the same, and are collapsed onto the single element $\phi(g)$ by ϕ. That is $\phi^{-1}[\{\phi(g)\}] = gH = Hg$. (Be sure that you understand the reason for the uses of (), [], and $\{\}$ in $\phi^{-1}[\{\phi(g)\}]$.) We have attempted to symbolize this collapsing in Fig. 13.14, where the shaded rectangle represents G, the solid vertical line segments represent the cosets of $H = \text{Ker}(\phi)$, and the horizontal line at the bottom represents G'. We view ϕ as projecting the elements of G, which are in the shaded rectangle, straight down onto elements of G', which are on the horizontal line segment at the bottom. Notice the downward arrow labeled ϕ at the left, starting at G and ending at G'. Elements of $H = \text{Ker}(\phi)$ thus lie on the solid vertical line segment in the shaded box lying over e', as labeled at the top of the figure.



13.14 Figure Cosets of H collapsed by ϕ.

13.15 Theorem Let $\phi : G \to G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\{\phi(a)\}] = \{x \in G \mid \phi(x) = \phi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

Proof We want to show that

$$\{x \in G \mid \phi(x) = \phi(a)\} = aH.$$

> There is a standard way to show that two sets are equal; show that each is a subset of the other.

Suppose that $\phi(x) = \phi(a)$. Then

$$\phi(a)^{-1}\phi(x) = e',$$

where e' is the identity of G'. By Theorem 13.12, we know that $\phi(a)^{-1} = \phi(a^{-1})$, so we have

$$\phi(a^{-1})\phi(x) = e'.$$

Since ϕ is a homomorphism, we have

$$\phi(a^{-1})\phi(x) = \phi(a^{-1}x), \qquad \text{so} \qquad \phi(a^{-1}x) = e'.$$

But this shows that $a^{-1}x$ is in $H = \text{Ker}(\phi)$, so $a^{-1}x = h$ for some $h \in H$, and $x = ah \in aH$. This shows that

$$\{x \in G \mid \phi(x) = \phi(a)\} \subseteq aH.$$

To show containment in the other direction, let $y \in aH$, so that $y = ah$ for some $h \in H$. Then

$$\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a),$$

so that $y \in \{x \in G \mid \phi(x) = \phi(a)\}$.

We leave the similar demonstration that $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$ to Exercise 52. ◆

13.16 Example Equation 5 of Section 1 shows that $|z_1 z_2| = |z_1||z_2|$ for complex numbers z_1 and z_2. This means that the absolute value function $|\ \ |$ is a homomorphism of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication onto the group $\mathbb{R}^+$ of positive real numbers under multiplication. Since $\{1\}$ is a subgroup of $\mathbb{R}^+$, Theorem 13.12 shows again that the complex numbers of magnitude 1 form a subgroup U of $\mathbb{C}^*$. Recall that the complex numbers can be viewed as filling the coordinate plane, and that the magnitude of a complex number is its distance from the origin. Consequently, the cosets of U are circles with center at the origin. Each circle is collapsed by this homomorphism onto its point of intersection with the positive real axis. ▲

We give an illustration of Theorem 13.15 from calculus.

13.17 Example Let D be the additive group of all differentiable functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$. Then differentiation gives us a map $\phi : D \to F$, where $\phi(f) = f'$ for $f \in F$. We easily see that ϕ is a homomorphism, for $\phi(f + g) = (f + g)' = f' + g' = \phi(f) + \phi(g)$; the derivative of a sum is the sum of the derivatives.

Now $\text{Ker}(\phi)$ consists of all functions f such that $f' = 0$, the zero constant function. Thus $\text{Ker}(\phi)$ consists of all constant functions, which form a subgroup C of F. Let us find all functions in D mapped into x^2 by ϕ, that is, all functions whose derivative is x^2. Now we know that $x^3/3$ is one such function. By Theorem 13.15, all such functions form the coset $x^3/3 + C$. Doesn't this look familiar? ▲

We will often use the following corollary of Theorem 13.15.

13.18 Corollary A group homomorphism $\phi : G \to G'$ is a one-to-one map if and only if $\text{Ker}(\phi) = \{e\}$.

Proof If $\text{Ker}(\phi) = \{e\}$, then for every $a \in G$, the elements mapped into $\phi(a)$ are precisely the elements of the left coset $a\{e\} = \{a\}$, which shows that ϕ is one to one.

Conversely, suppose ϕ is one to one. Now by Theorem 13.12, we know that $\phi(e) = e'$, the identity element of G'. Since ϕ is one to one, we see that e is the only element mapped into e' by ϕ, so $\text{Ker}(\phi) = \{e\}$. ◆

In view of Corollary 13.18, we modify the outline given prior to Example 3.8 for showing that a map ϕ is an isomorphism of binary structures when the structures are groups G and G'.

To Show $\phi : G \to G'$ Is an Isomorphism

Step 1 Show ϕ is a homomorphism.

Step 2 Show $\text{Ker}(\phi) = \{e\}$.

Step 3 Show ϕ maps G onto G'.

Theorem 13.15 shows that the kernel of a group homomorphism $\phi : G \to G'$ is a subgroup H of G whose left and right cosets coincide, so that $gH = Hg$ for all $g \in G$. We will see in Section 14 that when left and right cosets coincide, we can form a coset group, as discussed intuitively in Section 10. Furthermore, we will see that H then appears as the kernel of a homomorphism of G onto this coset group in a very natural way. Such subgroups H whose left and right cosets coincide are very useful in studying a group, and are given a special name. We will work with them a lot in Section 14.

Historical Note

Normal subgroups were introduced by Evariste Galois in 1831 as a tool for deciding whether a given polynomial equation was solvable by radicals. Galois noted that a subgroup H of a group G of permutations induced two decompositions of G into what we call *left cosets* and *right cosets.* If the two decompositions coincide, that is, if the left cosets are the same as the right cosets, Galois called the decomposition *proper*. Thus a subgroup giving a proper decomposition is what we call a *normal subgroup.* Galois stated that if the group of permutations of the roots of an equation has a proper decomposition, then one can solve the given equation if one can first solve an equation corresponding to the subgroup H and then an equation corresponding to the cosets.

Camille Jordan, in his commentaries on Galois's work in 1865 and 1869, elaborated on these ideas considerably. He also defined normal subgroups, although without using the term, essentially as on this page and likewise gave the first definition of a simple group (page 149).

13.19 Definition A subgroup H of a group G is **normal** if its left and right cosets coincide, that is, if $gH = Hg$ for all $g \in G$. ■

Note that all subgroups of abelian groups are normal.

13.20 Corollary If $\phi : G \to G'$ is a group homomorphism, then $\text{Ker}(\phi)$ is a normal subgroup of G.

Proof This follows immediately from the last sentence in the statement of Theorem 13.15 and Definition 13.19. ◆

For any group homomorphism $\phi : G \to G'$, two things are of primary importance: the *kernel of* ϕ, and the *image* $\phi[G]$ *of* G *in* G'. We have indicated the importance of

Ker(ϕ). Section 14 will indicate the importance of the image $\phi[G]$. Exercise 44 asks us to show that if $|G|$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

EXERCISES 13

Computations

In Exercises 1 through 15, determine whether the given map ϕ is a homomorphism. [*Hint:* The straightforward way to proceed is to check whether $\phi(ab) = \phi(a)\phi(b)$ for all a and b in the domain of ϕ. However, if we should happen to notice that $\phi^{-1}[\{e'\}]$ is not a subgroup whose left and right cosets coincide, or that ϕ does not satisfy the properties given in Exercise 44 or 45 for finite groups, then we can say at once that ϕ is not a homomorphism.]

1. Let $\phi : \mathbb{Z} \to \mathbb{R}$ under addition be given by $\phi(n) = n$.

2. Let $\phi : \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) =$ the greatest integer $\leq x$.

3. Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ under multiplication be given by $\phi(x) = |x|$.

4. Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder of x when divided by 2, as in the division algorithm.

5. Let $\phi : \mathbb{Z}_9 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder of x when divided by 2, as in the division algorithm.

6. Let $\phi : \mathbb{R} \to \mathbb{R}^*$, where $\mathbb{R}$ is additive and $\mathbb{R}^*$ is multiplicative, be given by $\phi(x) = 2^x$.

7. Let $\phi_i : G_i \to G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_r$ be given by $\phi_i(g_i) = (e_1, e_2, \ldots, g_i, \ldots, e_r)$, where $g_i \in G_i$ and e_j is the identity element of G_j. This is an **injection map**. Compare with Example 13.8.

8. Let G be any group and let $\phi : G \to G$ be given by $\phi(g) = g^{-1}$ for $g \in G$.

9. Let F be the additive group of functions mapping $\mathbb{R}$ into $\mathbb{R}$ having derivatives of all orders. Let $\phi : F \to F$ be given by $\phi(f) = f''$, the second derivative of f.

10. Let F be the additive group of all continuous functions mapping $\mathbb{R}$ into $\mathbb{R}$. Let $\mathbb{R}$ be the additive group of real numbers, and let $\phi : F \to \mathbb{R}$ be given by

$$\phi(f) = \int_0^4 f(x)dx.$$

11. Let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let $\phi : F \to F$ be given by $\phi(f) = 3f$.

12. Let M_n be the additive group of all $n \times n$ matrices with real entries, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi(A) = \det(A)$, the determinant of A, for $A \in M_n$.

13. Let M_n and $\mathbb{R}$ be as in Exercise 12. Let $\phi(A) = \text{tr}(A)$ for $A \in M_n$, where the **trace** tr(A) is the sum of the elements on the main diagonal of A, from the upper-left to the lower-right corner.

14. Let $GL(n, \mathbb{R})$ be the multiplicative group of invertible $n \times n$ matrices, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi : GL(n, \mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = \text{tr}(A)$, where tr(A) is defined in Exercise 13.

15. Let F be the multiplicative group of all continuous functions mapping $\mathbb{R}$ into $\mathbb{R}$ that are nonzero at every $x \in \mathbb{R}$. Let $\mathbb{R}^*$ be the multiplicative group of nonzero real numbers. Let $\phi : F \to \mathbb{R}^*$ be given by $\phi(f) = \int_0^1 f(x)dx$.

In Exercises 16 through 24, compute the indicated quantities for the given homomorphism ϕ. (See Exercise 46.)

16. Ker(ϕ) for $\phi : S_3 \to \mathbb{Z}_2$ in Example 13.3

17. Ker(ϕ) and $\phi(25)$ for $\phi : \mathbb{Z} \to \mathbb{Z}_7$ such that $\phi(1) = 4$

18. Ker(ϕ) and $\phi(18)$ for $\phi : \mathbb{Z} \to \mathbb{Z}_{10}$ such that $\phi(1) = 6$

19. Ker(ϕ) and $\phi(20)$ for $\phi : \mathbb{Z} \to S_8$ such that $\phi(1) = (1, 4, 2, 6)(2, 5, 7)$

20. Ker(ϕ) and $\phi(3)$ for $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ such that $\phi(1) = 8$

21. Ker(ϕ) and $\phi(14)$ for $\phi : \mathbb{Z}_{24} \to S_8$ where $\phi(1) = (2, 5)(1, 4, 6, 7)$

22. Ker(ϕ) and $\phi(-3, 2)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 3$ and $\phi(0, 1) = -5$

23. Ker(ϕ) and $\phi(4, 6)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$

24. Ker(ϕ) and $\phi(3, 10)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to S_{10}$ where $\phi(1, 0) = (3, 5)(2, 4)$ and $\phi(0, 1) = (1, 7)(6, 10, 8, 9)$

25. How many homomorphisms are there of $\mathbb{Z}$ onto $\mathbb{Z}$?

26. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}$?

27. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}_2$?

28. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gx$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

29. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gxg^{-1}$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

Concepts

In Exercises 30 and 31, 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.

30. A *homomorphism* is a map such that $\phi(xy) = \phi(x)\phi(y)$.

31. Let $\phi : G \to G'$ be a homomorphism of groups. The *kernel of* ϕ is $\{x \in G \mid \phi(x) = e'\}$ where e' is the identity in G'.

32. Mark each of the following true or false.

_____ **a.** A_n is a normal subgroup of S_n.

_____ **b.** For any two groups G and G', there exists a homomorphism of G into G'.

_____ **c.** Every homomorphism is a one-to-one map.

_____ **d.** A homomorphism is one to one if and only if the kernel consists of the identity element alone.

_____ **e.** The image of a group of 6 elements under some homomorphism may have 4 elements. (See Exercise 44.)

_____ **f.** The image of a group of 6 elements under a homomorphism may have 12 elements.

_____ **g.** There is a homomorphism of some group of 6 elements into some group of 12 elements.

_____ **h.** There is a homomorphism of some group of 6 elements into some group of 10 elements.

_____ **i.** A homomorphism may have an empty kernel.

_____ **j.** It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.

In Exercises 33 through 43, give an example of a nontrivial homomorphism ϕ for the given groups, if an example exists. If no such homomorphism exists, explain why that is so. You may use Exercises 44 and 45.

33. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$

34. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$

35. $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5$

36. $\phi : \mathbb{Z}_3 \to \mathbb{Z}$

37. $\phi : \mathbb{Z}_3 \to S_3$

38. $\phi : \mathbb{Z} \to S_3$

39. $\phi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z}$

40. $\phi : 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

41. $\phi : D_4 \to S_3$

42. $\phi : S_3 \to S_4$

43. $\phi : S_4 \to S_3$

Theory

44. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G|$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

45. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G'|$ is finite, then, $|\phi[G]|$ is finite and is a divisor of $|G'|$.

46. Let a group G be generated by $\{a_i \mid i \in I\}$, where I is some indexing set and $a_i \in G$ for all $i \in I$. Let $\phi : G \to G'$ and $\mu : G \to G'$ be two homomorphisms from G into a group G', such that $\phi(a_i) = \mu(a_i)$ for every $i \in I$. Prove that $\phi = \mu$. [Thus, for example, a homomorphism of a cyclic group is completely determined by its value on a generator of the group.] [*Hint*: Use Theorem 7.6 and, of course, Definition 13.1.]

47. Show that any group homomorphism $\phi : G \to G'$ where $|G|$ is a prime must either be the trivial homomorphism or a one-to-one map.

48. The **sign of an even permutation** is $+1$ and the **sign of an odd permutation** is -1. Observe that the map $\text{sgn}_n : S_n \to \{1, -1\}$ defined by

$$\text{sgn}_n(\sigma) = \text{sign of } \sigma$$

is a homomorphism of S_n onto the multiplicative group $\{1, -1\}$. What is the kernel? Compare with Example 13.3.

49. Show that if G, G', and G'' are groups and if $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\phi : G \to G''$ is a homomorphism.

50. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if for all $x, y \in G$, we have $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$.

51. Let G be any group and let a be any element of G. Let $\phi : \mathbb{Z} \to G$ be defined by $\phi(n) = a^n$. Show that ϕ is a homomorphism. Describe the image and the possibilities for the kernel of ϕ.

52. Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Prove the set equality $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$.

53. Let G be a group, Let $h, k \in G$ and let $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ be defined by $\phi(m, n) = h^m k^n$. Give a necessary and sufficient condition, involving h and k, for ϕ to be a homomorphism. Prove your condition.

54. Find a necessary and sufficient condition on G such that the map ϕ described in the preceding exercise is a homomorphism for *all* choices of $h, k \in G$.

55. Let G be a group, h an element of G, and n a positive integer. Let $\phi : \mathbb{Z}_n \to G$ be defined by $\phi(i) = h^i$ for $0 \leq i \leq n$. Give a necessary and sufficient condition (in terms of h and n) for ϕ to be a homomorphism. Prove your assertion.

SECTION 14 FACTOR GROUPS

Let H be a subgroup of a finite group G. Suppose we write a table for the group operation of G, listing element heads at the top and at the left as they occur in the left cosets of H. We illustrated this in Section 10. The body of the table may break up into blocks corresponding to the cosets (Table 10.5), giving a group operation on the cosets, or they may not break up that way (Table 10.9). We start this section by showing that if H is the kernel of a group homomorphism $\phi : G \to G'$, then the cosets of H (remember that left and right cosets then coincide) are indeed elements of a group whose binary operation is derived from the group operation of G.

Factor Groups from Homomorphisms

Let G be a group and let S be a set having the same cardinality as G. Then there is a one-to-one correspondence $\leftrightarrow$ between S and G. We can use $\leftrightarrow$ to define a binary operation on S, making S into a group isomorphic to G. Naively, we simply use the correspondence to rename each element of G by the name of its corresponding (under $\leftrightarrow$) element in S. We can describe explicitly the computation of xy for $x, y \in S$ as follows:

$$\text{if } x \leftrightarrow g_1 \quad \text{and} \quad y \leftrightarrow g_2 \quad \text{and} \quad z \leftrightarrow g_1 g_2, \quad \text{then} \quad xy = z. \tag{1}$$

The direction $\rightarrow$ of the one-to-one correspondence $s \leftrightarrow g$ between $s \in S$ and $g \in G$ gives us a one-to-one function μ mapping S onto G. (Of course, the direction $\leftarrow$ of $\leftrightarrow$ gives us the inverse function μ^{-1}). Expressed in terms of μ, the computation (1) of xy for $x, y \in S$ becomes

$$\text{if } \mu(x) = g_1 \quad \text{and} \quad \mu(y) = g_2 \quad \text{and} \quad \mu(z) = g_1 g_2, \quad \text{then} \quad xy = z. \tag{2}$$

The map $\mu : S \rightarrow G$ now becomes an isomorphism mapping the group S onto the group G. Notice that from (2), we obtain $\mu(xy) = \mu(z) = g_1 g_2 = \mu(x)\mu(y)$, the required homomorphism property.

Let G and G' be groups, let $\phi : G \rightarrow G'$ be a homomorphism, and let $H = \text{Ker}(\phi)$. Theorem 13.15 shows that for $a \in G$, we have $\phi^{-1}[\{\phi(a)\}] = aH = Ha$. We have a one-to-one correspondence $aH \leftrightarrow \phi(a)$ between cosets of H in G and elements of the subgroup $\phi[G]$ of G'. Remember that if $x \in aH$, so that $x = ah$ for some $h \in H$, then $\phi(x) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$, so the computation of the element of $\phi[G]$ corresponding to the coset $aH = xH$ is the same whether we compute it as $\phi(a)$ or as $\phi(x)$. Let us denote the set of all cosets of H by G/H. (We read G/H as "G over H" or as "G modulo H" or as "G mod H," but *never* as "G divided by H.")

In the preceding paragraph, we started with a homomorphism $\phi : G \rightarrow G'$ having kernel H, and we finished with the set G/H of cosets in one-to-one correspondence with the elements of the group $\phi[G]$. In our work above that, we had a set S with elements in one-to-one correspondence with those of a group G, and we made S into a group isomorphic to G with an isomorphism μ. Replacing S by G/H and replacing G by $\phi[G]$ in that construction, we can consider G/H to be a group isomorphic to $\phi[G]$ with that isomorphism μ. In terms of G/H and $\phi[G]$, the computation (2) of the product $(xH)(yH)$ for $xH, yH \in G/H$ becomes

$$\begin{aligned} &\text{if } \mu(xH) = \phi(x) \quad \text{and} \quad \mu(yH) = \phi(y) \quad \text{and} \quad \mu(zH) = \phi(x)\phi(y), \\ &\text{then} \quad (xH)(yH) = zH. \end{aligned} \tag{3}$$

But because ϕ is a homomorphism, we can easily find $z \in G$ such that $\mu(zH) = \phi(x)\phi(y)$; namely, we take $z = xy$ in G, and find that

$$\mu(zH) = \mu(xyH) = \phi(xy) = \phi(x)\phi(y).$$

This shows that the product $(xH)(yH)$ of two cosets is the coset $(xy)H$ that contains the product xy of x and y in G. While this computation of $(xH)(yH)$ may seem to depend on our choices x from xH and y from yH, our work above shows it does not. We demonstrate it again here because it is such an important point. If $h_1, h_2 \in H$ so that xh_1 is an element of xH and yh_2 is an element of yH, then there exists $h_3 \in H$ such

that $h_1 y = y h_3$ because $Hy = yH$ by Theorem 13.15. Thus we have

$$(xh_1)(yh_2) = x(h_1 y)h_2 = x(yh_3)h_2 = (xy)(h_3 h_2) \in (xy)H,$$

so we obtain the same coset. Computation of the product of two cosets is accomplished by *choosing* an element from each coset and taking, as product of the cosets, the coset that contains the product in G of the choices. Any time we define something (like a product) in terms of choices, it is important to show that it is **well defined,** which means that it is independent of the choices made. This is precisely what we have just done. We summarize this work in a theorem.

14.1 Theorem Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the cosets of H form a **factor group**, G/H, where $(aH)(bH) = (ab)H$. Also, the map $\mu : G/H \to \phi[G]$ defined by $\mu(aH) = \phi(a)$ is an isomorphism. Both coset multiplication and μ are well defined, independent of the choices a and b from the cosets.

14.2 Example Example 13.10 considered the map $\gamma : \mathbb{Z} \to \mathbb{Z}_n$, where $\gamma(m)$ is the remainder when m is divided by n in accordance with the division algorithm. We know that γ is a homomorphism. Of course, $\text{Ker}(\gamma) = n\mathbb{Z}$. By Theorem 14.1, we see that the factor group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. The cosets of $n\mathbb{Z}$ are the *residue classes modulo n*. For example, taking $n = 5$, we see the cosets of $5\mathbb{Z}$ are

$$\begin{aligned}
5\mathbb{Z} &= \{\cdots, -10, -5, 0, 5, 10, \cdots\},\\
1 + 5\mathbb{Z} &= \{\cdots, -9, -4, 1, 6, 11, \cdots\},\\
2 + 5\mathbb{Z} &= \{\cdots, -8, -3, 2, 7, 12, \cdots\},\\
3 + 5\mathbb{Z} &= \{\cdots, -7, -2, 3, 8, 13, \cdots\},\\
4 + 5\mathbb{Z} &= \{\cdots, -6, -1, 4, 9, 14, \cdots\}.
\end{aligned}$$

Note that the isomorphism $\mu : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_5$ of Theorem 14.1 assigns to each coset of $5\mathbb{Z}$ its smallest nonnegative element. That is, $\mu(5\mathbb{Z}) = 0$, $\mu(1 + 5\mathbb{Z}) = 1$, etc. ▲

It is very important that we learn how to compute in a factor group. We can multiply (add) two cosets by choosing *any* two representative elements, multiplying (adding) them and finding the coset in which the resulting product (sum) lies.

14.3 Example Consider the factor group $\mathbb{Z}/5\mathbb{Z}$ with the cosets shown above. We can add $(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$ by choosing 2 and 4, finding $2 + 4 = 6$, and noticing that 6 is in the coset $1 + 5\mathbb{Z}$. We could equally well add these two cosets by choosing 27 in $2 + 5\mathbb{Z}$ and -16 in $4 + 5\mathbb{Z}$; the sum $27 + (-16) = 11$ is also in the coset $1 + 5\mathbb{Z}$. ▲

The factor groups $\mathbb{Z}/n\mathbb{Z}$ in the preceding example are classics. Recall that we refer to the cosets of $n\mathbb{Z}$ as *residue classes modulo n*. Two integers in the same coset are *congruent modulo n*. This terminology is carried over to other factor groups. A factor group G/H is often called the **factor group of** G **modulo** H. Elements in the same coset of H are often said to be **congruent modulo** H. By abuse of notation, we may sometimes write $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ and think of $\mathbb{Z}_n$ as the additive group of residue classes of $\mathbb{Z}$ modulo $\langle n \rangle$, or abusing notation further, modulo n.

Factor Groups from Normal Subgroups

So far, we have obtained factor groups only from homomorphisms. Let G be a group and let H be a subgroup of G. Now H has both left cosets and right cosets, and in general, a left coset aH need not be the same set as the right coset Ha. Suppose we try to define a binary operation on left cosets by defining

$$(aH)(bH) = (ab)H \tag{4}$$

as in the statement of Theorem 14.1. Equation 4 attempts to define left coset multiplication by choosing representatives a and b from the cosets. Equation 4 is meaningless unless it gives a *well-defined* operation, independent of the representative elements a and b chosen from the cosets. The theorem that follows shows that Eq. 4 gives a well-defined binary operation if and only if H is a normal subgroup of G.

14.4 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 25.

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 14.4 shows that if left and right cosets of H coincide, then Eq. 4 gives a well-defined binary operation on cosets. We wonder whether the cosets do form a group with such coset multiplication. This is indeed true.

14.5 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 $a^{-1}H = (aH)^{-1}$. ◆

14.6 Definition The group G/H in the preceding corollary is the **factor group** (or **quotient group**) of G by H. ■

14.7 Example Since $\mathbb{Z}$ is an abelian group, $n\mathbb{Z}$ is a normal subgroup. Corollary 14.5 allows us to construct the factor group $\mathbb{Z}/n\mathbb{Z}$ with no reference to a homomorphism. As we observed in Example 14.2, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. ▲

14.8 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 1. 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 Example 4.2 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 14.8 shows that the group $\mathbb{R}/\langle c \rangle$ is isomorphic to the group $\mathbb{R}_c$. In Section 1, 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 $\mathbb{R}$.

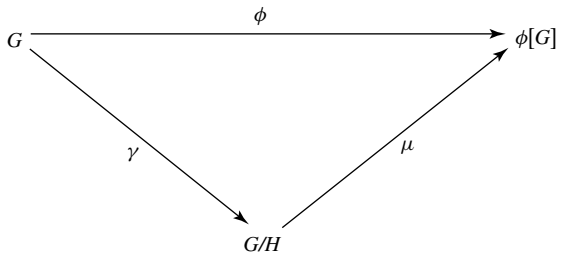
The Fundamental Homomorphism Theorem

We have seen that every homomorphism $\phi : G \to G'$ gives rise to a natural factor group (Theorem 14.1), namely, $G/\text{Ker}(\phi)$. We now show that each factor group G/H gives rise to a natural homomorphism having H as kernel.

14.9 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

$$\gamma(xy) = (xy)H = (xH)(yH) = \gamma(x)\gamma(y),$$



14.10 Figure

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. ◆

We have seen in Theorem 14.1 that if $\phi : G \to G'$ is a homomorphism with kernel H, then $\mu : G/H \to \phi[G]$ where $\mu(gH) = \phi(g)$ is an isomorphism. Theorem 14.9 shows that $\gamma : G \to G/H$ defined by $\gamma(g) = gH$ is a homomorphism. Figure 14.10 shows these groups and maps. We see that the homomorphism ϕ can be *factored,* $\phi = \mu\gamma$, where γ is a homomorphism and μ is an isomorphism of G/H with $\phi[G]$. We state this as a theorem.

14.11 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 $\phi(g) = \mu\gamma(g)$ for each $g \in G$.

The isomorphism μ in Theorem 14.11 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 14.11.

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.

14.12 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 11.12).

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 14.11, 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 $Hg \subseteq gH$.

We summarize our work as a theorem.

14.13 Theorem The following are three 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. $gH = Hg$ for all $g \in G$.

Condition (2) of Theorem 14.13 is often taken as the definition of a normal subgroup H of a group G.

14.14 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 $h \in H$. ▲

Exercise 29 of Section 13 shows that the map $i_g : G \to G$ defined by $i_g(x) = gxg^{-1}$ is a homomorphism of G into itself. 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.

14.15 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 14.13 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 $K = i_g[H]$ for some $g \in G$.

EXERCISES 14

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. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (1, 1)\rangle$

6. $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle (4, 3)\rangle$

7. $(\mathbb{Z}_2 \times S_3)/\langle (1, \rho_1)\rangle$

8. $(\mathbb{Z}_{11} \times \mathbb{Z}_{15})/\langle (1, 1)\rangle$

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. $(3, 1) + \langle (0, 2)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (0, 2)\rangle$

14. $(3, 3) + \langle (1, 2)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (1, 2)\rangle$

15. $(2, 0) + \langle (4, 4)\rangle$ in $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle (4, 4)\rangle$

16. Compute $i_{\rho_1}[H]$ for the subgroup $H = \{\rho_0, \mu_1\}$ of the group S_3 of Example 8.7.

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. Mark each of the following 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.** An inner automorphism of an abelian group must be just 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. Show that A_n is a normal subgroup of S_n and compute S_n/A_n; that is, find a known group to which S_n/A_n is isomorphic.

25. Complete the proof of Theorem 14.4 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 $Ha \subseteq aH$.

26. 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.)

27. 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.

28. 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.

29. Referring to Exercise 27, find all subgroups of S_3 (Example 8.7) that are conjugate to $\{\rho_0, \mu_2\}$.

30. Let H be a normal subgroup of a group G, and let $m = (G : H)$. Show that $a^m \in H$ for every $a \in G$.

31. Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.

32. 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 31.]

33. 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.

34. Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G.

35. 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.

36. 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 $x \in G$.]

37. **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.]

38. 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.

39. 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.)

40. Use the properties $\det(AB) = \det(A) \cdot \det(B)$ and $\det(I_n) = 1$ for $n \times n$ matrices to show the following:

a. The $n \times n$ matrices with determinant 1 form a normal subgroup of $GL(n, \mathbb{R})$.

b. The $n \times n$ matrices with determinant ± 1 form a normal subgroup of $GL(n, \mathbb{R})$.

41. 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.

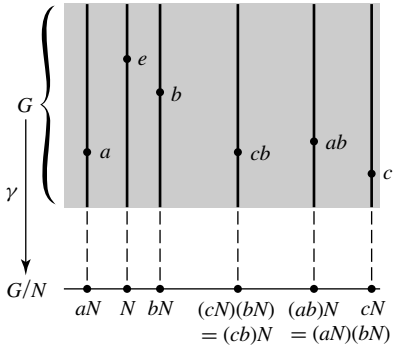
b. Show that if N is a normal subgroup of G, then the set of cosets of N is closed under the above operation on $\mathscr{P}(G)$, and that this operation agrees with the multiplication given by the formula in Corollary 14.5.

c. Show (without using Corollary 14.5) 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 15 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 collapse into a single element in the factor group. A visualization of this collapsing is provided by Fig. 15.1. Recall from Theorem 14.9 that $\gamma : G \to G/N$ defined by $\gamma(a) = aN$ for $a \in G$ is a homomorphism of G onto G/N. Figure 15.1 is very similar to Fig. 13.14, but in Fig. 15.1 the image group under the homomorphism is actually formed from G. We can view the "line" G/N at the bottom of the figure as obtained by collapsing to a point each coset of N in another copy of G. Each point of G/N thus corresponds to a whole vertical line 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.



15.1 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.

15.2 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 $\mathbb{Z}/\{0\}$. ▲

15.3 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 15.2 and 15.3 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.

15.4 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 15.5 becomes

15.5 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 15.4 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.

15.6 Example **(Falsity of the Converse of the Theorem of Lagrange)** The theorem of Lagrange states if H is a subgroup of a finite group G, then the order of H divides the order of G. We show that it is false that if d divides the order of G, then there must exist a subgroup H of G having order d. Namely, we show that A_4, which has order 12, contains no subgroup of order 6.

Suppose that H were a subgroup of A_4 having order 6. As observed before in Example 15.4, 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 11.12).

15.7 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 15.7 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*.

15.8 Theorem Let $G = H \times K$ be the direct product of groups H and K. Then $\overline{H} = \{(h, e) \mid h \in H\}$ is a normal subgroup of G. Also $G/\overline{H}$ is isomorphic to K in a natural way. Similarly, $G/\overline{K} \simeq H$ in a natural way.

Proof Consider the homomorphism $\pi_2 : H \times K \to K$, where $\pi_2(h, k) = k$. (See Example 13.8). Because $\text{Ker}(\pi_2) = \overline{H}$, we see that $\overline{H}$ is a normal subgroup of $H \times K$. Because π_2 is onto K, Theorem 14.11 tells us that $(H \times K)/\overline{H} \simeq K$. ◆

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.

15.9 Theorem A factor group of a cyclic group is cyclic.

Proof Let G be cyclic with generator a, and let N be a normal subgroup of G. We claim the coset aN generates G/N. We must compute all powers of aN. But this amounts to computing, in G, all powers of the representative a and all these powers give all elements in G. Hence the powers of aN certainly give all cosets of N and G/N is cyclic. ◆

15.10 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 $\mathbb{Z}_4 \times \mathbb{Z}_2$. ▲

15.11 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,

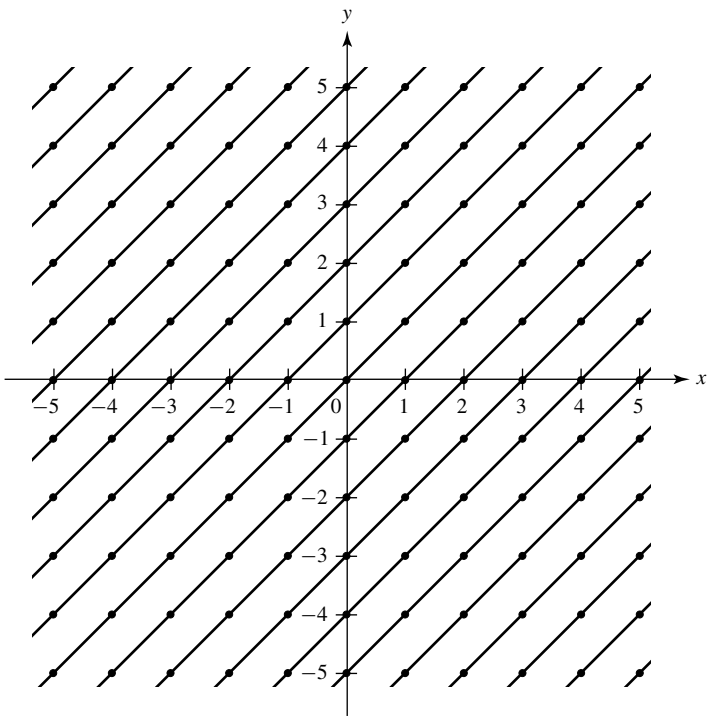
$$4(1, 0) = (1, 0) + (1, 0) + (1, 0) + (1, 0) = (0, 0)$$

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 $\mathbb{Z}_{12}$. ▲

15.12 Example Let us compute (that is, classify as in Theorem 11.12 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. 15.13. 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 $\mathbb{Z}$. ▲



15.13 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 subgroups. For example, Theorem 10.10 shows that a group of prime order can have no nontrivial proper subgroups of any sort.

15.14 Definition A group is **simple** if it is nontrivial and has no proper nontrivial normal subgroups. ■

15.15 Theorem The alternating group A_n is simple for $n \geq 5$.

Proof See Exercise 39. ◆

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 were recently completed. 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 new knowledge of all finite simple groups can now be used to solve some problems of finite group theory.

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 longstanding 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 13.12 on properties of a group homomorphism. The proof is left to Exercises 35 and 36.

15.16 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 15.16 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 $\phi(0) = \rho_0$ and $\phi(1) = \mu_1$ is a homomorphism, and $\mathbb{Z}_2$ is a normal subgroup of itself, but $\{\rho_0, \mu_1\}$ is not a normal subgroup of S_3.

We can now characterize when G/N is a simple group.

15.17 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. ■

15.18 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 14.9. 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 can not happen. Thus G/M is simple.

Conversely, Theorem 15.16 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 52 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.

15.19 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 8.8 for the group S_3 shows us that $Z(S_3) = \{\rho_0\}$, so the center of S_3 is trivial. (This is a special case of Exercise 38, 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 $\{\rho_0\} \times \mathbb{Z}_5$, 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 11.12 gives complete information about the structure of all sufficiently small 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.

15.20 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 7.6 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

$$\begin{aligned} (aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN). \end{aligned}$$

◆

15.21 Example For the group S_3 in Table 8.8, we find that one commutator is $\rho_1\mu_1\rho_1^{-1}\mu_1^{-1} = \rho_1\mu_1\rho_2\mu_1 = \mu_3\mu_2 = \rho_2$. We similarly find that $\rho_2\mu_1\rho_2^{-1}\mu_1^{-1} = \rho_2\mu_1\rho_1\mu_1 = \mu_2\mu_3 = \rho_1$. Thus the commutator subgroup C of S_3 contains A_3. Since A_3 is a normal subgroup of S_3 and S_3/A_3 is abelian, Theorem 15.20 shows that $C = A_3$. ▲

EXERCISES 15

Computations

In Exercises 1 through 12, 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. $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 2)\rangle$

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. Find both the center $Z(D_4)$ and the commutator subgroup C of the group D_4 of symmetries of the square in Table 8.12.

14. Find both the center and the commutator subgroup of $\mathbb{Z}_3 \times S_3$.

15. Find both the center and the commutator subgroup of $S_3 \times D_4$.

16. 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 11.12. 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 17 and 18, 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. The *center* of a group G contains all elements of G that commute with every element of G.

18. The *commutator subgroup* of a group G is $\{a^{-1}b^{-1}ab \mid a, b \in G\}$.

19. Mark each of the following 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 2.
_____ **d.** $\mathbb{R}/\mathbb{Z}$ under addition has elements of order n for all $n \in \mathbb{Z}^+$.
_____ **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 20 through 23, 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 $\mathbb{R}$.

20. Let K be the subgroup of F consisting of the constant functions. Find a subgroup of F to which F/K is isomorphic.

21. Let K^* be the subgroup of F^* consisting of the nonzero constant functions. Find a subgroup of F^* to which F^*/K^* is isomorphic.

22. 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?

23. 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 24 through 26, let U be the multiplicative group $\{z \in \mathbb{C} \mid |z| = 1\}$.

24. Let $z_0 \in U$. Show that $z_0U = \{z_0 z \mid z \in U\}$ is a subgroup of U, and compute U/z_0U.

25. To what group we have mentioned in the text is $U/\langle -1 \rangle$ isomorphic?

26. 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?

27. To what group mentioned in the text is the additive group $\mathbb{R}/\mathbb{Z}$ isomorphic?

28. Give an example of a group G having no elements of finite order > 1 but having a factor group G/H, all of whose elements are of finite order.

29. 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.

30. Describe the center of every simple

a. abelian group

b. nonabelian group.

31. Describe the commutator subgroup of every simple

a. abelian group

b. nonabelian group.

Proof Synopsis

32. Give a one-sentence synopsis of the proof of Theorem 15.9.

33. Give at most a two-sentence synopsis of the proof of Theorem 15.18.

Theory

34. Show that if a finite group G contains a nontrivial subgroup of index 2 in G, then G is not simple.

35. 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 $\phi[G]$.

36. 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.

37. 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 $Z(G) = G$).]

38. Using Exercise 37, show that a nonabelian group G of order pq where p and q are primes has a trivial center.

39. 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.]

40. 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.

41. 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.

42. 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 $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$.]

SECTION 16 †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 on a set. The next section will give an application to counting.

The Notion of a Group Action

Definition 2.1 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.

16.1 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. $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

† This section is a prerequisite only for Sections 17 and 36.