PART I

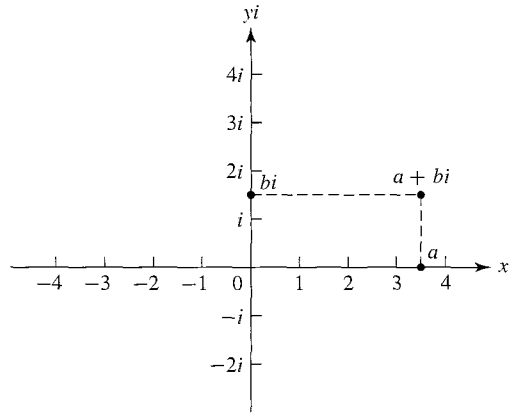
Groups and Subgroups

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 $z_1 = a + bc$ 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

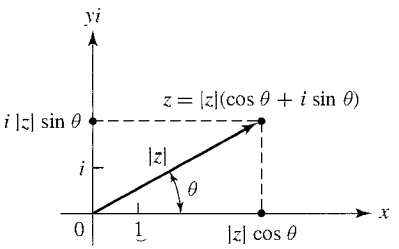
$$z = |z|(\cos\theta + i\sin\theta). \tag{4}$$

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

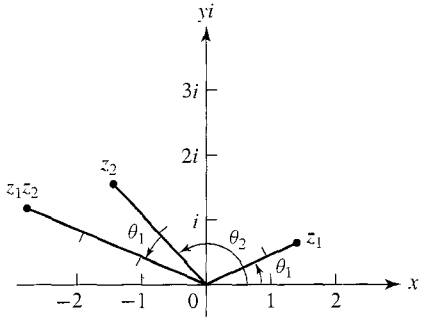
$z = |z|e^{i\theta}$. Let us set

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

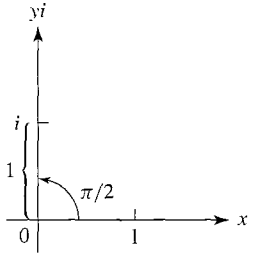
and compute their product in this form, assuming that the usual laws of exponentiation hold with complex number exponents. We obtain

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

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 $0 \leq \theta < 2\pi$ 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

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

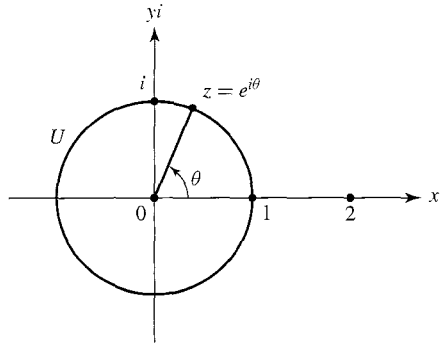
and division of $a + bi$ by nonzero $c + di$ can be performed using the device

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

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 $0 \leq \theta < 2\pi$. 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 $\theta_1 + \theta_2 \geq 2\pi$



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 $x \in \mathbb{R}$

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

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:

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

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 in 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 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

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

[†] 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 27 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 $\langle S, * \rangle$.

In the event that there are one-to-one mappings of S onto S', we usually show that $\langle S, * \rangle$ is not isomorphic to $\langle S', *' \rangle$ (if this is the case) by showing that one has some structural property that the other does not possess.

3.11 Example The sets $\mathbb{Z}$ and $\mathbb{Z}^+$ both have cardinality $\aleph_0$, and there are lots of one-to-one functions mapping $\mathbb{Z}$ onto $\mathbb{Z}^+$. However, the binary structures $\langle \mathbb{Z}, \cdot \rangle$ and $\langle \mathbb{Z}^+, \cdot \rangle$, where $\cdot$ is the usual multiplication, are not isomorphic. In $\langle \mathbb{Z}, \cdot \rangle$ there are two elements x such that $x \cdot x = x$, namely, 0 and 1. However, in $\langle \mathbb{Z}^+, \cdot \rangle$, there is only the single element 1. ▲

We list a few examples of possible structural properties and nonstructural properties of a binary structure $\langle S, * \rangle$ to get you thinking along the right line.

Possible Structural Properties	*Possible Nonstructural Properties*
1. The set has 4 elements.	a. The number 4 is an element.
2. The operation is commutative.	b. The operation is called "addition."
3. $x * x = x$ for all $x \in S$.	c. The elements of S are matrices.
4. The equation $a * x = b$ has a solution x in S for all $a, b \in S$.	d. S is a subset of $\mathbb{C}$.

We introduced the algebraic notions of commutativity and associativity in Section 2. One other structural notion that will be of interest to us is illustrated by Table 3.3, where for the binary operation $*''$ on the set $\{x, y, z\}$, we have $x *'' u = u *'' x = u$ for all choices possible choices, x, y, and z for u. Thus x plays the same role as 0 in $\langle \mathbb{R}, + \rangle$ where $0 + u = u + 0 = u$ for all $u \in \mathbb{R}$, and the same role as 1 in $\langle \mathbb{R}, \cdot \rangle$ where $1 \cdot u = u \cdot 1 = u$ for all $u \in \mathbb{R}$. Because Tables 3.1 and 3.2 give structures isomorphic to the one in Table 3.3, they must exhibit an element with a similar property. We see that $b * u = u * b = u$ for all elements u appearing in Table 3.1 and that $\$ *' u = u *' \$ = u$ for all elements u in Table 3.2. We give a formal definition of this structural notion and prove a little theorem.

3.12 Definition Let $\langle S, * \rangle$ be a binary structure. An element e of S is an **identity element for** $*$ if $e * s = s * e = s$ for all $s \in S$. ■

3.13 Theorem **(Uniqueness of Identity Element)** A binary structure $\langle S, * \rangle$ has at most one identity element. That is, if there is an identity element, it is unique.

Proof Proceeding in the standard way to show uniqueness, suppose that both e and $\bar{e}$ are elements of S serving as identity elements. We let them compete with each other. Regarding e as an identity element, we must have $e * \bar{e} = \bar{e}$. However, regarding $\bar{e}$ as an identity element, we must have $e * \bar{e} = e$. We thus obtain $e = \bar{e}$, showing that an identity element must be unique. ◆

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