

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

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

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

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

We summarize the results of this section.

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

### ■ EXERCISES 3

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

- |  |                                |   |
|--|--------------------------------|---|
| <b>1.</b> $i^3$                        | <b>2.</b> $i^4$                | <b>3.</b> $i^{26}$                                |
| <b>4.</b> $(-i)^{39}$                  | <b>5.</b> $(3 - 2i)(6 + i)$    | <b>6.</b> $(8 + 2i)(3 - i)$                       |
| <b>7.</b> $(2 - 3i)(4 + i) + (6 - 5i)$ | <b>8.</b> $(1 + i)^3$          | <b>9.</b> $(1 - i)^5$ (Use the binomial theorem.) |
| <b>10.</b> Find $ 5 - 12i $ .          | <b>11.</b> Find $ \pi + ei $ . |   |

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

- |                     |                     |                      |                      |
|---------------------|---------------------|----------------------|----------------------|
| <b>12.</b> $3 - 4i$ | <b>13.</b> $-1 - i$ | <b>14.</b> $12 + 5i$ | <b>15.</b> $-3 + 5i$ |
|---------------------|---------------------|----------------------|----------------------|

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

- |                      |                        |                         |                         |
|----------------------|------------------------|-------------------------|-------------------------|
| <b>16.</b> $z^4 = 1$ | <b>17.</b> $z^4 = -1$  | <b>18.</b> $z^3 = -125$ | <b>19.</b> $z^3 = -27i$ |
| <b>20.</b> $z^6 = 1$ | <b>21.</b> $z^6 = -64$ |                         |                         |

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

- |   |   |  |
|---|---|--|
| <b>22.</b> $10 +_{17} 16$   | <b>23.</b> $14 +_{99} 92$                           | <b>24.</b> $3.141 +_4 2.718$                   |
| <b>25.</b> $\frac{1}{2} +_1 \frac{7}{8}$  | <b>26.</b> $\frac{3\pi}{4} +_{2\pi} \frac{3\pi}{2}$ | <b>27.</b> $2\sqrt{2} +_{\sqrt{32}} 3\sqrt{2}$ |
| <b>28.</b> Explain why the expression $5 +_6 8$ in $\mathbb{R}_6$ makes no sense. |   |  |

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

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

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

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

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

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

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

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

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

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

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

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

40. Derive the formulas

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

and

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

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

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

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

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

43. Recall the power series expansions

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

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

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

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

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

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

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

## SECTION 4 NONABELIAN EXAMPLES

### Notation and Terminology

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

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

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

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

Let  $n$  be a positive integer. If  $a$  is an element of a group  $G$ , written multiplicatively, we denote the product  $aaa\dots a$  for  $n$  factors  $a$  by  $a^n$ . We let  $a^0$  be the identity element  $e$ , and denote the product  $a^{-1}a^{-1}a^{-1}\dots a^{-1}$  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:

$$\begin{aligned} a^{-2}a^5 &= a^{-1}a^{-1}aaaaa = a^{-1}(a^{-1}a)aaaa = a^{-1}aaaa = a^{-1}(ea)aaa \\ &= a^{-1}aaaa = (a^{-1}a)aaa = eaaa = (ea)aa = aaa = a^3. \end{aligned}$$

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

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

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

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

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

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

### Permutations

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

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

1 → 4                  1 → 3

2 → 2                  2 → 2

3 → 5                  3 → 4

4 → 3                  4 → 5

5 → 1                  5 → 3

4.4 Figure          4.5 Figure

**4.6 Definition** A **permutation of a set  $A$**  is a function  $\phi : A \rightarrow A$  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  $\sigma$  and  $\tau$  be permutations of  $A$  so that  $\sigma$  and  $\tau$  are both one-to-one functions mapping  $A$  onto  $A$ . The composite function  $\sigma \circ \tau$  defined schematically by

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

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

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