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

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

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

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

Properties of Group Tables

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

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

2.24 Table

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

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

2.25 Table

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

Now suppose that G' is any other group of three elements and imagine a table for G' with identity element appearing first. Since our filling out of the table for $G = \{e, a, b\}$ could be done in only one way, we see that if we take the table for G' and rename the identity e, the next element listed a, and the last element b, the resulting table for G' must be the same as the one we had for G. As explained above, this renaming gives an isomorphism of the group G' with the group G. Thus our work above can be summarized by saying that all groups with a single element are isomorphic, all groups with just two elements are isomorphic, and all groups with just three elements are isomorphic. We use the phrase *up to isomorphism* to express this identification. Thus we may say, "There is only one group of three elements, up to isomorphism."

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

EXERCISES 2

Computations

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

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

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

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

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

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

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

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

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

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

2.26 Table

$*$	a	b
a	a	b
b	b	b

2.27 Table

$*$	a	b
a	a	b
b	a	b

2.28 Table

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Are all groups of 4 elements commutative?

b. Find a way to relabel the four matrices

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

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

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

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

Concepts

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

2.29 Table

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25. Mark each of the following true or false.

_______ **a.** A group may have more than one identity element.
_______ **b.** Any two groups of three elements are isomorphic.
_______ **c.** In a group, each linear equation has a solution.
_______ **d.** The proper attitude toward a definition is to memorize it so that you can reproduce it word for word as in the text.
_______ **e.** Any definition a person gives for a group is correct provided that everything that is a group by that person's definition is also a group by the definition in the text.
_______ **f.** Any definition a person gives for a group is correct provided he or she can show that everything that satisfies the definition satisfies the one in the text and conversely.
_______ **g.** Every finite group of at most three elements is abelian.
_______ **h.** An equation of the form $a * x * b = c$ always has a unique solution in a group.
_______ **i.** The empty set can be considered a group.
_______ **j.** Every group is a binary algebraic structure.

Proof synopsis

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

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

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