Example 2-19. Consider the set of ordered pairs,

$$G = \{(0, 0), (0, 1), (1, 0), (1, 1)\},$$

and the operation $*$ defined by Table 2-1. In this group, the identity element is the pair $(0, 0)$, and every element is its own inverse. Here the verification of the associative law becomes a process of detailed enumeration of all possible cases that could arise.

Table 2-1

$*$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 0)$	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$(0, 1)$	$(0, 1)$	$(0, 0)$	$(1, 1)$	$(1, 0)$
$(1, 0)$	$(1, 0)$	$(1, 1)$	$(0, 0)$	$(0, 1)$
$(1, 1)$	$(1, 1)$	$(1, 0)$	$(0, 1)$	$(0, 0)$

Since the entire table is symmetric about the main diagonal (upper left to lower right), the group operation $*$ is commutative. Note that each element of G appears once and only once in each row and column of the table. Indeed, any multiplication table for a group has this feature.

Example 2-20. Let $P(X)$ be the power set of some fixed nonempty set X. As we have seen, the systems $(P(X), \cup)$ and $(P(X), \cap)$ possess identity elements $\emptyset$ and X, respectively, but neither system has inverses for any elements other than their respective identities. Consequently, $P(X)$ does not constitute a group with regard to the formulation of either unions or intersections. It is possible, however, to remedy this deficiency by defining another operation on $P(X)$ in terms of union and intersection which will result in a group structure.

More specifically, consider the operation Δ (the symbol is traditional) given by the formula

$$A \Delta B = (A - B) \cup (B - A),$$

for

$$A, B \in P(X).$$

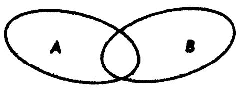

Figure 2-1

This operation, known as the *symmetric difference* of A and B, yields the set which is represented by the shaded area in Fig. 2-1. We shall leave as an exercise the verification that the symmetric difference operation is commutative and associative.

It is easy to see that for any set $A \subseteq X$ (that is, for any element of $P(X)$),

$$A \Delta \emptyset = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A,$$

which proves that the empty set $\emptyset$ serves as an identity element for Δ. Moreover,

$$A \Delta A = (A - A) \cup (A - A) = \emptyset \cup \emptyset = \emptyset.$$

This implies that each element of $P(X)$ is its own inverse. Consequently, the mathematical system $(P(X), \Delta)$ is a commutative group.

Example 2-21. As a simple example of a noncommutative group, let the set G consist of all ordered pairs of real numbers with nonzero first component:

$$G = \{(a, b) \mid a, b \in R^{\#}, a \neq 0\}.$$

Define the operation $*$ on G by the formula

$$(a, b) * (c, d) = (ac, bc + d).$$

The associativity of the operation follows from the familiar properties of the real numbers, for we have

$$\begin{aligned}[(a, b) * (c, d)] * (e, f) &= (ac, bc + d) * (e, f)\\ &= ((ac)e, (bc + d)e + f)\\ &= (a(ce), b(ce) + (de + f))\\ &= (a, b) * (ce, de + f)\\ &= (a, b) * [(c, d) * (e, f)].\end{aligned}$$

It is readily verified that the pair $(1, 0)$ serves as the identity element, while the inverse of $(a, b) \in G$ is $(1/a, -b/a)$. To see that the group $(G, *)$ is not commutative, merely consider the elements $(1, 2)$ and $(3, 4)$ of G:

$$(1, 2) * (3, 4) = (3, 10) \neq (3, 6) = (3, 4) * (1, 2).$$

Example 2-22. For another example of a noncommutative group, take the set G as consisting of the six functions $f_1, f_2, \ldots, f_6$, where for

$$x \in R^{\#} - \{0, 1\},$$

we define

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{x},$$

$$f_3(x) = 1 - x, \qquad f_4(x) = \frac{x - 1}{x},$$

$$f_5(x) = \frac{x}{x - 1}, \qquad f_6(x) = \frac{1}{1 - x}.$$

Let the group operation be that of functional composition.

Thus, as an illustration, we have

$$\begin{aligned}(f_2 \circ f_6)(x) = f_2(f_6(x)) &= f_2\left(\frac{1}{1 - x}\right) = \frac{1}{1/(1 - x)}\\ &= 1 - x = f_3(x),\end{aligned}$$

which implies that $f_2 \circ f_6 = f_3$. On the other hand,

$$\begin{aligned}(f_6 \circ f_2)(x) &= f_6(f_2(x)) \\ &= f_6\left(\frac{1}{x}\right) = \frac{1}{1 - 1/x} \\ &= \frac{x}{x - 1} = f_5(x),\end{aligned}$$

Table 2-2

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

so that $f_6 \circ f_2 = f_5$, which shows that the operation $*$ is not commutative. The multiplication for $(G, \circ)$ in this case is given by Table 2-2. Since functional composition is associative (Theorem 1-7), the system $(G, \circ)$ is certainly a semigroup. The operation table shows that f_1 is the identity element and the respective inverses are

$$\begin{aligned}f_1^{-1} &= f_1, & f_2^{-1} &= f_2, & f_3^{-1} &= f_3, \\ f_4^{-1} &= f_6, & f_5^{-1} &= f_5, & f_6^{-1} &= f_4.\end{aligned}$$

To encompass all the different groups above in a single concept obviously requires the formulation of the underlying group concept in the most general terms. This is precisely the point we hope to convey to the reader; the value of contemporary mathematics lies in its power to abstract and thus to lay bare the structurally essential relations between superficially distinct entities.

Historically, the notion of a group arose early in the nineteenth century out of attempts to solve polynomial equations. Galois was the first to use the word "group" in any technical sense when he considered the group of permutations of the roots of such equations. A major achievement in the evolution of the theory was Klein's classification, in the 1870's, of the various branches of geometry according to groups of transformations under which certain geometric properties remain invariant. It remained some time, however, before satisfactory group postulates, free of redundancy, were stated. Definition 2-11, first formulated in 1902, is attributed to the American mathematician E. V. Huntington.

In the twentieth century, group theory has embraced all branches of mathematics and, indeed, a wide variety of other fields. It is difficult to give examples without becoming too technical, but the theory of groups is now employed in the study of quantum mechanics, general relativity, and crystallography. In these areas, group theory is not only a tool with which calculations are made but also a source of concepts and principles for the formulation of new theories. A recent example can be found in the physics of fundamental particles with the discovery of a new "elementary particle" whose existence had been predicted from a classification scheme based on groups. It is certainly appropriate to begin our investigation of mathematical systems with this concept.

PROBLEMS

1. Determine which of the following binary operations on the set Q are associative and which are commutative.

   a) $a * b = 0$ b) $a * b = \frac{1}{2}(a + b)$
   c) $a * b = b$ d) $a * b = a + b - 1$

2. Suppose the system $(S, *)$ has an identity element; show that if the equation

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

holds for all possible choices of elements a, b, c and d of S, then the operation $*$ is both associative and commutative.

3. Prove that the set of ordered pairs of real numbers together with the operation $*$ defined on S by

$$(a, b) * (c, d) = (a + c, b + d + 2bd)$$

constitutes a commutative semigroup with identity.

4. Let us define a binary operation $*$ on the set $S = \{1, 2, 3, 4, 6\}$ as follows:

$$a * b = \gcd(a, b).$$

For example, $6 * 4 = 2$, $3 * 4 = 1$, etc. Show that $(S, *)$ is a commutative semigroup. [*Hint:* Problem 17, Section 1-2.]

5. Consider the three-element set $S = \{a, b, c\}$ and the operation $*$ given by the multiplication table below:

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

Verify that the pair $(S, *)$ is a commutative semigroup with identity, but not a group.

6. In the following instances, determine whether the systems $(G, *)$ described are commutative groups. For those systems failing to be so, indicate which axioms are not satisfied.

   a) $G = Z_+$, $a * b = \max\{a, b\}$,
   b) $G = Z$, $a * b = \min\{a, b\}$ (the smaller of a and b),
   c) $G = R^\#$, $a * b = a + b - ab$,
   d) $G = Z_+$, $a * b = \max\{a, b\} - \min\{a, b\}$,
   e) $G = Z \times Z$, $(a, b) * (c, d) = (a + c, b + d)$,
   f) $G = R^\# \times R^\#$, $(a, b) * (c, d) = (ac + bd, ad + bd)$,
   g) $G = R^\# \times R^\# - (0, 0)$, $(a, b) * (c, d) = (ac - bd, ad + bc)$.

7. Suppose that $a \in R^\# - \{0, 1\}$ and consider the set G of integral powers of a: $G = \{a^k \mid k \in Z\}$. If $\cdot$ denotes ordinary multiplication, prove that $(G, \cdot)$ is a group.

8. Let $G = \{1, (-1 + i\sqrt{3})/2, (-1 - i\sqrt{3})/2\}$, where $i^2 = -1$. Show that the system $(G, \cdot)$ is a group.

9. Consider the set G consisting of the four functions f_1, f_2, f_3, f_4:

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{x}, \qquad f_3(x) = -x, \qquad f_4(x) = -\frac{1}{x}$$

with $x \in R^\# - \{0\}$. Prove that $(G, \circ)$ is a commutative group, where $\circ$ denotes functional composition.

10. Prove that the symmetric difference operation

$$A \mathbin{\Delta} B = (A - B) \cup (B - A)$$

discussed in Example 2–20 may also be defined by the formula

$$A \mathbin{\Delta} B = (A \cup B) - (A \cap B).$$

11. Granting the associative law, show that the following two operation tables define groups:

*	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

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

12. If $G = \{a \in R^\# \mid -1 < a < 1\}$, verify that $(G, *)$ forms a commutative group, with the operation $*$ given by

$$a * b = \frac{a + b}{1 + ab} \qquad \text{for} \quad a, b \in G.$$

13. Let $(S, *)$ be a semigroup without identity and e be any element not in S. Define the operation $\circ$ on the set $S' = S \cup \{e\}$ by means of the rules

$$a \circ b = a * b \qquad \text{for all} \quad a, b \in S,$$

$$a \circ e = a = e \circ a \qquad \text{for all} \quad a \in S'.$$

Show that the pair $(S', \circ)$ is a semigroup with the identity element e; $(S', \circ)$ is said to be obtained by ***adjoining an identity.***

14. Prove that the following weakened set of axioms are actually equivalent to the classical axioms for a group as given in Definition 2–11: A group is a mathematical system $(G, *)$ for which

1) $*$ is an associative operation,
2) there exists an element e in G such that $a * e = a$ for all $a \in G$ (existence of a right identity),
3) for each $a \in G$, there exists an element a^{-1} in G such that $a * a^{-1} = e$ (existence of right inverses).