Corollary. If a and b are invertible elements of a semigroup with identity, then

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

To be sure, if the operation $*$ is commutative, then we do have

$$(a * b)^{-1} = a^{-1} * b^{-1};$$

however, in the absence of this hypothesis there is no guarantee that the inverse of a product is equal to the product of the respective inverses. The next example should help to make these notions clearer.

Example 2-23. Let G denote the set of all ordered pairs of real numbers with nonzero first component. If the binary operation $*$ is defined on the set G by the rule

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

then $(G, *)$ is a noncommutative group [Example 2-21]. The identity element of the group is the pair $(1, 0)$; the inverse of an element $(a, b) \in G$ is $(1/a, -b/a)$. A direct computation shows that

$$\big((1, 3) * (2, 4)\big)^{-1} = (2, 10)^{-1} = (\tfrac{1}{2}, -5),$$

while

$$(2, 4)^{-1} * (1, 3)^{-1} = (\tfrac{1}{2}, -2) * (1, -3) = (\tfrac{1}{2}, -5).$$

Thus $\big((1, 3) * (2, 4)\big)^{-1} = (2, 4)^{-1} * (1, 3)^{-1}$, as is guaranteed by Theorem 2-3. However, computing the product of the inverses in the order

$$(1, 3)^{-1} * (2, 4)^{-1},$$

we obtain

$$(1, 3)^{-1} * (2, 4)^{-1} = (1, -3) * (\tfrac{1}{2}, -2) = (\tfrac{1}{2}, -\tfrac{7}{2}),$$

so that

$$\big((1, 3) * (2, 4)\big)^{-1} \neq (1, 3)^{-1} * (2, 4)^{-1}.$$

For this group then, the inverse of a product of elements is not equal to the product of their respective inverses in direct order. This should not be particularly surprising inasmuch as the group $(G, *)$ is noncommutative.

The previous lemma is actually a special case of a result mentioned earlier which in effect asserts that parentheses are superfluous in a product of group elements, and consequently that their omission can lead to no misunderstanding. The exact story is told in the next theorem.

First, however, let us introduce some auxiliary notation: suppose $(S, *)$ is a semigroup and the elements $a_1, a_2, \ldots, a_n$ belong to S (where $n > 1$). Their

standard product, symbolized by $a_1 * a_2 * \cdots * a_n$, is defined recursively as

$$a_1 * a_2 * \cdots * a_n \quad (a_1 * a_2 * \cdots * a_{n-1}) * a_n.$$

When $n = 4$, for instance, $a_1 * a_2 * a_3 * a_4$ will turn out to be

$$\begin{aligned} a_1 * a_2 * a_3 * a_4 &= (a_1 * a_2 * a_3) * a_4 \\ &= ((a_1 * a_2) * a_3) * a_4. \end{aligned}$$

In essence, we are using induction to define a particular grouping of parentheses and therefore a particular element of S.

With this definition in mind, we now show that a product is determined solely by the order of its factors, and not on the manner of distributing parentheses.

Theorem 2–4. *(Generalized Associative Law).* Let $(S, *)$ be a semigroup and $a_1, a_2, \ldots, a_n$ be a set of $n \geq 3$ elements of S. Then all possible products of $a_1, a_2, \ldots, a_n$, taken in that order and arrived at by placing parentheses in any meaningful position, yield one and the same result.

Proof. The strategy we shall employ is to prove all products of the elements $a_1, a_2, \ldots, a_n$ are equal to their standard product $a_1 * a_2 * \cdots * a_n$; our argument proceeds by induction on n, where $n \geq 3$. In the case $n = 3$, the result follows directly from the associativity of $*$:

$$a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3 = a_1 * a_2 * a_3.$$

Next, assume that the assertion holds for all products of m factors, where $3 \leq m < n$, and let x be any product involving n factors.

Since x is obtained by successive applications of the operation $*$, there must be a final multiplication between two expressions having less than n factors. By the induction hypotheses, each of these two expressions equals the standard product, so that x may be written as

$$x = (a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_n), \qquad 1 \leq k < n.$$

By definition of the standard product,

$$a_{k+1} * a_{k+2} * \cdots * a_n = (a_{k+1} * a_{k+2} * \cdots * a_{n-1}) * a_n,$$

whence

$$x = (a_1 * a_2 * \cdots * a_k) * [(a_{k+1} * a_{k+2} * \cdots * a_{n-1}) * a_n].$$

The usual associative law now yields

$$x = [(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * a_{k+2} * \cdots * a_{n-1})] * a_n.$$

Applying first our induction assumption to the expression in brackets (which certainly contains less than n factors) and then the definition of the standard product again, we infer that

$$x = (a_1 * a_2 * \cdots * a_{n-1}) * a_n = a_1 * a_2 * \cdots * a_n.$$

This completes the induction step and therefore the proof of the theorem.

Given four elements $a_1, a_2, a_3, a_4 \in S$, parentheses can be legally inserted and the elements multiplied (in the given order) five different ways. Theorem 2-4 permits us to conclude that all these products are equal:

$$\begin{aligned}(((a_1 * a_2) * a_3) * a_4) &= (a_1 * (a_2 * a_3)) * a_4 \\ &= a_1 * ((a_2 * a_3) * a_4) \\ &= a_1 * (a_2 * (a_3 * a_4)) \\ &= (a_1 * a_2) * (a_3 * a_4).\end{aligned}$$

As a matter of notation, it will be our tendency to omit parentheses in writing products; the exception to this will be found on those occasions when we wish to emphasize the associative law or a certain grouping of elements.

Theorem 2-5. (*Cancellation Law*). If a, b, and c are elements of a group $(G, *)$ such that either $a * c = b * c$ or $c * a = c * b$, then $a = b$.

Proof. Since $c \in G$, c^{-1} exists in G. Multiplying the equation $a * c = b * c$ on the right side by c^{-1}, we obtain

$$(a * c) * c^{-1} = (b * c) * c^{-1}.$$

Then, by the associative law, this becomes

$$a * (c * c^{-1}) = b * (c * c^{-1}),$$

or $a * e = b * e$. Therefore $a = b$. Similarly, we can show that $c * a = c * b$ implies $a = b$.

Corollary. The only solution of the group equation $x * x = x$ is $x = e$.

Proof. The conclusion is an immediate consequence of the cancellation law and the fact that $x * x = x * e$.

In a system $(S, *)$, an element $x \in S$ is said to be *idempotent* provided $x * x = x$. What we have just shown is that a group possesses exactly one idempotent element, namely the group identity. For an illustration of a system in which every element is idempotent the student is referred to Problem 4, Section 2-1.

This last theorem allows us to cancel, from the same side, in equations involving group elements. We cannot conclude, however, that $a * c = c * b$ implies $a = b$, unless the group is known to be commutative.

An arbitrary binary operation need not satisfy the cancellation law. To see this, we consider the set $G = \{1, 2, 3\}$ under the following multiplication table:

*	1	2	3
1	1	2	3
2	2	1	2
3	3	2	1

On examining the table, we observe that $2 * 1 = 2 * 3$; but obviously $1 \neq 3$. The failure of the cancellation law in this instance results from the fact that when we multiply both sides of the equation $2 * 1 = 2 * 3$ by $2^{-1} = 2$, the element 2 does not associate with the product $2 * 3$; that is,

$$2 * (2 * 3) \neq (2 * 2) * 3.$$

Theorem 2–6. In a group $(G, *)$, the equations $a * x = b$ and $y * a = b$ have unique solutions.

Proof. First, $x = a^{-1} * b$ satisfies the group equation $a * x = b$, since

$$\begin{aligned} a * (a^{-1} * b) &= (a * a^{-1}) * b \\ &= e * b \\ &= b. \end{aligned}$$

This shows that there is at least one solution in G; it remains for us to show that there is only one. Suppose there is some other element $x' \in G$ such that $a * x' = b$. Then

$$a * x' = a * (a^{-1} * b),$$

so that by the cancellation law,

$$x' = a^{-1} * b, \qquad \text{or} \qquad x' = x.$$

The second part of the theorem may be proved in an analogous manner.

Corollary. In a multiplication table for a group, each element appears exactly once in each row and column.

Proof. For a proof by contradiction, suppose that the element b occurred twice in the row headed by a. There would then exist elements x_1 and x_2, with $x_1 \neq x_2$, such that

$$a * x_1 = b \qquad \text{and} \qquad a * x_2 = b.$$

However, this situation is plainly incompatible with the above theorem which asserts that there is one and only one solution of the equation $a * x = b$. A proof for columns can be obtained by imitating the argument for rows.

It can be shown that all groups with fewer than six elements are commutative; thus a noncommutative group must necessarily contain at least six elements. The proof of this fact is somewhat lengthy, although the actual details are not by themselves particularly difficult. The subsequent lemma will serve to isolate the most tedious aspect of the theorem.

Lemma. If a and b are noncommuting elements of a group $(G, *)$—that is, $a * b \neq b * a$—then the elements of the set,

$$\{e, a, b, a * b, b * a\},$$

are all distinct.

Proof. The basic idea of the proof is to examine the members of the set $\{e, a, b, a * b, b * a\}$ two at a time, and show that each of the ten possible equalities leads to a contradiction of the hypothesis

$$a * b \neq b * a.$$

On several occasions, the cancellation law is used without explicit reference. The argument runs as follows:

1) $e = a$ implies $a * b = e * b = b = b * e = b * a$,
2) $e = b$ implies $a * b = a * e = a = e * a = b * a$,
3) $e = a * b$ implies $a * e = e * a = (a * b) * a = a * (b * a)$, so that $e = b * a$ or $a * b = b * a$,
4) $e = b * a$ implies $e * a = a * e = a * (b * a) = (a * b) * a$, so that $e = a * b$ or $b * a = a * b$,
5) $a = b$ implies $a * b = a * a = b * a$,
6) $a = a * b$ implies $e = b$, reducing to case (2),
7) $a = b * a$ implies $e = b$, reducing to case (2),
8) $b = a * b$ implies $e = a$, reducing to case (1),
9) $b = b * a$ implies $e = a$, reducing to case (1),
10) $a * b \neq b * a$ contradicts the hypothesis.

The proof of the lemma is now complete.

Theorem 2-7. Any noncommutative group has at least six elements.

Proof. If $(G, *)$ is a noncommutative group, it must have a pair of noncommuting elements a and b. According to the lemma, the set $\{e, a, b, a * b, b * a\}$ then consists of distinct members. We now proceed to establish that one of the group elements $a * a$ or $a * b * a$ is distinct from these five; however, it is not possible to specify abstractly whether it is $a * a$ or $a * b * a$.

With the aid of the lemma, we first show that $a * a$ is different from each member of $\{a, b, a * b, b * a\}$. To start with, observe that

a) $a * a = a$ implies $a = e$, reducing to case (1) of the lemma,
b) $a * a = b$ implies $a * b = a * (a * a) = (a * a) * a = b * a$,
c) $a * a = a * b$ implies $a = b$, reducing to case (5),
d) $a * a = b * a$ implies $a = b$, reducing to case (5).

Thus, either $a * a \neq e$, in which case $a * a$ is the sixth distinct element of G or else $a * a = e$.

In this latter instance, we can show $a * b * a$ to be distinct from each of e, a, b, $a * b$, $b * a$ and consequently to be the required sixth element. The reasoning here depends on the fact that

$$a * (a * b * a) = (a * a) * (b * a) = e * (b * a) = b * a.$$

e) $a * b * a = e$ implies $b * a = a * (a * b * a) = a * e = a$, reducing to case (7),
f) $a * b * a = a$ implies $a * b = e$, reducing to case (3),
g) $a * b * a = b$ implies $a * b = a * (a * b * a) = b * a$,
h) $a * b * a = a * b$ implies $a = e$, reducing to case (1),
i) $a * b * a = b * a$ implies $a = e$, reducing to case (1),

which establishes the result. An alternative proof will be presented in Section 2-5.

The generalized associative law insures that the product $a * a * \cdots * a$ has an unambiguous meaning irrespective of how the factors are parenthesized. Designating the foregoing product by the symbol a^k (assuming there are k factors), we may introduce the notion of the positive powers of a. The next definition extends this idea to arbitrary integral powers.

Definition 2-12. In any group $(G, *)$, the *integral powers* of an element $a \in G$ are defined by

$$\begin{aligned} a^k &= a * a * \cdots * a \quad \text{(k factors)}, \\ a^0 &= e, \\ a^{-k} &= (a^{-1})^k, \end{aligned}$$

where $k \in Z_+$.

With these conventions, the customary laws of exponents have their counterpart in group theory.

Theorem 2-8. Let (G, *) be a group, $a \in G$, and $m, n \in Z$. The powers of a obey the following laws of exponents:

1) $a^n * a^m = a^{n+m} = a^m * a^n$, 2) $(a^n)^m = a^{nm} = (a^m)^n$,
3) $a^{-n} = (a^n)^{-1}$, 4) $e^n = e$.

The detailed proof of these statements requires a breakdown into "cases" and can safely be left as an exercise. We caution the reader that the property $(a * b)^n = a^n * b^n$ is not to be expected in an arbitrary group (a moment's reflection should convince one of this).

We shall now conclude this section with two particularly important examples of groups, since we shall have frequent occasion to refer to them in the future.

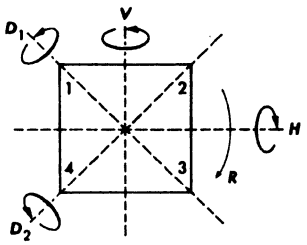

Figure 2-2

Example 2-24. The group to be introduced here is known as the *group of symmetries of a square*. Imagine a cardboard square having its sides parallel to the axes of a coordinate system and its center at the origin (Fig. 2-2).

The elements of the set G are taken to be certain rigid motions of the square. Permitted motions are the following: clockwise rotations R_{90}, R_{180}, R_{270}, and R_{360} about the center through angles of 90, 180, 270, and 360 degrees, respectively; reflections (flips out of the plane and back into it) H and V about the horizontal and vertical lines through the center; reflections D_1 and D_2 about the indicated diagonals. We can *multiply* two such motions by performing them in succession, beginning with the one on the right. Thus $X * Y$ means the motion that achieves the same result as Y followed by X.

For example, $H * R_{90}$ is that element of G which has the same net effect as R_{90} (a rotation clockwise through 90°) followed by H (a horizontal flip). By observing the manner in which the numbered corners of the square are shifted around, we see that $H * R_{90}$ produces the same result as the single motion D_2; so $H * R_{90} = D_2$. A similar analysis shows $R_{90} * H = D_1$ from which we infer that our multiplication is not commutative.

Table 2-3

*	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
R_{90}	R_{180}	R_{270}	R_{360}	R_{90}	D_1	D_2	V	H
R_{180}	R_{270}	R_{360}	R_{90}	R_{180}	V	H	D_2	D_1
R_{270}	R_{360}	R_{90}	R_{180}	R_{270}	D_2	D_1	H	V
R_{360}	R_{90}	R_{180}	R_{270}	R_{360}	H	V	D_1	D_2
H	D_2	V	D_1	H	R_{360}	R_{180}	R_{270}	R_{90}
V	D_1	H	D_2	V	R_{180}	R_{360}	R_{90}	R_{270}
D_1	H	D_2	V	D_1	R_{90}	R_{270}	R_{360}	R_{180}
D_2	V	D_1	H	D_2	R_{270}	R_{90}	R_{180}	R_{360}

The complete multiplication table for the operation * is shown in Table 2-3. Note that R_{360} serves as the identity element and each of R_{180}, R_{360}, H, V, D_1, and D_2 is its own inverse, whereas R_{90} and R_{270} are inverses of each other.

The associative law also holds, but this is not immediately obvious. We shall see later that the symmetries of the square are equivalent to a group of permutations of the set $\{1, 2, 3, 4\}$ (observe that a symmetry is completely described by its effect on the vertices) and associativity therefore follows from the associativity of functional composition. Granting this for the moment, the proof that $(G, *)$ constitutes a group is complete.

Similar groups may be defined for other geometric figures; in fact, for any regular n-sided polygon. Problem 14 at the end of this section deals with the group of symmetries of the equilateral triangle.

Example 2–25. Let $(G, *)$ be an arbitrary group. For a fixed element $a \in G$, define the *left-multiplication function* f_a: $G \to G$ by

$$f_a(x) = a * x \qquad \text{for each} \qquad x \in G.$$

That is, f_a multiplies (or translates) each element of G by a on the left. If $x \in G$, then

$$x = a * (a^{-1} * x) = f_a(a^{-1} * x),$$

so that f_a maps G onto itself. Moreover, f_a is one-to-one, for if $x, y \in G$ with $f_a(x) = f_a(y)$, then $a * x = a * y$. From the cancellation law, we conclude that $x = y$.

Suppose we combine two of these mappings, say f_a and f_b, under the usual composition of functions. For any $x \in G$, we see that

$$\begin{aligned}(f_a \circ f_b)(x) = f_a(f_b(x)) &= f_a(b * x) = a * (b * x) \\ &= (a * b) * x = f_{a*b}(x).\end{aligned}$$

This means that $f_a \circ f_b = f_{a*b}$, so that the set of all such functions is closed under the operation of functional composition.

For the sake of notation, set $F_G = \{f_a \mid a \in G\}$. Our aim is to show that the pair $(F_G, \circ)$ is actually a group.

Indeed, if e is the identity element for $(G, *)$, then f_e acts as the identity for $(F_G, \circ)$, since

$$f_a \circ f_e = f_{a*e} = f_a = f_{e*a} = f_e \circ f_a.$$

Moreover, $(f_a)^{-1} = f_{a^{-1}}$, for we have

$$f_a \circ f_{a^{-1}} = f_{a*a^{-1}} = f_e = f_{a^{-1}*a} = f_{a^{-1}} \circ f_a.$$

We already know that composition of functions is associative (Theorem 1–7), so it follows that $(F_G, \circ)$ forms a group.

PROBLEMS

1. Given that a, b, c, and d are elements of the semigroup $(G, *)$, prove that

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

2. Complete the proof of Theorem 2-8.
3. Prove the theorem: A group $(G, *)$ is commutative if and only if $(a * b)^{-1} = a^{-1} * b^{-1}$ for every $a, b \in G$.
4. Given a and b are elements of a group $(G, *)$, with $a * b = b * a$, show that $(a * b)^k = a^k * b^k$ for every integer $k \in Z$.
5. Let $(G, *)$ be a group such that $(a * b)^2 = a^2 * b^2$ for every $a, b \in G$. Prove that the group is commutative.
6. Given $a^2 = e$ for every element a of the group $(G, *)$, show that the group must be commutative.
7. A group $(G, *)$ is said to be *cyclic* if there exists an element $a \in G$ such that every element of G is of the form a^k for some integer k (positive, negative, or zero). Such an element a is called a *generator* of the group.
   a) Prove that any cyclic group is commutative.
   b) Given $G = \{1, -1, i, -i\}$, with $i^2 = -1$, show that $(G, \cdot)$ is a cyclic group. Which of its elements are generators?
8. Prove that if a and b are elements of a group $(G, *)$ with the property

$$a^{-1} * b * a = b^{-1} \quad \text{and} \quad b^{-1} * a * b = a^{-1},$$

   then $a^4 = e = b^4$.
9. Prove that if $(G, *)$ is a group having more than two elements, then there exist $a, b \in G$, with $a \neq b$, $a \neq e$, $b \neq e$, such that $a * b = b * a$.
10. If $(S, *)$ is a semigroup with identity and G the set of all elements of S having inverses with respect to the operation $*$, verify that the pair $(G, *)$ is a group.
11. Prove that a group may alternatively be defined as a semigroup $(G, *)$ in which, for all $a, b \in G$, each of the equations $a * x = b$ and $y * a = b$ has a solution in G. [*Hint:* Use the characterization of a group given in Problem 14, Section 2-1.]
12. Show that any semigroup $(S, *)$ with a finite number of elements possesses an idempotent element. [*Hint:* For $n > 1$, proceed by induction on n, the number of elements of S; given $a \in S$, let $A = \{a^k \mid k = 2, 3, \ldots\}$, and argue according to whether or not A contains the element a.]
13. For any system $(S, *)$, define the set

$$A = \{a \in S \mid a * (b * c) = (a * b) * c \text{ for all } b, c \in S\}.$$

    If $A \neq \emptyset$, prove that the pair $(A, *)$ is a semigroup.
14. Let the set G consist of certain rigid motions of an equilateral triangle. Permitted motions are three clockwise rotations R_{120}, R_{240}, and R_{360} about the center through angles of 120, 240, and 360 degrees, respectively, and three reflections L_1, L_2, and L_3 about lines l_1, l_2, and l_3 as indicated (Fig. 2-3). As usual, define the operation $*$ on G to be one motion followed by another. Prove that the system $(G, *)$ is a group.

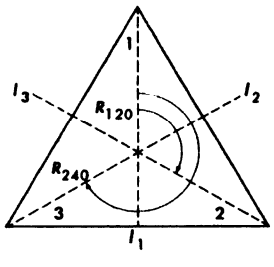

Figure 2-3