

Suppose that  $a * c = e = c * a$ . Then  $c = c * e = c * (a * b) = (c * a) * b = e * b = b$ , as desired. ■

As a result of the uniqueness assertions of the theorem, we may now give names to  $e$  and to  $b$ . We call  $e$  the *identity* of  $G$  and, if  $a * b = e = b * a$ , then we call  $b$  the *inverse* of  $a$  and denote it by  $a^{-1}$ .

**Corollary 1.11.** *If  $G$  is a group and  $a \in G$ , then*

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

*Proof.* By definition,  $(a^{-1})^{-1}$  is that element  $g \in G$  with  $a^{-1} * g = e = g * a^{-1}$ . But  $a$  is such an element, and so the uniqueness gives  $g = a$ . ■

**Definition.** If  $G$  is a group and  $a \in G$ , define the *powers* of  $a$  as follows: if  $n$  is a positive integer, then  $a^n$  is defined as in any semigroup; define  $a^0 = e$ ; define  $a^{-n} = (a^{-1})^n$ .

Even though the list of axioms defining a group is short, it is worthwhile to make it even shorter so it will be as easy as possible to verify that a particular example is, in fact, a group.

**Theorem 1.12.** *If  $G$  is a semigroup with an element  $e$  such that:*

- (i')  $e * a = a$  for all  $a \in G$ ; and  
 (ii') for each  $a \in G$  there is an element  $b \in G$  with  $b * a = e$ , then  $G$  is a group.

*Proof.* We claim that if  $x * x = x$  in  $G$ , then  $x = e$ . There is an element  $y \in G$  with  $y * x = e$ , and  $y * (x * x) = y * x = e$ . On the other hand,  $y * (x * x) = (y * x) * x = e * x = x$ . Therefore,  $x = e$ .

If  $b * a = e$ , let us show that  $a * b = e$ . Now  $(a * b) * (a * b) = a * [(b * a) * b] = a * [e * b] = a * b$ , and so our claim gives  $a * b = e$ . (Observe that we have used associativity for an expression having four factors.)

If  $a \in G$ , we must show that  $a * e = a$ . Choose  $b \in G$  with  $b * a = e = a * b$  (using our just finished calculation). Then  $a * e = a * (b * a) = (a * b) * a = e * a = a$ , as desired. ■

## EXERCISES

- 1.23. If  $G$  is a group and  $a_1, a_2, \dots, a_n \in G$ , then

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

Conclude that if  $n \geq 0$ , then  $(a^{-1})^n = (a^n)^{-1}$ .

- 1.24. Let  $a_1, a_2, \dots, a_n$  be elements of an abelian semigroup. If  $b_1, b_2, \dots, b_n$  is a rearrangement of the  $a_i$ , then

$$a_1 * a_2 * \dots * a_n = b_1 * b_2 * \dots * b_n.$$

- 1.25. Let  $a$  and  $b$  lie in a semigroup  $G$ . If  $a$  and  $b$  commute, then  $(a * b)^n = a^n * b^n$  for every  $n \geq 1$ ; if  $G$  is a group, then this equation holds for every  $n \in \mathbb{Z}$ .
- 1.26. A group in which  $x^2 = e$  for every  $x$  must be abelian.
- 1.27. (i) Let  $G$  be a finite abelian group containing no elements  $a \neq e$  with  $a^2 = e$ . Evaluate  $a_1 * a_2 * \cdots * a_n$ , where  $a_1, a_2, \dots, a_n$  is a list with no repetitions, of all the elements of  $G$ .  
(ii) Prove *Wilson's theorem*: If  $p$  is prime, then

$$(p - 1)! \equiv -1 \pmod{p}.$$

(Hint. The nonzero elements of  $\mathbb{Z}_p$  form a multiplicative group.)

1.28. (i) If  $\alpha = (1 \ 2 \ \dots \ r - 1 \ r)$ , then  $\alpha^{-1} = (r \ r - 1 \ \dots \ 2 \ 1)$ .

(ii) Find the inverse of  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 1 & 2 & 5 & 3 & 8 & 9 & 7 \end{pmatrix}$ .

1.29. Show that  $\alpha: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ , defined by  $\alpha(x) = 4x^2 - 3x^7$ , is a permutation of  $\mathbb{Z}_{11}$ , and write it as a product of disjoint cycles. What is the parity of  $\alpha$ ? What is  $\alpha^{-1}$ ?

- 1.30. Let  $G$  be a group, let  $a \in G$ , and let  $m, n \in \mathbb{Z}$  be (possibly negative) integers. Prove that  $a^m * a^n = a^{m+n} = a^n * a^m$  and  $(a^m)^n = a^{mn} = (a^n)^m$ .
- 1.31. Let  $G$  be a group, let  $a \in G$ , and let  $m$  and  $n$  be relatively prime integers. If  $a^m = e$ , show that there exists  $b \in G$  with  $a = b^n$ . (Hint. There are integers  $s$  and  $t$  with  $1 = sm + tn$ .)
- 1.32 (Cancellation Laws). In a group  $G$ , either of the equations  $a * b = a * c$  and  $b * a = c * a$  implies  $b = c$ .
- 1.33. Let  $G$  be a group and let  $a \in G$ .  
(i) For each  $a \in G$ , prove that the functions  $L_a: G \rightarrow G$ , defined by  $x \mapsto a * x$  (called *left translation* by  $a$ ), and  $R_a: G \rightarrow G$ , defined by  $x \mapsto x * a^{-1}$  (called *right translation* by  $a$ ), are bijections.  
(ii) For all  $a, b \in G$ , prove that  $L_{a*b} = L_a \circ L_b$  and  $R_{a*b} = R_b \circ R_a$ .  
(iii) For all  $a$  and  $b$ , prove that  $L_a \circ R_b = R_b \circ L_a$ .
- 1.34. Let  $G$  denote the multiplicative group of positive rationals. What is the identity of  $G$ ? If  $a \in G$ , what is its inverse?
- 1.35. Let  $n$  be a positive integer and let  $G$  be the multiplicative group of all  $n$ th roots of unity; that is,  $G$  consists of all complex numbers of the form  $e^{2\pi ik/n}$ , where  $k \in \mathbb{Z}$ . What is the identity of  $G$ ? If  $a \in G$ , what is its inverse? How many elements does  $G$  have?

1.36. Prove that the following four permutations form a group  $V$  (which is called the *4-group*):

$$1; \quad (1 \ 2)(3 \ 4); \quad (1 \ 3)(2 \ 4); \quad (1 \ 4)(2 \ 3).$$

1.37. Let  $\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ , and define  $1/0 = \infty$ ,  $1/\infty = 0$ ,  $\infty/\infty = 1$ , and  $1 - \infty = \infty - 1$ . Show that the six functions  $\hat{\mathbb{R}} \rightarrow \hat{\mathbb{R}}$ , given by  $x, 1/x, 1 - x, 1/(1 - x), x/(x - 1), (x - 1)/x$ , form a group with composition as operation.