9

SEMIGROUPS AND GROUPS

Prerequisites: Chapters 4, 5, and 6

The notion of a mathematical structure was introduced in Section 1.6. In the following chapters, other types of mathematical systems were developed; some, such as [propositions, $\wedge$, $\vee$, $\sim$], were not given specific names; but others, such as B_n, the Boolean algebra on n elements, were named. In this chapter, we identify two more types of mathematical structures, semigroups and groups. Semigroups will be used in our study of finite state machines in Chapter 10. We also develop the basic ideas of group theory, which we will apply to coding theory in Chapter 11.

9.1 BINARY OPERATIONS REVISITED

We defined binary operations earlier (see Section 1.6) and noted in Section 5.2 that a binary operation may be used to define a function. Here we turn the process around and define a binary operation as a function with certain properties.

A **binary operation on a set** A is an everywhere defined function $f: A \times A \to A$. Observe the following properties that a binary operation must satisfy:

1. Since $\text{Dom}(f) = A \times A$, f assigns an element $f(a, b)$ of A to each ordered pair (a, b) in $A \times A$. That is, the binary operation must be defined for each ordered pair of elements of A.
2. Since a binary operation is a function, only one element of A is assigned to each ordered pair.

Thus we can say that a binary operation is a rule that assigns to each ordered pair of elements of A a unique element of A. The reader should note that this definition is more restrictive than that given in Chapter 1, but we have made the change to simplify the discussion in this chapter. We shall now turn to a number of examples.

It is customary to denote binary operations by a symbol such as $*$, instead of f, and to denote the element assigned to (a, b) by $a * b$ [instead of $*(a, b)$]. It should be emphasized that if a and b are elements in A, then $a * b \in A$, and this property is often described by saying that A is **closed** under the operation $*$.

EXAMPLE 1 Let $A = Z$. Define $a * b$ as $a + b$. Then $*$ is a binary operation on Z. ■

EXAMPLE 2 Let $A = \mathbb{R}$. Define $a * b$ as a/b. Then $*$ is not a binary operation, since it is not defined for every ordered pair of elements of A. For example, $3 * 0$ is not defined, since we cannot divide by zero. ■

EXAMPLE 3 Let $A = Z^+$. Define $a * b$ as $a - b$. Then $*$ is not a binary operation since it does not assign an element of A to every ordered pair of elements of A; for example, $2 * 5 \notin A$. ■

EXAMPLE 4 Let $A = Z$. Define $a * b$ as a number less than both a and b. Then $*$ is not a binary operation, since it does not assign a *unique* element of A to each ordered pair of elements of A; for example, $8 * 6$ could be 5, 4, 3, 1, and so on. Thus, in this case, $*$ would be a relation from $A \times A$ to A, but not a function. ■

EXAMPLE 5 Let $A = Z$. Define $a * b$ as $\max\{a, b\}$. Then $*$ is a binary operation; for example, $2 * 4 = 4$, $-3 * (-5) = -3$. ■

EXAMPLE 6 Let $A = P(S)$, for some set S. If V and W are subsets of S, define $V * W$ as $V \cup W$. Then $*$ is a binary operation on A. Moreover, if we define $V *' W$ as $V \cap W$, then $*'$ is another binary operation on A. ■

As Example 6 shows, it is possible to define many binary operations on the same set.

EXAMPLE 7 Let M be the set of all $n \times n$ Boolean matrices for a fixed n. Define $\mathbf{A} * \mathbf{B}$ as $\mathbf{A} \vee \mathbf{B}$ (see Section 1.5). Then $*$ is a binary operation. This is also true of $\mathbf{A} \wedge \mathbf{B}$. ■

EXAMPLE 8 Let L be a lattice. Define $a * b$ as $a \wedge b$ (the greatest lower bound of a and b). Then $*$ is a binary operation on L This is also true of $a \vee b$ (the least upper bound of a and b). ■

Tables

If $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, we can define a binary operation on A by means of a table as shown in Figure 9.1. The entry in position i, j denotes the element $a_i * a_j$.

EXAMPLE 9 Let $A = \{0, 1\}$. We define binary operations $\vee$ and $\wedge$ by the following tables:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

■

$*$	a_1	a_2	$\cdots$	a_j	$\cdots$	a_n
a_1						
a_2						
$\vdots$						
a_i				$a_i * a_j$		
$\vdots$						
a_n						

Figure 9 1

If $A = \{a, b\}$, we shall now determine the number of binary operations that can be defined on A. Every binary operation $*$ on A can be described by a table

$*$	a	b
a		
b		

Since every blank can be filled in with the element a or b, we conclude that there are $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ or 16 ways to complete the table. Thus, there are 16 binary operations on A.

Properties of Binary Operations

Several of the properties defined for binary operations in Section 1.6 are of particular importance in this chapter. We repeat them here.

A binary operation on a set A is said to be **commutative** if

$$a * b = b * a$$

for all elements a and b in A.

EXAMPLE 10

The binary operation of addition on Z (as discussed in Example 1) is commutative. ■

EXAMPLE 11

The binary operation of subtraction on Z is not commutative, since

$$2 - 3 \neq 3 - 2. \quad ■$$

A binary operation that is described by a table is commutative if and only if the entries in the table are symmetric with respect to the main diagonal.

EXAMPLE 12

Which of the following binary operations on $A = \{a, b, c, d\}$ are commutative?

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

(a)

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

(b)

Solution The operation in (a) is not commutative, since $a * b$ is c while $b * a$ is b. The operation in (b) is commutative, since the entries in the table are symmetric with respect to the main diagonal. ■

A binary operation $*$ on a set A is said to be **associative** if

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

for all elements a, b, and c in A.

EXAMPLE 13

The binary operation of addition on Z is associative. ■

EXAMPLE 14

The binary operation of subtraction on Z is not associative, since

$$2 - (3 - 5) \neq (2 - 3) - 5. \qquad ■$$

EXAMPLE 15

Let L be a lattice. The binary operation defined by $a * b = a \wedge b$ (see Example 8) is commutative and associative. It also satisfies the **idempotent** property $a \wedge a = a$. A partial converse of this example is also true, as shown in Example 16. ■

EXAMPLE 16

Let $*$ be a binary operation on a set A, and suppose that $*$ satisfies the following properties for any a, b, and c in A.

1. $a = a * a$	Idempotent property
2. $a * b = b * a$	Commutative property
3. $a * (b * c) = (a * b) * c$	Associative property

Define a relation $\leq$ on A by

$$a \leq b \quad \text{if and only if} \quad a = a * b.$$

Show that $(A, \leq)$ is a poset, and for all a, b in A, GLB$(a, b) = a * b$.

Solution We must show that $\leq$ is reflexive, antisymmetric, and transitive. Since $a = a * a$, $a \leq a$ for all a in A, and $\leq$ is reflexive.

Now suppose that $a \leq b$ and $b \leq a$. Then, by definition and property 2, $a = a * b = b * a = b$, so $a = b$. Thus $\leq$ is antisymmetric.

If $a \leq b$ and $b \leq c$, then $a = a * b = a * (b * c) = (a * b) * c = a * c$, so $a \leq c$ and $\leq$ is transitive.

Finally, we must show that, for all a and b in A, $a*b = a \wedge b$ (the greatest lower bound of a and b with respect to $\leq$). We have $a * b = a * (b * b) = (a * b) * b$, so $a * b \leq b$. In a similar way, we can show that $a * b \leq a$, so $a * b$ is a lower bound for a and b. Now, if $c \leq a$ and $c \leq b$, then $c = c * a$ and $c = c * b$ by definition. Thus $c = (c * a) * b = c * (a * b)$, so $c \leq a * b$. This shows that $a * b$ is the greatest lower bound of a and b. ■

9.1 Exercises

In Exercises 1 *through* 8, *determine whether the description of* $*$ *is a valid definition of a binary operation on the set.*

1. On $\mathbb{R}$, where $a * b$ is ab (ordinary multiplication).

2. On Z^+, where $a * b$ is a/b.

3. On Z, where $a * b$ is a^b.

4. On Z^+, where $a * b$ is a^b.

5. On Z^+, where $a * b$ is $a - b$.

6. On $\mathbb{R}$, where $a * b$ is $a\sqrt{b}$.

7. On $\mathbb{R}$, where $a * b$ is the largest rational number that is less than ab.

8. On Z, where $a * b$ is $2a + b$.

In Exercises 9 *through* 17, *determine whether the binary operation* $*$ *is commutative and whether it is associative on the set.*

9. On Z^+, where $a * b$ is $a + b + 2$.

10. On Z, where $a * b$ is ab.

11. On $\mathbb{R}$, where $a * b$ is $a \times |b|$.

12. On the set of nonzero real numbers, where $a * b$ is a/b.

13. On $\mathbb{R}$, where $a * b$ is the minimum of a and b.

14. On the set of $n \times n$ Boolean matrices, where $\mathbf{A} * \mathbf{B}$ is $\mathbf{A} \odot \mathbf{B}$ (see Section 1.5).

15. On $\mathbb{R}$, where $a * b$ is $ab/3$.

16. On $\mathbb{R}$, where $a * b$ is $ab + 2b$.

17. On a lattice A, where $a * b$ is $a \vee b$.

18. Fill in the following table so that the binary operation $*$ is commutative.

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

19. Fill in the following table so that the binary operation $*$ is commutative and has the idempotent property.

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

20. Consider the binary operation $*$ defined on the set $A = \{a, b, c\}$ by the following table.

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

(a) Is $*$ a commutative operation?

(b) Compute $a * (b * c)$ and $(a * b) * c$.

(c) Is $*$ an associative operation?

21. Consider the binary operation $*$ defined on the set $A = \{a, b, c, d\}$ by the following table.

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

Compute

(a) $c * d$ and $d * c$.

(b) $b * d$ and $d * b$.

(c) $a * (b * c)$ and $(a * b) * c$.

(d) Is $*$ commutative? associative?

In Exercises 22 *and* 23, *complete the given table so that the binary operation* $*$ *is associative.*

22.

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

23.

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

24. Let A be a set with n elements. How many binary operations can be defined on A?

25. Let A be a set with n elements. How many commutative binary operations can be defined on A?

26. Let $A = \{a, b\}$.

(a) Make a table for each of the 16 binary operations that can be defined on A.

(b) Using part (a), identify the binary operations on A that are commutative.

27. Let $A = \{a, b\}$

(a) Using Exercise 26, identify the binary operations on A that are associative.

(b) Using Exercise 26, identify the binary operations on A that satisfy the idempotent property.

28. Let $*$ be a binary operation on a set A, and suppose that $*$ satisfies the idempotent, commutative, and associative properties, as discussed in Example 16. Define a relation $\leq$ on A by $a \leq b$ if and only if $b = a * b$. Show that $(A, \leq)$ is a poset and, for all a and b, $\text{LUB}(a, b) = a * b$.

29. Describe how the definition of a binary operation on a set A is different from the definition of a binary operation given in Section 1.6. Explain also whether a binary operation on a set is or is not a binary operation according to the earlier definition.

9.2 SEMIGROUPS

In this section we define a simple mathematical structure, consisting of a set together with a binary operation, that has many important applications.

A **semigroup** is a nonempty set S together with an associative binary operation $*$ defined on S. We shall denote the semigroup by $(S, *)$ or, when it is clear what the operation $*$ is, simply by S. We also refer to $a * b$ as the **product** of a and b. The semigroup $(S, *)$ is said to be commutative if $*$ is a commutative operation.

EXAMPLE 1

It follows from Section 9.1 that $(Z, +)$ is a commutative semigroup. ■

EXAMPLE 2

The set $P(S)$, where S is a set, together with the operation of union is a commutative semigroup. ■

EXAMPLE 3

The set Z with the binary operation of subtraction is not a semigroup, since subtraction is not associative. ■

EXAMPLE 4

Let S be a fixed nonempty set, and let S^S be the set of all functions $f\colon S \to S$. If f and g are elements of S^S, we define $f * g$ as $f \circ g$, the composite function. Then $*$ is a binary operation on S^S, and it follows from Section 4.7 that $*$ is associative. Hence $(S^S, *)$ is a semigroup. The semigroup S^S is not commutative. ■

EXAMPLE 5

Let $(L, \leq)$ be a lattice. Define a binary operation on L by $a * b = a \vee b$. Then L is a semigroup. ■

EXAMPLE 6

Let $A = \{a_1, a_2, \ldots, a_n\}$ be a nonempty set. Recall from Section 1.3 that A^* is the set of all finite sequences of elements of A. That is, A^* consists of all words that can be formed from the alphabet A. Let α and β be elements of A^*. Observe that catenation is a binary operation $\cdot$ on A^*. Recall that if $\alpha = a_1 a_2 \cdots a_n$ and

$\beta = b_1 b_2 \cdots b_k$, then $\alpha \cdot \beta = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_k$ It is easy to see that if α, β, and γ are any elements of A^*, then

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

so that $\cdot$ is an associative binary operation, and $(A^*, \cdot)$ is a semigroup. The semigroup $(A^*, \cdot)$ is called the **free semigroup generated by** A. ■

In a semigroup $(S, *)$ we can establish the following generalization of the associative property; we omit the proof.

Theorem 1 If $a_1, a_2, \ldots, a_n$, $n \geq 3$, are arbitrary elements of a semigroup, then all products of the elements $a_1, a_2, \ldots, a_n$ that can be formed by inserting meaningful parentheses arbitrarily are equal. ●

EXAMPLE 7 Theorem 1 shows that the products

$$((a_1 * a_2) * a_3) * a_4, \quad a_1 * (a_2 * (a_3 * a_4)), \quad (a_1 * (a_2 * a_3)) * a_4$$

are all equal. ■

If $a_1, a_2, \ldots, a_n$ are elements in a semigroup $(S, *)$, we shall write their product as

$$a_1 * a_2 * \cdots * a_n,$$

omitting the parentheses.

An element e in a semigroup $(S, *)$ is called an **identity** element if

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

for all $a \in S$. As shown by Theorem 1, Section 1.6, an identity element must be unique.

EXAMPLE 8 The number 0 is an identity in the semigroup $(Z, +)$. ■

EXAMPLE 9 The semigroup $(Z^+, +)$ has no identity element. ■

A **monoid** is a semigroup $(S, *)$ that has an identity.

EXAMPLE 10 The semigroup $P(S)$ defined in Example 2 has the identity $\varnothing$, since

$$\varnothing * A = \varnothing \cup A = A = A \cup \varnothing = A * \varnothing$$

for any element $A \in P(S)$. Hence $P(S)$ is a monoid. ■

EXAMPLE 11 The semigroup S^S defined in Example 4 has the identity 1_S, since

$$1_S * f = 1_S \circ f = f \circ 1_S = f * 1_S$$

for any element $f \in S^S$, we see that S^S is a monoid ■

EXAMPLE 12 The semigroup A^* defined in Example 6 is actually a monoid with identity Λ, the empty sequence, since $\alpha \cdot \Lambda = \Lambda \cdot \alpha = \alpha$ for all $\alpha \in A^*$. ■

EXAMPLE 13 The set of all relations on a set A is a monoid under the operation of composition. The identity element is the equality relation Δ (see Section 4.7). ■

Let $(S, *)$ be a semigroup and let T be a subset of S. If T is closed under the operation $*$ (that is, $a * b \in T$ whenever a and b are elements of T), then $(T, *)$ is called a **subsemigroup** of $(S, *)$. Similarly, let $(S, *)$ be a monoid with identity e, and let T be a nonempty subset of S. If T is closed under the operation $*$ and $e \in T$, then $(T, *)$ is called a **submonoid** of $(S, *)$.

Observe that the associative property holds in any subset of a semigroup so that a subsemigroup $(T, *)$ of a semigroup $(S, *)$ is itself a semigroup. Similarly, a submonoid of a monoid is itself a monoid.

EXAMPLE 14 If T is the set of all even integers, then $(T, \times)$ is a subsemigroup of the monoid $(Z, \times)$, where $\times$ is ordinary multiplication, but it is not a submonoid since the identity of Z, the number 1, does not belong to T. ■

EXAMPLE 15 If $(S, *)$ is a semigroup, then $(S, *)$ is a subsemigroup of $(S, *)$. Similarly, let $(S, *)$ be a monoid. Then $(S, *)$ is a submonoid of $(S, *)$, and if $T = \{e\}$, then $(T, *)$ is also a submonoid of $(S, *)$. ■

Suppose that $(S, *)$ is a semigroup, and let $a \in S$. For $n \in Z^+$, we define the powers of a^n recursively as follows:

$$a^1 = a, \quad a^n = a^{n-1} * a, \qquad n \geq 2$$

Moreover, if $(S, *)$ is a monoid, we also define

$$a^0 = e.$$

It can be shown that if m and n are nonnegative integers, then

$$a^m * a^n = a^{m+n}.$$

EXAMPLE 16 (a) If $(S, *)$ is a semigroup, $a \in S$, and

$$T = \{a^i \mid i \in Z^+\},$$

then $(T, *)$ is a subsemigroup of $(S, *)$.

(b) If $(S, *)$ is a monoid, $a \in S$, and

$$T = \{a^i \mid i \in Z^+ \text{ or } i = 0\},$$

then $(T, *)$ is a submonoid of $(S, *)$. ■

Isomorphism and Homomorphism

An isomorphism between two posets was defined in Section 6.1 as a one-to-one correspondence that preserved order relations, the distinguishing feature of posets. We now define an isomorphism between two semigroups as a one-to-one correspondence that preserves the binary operations. In general, an isomorphism between two mathematical structures of the same type should preserve the distinguishing features of the structures.

Let $(S, *)$ and $(T, *')$ be two semigroups. A function $f\colon S \to T$ is called an **isomorphism** from $(S, *)$ to $(T, *')$ if it is a one-to-one correspondence from S to T, and if

$$f(a * b) = f(a) *' f(b)$$

for all a and b in S.

If f is an isomorphism from $(S, *)$ to $(T, *')$, then, since f is a one-to-one correspondence, it follows from Theorem 1 of Section 5.1 that f^{-1} exists and is a one-to-one correspondence from T to S. We now show that f^{-1} is an isomorphism from $(T, *')$ to $(S, *)$. Let a' and b' be any elements of T. Since f is onto, we can find elements a and b in S such that $f(a) = a'$ and $f(b) = b'$. Then $a = f^{-1}(a')$ and $b = f^{-1}(b')$. Now

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

Hence f^{-1} is an isomorphism.

We now say that the semigroups $(S, *)$ and $(T, *')$ are **isomorphic** and we write $S \simeq T$.

To show that two semigroups $(S, *)$ and $(T, *')$ are isomorphic, we use the following procedure:

STEP 1: Define a function $f\colon S \to T$ with $\mathrm{Dom}(f) = S$.

STEP 2: Show that f is one-to-one.

STEP 3: Show that f is onto.

STEP 4: Show that $f(a * b) = f(a) *' f(b)$.

EXAMPLE 17

Let T be the set of all even integers. Show that the semigroups $(Z, +)$ and $(T, +)$ are isomorphic.

Solution

STEP 1: We define the function $f\colon Z \to T$ by $f(a) = 2a$.

STEP 2: We now show that f is one-to-one as follows. Suppose that $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$, so $a_1 = a_2$. Hence f is one-to-one.

STEP 3: We next show that f is onto. Suppose that b is any even integer. Then $a = b/2 \in Z$ and

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

so f is onto.

***STEP 4*:** We have

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

Hence $(Z, +)$ and $(T, +)$ are isomorphic semigroups. ■

In general, it is rather straightforward to verify that a given function $f\colon S \to T$ is or is not an isomorphism. However, it is generally more difficult to show that two semigroups are isomorphic, because one has to create the isomorphism f.

As in the case of poset or lattice isomorphisms, when two semigroups $(S, *)$ and $(T, *')$ are isomorphic, they can differ only in the nature of their elements; their semigroup structures are identical. If S and T are finite semigroups, their respective binary operations can be given by tables. Then S and T are isomorphic if we can rearrange and relabel the elements of S so that its table is identical with that of T.

EXAMPLE 18 Let $S = \{a, b, c\}$ and $T = \{x, y, z\}$. It is easy to verify that the following operation tables give semigroup structures for S and T, respectively.

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

$*$	x	y	z
x	z	x	y
y	x	y	z
z	y	z	x

Let

$$f(a) = y$$
$$f(b) = x$$
$$f(c) = z.$$

Replacing the elements in S by their images and rearranging the table, we obtain exactly the table for T. Thus S and T are isomorphic. ■

Theorem 2 Let $(S, *)$ and $(T, *')$ be monoids with identities e and e', respectively. Let $f\colon S \to T$ be an isomorphism. Then $f(e) = e'$. ●

Proof Let b be any element of T. Since f is onto, there is an element a in S such that $f(a) = b$. Then

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

Similarly, since $a = e * a$, $b = f(e) *' b$. Thus for any $b \in T$,

$$b = b *' f(e) = f(e) *' b,$$

which means that $f(e)$ is an identity for T. Thus since the identity is unique, it follows that $f(e) = e'$. ▼

If $(S, *)$ and $(T, *')$ are semigroups such that S has an identity and T does not, it then follows from Theorem 2 that $(S, *)$ and $(T, *')$ cannot be isomorphic.

EXAMPLE 19 Let T be the set of all even integers and let $\times$ be ordinary multiplication. Then the semigroups $(Z, \times)$ and $(T, \times)$ are not isomorphic, since Z has an identity and T does not. ■

By dropping the conditions of one to one and onto in the definition of an isomorphism of two semigroups, we get another important method for comparing the algebraic structures of the two semigroups.

Let $(S, *)$ and $(T, *')$ be two semigroups. An everywhere-defined function $f\colon S \to T$ is called a **homomorphism** from $(S, *)$ to $(T, *')$ if

$$f(a * b) = f(a) *' f(b)$$

for all a and b in S. If f is also onto, we say that T is a **homomorphic image** of S.

EXAMPLE 20 Let $A = \{0, 1\}$ and consider the semigroups $(A^*, \cdot)$ and $(A, +)$, where $\cdot$ is the catenation operation and $+$ is defined by the table

+	0	1
0	0	1
1	1	0

Define the function $f\colon A^* \to A$ by

$$f(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ has an odd number of 1's} \\ 0 & \text{if } \alpha \text{ has an even number of 1's.} \end{cases}$$

It is easy to verify that if α and β are any elements of A^*, then

$$f(\alpha \cdot \beta) = f(\alpha) + f(\beta).$$

Thus f is a homomorphism. The function f is onto since

$$f(0) = 0$$
$$f(1) = 1$$

but f is not an isomorphism, since it is not one to one. ■

The difference between an isomorphism and a homomorphism is that an isomorphism must be one to one and onto. For both an isomorphism and a homomorphism, the image of a product is the product of the images.

The proof of the following theorem, which is left as an exercise for the reader, is completely analogous to the proof of Theorem 2.

Theorem 3 Let $(S, *)$ and $(T, *')$ be monoids with identities e and e', respectively. Let $f\colon S \to T$ be a homomorphism from $(S, *)$ onto $(T, *')$. Then $f(e) = e'$. ●

Theorem 3 is a stronger, or more general, statement than Theorem 2, because it requires fewer (weaker) conditions for the conclusion.

Theorem 3, together with the following two theorems, shows that, if a semigroup $(T, *')$ is a homomorphic image of the semigroup $(S, *)$, then $(T, *')$ has a strong algebraic resemblance to $(S, *)$.

Theorem 4 Let f be a homomorphism from a semigroup $(S, *)$ to a semigroup $(T, *')$. If S' is a subsemigroup of $(S, *)$, then

$$f(S') = \{t \in T \mid t = f(s) \text{ for some } s \in S'\},$$

the image of S' under f, is a subsemigroup of $(T, *')$. ●

Proof If t_1 and t_2 are any elements of $f(S')$, then there exist s_1 and s_2 in S' with

$$t_1 = f(s_1) \quad \text{and} \quad t_2 = f(s_2).$$

Then

$$t_1 *' t_2 = f(s_1) *' f(s_2) = f(s_1 * s_2) = f(s_3),$$

where $s_3 = s_1 * s_2 \in S'$. Hence $t_1 *' t_2 \in f(S')$.

Thus $f(S')$ is closed under the operation $*'$. Since the associative property holds in T, it holds in $f(S')$, so $f(S')$ is a subsemigroup of $(T, *')$. ▼

Theorem 5 If f is a homomorphism from a commutative semigroup $(S, *)$ onto a semigroup $(T, *')$, then $(T, *')$ is also commutative. ●

Proof Let t_1 and t_2 be any elements of T. Then there exist s_1 and s_2 in S with

$$t_1 = f(s_1) \quad \text{and} \quad t_2 = f(s_2).$$

Therefore,

$$t_1 *' t_2 = f(s_1) *' f(s_2) = f(s_1 * s_2) = f(s_2 * s_1) = f(s_2) *' f(s_1) = t_2 *' t_1.$$

Hence $(T, *')$ is also commutative. ▼

9.2 Exercises

1. Let $A = \{a, b\}$. Which of the following tables define a semigroup on A? Which define a monoid on A?

(a)

$*$	a	b
a	a	b
b	a	a

(b)

$*$	a	b
a	a	b
b	b	b

2. Let $A = \{a, b\}$. Which of the following tables define a semigroup on A? Which define a monoid on A?

(a)

$*$	a	b
a	b	a
b	a	b

(b)

$*$	a	b
a	a	b
b	b	a

3. Let $A = \{a, b\}$. Which of the following tables define a semigroup on A? Which define a monoid on A?

(a)

$*$	a	b
a	a	a
b	b	b

(b)

$*$	a	b
a	b	b
b	a	a

In Exercises 4 through 14, determine whether the set together with the binary operation is a semigroup, a monoid, or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid, determine if it is commutative.

4. Z^+, where $*$ is defined as ordinary multiplication.

5. Z^-, where $a * b$ is defined as $\max\{a, b\}$.

6. Z^+, where $a * b$ is defined as $\text{GCD}\{a, b\}$.

7. Z^+, where $a * b$ is defined as a.

8. The nonzero real numbers, where $*$ is ordinary multiplication.

9. $P(S)$, with S a set, where $*$ is defined as intersection.

10. A Boolean algebra B, where $a * b$ is defined as $a \wedge b$.

11. $S = \{1, 2, 3, 6, 12\}$, where $a * b$ is defined as $\text{GCD}(a, b)$.

12. $S = \{1, 2, 3, 6, 9, 18\}$, where $a * b$ is defined as $\text{LCM}(a, b)$.

13. Z, where $a * b = a + b - ab$.

14. The even integers, where $a * b$ is defined as $\dfrac{ab}{2}$.

15. Does the following table define a semigroup?

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

16. Does the following table define a semigroup?

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

17. Complete the following table to obtain a semigroup.

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

18. Complete the following table so that it defines a monoid.

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

19. Let $S = \{a, b\}$. Write the operation table for the semigroup S^S. Is the semigroup commutative?

20. Let $S = \{a, b\}$. Write the operation table for the semigroup $(P(S), \cup)$.

21. Let $A = \{a, b, c\}$ and consider the semigroup $(A^*, \cdot)$, where $\cdot$ is the operation of catenation. If $\alpha = abac$, $\beta = cba$, and $\gamma = babc$, compute

(a) $(\alpha{\cdot}\beta){\cdot}\gamma$ (b) $\gamma{\cdot}(\alpha{\cdot}\alpha)$ (c) $(\gamma{\cdot}\beta){\cdot}\alpha$

22. Prove or disprove that the intersection of two subsemigroups of a semigroup $(S, *)$ is a subsemigroup of $(S, *)$.

23. Prove or disprove that the intersection of two submonoids of a monoid $(S, *)$ is a submonoid of $(S, *)$.

24. Let $A = \{0, 1\}$, and consider the semigroup $(A^*, \cdot)$, where $\cdot$ is the operation of catenation. Let T be the subset of A^* consisting of all sequences having an odd number of 1's. Is $(T, \cdot)$ a subsemigroup of $(A, \cdot)$?

25. Let $A = \{a, b\}$. Are there two semigroups $(A, *)$ and $(A, *')$ that are not isomorphic?

26. An element x in a monoid is called an **idempotent** if $x^2 = x * x = x$. Show that the set of all idempotents in a commutative monoid S is a submonoid of S.

27. Let $(S_1, *_1)$, $(S_2, *_2)$, and $(S_3, *_3)$ be semigroups and $f\colon S_1 \to S_2$ and $g\colon S_2 \to S_3$ be homomorphisms. Prove that $g \circ f$ is a homomorphism from S_1 to S_3.

28. Let $(S_1, *)$, $(S_2, *')$, and $(S_3, *'')$ be semigroups, and let $f \cdot S_1 \to S_2$ and $g\colon S_2 \to S_3$ be isomorphisms. Show that $g \circ f\colon S_1 \to S_3$ is an isomorphism.

29. Which properties of f are used in the proof of Theorem 2?

30. Explain why the proof of Theorem 1 can be used as a proof of Theorem 3.

31. Let R^+ be the set of all positive real numbers. Show that the function $f \cdot R^+ \to R$ defined by $f(x) = \ln x$ is an isomorphism of the semigroup $(R^+, \times)$ to the semigroup $(R, +)$, where $\times$ and $+$ are ordinary multiplication and addition, respectively

9.3 PRODUCTS AND QUOTIENTS OF SEMIGROUPS

In this section we shall obtain new semigroups from existing semigroups.

Theorem 1 If $(S, *)$ and $(T, *')$ are semigroups, then $(S \times T, *'')$ is a semigroup, where $*''$ is defined by $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$. ●

Proof The proof is left as an exercise. ▼

It follows at once from Theorem 1 that if S and T are monoids with identities e_S and e_T, respectively, then $S \times T$ is a monoid with identity (e_S, e_T).

We now turn to a discussion of equivalence relations on a semigroup $(S, *)$. Since a semigroup is not merely a set, we shall find that certain equivalence relations on a semigroup give additional information about the structure of the semigroup.

An equivalence relation R on the semigroup $(S, *)$ is called a **congruence relation** if

$$a \; R \; a' \quad \text{and} \quad b \; R \; b' \quad \text{imply} \quad (a * b) \; R \; (a' * b').$$

EXAMPLE 1

Consider the semigroup $(Z, +)$ and the equivalence relation R on Z defined by

$$a \; R \; b \quad \text{if and only if} \quad a \equiv b \pmod{2}.$$

Recall that we discussed this equivalence relation in Section 4.5. Remember that if $a \equiv b \pmod{2}$, then $2 \mid (a - b)$. We now show that this relation is a congruence relation as follows.

If

$$a \equiv b \pmod{2} \quad \text{and} \quad c \equiv d \pmod{2},$$

then 2 divides $a - b$ and 2 divides $c - d$, so

$$a - b = 2m \quad \text{and} \quad c - d = 2n,$$

where m and n are in Z. Adding, we have

$$(a - b) + (c - d) = 2m + 2n$$

or

$$(a + c) - (b + d) = 2(m + n),$$

so

$$a + c \equiv b + d \pmod{2}.$$

Hence the relation is a congruence relation. ■

EXAMPLE 2

Let $A = \{0, 1\}$ and consider the free semigroup $(A^*, \cdot)$ generated by A. Define the following relation on A:

$$\alpha \; R \; \beta \quad \text{if and only if} \quad \alpha \text{ and } \beta \text{ have the same number of 1's.}$$

Show that R is a congruence relation on $(A^*, \cdot)$.

Solution We first show that R is an equivalence relation. We have

1. $\alpha \; R \; \alpha$ for any $\alpha \in A^*$.
2. If $\alpha \; R \; \beta$, then α and β have the same number of 1's, so $\beta \; R \; \alpha$.
3. If $\alpha \; R \; \beta$ and $\beta \; R \; \gamma$, then α and β have the same number of 1's and β and γ have the same number of 1's, so α and γ have the same number of 1's. Hence $\alpha \; R \; \gamma$.

We next show that R is a congruence relation. Suppose that $\alpha \; R \; \alpha'$ and $\beta \; R \; \beta'$. Then α and α' have the same number of 1's and β and β' have the same number of 1's. Since the number of 1's in $\alpha \cdot \beta$ is the sum of the number of 1's in α and the number of 1's in β, we conclude that the number of 1's in $\alpha \cdot \beta$ is the same as the number of 1's in $\alpha' \cdot \beta'$. Hence

$$(\alpha \cdot \beta) \; R \; (\alpha' \cdot \beta')$$

and thus R is a congruence relation. ■

EXAMPLE 3 Consider the semigroup $(Z, +)$, where $+$ is ordinary addition. Let $f(x) = x^2 - x - 2$. We now define the following relation on Z:

$$a \; R \; b \quad \text{if and only if} \quad f(a) = f(b).$$

It is straightforward to verify that R is an equivalence relation on Z. However, R is not a congruence relation since we have

$$-1 \; R \; 2 \qquad \text{since } f(-1) = f(2) = 0$$

and

$$-2 \; R \; 3 \qquad \text{since } f(-2) = f(3) = 4$$

but

$$(-1 + -2) \not R \; (2 + 3)$$

since $f(-3) = 10$ and $f(5) = 18$. ■

Recall from Section 4.5 that an equivalence relation R on the semigroup $(S, *)$ determines a partition of S. We let $[a] = R(a)$ be the equivalence class containing a and S/R denote the set of all equivalence classes. The notation $[a]$ is more traditional in this setting and produces less confusing computations.

Theorem 2 Let R be a congruence relation on the semigroup $(S, *)$. Consider the relation $\circledast$ from $S/R \times S/R$ to S/R in which the ordered pair $([a], [b])$ is, for a and b in S, related to $[a * b]$.

(a) $\circledast$ is a function from $S/R \times S/R$ to S/R, and as usual we denote $\circledast([a], [b])$ by $[a] \circledast [b]$. Thus $[a] \circledast [b] = [a * b]$.

(b) $(S/R, \circledast)$ is a semigroup. ●

Proof Suppose that $([a], [b]) = ([a'], [b'])$. Then $a \; R \; a'$ and $b \; R \; b'$, so we must have $a * b \; R \; a' * b'$, since R is a congruence relation. Thus $[a * b] = [a' * b']$; that is, $\circledast$ is a function. This means that $\circledast$ is a binary operation on S/R.

Next, we must verify that $\circledast$ is an associative operation. We have

$$\begin{aligned}
[a] \circledast ([b] \circledast [c]) &= [a] \circledast [b * c] \\
&= [a * (b * c)] \\
&= [(a * b) * c] \quad \text{by the associative property of } * \text{ in } S \\
&= [a * b] \circledast [c] \\
&= ([a] \circledast [b]) \circledast [c].
\end{aligned}$$

Hence S/R is a semigroup. We call S/R the **quotient semigroup** or **factor semigroup**. Observe that $\circledast$ is a type of "quotient binary relation" on S/R that is constructed from the original binary relation $*$ on S by the congruence relation R. ▼

Corollary 1 Let R be a congruence relation on the monoid $(S, *)$. If we define the operation $\circledast$ in S/R by $[a] \circledast [b] = [a * b]$, then $(S/R, \circledast)$ is a monoid. ●

Proof If e is the identity in $(S, *)$, then it is easy to verify that $[e]$ is the identity in $(S/R, \circledast)$. ▼

EXAMPLE 4 Consider the situation in Example 2. Since R is a congruence relation on the monoid $S = (A^*, \cdot)$, we conclude that $(S/R, \odot)$ is a monoid, where

$$[\alpha] \odot [\beta] = [\alpha \cdot \beta].$$ ■

EXAMPLE 5 As has already been pointed out in Section 4.5, we can repeat Example 4 of that section with the positive integer n instead of 2. That is, we define the following relation on the semigroup $(Z, +)$:

$$a\ R\ b \quad \text{if and only if} \quad a \equiv b \pmod{n}.$$

Using exactly the same method as in Example 4 in Section 4.5, we show that R is an equivalence relation and, as in the case of $n = 2$, $a \equiv b \pmod{n}$ implies $n \mid (a - b)$. Thus, if n is 4, then

$$2 \equiv 6 \pmod{4}$$

and 4 divides $(2 - 6)$. We also leave it for the reader to show that $\equiv \pmod{n}$ is a congruence relation on Z.

We now let $n = 4$ and we compute the equivalence classes determined by the congruence relation $\equiv \pmod{4}$ on Z. We obtain

$$\begin{aligned}
[0] &= \{\ldots, -8, -4, 0, 4, 8, 12, \ldots, \} = [4] = [8] = \cdots \\
[1] &= \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\} = [5] = [9] = \cdots \\
[2] &= \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\} = [6] = [10] = \cdots \\
[3] &= \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\} = [7] = [11] = \cdots.
\end{aligned}$$

These are all the distinct equivalence classes that form the quotient set $Z/\equiv \pmod{4}$. It is customary to denote the quotient set $Z/\equiv \pmod{n}$ by Z_n; Z_n is a monoid with operation $\oplus$ and identity $[0]$. We now determine the addition table for the semigroup Z_4 with operation $\oplus$.

⊕	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The entries in this table are obtained from

$$[a] \oplus [b] = [a + b].$$

Thus

$$\begin{aligned}[1] \oplus [2] &= [1+2] = [3]\\ [1] \oplus [3] &= [1+3] = [4] = [0]\\ [2] \oplus [3] &= [2+3] = [5] = [1]\\ [3] \oplus [3] &= [3+3] = [6] = [2].\end{aligned}$$

It can be shown that, in general, Z_n has the n equivalence classes

$$[0], [1], [2], \ldots, [n-1]$$

and that

$$[a] \oplus [b] = [r],$$

where r is the remainder when $a+b$ is divided by n. Thus, if n is 6,

$$\begin{aligned}[2] \oplus [3] &= [5]\\ [3] \oplus [5] &= [2]\\ [3] \oplus [3] &= [0].\end{aligned}$$

■

We shall now examine the connection between the structure of a semigroup $(S, *)$ and the quotient semigroup $(S/R, \circledast)$, where R is a congruence relation on $(S, *)$.

Theorem 3 Let R be a congruence relation on a semigroup $(S, *)$, and let $(S/R, \circledast)$ be the corresponding quotient semigroup. Then the function $f_R\colon S \to S/R$ defined by

$$f_R(a) = [a]$$

is an onto homomorphism, called the **natural homomorphism**. ●

Proof If $[a] \in S/R$, then $f_R(a) = [a]$, so f_R is an onto function. Moreover, if a and b are elements of S, then

$$f_R(a * b) = [a * b] = [a] \circledast [b] = f_R(a) \circledast f_R(b),$$

so f_R is a homomorphism. ▼

Theorem 4 Fundamental Homomorphism Theorem Let $f\colon S \to T$ be a homomorphism of the semigroup $(S, *)$ onto the semigroup $(T, *')$. Let R be the relation on S defined by $a\ R\ b$ if and only if $f(a) = f(b)$, for a and b in S. Then

(a) R is a congruence relation.

(b) $(T, *')$ and the quotient semigroup $(S/R, \circledast)$ are isomorphic. ●

Proof

(a) We show that R is an equivalence relation. First, $a\ R\ a$ for every $a \in S$, since $f(a) = f(a)$. Next, if $a\ R\ b$, then $f(a) = f(b)$, so $b\ R\ a$. Finally, if $a\ R\ b$ and $b\ R\ c$, then $f(a) = f(b)$ and $f(b) = f(c)$, so $f(a) = f(c)$ and $a\ R\ c$. Hence R is an equivalence relation. Now suppose that $a\ R\ a_1$ and $b\ R\ b_1$. Then

$$f(a) = f(a_1) \quad \text{and} \quad f(b) = f(b_1).$$

Multiplying in T, we obtain

$$f(a) *' f(b) = f(a_1) *' f(b_1).$$

Since f is a homomorphism, this last equation can be rewritten as

$$f(a * b) = f(a_1 * b_1).$$

Hence

$$(a * b)\ R\ (a_1 * b_1)$$

and R is a congruence relation.

(b) We now consider the relation $\overline{f}$ from S/R to T defined as follows:

$$\overline{f} = \{([a], f(a)) \mid [a] \in S/R\}.$$

We first show that $\overline{f}$ is a function. Suppose that $[a] = [a']$ Then $a\ R\ a'$, so $f(a) = f(a')$, which implies that $\overline{f}$ is a function. We may now write $\overline{f}: S/R \to T$, where $\overline{f}([a]) = f(a)$ for $[a] \in S/R$.

We next show that $\overline{f}$ is one to one Suppose that $\overline{f}([a]) = \overline{f}([a'])$. Then

$$f(a) = f(a').$$

So $a\ R\ a'$, which implies that $[a] = [a']$. Hence $\overline{f}$ is one to one.

Now we show that $\overline{f}$ is onto. Suppose that $b \in T$. Since f is onto, $f(a) = b$ for some element a in S. Then

$$\overline{f}([a]) = f(a) = b.$$

So $\overline{f}$ is onto.

Finally,

$$\begin{aligned}\overline{f}([a] \circledast [b]) &= \overline{f}([a * b]) \\ &= f(a * b) = f(a) *' f(b) \\ &= \overline{f}([a]) *' \overline{f}([b]).\end{aligned}$$

Hence $\overline{f}$ is an isomorphism. ▼

EXAMPLE 6 Let $A = \{0, 1\}$, and consider the free semigroup A^* generated by A under the operation of catenation. Note that A^* is a monoid with the empty string Λ as its identity. Let N be the set of all nonnegative integers. Then N is a semigroup under the operation of ordinary addition, denoted by $(N, +)$. The function $f: A^* \to N$ defined by

$$f(\alpha) = \text{the number of 1's in } \alpha$$

is readily checked to be a homomorphism. Let R be the following relation on A^*:

$$\alpha \; R \; \beta \quad \text{if and only if} \quad f(\alpha) = f(\beta).$$

That is, $\alpha \; R \; \beta$ if and only if α and β have the same number of 1's. Theorem 4 implies that $A^*/R \simeq N$ under the isomorphism $\overline{f}\colon A^*/R \to N$ defined by

$$\overline{f}([\alpha]) = f(\alpha) = \text{the number of 1's in } \alpha. \qquad \blacksquare$$

$$\begin{tikzcd}
S \arrow[rr, "f"] \arrow[dr, "f_R"'] & & T \\
& S/T \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

Figure 9.2

Theorem 4(b) can be described by the diagram shown in Figure 9.2. Here f_R is the natural homomorphism. It follows from the definitions of f_R and $\overline{f}$ that

$$\overline{f} \circ f_R = f$$

since

$$(\overline{f} \circ f_R)(a) = \overline{f}(f_R(a)) = \overline{f}([a]) = f(a).$$

9.3 Exercises

1. Let $(S, *)$ and $(T, *')$ be commutative semigroups. Show that $S \times T$ (see Theorem 1) is also a commutative semigroup.

2. Let $(S, *)$ and $(T, *')$ be monoids. Show that $S \times T$ is also a monoid. Show that the identity of $S \times T$ is (e_S, e_T).

3. Let $(S, *)$ and $(T, *')$ be semigroups. Show that the function $f\colon S \times T \to S$ defined by $f(s, t) = s$ is a homomorphism of the semigroup $S \times T$ onto the semigroup S.

4. Let $(S, *)$ and $(T, *')$ be semigroups. Show that $S \times T$ and $T \times S$ are isomorphic semigroups.

5. Prove Theorem 1.

In Exercises 6 *through* 15, *determine whether the relation R on the semigroup S is a congruence relation.*

6. $S = Z$ under the operation of ordinary addition; $a \; R \; b$ if and only if 2 does not divide $a - b$.

7. $S = Z$ under the operation of ordinary addition; $a \; R \; b$ if and only if $a + b$ is even.

8. $S =$ any semigroup; $a \; R \; b$ if and only if $a = b$.

9. $S =$ the set of all rational numbers under the operation of addition; $a/b \; R \; c/d$ if and only if $ad = bc$.

10. $S =$ the set of all rational numbers under the operation of multiplication; $a/b \; R \; c/d$ if and only if $ad = bc$.

11. $S = Z$ under the operation of ordinary addition; $a \; R \; b$ if and only if $a \equiv b \pmod 3$.

12. $S = Z$ under the operation of ordinary addition; $a \; R \; b$ if and only if a and b are both even or a and b are both odd.

13. $S = Z^+$ under the operation of ordinary multiplication; $a \; R \; b$ if and only if $|a - b| \leq 2$.

14. $A = \{0, 1\}$ and $S = A^*$, the free semigroup generated by A under the operation of catenation; $\alpha \; R \; \beta$ if and only if α and β both have an even number of 1's or both have an odd number of 1's.

15. $S = \{0, 1\}$ under the operation $*$ defined by the table

$*$	0	1
0	0	1
1	1	0

$a \; R \; b$ if and only if $a * a = b * b$. (*Hint*: Observe that if x is any element in S, then $x * x = 0$.)

16. Show that the intersection of two congruence relations on a semigroup is a congruence relation.

17. Show that the composition of two congruence relations on a semigroup need not be a congruence relation.

18. Describe the quotient semigroup for S and R given in Exercise 10.

19. Describe the quotient semigroup for S and R given in Exercise 11.

20. Describe the quotient semigroup for S and R given in Exercise 12.

21. Describe the quotient semigroup for $S = Z$ with ordinary addition and R defined by $a \; R \; b$ if and only if $a \equiv b$ (mod 5).

22. Consider the semigroup $S = \{a, b, c, d\}$ with the following operation table.

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

Consider the congruence relation $R = \{(a, a), (a, b), (b, a), (b, b), (c. c), (c, d), (d, c), (d. d)\}$ on S.

(a) Write the operation table of the quotient semigroup S/R.

(b) Describe the natural homomorphism $f_R \colon S \to S/R$.

23. Consider the monoid $S = \{e, a, b, c\}$ with the following operation table.

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

Consider the congruence relation $R = \{(e, e), (e, a), (a, e), (a, a), (b, b), (b, c), (c, b), (c, c)\}$ on S.

(a) Write the operation table of the quotient monoid S/R.

(b) Describe the natural homomorphism $f_R .\ S \to S/R$.

24. Let $A = \{0, 1\}$ and consider the free semigroup A^* generated by A under the operation of catenation. Let N be the semigroup of all nonnegative integers under the operation of ordinary addition.

(a) Verify that the function $f \colon A^* \to N$, defined by $f(\alpha) =$ the number of digits in α, is a homomorphism.

(b) Let R be the following relation on $A^*\cdot$ $\alpha\ R\ \beta$ if and only if $f(\alpha) = f(\beta)$. Show that R is a congruence relation on A^*.

(c) Show that A^*/R and N are isomorphic.

25. Describe the strategy of the proof of Theorem 4. Outline the proof.

9.4 GROUPS

In this section we examine a special type of monoid, called a group, that has applications in every area where symmetry occurs. Applications of groups can be found in mathematics, physics, and chemistry, as well as in less obvious areas such as sociology. Recent and exciting applications of group theory have arisen in fields such as particle physics and in the solutions of puzzles such as Rubik's cube. In this book, we shall present an important application of group theory to binary codes in Section 11.2.

A **group** $(G, *)$ is a monoid, with identity e, that has the additional property that for every element $a \in G$ there exists an element $a' \in G$ such that $a * a' = a' * a = e$. Thus a group is a set together with a binary operation $*$ on G such that

1. $(a * b) * c = a * (b * c)$ for any elements a, b, and c in G.
2. There is a unique element e in G such that
$$a * e = e * a \qquad \text{for any } a \in G.$$
3. For every $a \in G$, there is an element $a' \in G$, called an **inverse** of a, such that
$$a * a' = a' * a = e.$$

Observe that if $(G, *)$ is a group, then $*$ is a binary operation, so G must be closed under $*$; that is,

$$a * b \in G \qquad \text{for any elements } a \text{ and } b \text{ in } G.$$

To simplify our notation, from now on when only one group $(G, *)$ is under consideration and there is no possibility of confusion, we shall write the product $a * b$ of the elements a and b in the group $(G, *)$ simply as ab, and we shall also refer to $(G, *)$ simply as G.

A group G is said to be **Abelian** if $ab = ba$ for all elements a and b in G.

EXAMPLE 1 The set of all integers Z with the operation of ordinary addition is an Abelian group. If $a \in Z$, then an inverse of a is its opposite $-a$. ■

EXAMPLE 2 The set Z^+ under the operation of ordinary multiplication is not a group since, for example, the element 2 in Z^+ has no inverse. However, this set together with the given operation is a monoid. ■

EXAMPLE 3 The set of all nonzero real numbers under the operation of ordinary multiplication is a group. An inverse of $a \neq 0$ is $1/a$. ■

EXAMPLE 4 Let G be the set of all nonzero real numbers and let

$$a * b = \frac{ab}{2}.$$

Show that $(G, *)$ is an Abelian group.

Solution We first verify that $*$ is a binary operation. If a and b are elements of G, then $ab/2$ is a nonzero real number and hence is in G. We next verify associativity. Since

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4}$$

and since

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)c}{4},$$

the operation $*$ is associative.

The number 2 is the identity in G, for if $a \in G$, then

$$a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a.$$

Finally, if $a \in G$, then $a' = 4/a$ is an inverse of a, since

$$a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a.$$

Since $a * b = b * a$ for all a and b in G, we conclude that G is an Abelian group. ■

Before proceeding with additional examples of groups, we develop several important properties that are satisfied in any group G.

Theorem 1 Let G be a group. Each element a in G has only one inverse in G. ●

Proof Let a' and a'' be inverses of a. Then

$$a'(aa'') = a'e = a'$$

and

$$(a'a)a'' = ea'' = a''.$$

Hence, by associativity,

$$a' = a''. \qquad ▼$$

From now on we shall denote the inverse of a by a^{-1}. Thus in a group G we have

$$aa^{-1} = a^{-1}a = e.$$

Theorem 2 Let G be a group and let a, b, and c be elements of G. Then

(a) $ab = ac$ implies that $b = c$ (**left cancellation property**).

(b) $ba = ca$ implies that $b = c$ (**right cancellation property**). ●

Proof

(a) Suppose that

$$ab = ac.$$

Multiplying both sides of this equation by a^{-1} on the left, we obtain

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) && \\ (a^{-1}a)b &= (a^{-1}a)c && \text{by associativity} \\ eb &= ec && \text{by the definition of an inverse} \\ b &= c && \text{by definition of an identity.} \end{aligned}$$

(b) The proof is similar to that of part (a). ▼

Theorem 3 Let G be a group and let a and b be elements of G. Then

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

(b) $(ab)^{-1} = b^{-1}a^{-1}$. ●

Proof

(a) We show that a acts as an inverse for a^{-1}:

$$a^{-1}a = aa^{-1} = e.$$

Since the inverse of an element is unique, we conclude that $(a^{-1})^{-1} = a$.

(b) We easily verify that

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

and, similarly,

$$(b^{-1}a^{-1})(ab) = e,$$

so

$$(ab)^{-1} = b^{-1}a^{-1}. \qquad ▼$$

Theorem 4 Let G be a group, and let a and b be elements of G. Then

(a) The equation $ax = b$ has a unique solution in G.

(b) The equation $ya = b$ has a unique solution in G. ●

Proof

(a) The element $x = a^{-1}b$ is a solution of the equation $ax = b$, since

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

Suppose now that x_1 and x_2 are two solutions of the equation $ax = b$. Then

$$ax_1 = b \quad \text{and} \quad ax_2 = b.$$

Hence

$$ax_1 = ax_2.$$

Theorem 2 implies that $x_1 = x_2$.

(b) The proof is similar to that of part (a). ▼

From our discussion of monoids, we know that if a group G has a finite number of elements, then its binary operation can be given by a table, which is generally called a **multiplication table**. The multiplication table of a group $G = \{a_1, a_2, \ldots, a_n\}$ under the binary operation $*$ must satisfy the following properties:

1. The row labeled by e must be

$$a_1, a_2, \ldots, a_n$$

and the column labeled by e must be

$$\begin{matrix} a_1 \\ a_2 \\ \vdots \\ a_n. \end{matrix}$$

2. From Theorem 4, it follows that each element b of the group must appear exactly once in each row and column of the table Thus each row and column is a permutation of the elements $a_1, a_2, \ldots, a_n$ of G, and each row (and each column) determines a different permutation.

If G is a group that has a finite number of elements, we say that G is a **finite group**, and the **order** of G is the number of elements $|G|$ in G. We shall now determine the multiplication tables of all nonisomorphic groups of orders 1, 2, 3, and 4.

If G is a group of order 1, then $G = \{e\}$, and we have $ee = e$. Now let $G = \{e, a\}$ be a group of order 2. Then we obtain a multiplication table (Table 9.1) where we need to fill in the blank. The blank can be filled in by e or by a. Since there can be no repeats in any row or column, we must write e in the blank. The multiplication table shown in Table 9.2 satisfies the associativity property and the other properties of a group, so it is the multiplication table of a group of order 2.

Table 9.1

	e	a
e	e	a
a	a	

Table 9.2

	e	a
e	e	a
a	a	e

Table 9.3

	e	a	b
e	e	a	b
a	a		
b	b		

Table 9.4

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Next, let $G = \{e, a, b\}$ be a group of order 3. We have a multiplication table (Table 9.3) where we must fill in four blanks. A little experimentation shows that we can only complete the table as shown in Table 9.4. It can be shown (a tedious task) that Table 9.4 satisfies the associative property and the other properties of a group. Thus it is the multiplication table of a group of order 3. Observe that the groups of orders 1, 2, and 3 are also Abelian and that there is just one group of each order for a fixed labeling of the elements.

We next come to a group $G = \{e, a, b, c\}$ of order 4. It is not difficult to show that the possible multiplication table for G can be completed as shown in Tables 9.5 through 9.8. It can be shown that each of these tables satisfies the associative property and the other properties of a group. Thus there are four possible multiplication tables for a group of order 4. Again, observe that a group of order 4 is Abelian. We shall return to groups of order 4 toward the end of this section, where we shall see that there are only two and not four different nonisomorphic groups of order 4.

Table 9.5

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 9.6

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table 9.7

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 9.8

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

EXAMPLE 5

Let $B = \{0, 1\}$, and let $+$ be the operation defined on B as follows:

$+$	0	1
0	0	1
1	1	0

Then B is a group. In this group, every element is its own inverse. ■

We next turn to an important example of a group.

EXAMPLE 6

Consider the equilateral triangle shown in Figure 9.3 with vertices 1, 2, and 3. A **symmetry** of the triangle (or of any geometrical figure) is a one-to-one correspondence from the set of points forming the triangle (the geometrical figure) to itself that preserves the distance between adjacent points. Since the triangle is determined by its vertices, a symmetry of the triangle is merely a permutation of the vertices that preserves the distance between adjacent points. Let l_1, l_2, and l_3 be the angle bisectors of the corresponding angles as shown in Figure 9.3, and let O be their point of intersection.

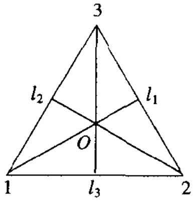


Figure 9.3

We now describe the symmetries of this triangle. First, there is a counterclockwise rotation f_2 of the triangle about O through 120°. Then f_2 can be written (see Section 5.3) as the permutation

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

We next obtain a counterclockwise rotation f_3 about O through 240°, which can be written as the permutation

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Finally, there is a counterclockwise rotation f_1 about O through 360°, which can be written as the permutation

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Of course, f_1 can also be viewed as the result of rotating the triangle about O through 0°.

We may also obtain three additional symmetries of the triangle, g_1, g_2, and g_3, by reflecting about the lines l_1, l_2, and l_3, respectively. We may denote these reflections as the following permutations:

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Observe that the set of all symmetries of the triangle is described by the set of permutations of the set $\{1, 2, 3\}$, which is considered in Section 5.3 and is denoted by S_3. Thus

$$S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}.$$

We now introduce the operation $*$, *followed by*, on the set S_3, and we obtain the multiplication table shown in Table 9.9.

Table 9.9

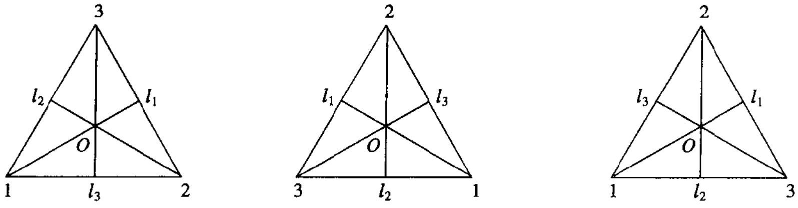
$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1

Each of the entries in this table can be obtained in one of two ways: algebraically or geometrically. For example, suppose that we want to compute $f_2 * g_2$. Geometrically, we proceed as in Figure 9.4. Note that "followed by" here refers to the geometric order. To compute $f_2 * g_2$ algebraically, we compute $f_2 \circ g_2$.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1$$

and find that $f_2 * g_2 = g_1$.

Since composition of functions is always associative, we see that $*$ is an associative operation on S_3. Observe that f_1 is the identity in S_3 and that every element of S_3 has a unique inverse in S_3. For example, $f_2^{-1} = f_3$. Hence S_3 is a group called the **group of symmetries of the triangle**. Observe that S_3 is the first example that we have given of a group that is not Abelian. ■



Given triangle

Triangle resulting after applying f_2

Triangle resulting after applying g_2 to the triangle at the left

Figure 9.4

EXAMPLE 7

The set of all permutations of n elements is a group of order $n!$ under the operation of composition. This group is called the **symmetric group on n letters** and is denoted by S_n. We have seen that S_3 also represents the group of symmetries of the equilateral triangle. ■

As in Example 6, we can also consider the group of symmetries of a square. However, it turns out that this group is of order 8, so it does not agree with the group S_4, whose order is $4! = 24$.

EXAMPLE 8

In Section 9.3 we discussed the monoid Z_n. We now show that Z_n is a group as follows. Let $[a] \in Z_n$. Then we may assume that $0 \leq a < n$. Moreover, $[n - a] \in Z_n$ and since

$$[a] \oplus [n - a] = [a + n - a] = [n] = [0],$$

we conclude that $[n - a]$ is the inverse of $[a]$. Thus, if n is 6, then [2] is the inverse of [4]. Observe that Z_n is an Abelian group. ■

We next turn to a discussion of important subsets of a group. Let H be a subset of a group G such that

(a) The identity e of G belongs to H.

(b) If a and b belong to H, then $ab \in H$.

(c) If $a \in H$, then $a^{-1} \in H$.

Then H is called a **subgroup** of G. Part (b) says that H is a subsemigroup of G. Thus a subgroup of G can be viewed as a subsemigroup having properties (a) and (c).

Observe that if G is a group and H is a subgroup of G, then H is also a group with respect to the operation in G, since the associative property in G also holds in H.

EXAMPLE 9 Let G be a group. Then G and $H = \{e\}$ are subgroups of G, called the **trivial** subgroups of G. ■

EXAMPLE 10 Consider S_3, the group of symmetries of the equilateral triangle, whose multiplication table is shown in Table 9.9. It is easy to verify that $H = \{f_1, f_2, f_3\}$ is a subgroup of S_3. ■

EXAMPLE 11 Let A_n be the set of all even permutations (see Section 5.4) in the group S_n. It can be shown from the definition of even permutation that A_n is a subgroup of S_n, called the **alternating group on *n* letters**. ■

EXAMPLE 12 Let G be a group and let $a \in G$. Since a group is a monoid, we have already defined, in Section 9.2, a^n for $n \in Z^+$ as $aa \cdots a$ (n factors), and a^0 as e. If n is a negative integer, we now define a^{-n} as $a^{-1}a^{-1} \cdots a^{-1}$ (n factors). Then, if n and m are any integers, we have

$$a^n a^m = a^{n+m}.$$

It is easy to show that

$$H = \{a^i \mid i \in Z\}$$

is a subgroup of G. ■

Let $(G, *)$ and $(G', *')$ be two groups. Since groups are also semigroups, we can consider isomorphisms and homomorphisms from $(G, *)$ to $(G', *')$.

Since an isomorphism must be a one-to-one and onto function, it follows that two groups whose orders are unequal cannot possibly be isomorphic.

EXAMPLE 13 Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. Let $f: G \to G'$ be defined by $f(x) = e^x$. We now show that f is an isomorphism.

If $f(a) = f(b)$, so that $e^a = e^b$, then $a = b$. Thus f is one to one. If $c \in G'$, then $\ln c \in G$ and

$$f(\ln c) = e^{\ln c} = c,$$

so f is onto. Finally,

$$f(a + b) = e^{a+b} = e^a e^b = f(a)f(b).$$

Hence f is an isomorphism. ■

EXAMPLE 14 Let G be the symmetric group of n letters, and let G' be the group B defined in Example 5. Let $f: G \to G'$ be defined as follows: for $p \in G$,

$$f(p) = \begin{cases} 0 & \text{if } p \in A_n \quad \text{(the subgroup of all even permutations in } G\text{)} \\ 1 & \text{if } p \notin A_n. \end{cases}$$

Then f is a homomorphism. ■

EXAMPLE 15 Let G be the group of integers under addition, and let G' be the group Z_n as discussed in Example 8. Let $f: G \to G'$ be defined as follows: If $m \in G$, then $f(m) = [r]$, where r is the remainder when m is divided by n. We now show that f is a homomorphism of G onto G'.

Let $[r] \in Z_n$. Then we may assume that $0 \leq r < n$, so

$$r = 0 \cdot n + r,$$

which means that the remainder when r is divided by n is r. Hence

$$f(r) = [r]$$

and thus f is onto.

Next, let a and b be elements of G expressed as

$$a = q_1 n + r_1, \qquad \text{where } 0 \leq r_1 < n, \text{ and } r_1 \text{ and } q_1 \text{ are integers} \tag{1}$$

$$b = q_2 n + r_2, \qquad \text{where } 0 \leq r_2 < n, \text{ and } r_2 \text{ and } q_2 \text{ are integers} \tag{2}$$

so that

$$f(a) = [r_1] \quad \text{and} \quad f(b) = [r_2].$$

Then

$$f(a) + f(b) = [r_1] + [r_2] = [r_1 + r_2].$$

To find $[r_1 + r_2]$, we need the remainder when $r_1 + r_2$ is divided by n. Write

$$r_1 + r_2 = q_3 n + r_3, \qquad \text{where } 0 \leq r_3 < n, \text{ and } r_3 \text{ and } q_3 \text{ are integers.}$$

Thus

$$f(a) + f(b) = [r_3].$$

Adding, we have

$$a + b = q_1 n + q_2 n + r_1 + r_2 = (q_1 + q_2 + q_3)n + r_3,$$

so

$$f(a + b) = [r_1 + r_2] = [r_3].$$

Hence

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

which implies that f is a homomorphism.

Note that when n is 2, f assigns each even integer to [0] and each odd integer to [1]. ■

Theorem 5 Let $(G, *)$ and $(G', *')$ be two groups, and let $f\colon G \to G'$ be a homomorphism from G to G'.

(a) If e is the identity in G and e' is the identity in G', then $f(e) = e'$.

(b) If $a \in G$, then $f(a^{-1}) = (f(a))^{-1}$.

(c) If H is a subgroup of G, then

$$f(H) = \{f(h) \mid h \in H\}$$

is a subgroup of G'. ●

Proof

(a) Let $x = f(e)$. Then

$$x *' x = f(e) *' f(e) = f(e * e) = f(e) = x,$$

so $x *' x = x$. Multiplying both sides by x^{-1} on the right, we obtain

$$x = x *' x *' x^{-1} = x *' x^{-1} = e'.$$

Thus $f(e) = e'$.

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

$$f(a * a^{-1}) = f(e) = e' \quad \text{by part (a)}$$

or

$$f(a) *' f(a^{-1}) = e' \quad \text{since } f \text{ is a homomorphism.}$$

Similarly,

$$f(a^{-1}) *' f(a) = e'.$$

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

(c) This follows from Theorem 4 of Section 9.2 and parts (a) and (b). ▼

EXAMPLE 16 The groups S_3 and Z_6 are both of order 6. However, S_3 is not Abelian and Z_6 is Abelian. Hence they are not isomorphic. Remember that an isomorphism preserves all properties defined in terms of the group operations. ■

EXAMPLE 17 Earlier in this section we found four possible multiplication tables (Tables 9.5 through 9.8) for a group or order 4. We now show that the groups with multiplication Tables 9.6, 9.7, and 9.8 are isomorphic as follows. Let $G = \{e, a, b, c\}$ be the group whose multiplication table is Table 9.6, and let $G' = \{e', a', b', c'\}$ be the group whose multiplication table is Table 9.7, where we put primes on every entry in this last table. Let $f\colon G \to G'$ be defined by $f(e) = e'$, $f(a) = b'$, $f(b) = a'$, $f(c) = c'$. We can then verify that under this renaming of elements the two tables become identical, so the corresponding groups are isomorphic. Similarly, let $G'' = \{e'', a'', b'', c''\}$ be the group whose multiplication table is Table 9.8, where we put double primes on every entry in this last table. Let $g\colon G \to G''$ be defined by $g(e) = e''$, $g(a) = c''$, $g(b) = b''$, $g(c) = a''$. We can then verify that under this renaming of elements the two tables become identical, so the corresponding groups are isomorphic. That is, the groups given by Tables 9.6, 9.7, and 9.8 are isomorphic.

Now, how can we be sure that Tables 9.5 and 9.6 do not yield isomorphic groups? Observe that if x is any element in the group determined by Table 9.5, then $x^2 = e$. If the groups were isomorphic, then the group determined by Table 9.6 would have the same property. Since it does not, we conclude that these groups are not isomorphic. Thus there are exactly two nonisomorphic groups of order 4.

The group with multiplication Table 9.5 is called the **Klein 4 group** and it is denoted by V. The one with multiplication Table 9 6, 9.7, or 9.8 is denoted by Z_4, since a relabeling of the elements of Z_4 results in this multiplication table. ■

9.4 Exercises

In Exercises 1 *through* 11, *determine whether the set together with the binary operation is a group. If it is a group, determine if it is Abelian; specify the identity and the inverse of a generic element.*

1. Z, where $*$ is ordinary multiplication.

2. Z, where $*$ is ordinary subtraction.

3. Q, the set of all rational numbers under the operation of addition.

4. Q, the set of all rational numbers under the operation of multiplication.

5. $\mathbb{R}$, under the operation of multiplication.

6. $\mathbb{R}$, where $a * b = a + b + 2$.

7. Z^+, under the operation of addition.

8. The real numbers that are not equal to -1, where $a * b = a + b + ab$.

9. The set of odd integers under the operation of multiplication.

10. The set of all $m \times n$ matrices under the operation of matrix addition.

11. If S is a nonempty set, the set $P(S)$, where $A * B = A \oplus B$. (See Section 1.2.)

12. Let $S = \{x \mid x \text{ is a real number and } x \neq 0, x \neq -1\}$. Consider the following functions $f_i \colon S \to S$, $i = 1, 2, \ldots, 6$:

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

$$f_4(x) = \frac{1}{1-x}, \quad f_5(x) = 1 - \frac{1}{x}, \quad f_6(x) = \frac{x}{x-1}.$$

Show that $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a group under the operation of composition. Give the multiplication table of G.

13. Consider S_3, the group of symmetries of the equilateral triangle, and the group in Exercise 12. Prove or disprove that these two groups are isomorphic.

14. Show that the mapping in Example 14 is a homomorphism.

15. Let G be the group defined in Example 4. Solve the following equations:

(a) $3 * x = 4$ (b) $y * 5 = -2$

16. Let G be a group with identity e. Show that if $a^2 = e$ for all a in G, then G is Abelian.

17. Consider the square shown in Figure 9.5.

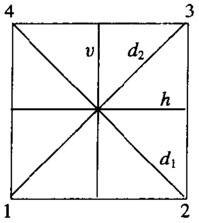


Figure 9.5

The symmetries of the square are as follows:

Rotations f_1, f_2, f_3, and f_4 through 0°, 90°, 180°, and 270°, respectively

f_5 and f_6, reflections about the lines v and h, respectively

f_7 and f_8, reflections about the diagonals d_1 and d_2, respectively

Write the multiplication table of D_4, the group of symmetries of the square.

18. Let G be a group Show by mathematical induction that if $ab = ba$, then $(ab)^n = a^n b^n$ for $n \in Z^+$.

19. Let G be a finite group with identity e, and let a be an arbitrary element of G. Prove that there exists a nonnegative integer n such that $a^n = e$.

20. Let G be the nonzero integers under the operation of multiplication, and let $H = \{3^n \mid n \in Z\}$. Is H a subgroup of G?

21. Let G be the group of integers under the operation of addition, and let $H = \{3k \mid k \in Z\}$. Is H a subgroup of G?

22. Let G be an Abelian group with identity e, and let $H = \{x \mid x^2 = e\}$. Show that H is a subgroup of G.

23. Let G be a group, and let $H = \{x \mid x \in G \text{ and } xy = yx$ for all $y \in G\}$. Prove that H is a subgroup of G.

24. Let G be a group and let $a \in G$. Define $H_a = \{x \mid x \in G$ and $xa = ax\}$. Prove that H_a is a subgroup of G.

25. Let A_n be the set of all even permutations in S_n. Show that A_n is a subgroup of S_n.

26. Let H and K be subgroups of a group G.

(a) Prove that $H \cap K$ is a subgroup of G.

(b) Show that $H \cup K$ need not be a subgroup of G.

27. Find all subgroups of the group given in Exercise 17.

28. Let G be an Abelian group and n a fixed integer. Prove that the function $f: G \to G$ defined by $f(a) = a^n$, for $a \in G$, is a homomorphism.

29. Prove that the function $f(x) = |x|$ is a homomorphism from the group G of nonzero real numbers under multiplication to the group G' of positive real numbers under multiplication.

30. Let G be a group with identity e. Show that the function $f: G \to G$ defined by $f(a) = e$ for all $a \in G$ is a homomorphism.

31. Let G be a group. Show that the function $f: G \to G$ defined by $f(a) = a^2$ is a homomorphism if and only if G is Abelian.

32. Let G be a group. Show that the function $f: G \to G$ defined by $f(a) = a^{-1}$ is an isomorphism if and only if G is Abelian.

33. Let G be a group and let a be a fixed element of G. Show that the function $f_a: G \to G$ defined by $f_a(x) = axa^{-1}$, for $x \in G$, is an isomorphism.

34. Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation of $a^i a^j = a^r$, where $i + j \equiv r \pmod 6$. Prove that G and Z_6 are isomorphic.

9.5 PRODUCTS AND QUOTIENTS OF GROUPS

In this section, we shall obtain new groups from other groups by using the ideas of product and quotient. Since a group has more structure than a semigroup, our results will be deeper than analogous results for semigroups as discussed in Section 9.3.

Theorem 1 If G_1 and G_2 are groups, then $G = G_1 \times G_2$ is a group with binary operation defined by

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2). \qquad \bullet$$

Proof By Theorem 1, Section 9.3, we have that G is a semigroup. The existence of an identity and inverses is easy to verify. ▼

EXAMPLE 1 Let G_1 and G_2 be the group Z_2. For simplicity of notation, we shall write the elements of Z_2 as $\bar{0}$ and $\bar{1}$, respectively, instead of $[0]$ and $[1]$. Then the multiplication table of $G = G_1 \times G_2$ is given in Table 9.10.

Since G is a group of order 4, it must be isomorphic to V or to Z_4 (see Section 9.4), the only groups of order 4. By looking at the multiplication tables, we see that the function $f: V \to Z_2 \times Z_2$ defined by $f(e) = (\bar{0}, \bar{0})$, $f(a) = (\bar{1}, \bar{0})$, $f(b) = (\bar{0}, \bar{1})$, and $f(c) = (\bar{1}, \bar{1})$ is an isomorphism. ■

Table 9.10 Multiplication Table of $Z_2 \times Z_2$

	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{0}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$
$(\bar{1}, \bar{0})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$
$(\bar{0}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{0})$	$(\bar{1}, \bar{0})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{0}, \bar{1})$	$(\bar{1}, \bar{0})$	$(\bar{0}, \bar{0})$

If we repeat Example 1 with Z_2 and Z_3, we find that $Z_2 \times Z_3 \simeq Z_6$. It can be shown, in general, that $Z_m \times Z_n \simeq Z_{mn}$ if and only if $\text{GCD}(m, n) = 1$, that is, if and only if m and n are relatively prime.

Theorem 1 can obviously be extended to show that if $G_1, G_2, \ldots, G_n$ are groups, then $G = G_1 \times G_2 \times \cdots G_n$ is also a group.

EXAMPLE 2

Let $B = \{0, 1\}$ be the group defined in Example 5 of Section 9.4, where $+$ is defined as follows:

$+$	0	1
0	0	1
1	1	0

Then $B^n = B \times B \times \cdots \times B$ (n factors) is a group with operation $\oplus$ defined by

$$(x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

The identity of B^n is $(0, 0, \ldots, 0)$, and every element is its own inverse. This group is essentially the same as the Boolean algebra B_n defined in Section 6.4, but the binary operation is very different from $\wedge$ and $\vee$. ■

A congruence relation on a group is simply a congruence relation on the group when it is viewed as a semigroup. We now discuss quotient structures determined by a congruence relation on a group.

Theorem 2 Let R be a congruence relation on the group $(G, *)$. Then the semigroup $(G/R, \circledast)$ is a group, where the operation $\circledast$ is defined on G/R by

$$[a] \circledast [b] = [a * b] \quad \text{(see Section 9.3).}$$ ●

Proof Since a group is a monoid, we know from Corollary 1 of Section 9.3 that G/R is a monoid. We need to show that each element of G/R has an inverse. Let $[a] \in G/R$. Then $[a^{-1}] \in G/R$, and

$$[a] \circledast [a^{-1}] = [a * a^{-1}] = [e].$$

So $[a]^{-1} = [a^{-1}]$. Hence $(G/R, \circledast)$ is a group. ■

Since the definitions of homomorphism, isomorphism, and congruence for groups involve only the semigroup and monoid structure of groups, the following corollary is an immediate consequence of Theorems 3 and 4 of Section 9.3.

Corollary 1 (a) If R is a congruence relation on a group G, then the function $f_R\colon G \to G/R$, given by $f_R(a) = [a]$, is a group homomorphism.

(b) If $f\colon G \to G'$ is a homomorphism from the group $(G, *)$ onto the group $(G', *')$, and R is the relation defined on G by $a \; R \; b$ if and only if $f(a) = f(b)$, for a and b in G, then

1. R is a congruence relation.
2. The function $\overline{f}\colon G/R \to G'$, given by $\overline{f}([a]) = f(a)$, is an isomorphism from the group $(G/R, \circledast)$ onto the group $(G', *')$. ●

Congruence relations on groups have a very special form, which we will now develop. Let H be a subgroup of a group G, and let $a \in G$. The **left coset** of H in G determined by a is the set $aH = \{ah \mid h \in H\}$. The **right coset** of H in G determined by a is the set $Ha = \{ha \mid h \in H\}$. Finally, we will say that a subgroup H of G is **normal** if $aH = Ha$ for all a in G.

Warning: If $Ha = aH$, it does *not* follow that, for $h \in H$ and $a \in G$, $ha = ah$. It does follows that $ha = ah'$, where h' is some element in H.

If H is a subgroup of G, we shall need in some applications to compute all the left cosets of H in G. First, suppose that $a \in H$. Then $aH \subseteq H$, since H is a subgroup of G; moreover, if $h \in H$, then $h = ah'$, where $h' = a^{-1}h \in H$, so that $H \subseteq aH$. Thus, if $a \in H$, then $aH = H$. This means that, when finding all the cosets of H, we need not compute aH for $a \in H$, since it will always be H.

EXAMPLE 3 Let G be the symmetric group S_3 discussed in Example 6 of Section 9 4. The subset $H = \{f_1, g_2\}$ is a subgroup of G. Compute all the distinct left cosets of H in G.

Solution If $a \in H$, then $aH = H$. Thus

$$f_1H = g_2H = H.$$

Also,

$$\begin{aligned} f_2H &= \{f_2, g_1\} \\ f_3H &= \{f_3, g_3\} \\ g_1H &= \{g_1, f_2\} = f_2H \\ g_3H &= \{g_3, f_3\} = f_3H. \end{aligned}$$

The distinct left cosets of H in G are H, f_2H, and f_3H. ■

EXAMPLE 4 Let G and H be as in Example 3 Then the right coset $Hf_2 = \{f_2, g_3\}$. In Example 3 we saw that $f_2H = \{f_2, g_1\}$. It follows that H is not a normal subgroup of G. ■

EXAMPLE 5 Show that if G is an Abelian group, then every subgroup of G is a normal subgroup.

Solution Let H be a subgroup of G and let $a \in G$ and $h \in H$. Then $ha = ah$, so $Ha = aH$, which implies that H is a normal subgroup of G. ■

Theorem 3 Let R be a congruence relation on a group G, and let $H = [e]$, the equivalence class containing the identity. Then H is a normal subgroup of G and, for each $a \in G$, $[a] = aH = Ha$. ●

Proof Let a and b be any elements in G. Since R is an equivalence relation, $b \in [a]$ if and only if $[b] = [a]$. Also, G/R is a group by Theorem 2. Therefore, $[b] = [a]$ if and only if $[e] = [a]^{-1}[b] = [a^{-1}b]$. Thus $b \in [a]$ if and only if $H = [e] = [a^{-1}b]$. That is, $b \in [a]$ if and only if $a^{-1}b \in H$ or $b \in aH$. This proves that $[a] = aH$ for every $a \in G$. We can show similarly that $b \in [a]$ if and only if $H = [e] = [b][a]^{-1} = [ba^{-1}]$. This is equivalent to the statement $[a] = Ha$. Thus $[a] = aH = Ha$, and H is normal. ▼

Combining Theorem 3 with Corollary 1, we see that in this case the quotient group G/R consists of all the left cosets of $N = [e]$. The operation in G/R is given by

$$(aN)(bN) = [a] \circledast [b] = [ab] = abN$$

and the function $f_R\colon G \to G/R$, defined by $f_R(a) = aN$, is a homomorphism from G onto G/R. For this reason, we will often write G/R as G/N.

We next consider the question of whether every normal subgroup of a group G is the equivalence class of the identity of G for some congruence relation.

Theorem 4 Let N be a normal subgroup of a group G, and let R be the following relation on G:

$$a\ R\ b \quad \text{if and only if} \quad a^{-1}b \in N.$$

Then

(a) R is a congruence relation on G.

(b) N is the equivalence class $[e]$ relative to R, where e is the identity of G.

Proof

(a) Let $a \in G$. Then $a\ R\ a$, since $a^{-1}a = e \in N$, so R is reflexive. Next, suppose that $a\ R\ b$, so that $a^{-1}b \in N$. Then $(a^{-1}b)^{-1} = b^{-1}a \in N$, so $b\ R\ a$. Hence R is symmetric. Finally, suppose that $a\ R\ b$ and $b\ R\ c$. Then $a^{-1}b \in N$ and $b^{-1}c \in N$. Then $(a^{-1}b)(b^{-1}c) = a^{-1}c \in N$, so $a\ R\ c$. Hence R is transitive. Thus R is an equivalence relation on G.

Next we show that R is a congruence relation on G. Suppose that $a\ R\ b$ and $c\ R\ d$. Then $a^{-1}b \in N$ and $c^{-1}d \in N$. Since N is normal, $Nd = dN$; that is, for any $n_1 \in N$, $n_1d = dn_2$ for some $n_2 \in N$. In particular, since $a^{-1}b \in N$, we have $a^{-1}bd = dn_2$ for some $n_2 \in N$. Then $(ac)^{-1}bd = (c^{-1}a^{-1})(bd) = c^{-1}(a^{-1}b)d = (c^{-1}d)n_2 \in N$, so $ac\ R\ bd$. Hence R is a congruence relation on G.

(b) Suppose that $x \in N$. Then $x^{-1}e = x^{-1} \in N$ since N is a subgroup, so $x\ R\ e$ and therefore $x \in [e]$. Thus $N \subseteq [e]$. Conversely, if $x \in [e]$, then $x\ R\ e$, so $x^{-1}e = x^{-1} \in N$. Then $x \in N$ and $[e] \subseteq N$. Hence $N = [e]$. ▼

We see, thanks to Theorems 3 and 4, that if G is any group, then the equivalence classes with respect to a congruence relation on G are always the cosets of some normal subgroup of G. Conversely, the cosets of any normal subgroup of G are just the equivalence classes with respect to some congruence relation on G. We may now, therefore, translate Corollary 1(b) as follows: Let f be a homomorphism from a group $(G, *)$ onto a group $(G', *')$, and let the **kernel** of f, $\ker(f)$, be defined by

$$\ker(f) = \{a \in G \mid f(a) = e'\}.$$

Then

(a) $\ker(f)$ is a normal subgroup of G.

(b) The quotient group $G/\ker(f)$ is isomorphic to G'.

This follows from Corollary 1 and Theorem 3, since if R is the congruence relation on G given by

$$a\ R\ b \quad \text{if and only if} \quad f(a) = f(b),$$

then it is easy to show that $\ker(f) = [e]$.

EXAMPLE 6 Consider the homomorphism f from Z onto Z_n defined by

$$f(m) = [r],$$

where r is the remainder when m is divided by n. (See Example 15 of Section 9.4.) Find $\ker(f)$.

Solution An integer m in Z belongs to $\ker(f)$ if and only if $f(m) = [0]$, that is, if and only if m is a multiple of n. Hence $\ker(f) = nZ$. ■

9.5 Exercises

1. Write the multiplication table for the group $Z_2 \times Z_3$.

2. Prove that if G and G' are Abelian groups, then $G \times G'$ is an Abelian group.

3. Let G_1 and G_2 be groups. Prove that $G_1 \times G_2$ and $G_2 \times G_1$ are isomorphic.

4. Let G_1 and G_2 be groups. Show that the function $f: G_1 \times G_2 \to G_1$ defined by $f(a, b) = a$, for $a \in G_1$ and $b \in G_2$, is a homomorphism.

5. Determine the operational table of the quotient group $Z/3Z$, where Z has operation $+$.

6. Let Z be the group of integers under the operation of addition. Prove that the function $f: Z \times Z \to Z$ defined by $f(a, b) = a + b$ is a homomorphism.

7. Let $G = Z_4$. Determine all the left cosets of $H = \{[0]\}$ in G.

8. Let $G = Z_4$. Determine all the left cosets of $H = \{[0], [2]\}$ in G.

9. Let $G = Z_4$. Determine all the left cosets of $H = \{[0], [1], [2], [3]\}$ in G.

10. Let $G = S_3$. Determine all the left cosets of $H = \{f_1, g_1\}$ in G.

11. Let $G = S_3$ Determine all the left cosets of $H = \{f_1, g_3\}$ in G.

12. Let $G = S_3$. Determine all the left cosets of $H = \{f_1, f_2, f_3\}$ in G.

13. Let $G = S_3$. Determine all the left cosets of $H = \{f_1\}$ in G.

14. Let $G = S_3$. Determine all the left cosets of $H = \{f_1, f_2, f_3, g_1, g_2, g_3\}$ in G.

15. Let $G = Z_8$ Determine all the left cosets of $H = \{[0], [4]\}$ in G.

16. Let $G = Z_8$ Determine all the left cosets of $H = \{[0], [2], [4], [6]\}$ in G

17. Let Z be the group of integers under the operation of addition, and let $G = Z \times Z$. Consider the subgroup $H = \{(x, y) \mid x = y\}$ of G. Describe the left cosets of H in G.

18. Let N be a subgroup of a group G, and let $a \in G$. Define
$$a^{-1}Na = \{a^{-1}na \mid n \in N\}.$$
Prove that N is a normal subgroup of G if and only if $a^{-1}Na = N$ for all $a \in G$.

19. Let N be a subgroup of group G. Prove that N is a normal subgroup of G if and only if $a^{-1}Na \subseteq N$ for all $a \in G$.

20. Find all the normal subgroups of S_3.

21. Find all the normal subgroups of D_4. (See Exercise 17 of Section 9.4.)

22. Let G be a group, and let $H = \{x \mid x \in G$ and $xa = ax$ for all $a \in G\}$. Show that H is a normal subgroup of G.

23. Let H be a subgroup of a group G. Prove that every left coset aH of H has the same number of elements as H by showing that the function $f_a \colon H \to aH$ defined by $f_a(h) = ah$, for $h \in H$, is one to one and onto.

24. Let H and K be normal subgroups of G. Show that $H \cap K$ is a normal subgroup of G.

25. Let G be a group and H a subgroup of G. Let S be the set of all left cosets of H in G, and let T be the set of all right cosets of H in G. Prove that the function $f \colon S \to T$ defined by $f(aH) = Ha^{-1}$ is one to one and onto.

26. Let G_1 and G_2 be groups. Let $f \colon G_1 \times G_2 \to G_2$ be the homomorphism from $G_1 \times G_2$ onto G_2 given by $f((g_1, g_2)) = g_2$. Compute $\ker(f)$.

27. Let f be a homomorphism from a group G_1 onto a group G_2, and suppose that G_2 is Abelian. Show that $\ker(f)$ contains all elements of G_1 of the form $aba^{-1}b^{-1}$, where a and b are arbitrary in G_1.

28. Let G be an Abelian group and N a subgroup of G. Prove that G/N is an Abelian group.

29. Let H be a subgroup of the finite group G and suppose that there are only two left cosets of H in G. Prove that H is a normal subgroup of G.

30. Let H and N be subgroups of the group G. Prove that if N is a normal subgroup of G, then $H \cap N$ is a normal subgroup of H.

31. Let $f \colon G \to G'$ be a group homomorphism. Prove that f is one to one if and only if $\ker(f) = \{e\}$.

TIPS FOR PROOFS

The proofs in this chapter are mostly simple direct proofs, in part because we have introduced several new mathematical structures (semigroup, monoids, groups, Abelian groups). With a new structure we first explore the simple consequences of the definitions; for example, Theorem 1, Section 9.2. However, proofs of uniqueness are frequently indirect as in Theorems 1 and 4 in Section 9.4.

The idea of a substructure appears several times in this chapter. In general, to prove that a subset forms a substructure of a mathematical structure, we show that the subset together with the operation(s) satisfy the definition of this type of structure. But any global property such as associativity is inherited by the subset so we need only check closure properties and properties involving special elements. Thus, to show that a subset is a subgroup, we check closure for the multiplication, that the identity belongs to the subset, and that the inverse of each element in the subset belongs to the subset.

Isomorphism is a powerful tool for proving statements, since, roughly speaking, establishing an isomorphism between two structures allows us to transfer knowledge about one structure to the other. This can be seen in Theorem 4, Section 9.2.

KEY IDEAS FOR REVIEW

- Binary operation on A: everywhere defined function $f \colon A \times A \to A$
- Commutative binary operation: $a * b = b * a$
- Associative binary operation: $a * (b * c) = (a * b) * c$
- Semigroup: nonempty set S together with an associative binary operation $*$ defined on S
- Monoid: semigroup that has an identity
- Subsemigroup $(T, *)$ of semigroup $(S, *)$: T is a nonempty subset of S and $a * b \in T$ whenever a and b are in T.
- Submonoid $(T, *)$ of monoid $(S, *)$: T is a nonempty subset of S, $e \in T$, and $a * b \in T$ whenever a and b are in T.

- Isomorphism: see page 327
- Homomorphism: see page 329
- Theorem. Let $(S, *)$ and $(T, *')$ be monoids with identities e and e', respectively, and suppose that $f: S \to T$ is an isomorphism. Then $f(e) = e'$.
- Theorem: If $(S, *)$ and $(T, *')$ are semigroups, then $(S \times T, *'')$ is a semigroup, where $*''$ is defined by

$$(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2).$$

- Congruence relation R on semigroup $(S, *)$: equivalence relation R such that $a\ R\ a'$ and $b\ R\ b'$ imply that $(a * b)\ R\ (a' * b')$
- Theorem: Let R be a congruence relation on the semigroup $(S, *)$. Define the operation $\circledast$ in S/R as follows:

$$[a] \circledast [b] = [a * b].$$

  Then $(S/R, \circledast)$ is a semigroup.
- Quotient semigroup or factor semigroup S/R: see page 333
- Z_n: see page 334
- Theorem (fundamental homomorphism theorem): Let $f: S \to T$ be a homomorphism of the semigroup $(S, *)$ onto the semigroup $(T, *')$. Let R be the relation on S defined by $a\ R\ b$ if and only if $f(a) = f(b)$, for a and b in S. Then
  (a) R is a congruence relation.
  (b) T is isomorphic to S/R.
- Group $(G, *)$: monoid with identity e such that for every $a \in G$ there exists $a' \in G$ with the property that $a * a' = a' * a = e$.
- Theorem: Let G be a group, and let a, b, and c be elements of G. Then
  (a) $ab = ac$ implies that $b = c$ (left cancellation property).
  (b) $ba = ca$ implies that $b = c$ (right cancellation property).
- Theorem: Let G be a group, and let a and b be elements of G. Then
  (a) $(a^{-1})^{-1} = a$.
  (b) $(ab)^{-1} = b^{-1}a^{-1}$.
- Order of a group G: $|G|$, the number of elements in G
- S_n: the symmetric group on n letters
- Subgroup: see page 344
- Theorem: Let R be a congruence relation on the group $(G, *)$. Then the semigroup $(G/R, \circledast)$ is a group, where the operation $\circledast$ is defined in G/R by

$$[a] \circledast [b] = [a * b].$$

- Left coset aH of H in G determined by a: $\{ah \mid h \in H\}$
- Normal subgroup: subgroup H such that $aH = Ha$ for all a in G
- Theorem: Let R be a congruence relation on a group G, and let $H = [e]$, the equivalence class containing the identity. Then H is a normal subgroup of G and, for each $a \in G$, $[a] = aH = Ha$.
- Theorem: Let N be a normal subgroup of a group G, and let R be the following relation on G:

$$a\ R\ b \quad \text{if and only if} \quad a^{-1}b \in N.$$

  Then
  (a) R is a congruence relation on G.
  (b) N is the equivalence class $[e]$ relative to R, where e is the identity of G.

CODING EXERCISES

For each of the following, write the requested program or subroutine in pseudocode (as described in Appendix A) or in a programming language that you know. Test your code either with a paper-and-pencil trace or with a computer run

Let Z_n be as defined in Section 9.3.

1. Write a function SUM that takes two elements of Z_n, $[x]$ and $[y]$ and returns their sum $[x] \oplus [y]$. The user should be able to input a choice for n.
2. Let $H = \{[0], [2]\}$. Write a subroutine that computes the left cosets of H in Z_6.
3. Let $H = \{[0], [2], [4], [6]\}$. Write a subroutine that computes the right cosets of H in Z_8.
4. Write a program that given a finite operation table will determine if the operation satisfies the associative property.
5. Write a program that given a finite group G and a subgroup H determines if H is a normal subgroup of G.