Chapter 2

Introduction to Groups

There are four major sources from which group theory evolved, namely, classical algebra, number theory, geometry, and analysis. Classical algebra originated in 1770 with J.L. Lagrange's work on polynomial equations. His work appeared in a memoir entitled, "Réflexions sur la résolution algébrique des équations." C.F. Gauss is considered the originator of number theory with his work, "*Disquistiones Arithmeticae*," which was published in 1801. F. Klein's lecture in 1872, "A Comparative Review of Recent Researches in Geometry," dealt with the classification of geometry as the study of invariants under groups of transformations. The impact of his lecture was so strong as to allow Klein to be considered as the originator of this source of group theory. The originators of the analysis source are S. Lie (1874) and H. Poincaré and F. Klein (1876).

2.1 Elementary Properties of Groups

In this chapter, and in fact in the remainder of the text, we will be concerned with mathematical systems. These systems are composed of a nonempty set together with binary operations defined on this set so that certain properties hold. From these properties, results concerning these systems are derived. This axiomatic approach to abstract algebra unifies diverse examples and also strips away nonessential ideas.

Although noted for his geometry, Euclid inspired the use of the axiomatic method, which has proved so indispensable in mathematics. His axiomatic approach also affected philosophy, where in the 17th century Baruch Spinoza laid down (in The *Ethics*) an axiomatic system from which he was able to prove the existence of God. His proof, of course, depended on his axioms. His proof lost its conviction with the emergence of noneuclidean geometries whose axioms were as logical and practical as Euclid's.

We will be primarily concerned with mathematical systems called groups in this chapter. The theory of groups is one of the oldest branches of abstract

algebra. The first effective use of groups was in the early nineteenth centu by A. Cauchy and E. Galois. They used groups to describe the effect of perm tations of roots of a polynomial equation. Their use of groups was not bas on an axiomatic approach. In 1854, A. Cayley gave the first postulates for group. However, his definition was lost sight of. Kronecker again set down t axioms for an Abelian group in 1870. H. Weber gave the definition for fini groups (in 1882) and the definition for infinite groups in 1883.

As previously mentioned, the notion of a group arose from the study one-one functions on the set of roots of a polynomial equation. We have see that the set S of all one-one functions from a set X onto itself satisfies th following properties:

(i) Composition of functions, $\circ$, is a binary operation on S.

(ii) For all $f, g, h \in S$, $f \circ (g \circ h) = (f \circ g) \circ h$.

(iii) There exists $i \in S$ such that $f \circ i = f = i \circ f$ for all $f \in S$.

(iv) For all $f \in S$ there exists an element $f^{-1} \in S$ such that $f \circ f^{-1} = i =$ $f^{-1} \circ f$.

These properties lead us to the definition of an abstract group.

Definition 2.1.1 *A* ***group*** *is an ordered pair $(G, *)$, where G is a nonemp set and $*$ is a binary operation on G such that the following properties hold:*

(G1) For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$ ***(associative law).***

(G2) There exists $e \in G$ such that for all $a \in G$, $a*e = a = e*a$ ***(existenc of an identity).***

(G3) For all $a \in G$, there exists $b \in G$ such that $a*b = e = b*a$ ***(existenc of an inverse).***

Thus, a group is a mathematical system $(G, *)$ satisfying axioms G1 to G3

In what follows, we will see several examples of groups. However, let us first observe the following important properties of groups.

Theorem 2.1.2 *Let $(G, *)$ be a group.*

(i) There exists a unique element $e \in G$ such that $e * a = a = a * e$ for al $a \in G$.

(ii) For all $a \in G$, there exists a unique $b \in G$ such that $a * b = e = b * a$.

Proof. (i) By G2, there exists $e \in G$ such that $e * a = a = a * e$ for al $a \in G$. Since $(G, *)$ is a mathematical system, e is unique by Theorem 1.6.1

(ii) Let $a \in G$. By G3, there exists $b \in G$ such that $a*b = e = b*a$. Suppos

there exists $c \in G$ such that $a * c = e = c * a$. We show that $b = c$. Now

$$\begin{aligned} b &= b * e \\ &= b * (a * c) && \text{(substituting } e = a * c) \\ &= (b * a) * c && \text{(using the associativity of } *) \\ &= e * c && \text{(since } b * a = e) \\ &= c. \end{aligned}$$

Thus, b is unique. ■

The unique element $e \in G$ that satisfies G2 is called the **identity** element of the group $(G, *)$. Let $a \in G$. Then the unique element $b \in G$ that satisfies G3 is called the **inverse** of a and is denoted by a^{-1}.

If a group $(G, *)$ has the property that $a * b = b * a$ for all $a, b \in G$, then $(G, *)$ is called a **commutative** or **Abelian** group. A group $(G, *)$ is called **noncommutative** if it is not commutative.

Example 2.1.3 *Consider* $\mathbf{Z}$, *the set of integers, together with the binary operation* $+$, *where* $+$ *is the usual addition. We know that* $+$ *is associative. Now* $0 \in \mathbf{Z}$ *and for all* $a \in \mathbf{Z}$, $a + 0 = a = 0 + a$ *and so* 0 *is the identity. Also, for all* $a \in \mathbf{Z}$, $-a \in \mathbf{Z}$ *and* $a + (-a) = 0 = (-a) + a$. *That is,* $-a$ *is the inverse of* a. *Hence, it now follows that* $(\mathbf{Z}, +)$ *is a group. Since* $a + b = b + a$ *for all* $a, b \in \mathbf{Z}$, $+$ *is commutative. Thus,* $(\mathbf{Z}, +)$ *is a commutative group.*

Similarly, we can show that $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$, $(\mathbf{C}, +)$, $(\mathbf{Q}\backslash\{0\}, \cdot)$, $(\mathbf{R}\backslash\{0\}, \cdot)$, $(\mathbf{C}\backslash\{0\}, \cdot)$ *are all examples of commutative groups, where* $+$ *is the usual addition and* $\cdot$ *is the usual multiplication. Note that for each of the groups* $(\mathbf{Q}\backslash\{0\}, \cdot)$, $(\mathbf{R}\backslash\{0\}, \cdot)$, $(\mathbf{C}\backslash\{0\}, \cdot)$ *the identity element is* 1.

Example 2.1.4 *Let* a *be any fixed integer. Let* $G = \{na \mid n \in \mathbf{Z}\}$. *Then* $(G, +)$ *is a commutative group, where* $+$ *is the usual addition of integers. Note that* $0 = 0 \cdot a$ *and* $-(na) = (-n)a$ *are members of* G.

Gauss's work yielded many new directions of research in Abelian groups. The next two examples are due to Gauss.

Example 2.1.5 *Consider* $\mathbf{Z}_n$ (*Examples* 1.3.11 *and* 1.3.17). *Define* $+_n$ *on* $\mathbf{Z}_n$ *by*

$$[a] +_n [b] = [a + b]$$

for all $[a], [b] \in \mathbf{Z}_n$. *We show that* $(\mathbf{Z}_n, +_n)$ *is a commutative group.*

We first prove that $+_n$ *is a binary operation. Let* $[a], [b], [c], [d] \in \mathbf{Z}_n$. *Suppose* $[a] = [c]$ *and* $[b] = [d]$. *Then* $n|(a-c)$ *and* $n|(b-d)$, *i.e., there exist integers* s *and* t *such that* $ns = a - c$ *and* $nt = b - d$. *Hence,* $n(s+t) = ((a+b) - (c+d))$ *and so* $n|((a + b) - (c + d))$. *This implies that* $a + b \equiv_n c + d$. *Therefore,*

$[a+b] = [c+d]$. *As a result* $+_n$ *is well defined and so* $+_n$ *is a binary operation. For all* $[a], [b], [c] \in \mathbf{Z}_n$, $([a] +_n [b]) +_n [c] = [a+b] +_n [c] = [(a+b)+c] = [a+(b+c)] = [a] +_n [b+c] = [a] +_n ([b] +_n [c])$. *Hence,* $+_n$ *is associative. Now* $[0] \in \mathbf{Z}_n$ *and for all* $[a] \in \mathbf{Z}_n$,

$$[a] +_n [0] = [a+0] = [a] = [0+a] = [0] +_n [a].$$

This shows that $[0]$ *is the identity element. Also, for all* $[a] \in \mathbf{Z}_n$, $[-a] \in \mathbf{Z}_n$ *and*

$$[a] +_n [-a] = [a-a] = [0] = [-a+a] = [-a] +_n [a].$$

Thus, $[-a]$ *is the inverse of* $[a]$. *Finally, for all* $[a], [b] \in \mathbf{Z}_n$

$$[a] +_n [b] = [a+b] = [b+a] = [b] +_n [a]$$

and so $+_n$ *is commutative. Hence,* $(\mathbf{Z}_n, +_n)$ *is a commutative group.*

Example 2.1.6 *Consider* $\mathbf{Z}_n$ *(Examples* 1.3.11 *and* 1.3.17*). Define* $\cdot_n$ *on* $\mathbf{Z}_n$ *by*

$$[a] \cdot_n [b] = [ab]$$

for all $[a], [b] \in \mathbf{Z}_n$. *With the help of a little calculation as in Example* 2.1.5, *we can show that* $\cdot_n$ *is a binary operation on* $\mathbf{Z}_n$ *and* $\cdot_n$ *is associative. Now* $[1] \in \mathbf{Z}_n$ *and for all* $[a] \in \mathbf{Z}_n$,

$$[a] \cdot_n [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \cdot_n [a].$$

This implies that $[1]$ *is the identity element. We now show that if* $[a] \in \mathbf{Z}_n$ *and* $[a] \neq [0]$, *then* $[a]$ *has an inverse if and only if* $\gcd(a, n) = 1$.

Let $[a] \in \mathbf{Z}_n$ *and* $[a] \neq [0]$. *Suppose* $\gcd(a, n) = 1$. *Then there exist* $b, r \in \mathbf{Z}$ *such that* $ab + nr = 1$ *by Theorem* 1.2.11, *i.e.,* $ab - 1 = -nr$. *This implies that* $[ab] = [1]$ *or* $[a] \cdot_n [b] = [1]$. *Since* $ab = ba$, *we also have* $[b] \cdot_n [a] = [ba] = [ab] = [1]$. *Thus, there exists* $[b] \in \mathbf{Z}_n$ *such that* $[a][b] = [1] = [b][a]$ *and so* $[a]$ *has an inverse. Conversely, suppose* $[a] \in \mathbf{Z}_n$, $[a] \neq [0]$ *and* $[a]$ *has an inverse. Then there exists* $[b] \in \mathbf{Z}_n$ *such that* $[a][b] = [1]$. *This implies that* $n|(ab-1)$ *(by Exercise* 11, *page* 30*) and so* $ab - 1 = nr$ *for some* $r \in \mathbf{Z}$. *Thus,* $ab - nr = 1$ *and hence by Theorem* 1.2.11, $\gcd(a, n) = 1$. *This proves our claim.*

Thus, we see that in general, not every element of $\mathbf{Z}_n \backslash \{[0]\}$ *has an inverse. For example if* $n = 6$, *then the only elements of* $\mathbf{Z}_6$ *that have inverses are* $[1]$, $[3]$ *and* $[5]$. *Hence, in general* $(\mathbf{Z}_n \backslash \{[0]\}, \cdot_n)$ *is not a group.*

Let U_n *be the set of all elements of* $\mathbf{Z}_n \backslash \{[0]\}$ *that have an inverse in* $(\mathbf{Z}_n \backslash \{[0]\}, \cdot_n)$, *i.e.,*

$$U_n = \{[a] \in \mathbf{Z}_n \backslash \{[0]\} \mid \gcd(a, n) = 1\}.$$

We ask the reader to verify in Exercise 10 *(page* 78*) that* $(U_n, \cdot_n)$ *is a group.*

Note that for $n = 8$, $U_8 = \{[1], [3], [5], [7]\}$ *and for* $n = 7$,

$$U_7 = \{[1], [2], [3], [4], [5], [6]\} = \mathbf{Z}_7 \backslash \{[0]\}.$$

Example 2.1.7 *Let*

$$\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}.$$

Then $(\mathbf{Q}[\sqrt{2}], +)$ *and* $(\mathbf{Q}[\sqrt{2}]\backslash\{0\}, \cdot)$ *are commutative groups, where* $+$ *is the usual addition and* $\cdot$ *is the usual multiplication. The identity of* $(\mathbf{Q}[\sqrt{2}], +)$ *is* $0 + 0\sqrt{2}$ *and the inverse of* $a + b\sqrt{2}$ *is* $-a + (-b)\sqrt{2}$. *The identity of* $(\mathbf{Q}[\sqrt{2}]\backslash\{0\}, \cdot)$ *is* $1 = 1 + 0\sqrt{2}$ *and the inverse of* $a + b\sqrt{2} \neq 0$ *is* $\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$.

Example 2.1.8 *Let* $\mathcal{P}(X)$ *be the power set of a set* X. *Consider the operation* Δ *(symmetric difference, Exercise 6, page 6) on* $\mathcal{P}(X)$. *Then for all* A, $B \in \mathcal{P}(X)$,

$$A\Delta B = (A\backslash B) \cup (B\backslash A).$$

$(\mathcal{P}(X), \Delta)$ *is a commutative group. The empty set* ϕ *is the identity of* $(\mathcal{P}(X), \Delta)$ *and every element of* $\mathcal{P}(X)$ *is its own inverse. We warn the reader that verification of the associative law is tedious.*

Example 2.1.9 *Let* X *be a set and* S_X *the set of all one-one functions of* X *onto* X. *Since* i_X, *the identity function on* X, *is one-one and onto* X, $i_X \in S_X$. *Thus,* $S_X \neq \phi$. *Let* $f, g \in S_X$. *Then* $f \circ g$ *is a one-one function of* X *onto* X *by Theorem* 1.5.11. *Hence,* $f \circ g \in S_X$. *By Theorem* 1.5.13, $\circ$ *is associative. Also, for all* $f \in S_X$, $f^{-1} \in S_X$ *and* $f \circ f^{-1} = i_X = f^{-1} \circ f$. *Consequently,* $(S_X, \circ)$ *is a group. However,* $(S_X, \circ)$ *is not necessarily commutative. For example, let* $X = \{a, b, c\}$. *Let* $f, g \in S_X$ *be defined by* $f(a) = b$, $f(b) = a$, $f(c) = c$, $g(a) = b$, $g(b) = c$, $g(c) = a$. *Then* $(f \circ g)(b) = f(g(b)) = f(c) = c$ *and* $(g \circ f)(b) = g(f(b)) = g(a) = b$. *Hence,* $f \circ g \neq g \circ f$. *Thus,* $(S_X, \circ)$ *is not commutative.*

Example 2.1.10 *Let* $GL(2, \mathbf{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbf{R},\ ad - bc \neq 0 \right\}$. *Define a binary operation* $*$ *on* $GL(2, \mathbf{R})$ *by*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} u & v \\ w & s \end{bmatrix} = \begin{bmatrix} au + bw & av + bs \\ cu + dw & cv + ds \end{bmatrix}$$

for all $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} u & v \\ w & s \end{bmatrix} \in GL(2, \mathbf{R})$. *This binary operation is the usual matrix multiplication. Since matrix multiplication is associative, we have* $*$ *is associative. The element* $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in GL(2, \mathbf{R})$ *and is the identity element of*

$GL(2,\mathbf{R})$. *Let* $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbf{R})$. *Then* $ad - bc \neq 0$. *Consider the mat* $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$. *Since*

$$\frac{d}{ad-bc} \cdot \frac{a}{ad-bc} - \frac{-b}{ad-bc} \cdot \frac{-c}{ad-bc} = \frac{1}{ad-bc} \neq 0,$$

we have

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} \in GL(2,\mathbf{R}).$$

Now

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} * \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} * \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$ *is the inverse of* $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. *Hence,* $(GL(2,\mathbf{R}),*)$ *is group. Now*

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in GL(2,\mathbf{R})$$

and

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Hence, $(GL(2,\mathbf{R}),*)$ *is a noncommutative group.*

The group in Example 2.1.10 is known as the **general linear group degree 2**.

We now prove some elementary properties of a group in the following th orem.

Theorem 2.1.11 *Let* $(G,*)$ *be a group.*

(i) $(a^{-1})^{-1} = a$ *for all* $a \in G$.

(ii) $(a*b)^{-1} = b^{-1} * a^{-1}$ *for all* $a, b \in G$.

(iii) ***(Cancellation Law)*** *For all* $a, b, c \in G$, *if either* $a*c = b*c$ $c*a = c*b$, *then* $a = b$.

(iv) For all $a, b \in G$, *the equations* $a*x = b$ *and* $y*a = b$ *have uniq solutions in* G *for* x *and* y.

Proof. (i) Let $a \in G$. Then $a^{-1} * a = e = a * a^{-1}$ and so a is an inverse of a^{-1}. Since the inverse of an element is unique in a group (Theorem 2.1.2) and since $(a^{-1})^{-1}$ denotes the inverse of a^{-1}, it follows that $a = (a^{-1})^{-1}$.

(ii) Let $a, b \in G$. Then

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

Similarly, $(b^{-1} * a^{-1}) * (a * b) = e$. Hence, $b^{-1} * a^{-1}$ is an inverse of $a * b$. Since the inverse of an element is unique in a group and since $(a * b)^{-1}$ denotes the inverse of $a * b$, it follows that $(a * b)^{-1} = b^{-1} * a^{-1}$.

(iii) Let $a, b, c \in G$. Suppose $a * c = b * c$. Now $(a * c) * c^{-1} = (b * c) * c^{-1}$ implies that $a * (c * c^{-1}) = b * (c * c^{-1})$. Hence, $a * e = b * e$ or $a = b$. Similarly, if $c * a = c * b$, then $a = b$.

(iv) Let $a, b \in G$. First we consider the equation $a * x = b$. Now $a^{-1} * b \in G$. Substituting $a^{-1} * b$ for x in the equation $a * x = b$, we obtain

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

Thus, $a^{-1} * b$ is a solution of the equation $a * x = b$. We now establish the uniqueness of the solution. Suppose c is any solution of $a * x = b$. Then $a * c = b$. Hence,

$$\begin{aligned}c &= e * c \\ &= (a^{-1} * a) * c && \text{(since } a^{-1} * a = e\text{)} \\ &= a^{-1} * (a * c) && \text{(since } * \text{ is associative)} \\ &= a^{-1} * b && \text{(since } a * c = b\text{).}\end{aligned}$$

This yields the uniqueness of the solution. Similar arguments hold for the equation $y * a = b$. ■

Corollary 2.1.12 *Let $(G, *)$ be a group and $a \in G$. If $a * a = a$, then $a = e$.* ■

Proof. Since $a = a * a$, we have $a * a = a * e$. By the cancellation law, $a = e$.

Corollary 2.1.13 *In a multiplication table for a group $(G, *)$, each element appears exactly once in each row and exactly once in each column.*

Proof. Let $b \in G$ be such that b occurs twice in the row marked by $a \in G$. Then there exists $u, v \in G$ with $u \neq v$ such that $a * u = b$ and $a * v = b$. Thus, the equation $a * x = b$ has two distinct solutions, u and v. This is a contradiction to Theorem 2.1.11(iv) since the equation $a * x = b$ has a unique solution for x. A similar argument for columns can be used. ■

Let $(G, *)$ be a group and $a, b, c \in G$. Then by the associative law, $a*(b*c) = (a*b)*c$. Hence, we can define $a*b*c = a*(b*c) = (a*b)*c$. Let $a, b, c, d \in G$. Then $(a * b * c) * d = (a * (b * c)) * d = a * ((b * c) * d)) = a * (b * (c * d)) = (a * b) * (c * d) = ((a * b) * c) * d$. Thus, there is more than one way of inserting parentheses in the expression $a * b * c * d$ to produce a "meaningful product" of a, b, c, d (in this order). We now extend this notion to any finite number of elements.

Definition 2.1.14 *Let $(G, *)$ be a group and $a_1, a_2, \ldots, a_n \in G$ be n elements of G (not necessarily distinct). The* ***meaningful product*** *of $a_1, a_2, \ldots, a_n$ (in this order) is defined as follows: If $n = 1$, then the meaningful product is a_1. If $n > 1$, then the meaningful product of $a_1, a_2, \ldots, a_n$ is any product of the form*

$$(a_1 * \cdots * a_m) * (a_{m+1} * \cdots * a_n),$$

where $1 \leq m < n$ and $(a_1 * \cdots * a_m)$ and $(a_{m+1} * \cdots * a_n)$ are meaningful products of m and $n - m$ elements, respectively.

Definition 2.1.15 *Let $(G, *)$ be a group and $a_1, a_2, \ldots, a_n \in G$, $n \geq 1$. The* ***standard product*** *of $a_1, a_2, \ldots, a_n$ denoted by $a_1 * a_2 * \cdots * a_n$ is defined recursively as*

$$\begin{aligned} a_1 &= a_1 \\ a_1 * a_2 * \cdots * a_n &= (a_1 * a_2 * \cdots * a_{n-1}) * a_n \text{ if } n > 1. \end{aligned}$$

In the next theorem, we establish the equality between any meaningful product and standard product.

Theorem 2.1.16 *Let $(G, *)$ be a group and $a_1, a_2, \ldots, a_n \in G$, $n \geq 1$. Then all possible meaningful products of $a_1, a_2, \ldots, a_n$ (in this order) are equal to the standard product of $a_1, a_2, \ldots, a_n$ (in this order).*

Proof. We prove the result by induction. If $n = 1$, then a_1 is the only meaningful product of a_1, which is equal to the standard product a_1 of a_1. Thus, the result is true if $n = 1$. Suppose that the theorem is true for all integers m such that $1 \leq m < n$. Let $a_1, a_2, \ldots, a_n \in G$. Let $(a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_n)$ be a meaningful product of $a_1, a_2, \ldots, a_n$ (in this order). Now $t < n$ and $n - t < n$. If $t = n - 1$, then $(a_1 * a_2 * \cdots * a_t) * a_{t+1} = a_1 * a_2 * \cdots * a_t * a_{t+1}$. Suppose $t < n - 1$.

Then $(a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_n) = (a_1 * \cdots * a_t) * ((a_{t+1} * \cdots * a_{n-1}) * a_n) = ((a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_{n-1})) * a_n = (a_1 * a_2 * \cdots * a_{n-1}) * a_n = a_1 * \cdots * a_n$ since by the induction hypothesis $(a_1 * \cdots * a_t) * (a_{t+1} * \cdots * a_{n-1}) = a_1 * a_2 * \cdots * a_{n-1}$. Hence, the result is true for n. The result now follows by induction. ■

We have seen several examples of groups. In order to show that a given set with a given binary operation is a group, we need to verify G1 to G3 of Definition 2.1.1. However, it would be helpful if we had some criteria that could be used to show whether a given set with a binary operation is a group or not instead of verifying all the properties G1–G3 explicitly. Partly for this reason we define what a semigroup is. Following the examples, we develop some results that can be used to test whether a given set with a binary operation is a group or not.

Definition 2.1.17 *A* ***semigroup*** *is an ordered pair $(S, *)$, where S is a nonempty set and $*$ is an associative binary operation on S.*

Thus, a semigroup is a mathematical system with one binary operation such that the binary operation is associative. We note that every group $(G, *)$ is a semigroup.

A semigroup $(S, *)$ is **commutative** if $*$ is commutative, i.e., $a * b = b * a$ for all $a, b \in S$. A semigroup $(S, *)$ which is not commutative is called **noncommutative.**

Let $(S, *)$ be a semigroup. We say that $(S, *)$ is with identity if the mathematical system $(S, *)$ has an identity. An element $a \in S$ is called **idempotent** if $a * a = a$.

Example 2.1.18 *Consider* $\mathbf{N}$*, the set of positive integers. We know that addition of positive integers is again a positive integer. Thus, $+$ is a binary operation on* $\mathbf{N}$*. We also know that $+$ is associative and commutative. Thus, $(\mathbf{N}, +)$ is a commutative semigroup.*

Example 2.1.19 *Let X be a nonempty set and S the set of all functions $f : X \to X$. If $\circ$ denotes the composition of functions, then $(S, \circ)$ is a semigroup with identity. The associativity of $\circ$ follows from Theorem* 1.5.13*. When X has two or more elements, the semigroup $(S, \circ)$ is noncommutative. For example, let $X = \{a, b\}$. Let $g, h \in S$ be defined by $g(a) = b$, $g(b) = b$, $h(a) = b$, $h(b) = a$. Then $(g \circ h)(a) = b \neq a = (h \circ g)(a)$. Therefore, $g \circ h \neq h \circ g$. Let $f \in S$ be defined by $f(a) = a$ and $f(b) = a$. Now $(f \circ g)(x) = f(g(x)) = a = f(h(x)) = (f \circ h)(x)$ for all $x \in G$. Hence, $f \circ g = f \circ h$. But $g \neq h$. This shows that the cancellation laws do not hold in S. Thus, $(S, \circ)$ is not a group.*

Example 2.1.20 *Let X be a set with two or more elements and S' the set of functions $f : X \to X$ which are not one-one. Then $(S', \circ)$ is a noncommutative semigroup without identity.*

Example 2.1.21 *Let X be a set and $\mathcal{P}(X)$ the power set of X. Then $(\mathcal{P}(X), \cup)$ and $(\mathcal{P}(X), \cap)$ are commutative semigroups with identity. The identity of $(\mathcal{P}(X), \cup)$ is ϕ and the identity of $(\mathcal{P}(X), \cap)$ is X.*

The following three theorems give necessary and sufficient conditions for a semigroup to be a group.

Theorem 2.1.22 *A semigroup $(S, *)$ is a group if and only if*
(i) there exists $e \in S$ such that $e * a = a$ for all $a \in S$ and
(ii) for all $a \in S$ there exists $b \in S$ such that $b * a = e$.

Proof. Suppose $(S, *)$ is a semigroup that satisfies (i) and (ii). Let a be an element of S. Then there exists $b \in S$ such that $b * a = e$ by (ii). For $b \in S$ there exists $c \in S$ such that $c * b = e$ by (ii). Now

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

and

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

Hence, $a * b = e = b * a$. Also,

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

Thus, $a * e = a = e * a$. This shows that e is the identity element of S. Now since $a * b = e = b * a$, we have $b = a^{-1}$. Therefore, $(S, *)$ is a group. The converse follows from the definition of a group. ■

Theorem 2.1.23 *A semigroup $(S, *)$ is a group if and only if for all $a, b \in S$ the equations $a * x = b$ and $y * a = b$ have solutions in S for x and y.*

Proof. Suppose the given equations have solutions in S. Let $a \in S$. Consider the equation $y * a = a$. By our assumption, $y * a = a$ has a solution $u \in S$, say. Then $u * a = a$. Let b be any element of S. Consider the equation $a * x = b$. Again by our assumption, $a * x = b$ has a solution in S. Let $c \in S$ be a solution of $a * x = b$. Then $a * c = b$. Now

$$\begin{aligned} u * b &= u * (a * c) && \text{(since } b = a * c\text{)} \\ &= (u * a) * c && \text{(since } * \text{ is asociative)} \\ &= a * c && \text{(since } u * a = a\text{)} \\ &= b. \end{aligned}$$

Since b was an arbitrary element of S, we find that $u * b = b$ for all $b \in S$. Thus, $(S, *)$ satisfies (i) of Theorem 2.1.22. Consider the equation $y * a = u$. Let $d \in S$ be a solution of $y * a = u$. Then $d * a = u$. This shows that $(S, *)$ satisfies (ii) of Theorem 2.1.22. Hence, $(S, *)$ is a group by Theorem 2.1.22.

The converse follows by Theorem 2.1.11(iv). ■

Theorem 2.1.24 *A finite semigroup $(S, *)$ is a group if and only if $(S, *)$ satisfies the cancellation laws (i.e., $a * c = b * c$ implies $a = b$ and $c * a = c * b$ implies $a = b$ for all $a, b, c \in S$).*

Proof. Let $(S, *)$ be a finite semigroup satisfying the cancellation laws. Let $a, b \in S$. Consider the equation $a * x = b$. We show that this equation has a solution in S. Let us write $S = \{a_1, a_2, \ldots, a_n\}$, where the a_i's are all distinct elements of S. Since S is a semigroup, $a * a_i \in S$ for all $i = 1, 2, \ldots, n$. Thus, $\{a*a_1, a*a_2, \ldots, a*a_n\} \subseteq S$. Suppose $a*a_i = a*a_j$ for some $i \neq j$. Then by the cancellation law we have $a_i = a_j$, which is a contradiction since $a_i \neq a_j$. Hence, all elements in $\{a * a_1, a * a_2, \ldots, a * a_n\}$ are distinct. Thus, $S = \{a * a_1, a * a_2, \ldots, a*a_n\}$. Let $b \in S$. Then $b = a*a_k$ for some $a_k \in S$. Therefore, the equation $a*x = b$ has a solution in S. Similarly, we can show that the equation $y*a = b$ has a solution in S. Hence, by Theorem 2.1.23, $(S, *)$ is a group. The converse follows by Theorem 2.1.11(iii). ■

Let $(G, *)$ be a group, $a \in G$, and $n \in \mathbf{Z}$. We now define the **integral power** a^n of a as follows:

$$\begin{aligned} a^0 &= e \\ a^n &= a * a^{n-1} \text{ if } n > 0 \\ a^n &= (a^{-1})^{-n} \text{ if } n < 0. \end{aligned}$$

Note that $a^n = (a^{-n})^{-1}$ if $n < 0$. In the exercises at the end of this section, we ask the reader to verify certain basic properties of integral powers. It should be pointed out that when we use additive notation for the binary operation $*$, we speak of multiples of an element a of the group $(G, +)$, which are defined as follows:

$$\begin{aligned} 0a &= 0, \text{ where the 0 on the right-hand side denotes the identity of the group } (G, +) \text{ and the 0 on the left-hand side denotes the integer 0.} \\ na &= a + (n-1)a \quad \text{if } n > 0 \\ na &= (-n)(-a) \quad \text{if } n < 0. \end{aligned}$$

For example, in $(\mathbf{Z}_6, +_6)$, $2[3] = [3] +_6 [3] = [6] = [0]$. By the notation na, we do not mean n and a multiplied together since no multiplicative operation between elements of $\mathbf{Z}$ and G has been defined.

Definition 2.1.25 *A group $(G, *)$ is called a* ***finite group*** *if G has only finite number of elements. The* ***order,*** *written $|G|$, of a group $(G, *)$ is the number of elements of G.*

Example 2.1.5 shows that for every positive integer n, there is a commutative group of order n.

The groups in Examples 2.1.5 and 2.1.6 are finite groups.

A group with an infinite number of elements is referred to as an **infinite group**. Klein and Lie's use of groups in geometry influenced the turn from finite groups to infinite groups.

The groups in Examples 2.1.3, 2.1.4, and 2.1.7 are infinite groups.

Let G be a finite group and $a \in G$. Now $a^2 = a * a \in G$ and by induction we can show that $a^m \in G$ for all $m \geq 1$. Thus, $\{a, a^2, \ldots, a^m, \ldots\} \subseteq G$. Since G is finite, all elements of the set $\{a, a^2, \ldots, a^m, \ldots\}$ cannot be distinct. Hence $a^k = a^l$ for some positive integers k, l, $k > l$. This implies that $a^{k-l} = e$. Let us write $n = k - l$. Therefore, $a^n = e$ for some positive integer n. Also, if G is an infinite group and $a \in G$, then it may still be possible that $a^n = e$ for some positive integer n. This leads us to the following definition.

Definition 2.1.26 *Let $(G, *)$ be a group and $a \in G$. If there exists a positive integer n such that $a^n = e$, then the smallest such positive integer is called the* ***order*** *of a. If no such positive integer n exists, then we say that a is of infinite* ***order.***

We denote the order of an element a of a group $(G, *)$ by $o(a)$.

The concept of the order of an element is very important in group theory. We shall see in later chapters how effectively information about the order of an element of a group reveals the nature of the group and in several instances leads us to determine the structure of the group itself.

Example 2.1.27 *Consider the group $(\mathbf{Z}_6, +_6)$. $\mathbf{Z}_6$ has order 6. The elements $[0]$, $[1]$, $[2]$, $[3]$, $[4]$, $[5]$ have orders 1, 6, 3, 2, 3, 6, respectively. For example, $2[3] = [3] +_6 [3] = [6] = [0]$ and 2 is the smallest positive integer n such that $n[3] = [0]$.*

Let G be a group and $a \in G$. If $o(a)$ is infinite, then by the definition of the order of an element it follows that $o(a^k)$ is also infinite for all $k \geq 1$, i.e., the order of every positive power of a is also infinite. If $o(a)$ is finite, then the next theorem tells us how to compute the order of various powers of a.

Theorem 2.1.28 *Let $(G, *)$ be a group and a be an element of G such that $o(a) = n$.*

(i) If $a^m = e$ for some positive integer m, then n divides m.

(ii) For every positive integer t,

$$o(a^t) = \frac{n}{\gcd(t,n)}.$$

Proof. (i) By the division algorithm, there exist $q, r \in \mathbf{Z}$ such that $m = nq + r$, where $0 \leq r < n$. Now $a^r = a^{m-nq} = a^m * a^{-nq} = a^m * (a^n)^{-q} = e * (e)^{-q} = e$. Since n is the smallest positive integer such that $a^n = e$ and $a^r = e$, it follows that $r = 0$. Thus, $m = nq$. This implies that n divides m.

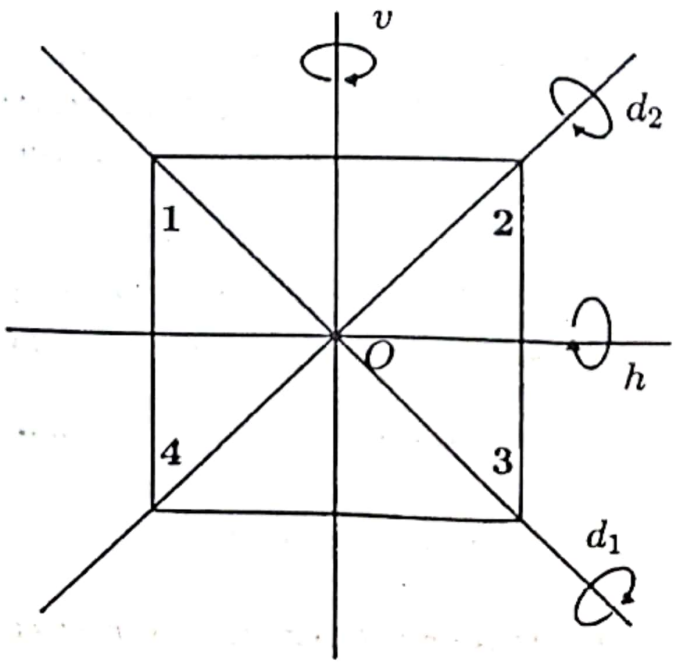
(ii) Let $o(a^t) = k$. Then $a^{kt} = e$. By (i), n divides kt. Thus, there exists $r \in \mathbf{Z}$ such that $kt = nr$. Let $\gcd(t,n) = d$. Then there exist integers u and v such that $t = du$ and $n = dv$ and $\gcd(u,v) = 1$ by Exercise 9 (page 20). Now $kt = nr$ implies that $kdu = dvr$. Hence, $ku = rv$. Thus, v divides ku. Since $\gcd(u,v) = 1$, v divides k. Thus, $\frac{n}{d}$ divides k. Now $(a^t)^{\frac{n}{d}} = a^{\frac{nt}{d}} = a^{\frac{ndu}{d}} = a^{nu} = (a^n)^u = e^u = e$. Since $o(a^t) = k$, k divides $\frac{n}{d}$. Since k and $\frac{n}{d}$ are positive integers, $k = \frac{n}{d}$. Hence, $o(a^t) = k = \frac{n}{d} = \frac{n}{\gcd(t,n)}$. ■

A group $(G, *)$ is called a **torsion group** if every element of G is of finite order. If every nonidentity element of G is of infinite order, then G is called a **torsion-free group.**

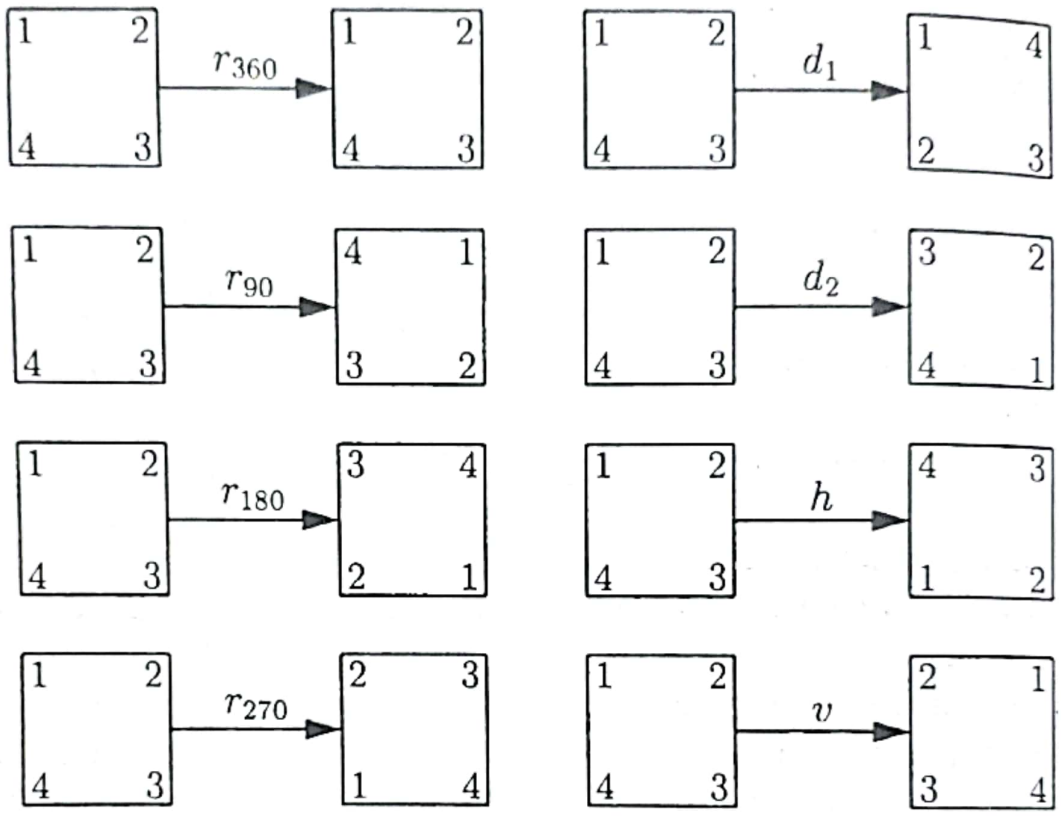
The group of Example 2.1.27 is a torsion group. The groups $(\mathbf{R}, +)$, $(\mathbf{R}^+, \cdot)$, $(\mathbf{Q}^+, \cdot)$ are torsion-free groups. The group $(\mathbf{R}\backslash\{0\}, \cdot)$ is neither a torsion group nor a torsion-free group, since -1 is of order 2 and all other nonidentity elements are of infinite order.

We close this chapter with the following example. The ideas set forth in this example are due to Klein.

Example 2.1.29 *Imagine a square having its sides parallel to the axes of a coordinate system and its center at the origin.*



We label the vertices as in the figure and we allow the following rigid m tions of the square: clockwise rotations of the square about the center o through angles of 90°, 180°, 270°, 360°, say, r_{90}, r_{180}, r_{270}, r_{360}, respectiv reflections h and v about the horizontal and vertical axes; reflections d_1, about the diagonals. The following figures should prove helpful.



A multiplication $*$ on two rigid motions can be defined by performing t such motions in succession. For example, $r_{90} * h$ is determined by first perfor ing motion h and then the motion r_{90}. We see that $r_{90} * h = d_1$. The compl multiplication table for the operation $*$ follows.

$*$	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{360}	r_{360}	r_{90}	r_{180}	r_{270}	h	v	d_1	d_2
r_{90}	r_{90}	r_{180}	r_{270}	r_{360}	d_1	d_2	v	h
r_{180}	r_{180}	r_{270}	r_{360}	r_{90}	v	h	d_2	d_1
r_{270}	r_{270}	r_{360}	r_{90}	r_{180}	d_2	d_1	h	v
h	h	d_2	v	d_1	r_{360}	r_{180}	r_{270}	r_{90}
v	v	d_1	h	d_2	r_{180}	r_{360}	r_{90}	r_{270}
d_1	d_1	h	d_2	v	r_{90}	r_{270}	r_{360}	r_{180}
d_2	d_2	v	d_1	h	r_{270}	r_{90}	r_{180}	r_{360}

We leave it for the reader to verify that the set of rigid motions is a gro under the operation $*$. This group is known as the ***group of symmetries the square****. Let us denote this group by Sym. Then*

$$Sym = \{r_{360}, r_{90}, r_{180}, r_{270}, h, v, d_1, d_2\}.$$