Chapter 3
Groups

The theory of groups is the oldest branch of modern algebra. The concept of a group is surely one of the central ideas of mathematics. A group is a set in which you can perform one operation with some nice properties. In this chapter we introduce the basic concepts of group theory.

3.1 A Short History of Group Theory

The concept of a group is one of the most fundamental in modern mathematics. Group theory can be considered the study of symmetry: the collection of symmetries of some object preserving some of its structure forms a group; in some sense all groups arise this way. Although permutations had been studied earlier, the theory of groups really began with Galois (1811–1832) who demonstrated that polynomials are best understood by examining certain groups of permutations of their roots. Since that time, groups have arisen in almost every branch of mathematics. There are three historical roots of group theory:

(1) The theory of algebraic equations;
(2) Number theory;
(3) Geometry.

Euler, Gauss, Lagrange, Abel, and Galois were early researchers in the field of group theory. Galois is honored as the first mathematician linking group theory and field theory, with the theory that is now called Galois theory.

Permutations were first studied by Lagrange (1770, 1771) on the theory of algebraic equations. Lagrange's main object was to find out why cubic equations could be solved algebraically. In studying the cubic, for example, Lagrange assumes the roots of a given cubic equation are x', x'', and x'''. Then, taking 1, w, and w^2 as the cube roots of unity, he examines the expression

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_3

$$R = x' + wx'' + w^2x'''$$

and notes that it takes just two different values under the six permutations of the roots x', x'', and x'''. But, he could not fully develop this insight because he viewed permutations only as rearrangements, and not as bijections that can be composed. The composition of permutations does appear in the works of Ruffini and Abbati about 1800; in 1815 Cauchy established the calculus of permutations.

Galois found that if $r_1, r_2, \ldots, r_n$ are the n roots of an equation, there is always a group of permutations of the rs such that every function of the roots invariable by the substitutions of the group is rationally known, and conversely, every rationally determinable function of the roots is invariant under the substitutions of the group. Galois also contributed to the theory of modular equations and to that of elliptic functions. His first publication on the group theory was made at the age of 18 (1829), but his contributions attracted little attention until the publication of his collected papers in 1846.

The number-theoretic strand was started by Euler and taken up by Gauss, who developed modular arithmetic and considered additive and multiplicative groups related to quadratic fields. Indeed, in 1761, Euler studied modular arithmetic. In particular, he examined the remainders of powers of a number modulo n. Although Euler's work is, of course, not stated in group-theoretic terms, he does provide an example of the decomposition of an abelian group into cosets of a subgroup. He also proves a special case of the order of a subgroup is being a divisor of the order of the group.

Gauss in 1801 was to take Euler's work much further and gives a considerable amount of work on modular arithmetic which amounts to a fair amount of theory of abelian groups. He examines orders of elements and proves (although not in this notation) that there is a subgroup for every number dividing the order of a cyclic group. Gauss also examined other abelian groups. He looked at binary quadratic forms

$$ax^2 + 2bxy + cy^2,$$

where a, b, and c are integers. Gauss examined the behavior of forms under transformations and substitutions. He partitions forms into classes and then defines a composition on the classes. Gauss proves that the order of composition of three forms is immaterial, so in modern language, the associative law holds. In fact, Gauss has a finite abelian group, and later (in 1869) Schering, who edited Gauss's works, found a basis for this abelian group.

Geometry has been studied for a very long time, so it is reasonable to ask what happened to geometry at the beginning of the nineteenth century that contributed to the rise of the group concept. Geometry had begun to lose its *metric* character with projective and non-Euclidean geometries being studied. Also the movement to study geometry in n dimensions led to an abstraction in geometry itself. The difference between metric and incidence geometry comes from the work of Monge, his student Carnot, and perhaps, most importantly, the work of Poncelet. Non-Euclidean geometry was studied by Lambert, Gauss, Lobachevsky, and, János Bolyai, among others.

Möbius in 1827, although he was completely unaware of the group concept, began to classify geometries using the fact that a particular geometry studies properties invariant under a particular group. Steiner in 1832 studied notions of synthetic geometry which were to eventually become part of the study of transformation groups.

Arthur Cayley and Augustin Louis Cauchy were among the first to appreciate the importance of the theory, and to the latter especially are due to a number of important theorems. The subject was popularized by Serret, Camille Jordan, and Eugen Netto. Other group theorists of the nineteenth century were Bertrand, Charles Hermite, Frobenius, Leopold Kronecker, and Emile Mathieu.

It was Walther von Dyck who, in 1882, gave the modern definition of a group.

The study of what are now called Lie groups, and their discrete subgroups, as transformation groups, started systematically in 1884 by Sophus Lie; followed by the works of Killing, Study, Schur, Maurer, and Cartan. The discontinuous (discrete group) theory was built up by Felix Klein, Lie, Poincaré, and Charles Emile Picard, in connection in particular with modular forms.

Other important mathematicians in this subject area include Emil Artin, Emmy Noether, Ludwig Sylow, and many others (Fig. 3.1).

3.2 Binary Operations

We are used to addition and multiplication of real numbers. These operations combine two real numbers to generate a unique single real number. So, we can look at these operations as functions on the set $\mathbb{R} \times \mathbb{R}$ defined by

$$\begin{aligned} + : \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (a, b) &\to a + b \end{aligned}$$

and

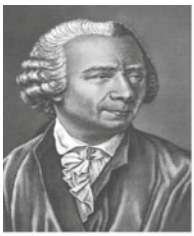
$$\begin{aligned} \cdot : \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (a, b) &\to a \cdot b \end{aligned}$$

These operations are examples of binary operations. The general definition of a binary operation is as follows:

Definition 3.1 Let S be a non-empty set. A *binary operation* on S is a function $\star : S \times S \to S$ that maps each ordered pair (x, y) of S to an element $\star(x, y)$ of S. For convenience we write $a \star b$ instead of $\star(a, b)$. The set S is said to be *closed under the operation* $\star$. The pair $(S, \star)$ (or just S, if there is no fear of confusion) is called a *groupoid*.

Binary operations are usually denoted by special symbols $+$, $-$, $\cdot$, $\times$, $\star$, $*$, $\circ$, $\oplus$, $\odot$, $\vee$, $\wedge$, $\cup$, $\cap$ rather than by letters.

Example 3.2 The ordinary operations of addition "$+$", subtraction "$-$", and multiplication "$\cdot$" are binary operations on $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. Subtraction is not a binary



(a) L. Euler (1707–1783)

(b) J. L. Lagrange (1736–1813)

(c) A. F. Möbius (1790–1868)

(d) J. Steiner (1796–1863)

(e) N. H. Abel (1802–1829)

(f) É. Galois (1811–1832)

(g) A. Cayley (1821–1895)

(h) L. Sylow (1832–1918)

(i) C. Jordan (1838–1922)

(j) F. Klein (1849–1925)

(k) E. Noether (1882–1935)

(l) E. Artin (1898–1962)

Fig. 3.1 Pictures of some famous mathematicians

operation on $\mathbb{N}$, because $3 - 7$ is not in $\mathbb{N}$. Division is not a binary operation on $\mathbb{Q}$, however, division is a binary operation on $\mathbb{Q} \setminus \{0\}$.

Example 3.3 Exponential operation $a \star b = a^b$ is a binary operation on the set $\mathbb{N}$ of natural numbers while it is not a binary operation on the set $\mathbb{Z}$ of integers.

Binary operators can be defined on arbitrary sets, not only sets of numbers.

Example 3.4 We might consider a set S of colors, and define a binary operation $\oplus$ which tells us how to combine two colors to form another color. If Red, Blue, Green, Yellow, and Purple are elements of S, then we can write Red $\oplus$ Blue = Purple, since we can combine the first two colors to make the third.

Example 3.5 If X is a set, then union "$\cup$" and intersection "$\cap$" are binary operations on $\mathcal{P}(X)$.

Example 3.6 Let $\mathbb{P}$ be the set of all propositions. Then, "*and*" and "*or*" are binary operations on $\mathbb{P}$. In mathematical logic "*and*" is usually represented by $\wedge$, and "*or*" is represented by $\vee$.

Example 3.7 We noted earlier that binary operations can act not only on numbers but also on arbitrary elements, such as colors or other sets. Here we consider the set $S = \{R_0,\ R_1,\ R_2,\ R_3,\ S_0,\ S_1,\ S_2,\ S_3\}$ as defined in Example 2.17, a set of geometric transformations, which we can combine. We can consider the binary operation of combining these geometric transformations by doing one and then doing the other.

Definition 3.8 One way of describing a binary operation $\star$ on a set S (provided S is not too big) is to form a grid with rows and columns labeled by the elements of S, and enter the element $a \star b$ in the cell in row a and column b (for all $a, b \in S$). This is called a *multiplication table* or a *Cayley table*.

Let $\star$ be be a binary operation on a finite set $S = \{a_1,\ a_2,\ \ldots,\ a_n\}$ having n elements. We construct a Cayley table for $\star$ as follows:

$\star$	a_1	a_2	$\ldots$	a_n
a_1	$a_1 \star a_1$	$a_1 \star a_2$	$\ldots$	$a_1 \star a_n$
a_2	$a_2 \star a_1$	$a_2 \star a_2$	$\ldots$	$a_2 \star a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_n	$a_n \star a_1$	$a_n \star a_2$	$\ldots$	$a_n \star a_n$

Let $\star$ be a binary operation on a set S. There are a number of interesting properties that a binary operation may or may not have. Specifying a list of properties that a binary operation must satisfy will allow us to define deep mathematical objects such as groups.

- $\star$ is *commutative* if $a \star b = b \star a$, for all $a, b \in S$.
- $\star$ is *associative* if $a \star (b \star c) = (a \star b) \star c$, for all $a, b, c \in S$.

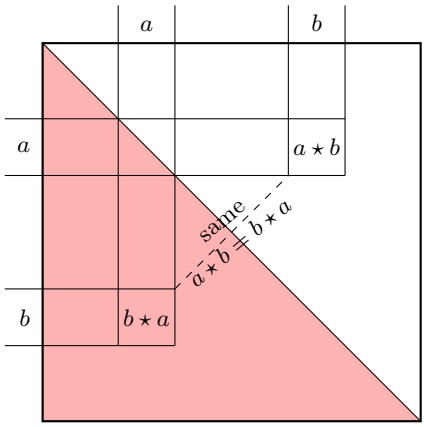


Fig. 3.2 Cayley table of a commutative binary operation

Let S be finite. The property that $a \star b = b \star a$, for all $a, b \in S$, means that the Cayley table must be symmetric across the main diagonal, see Fig. 3.2.

Example 3.9 (1) Let $S = \mathbb{R}$ and $a \star b = a$, for all $a, b \in S$. Then $3 \star 5 = 3$ and $5 \star 3 = 5$, and so $\star$ is not commutative. However, if $a, b, c \in S$, then $a \star (b \star c) = a = a \star b = (a \star b) \star c$, and hence $\star$ is associative.

(2) Let $S = \mathbb{Q} \setminus \{0\}$ and $a \star b = a/b$, for all $a, b \in S$. Then $1 \star 3 = 1/3 \neq 3 = 3/1$, and so $\star$ is not commutative. Also, we have

$$1 \star (2 \star 3) = 1 \star (2/3) = 3/2 \neq 1/6 = (1/2) \star 3 = (1 \star 2) \star 3.$$

Hence $\star$ is not associative.

Exercises

1. Is $(\mathbb{Z}, \star)$ a groupoid if $\star$ is defined, for each $x, y \in \mathbb{Z}$, by
   (a) $x \star y = \sqrt{x + y}$;
   (b) $x \star y = (x + y)^2$;
   (c) $x \star y = x - y - xy$;
   (d) $x \star y = 0$.
2. Define $\star$ on $\mathbb{Q}$ as $a \star b = ab + 1$, for all $a, b \in \mathbb{Q}$. Is $\star$ associative (prove or find a counterexample)?
3. Prove that if $\star$ is an associative and commutative binary operation on a set S, then $(a \star b) \star (c \star d) = \big((d \star c) \star a\big) \star b$, for all $a, b, c, d \in S$.
4. Let S be a finite set containing n elements. Find the total number of binary operations on S.

5. Let S be a finite set containing n elements. Show that the total number of commutative binary operation on S is $n^{n(n-1)/2}$.

3.3 Semigroups and Monoids (Optional)

A semigroup is an algebraic structure consisting of a non-empty set together with an associative binary operation. The formal study of semigroups began in the early twentieth century. Semigroups are important in many areas of mathematics. We give here some basic definitions and very basic results concerning semigroups.

Definition 3.10 A *semigroup* is a pair $(S, \star)$ in which S is a non-empty set and $\star$ is a binary associative operation on S.

Semigroups are therefore one of the most basic types of algebraic structure.

For an element $x \in S$ we let x^n be the product of x with itself n times. So, $x^1 = x$, $x^2 = x \star x$, and $x^{n+1} = x^n \star x$ for $n \geq 1$.

Let $x_1, x_2, \ldots, x_n$ be a sequence of elements of a semigroup $(S, \star)$. We define

$$\begin{aligned} p_1 &= x_1, \\ p_k &= p_{k-1} \star x_k, \quad \text{for } k > 1. \end{aligned}$$

Now an arbitrary product of n elements of S is determined by an expression involving n elements of S together with equal numbers of left and right parentheses that determine the order in which the product is evaluated. The general associative law ensures that the value of such a product is determined only by the order in which the elements of the semigroup occur within that product. Thus a product of n elements of S has the value $x_1 \star x_2 \star \ldots \star x_n$, where $x_1, x_2, \ldots, x_n$ are the elements to be multiplied, listed in the order in which they occur in the expression defining the product.

Example 3.11 Given four elements x_1, x_2, x_3, and x_4 of a semigroup $(S, \star)$, the products

$$\begin{aligned} &((x_1 \star x_2) \star x_3) \star x_4, \quad (x_1 \star x_2) \star (x_3 \star x_4), \quad (x_1 \star (x_2 \star x_3)) \star x_4, \\ &x_1 \star ((x_2 \star x_3) \star x_4), \quad x_1 \star (x_2 \star (x_3 \star x_4)), \end{aligned}$$

all have the same value. Note that according to the above definition, $p_4 = ((x_1 \star x_2) \star x_3) \star x_4$.

Theorem 3.12 (General Associative Law) *Let $(S, \star)$ be a semigroup and $x_1, x_2, \ldots, x_n \in S$. Every way of inserting balanced pairs of brackets into the product $x_1 \star x_2 \star \ldots \star x_n$ give the same result.*

Proof We prove that any insertion of brackets into the product gives the same result as $x_1 \star (x_2 \star (x_3 \star \ldots \star x_n) \ldots)$. We proceed by mathematical induction on n. For

$n = 1$, the result is trivially true, for there is only one way to insert balanced pairs of brackets into the product x_1. This is the base case of the induction.

So, assume that the result holds for all $n < k$; we aim to show it is true for k. Take some bracketing of the product $x_1, x_2, \ldots, x_k$ and let y be the result. This bracketing is a product of some bracketing of $x_1, \ldots, x_j$ and some bracketing of $x_{j+1}, \ldots, x_k$ for some $1 \leq j < k$. Now, we consider the following two cases:

Case 1: Suppose that $j = 1$. By the assumption, the result of inserting brackets into $x_{j+1} \star \ldots \star x_k = x_2 \star \ldots \star x_k$ is equal to $x_2 \star (x_3 \star (\ldots x_k) \ldots)$. Thus, $y = x_1 \star (x_2 \star (x_3 \star (\ldots x_k) \ldots))$, which is the result with $n = k$.

Case 2: Suppose that $j > 1$. By the assumption, the result of the bracketing of $x_1 \star \ldots \star x_j$ is $x_1 \star (x_2 \star (\ldots x_j) \ldots)$ and the result of the bracketing of $x_{j+1} \star \ldots \star x_k$ is $x_{j+1} \star (x_{j+2} \star (\ldots x_k) \ldots)$. Consequently, we obtain

$$\begin{aligned} y &= \big(x_1 \star (x_2 \star (\ldots x_j) \ldots)\big)\big(x_{j+1} \star (x_{j+2} \star (\ldots x_k) \ldots)\big) \\ &= x_1 \star \big(((x_2 \star (\ldots x_j) \ldots)) \star (x_{j+1} \star (x_{j+1} \star (\ldots x_k) \ldots))\big) \text{ (by associativity)} \\ &= x_1 \star (x_2 \star (x_3 \ldots x_k) \ldots) \text{ (by assumption } n = k - 1), \end{aligned}$$

which is the result with $n = k$.

Therefore, by induction, the result holds for all n. ■

A semigroup S is *finite* if it has only a finitely many elements. A semigroup S is *commutative*, if it satisfies $x \star y = y \star x$, for all $x, y \in S$. If there exists e in S such that for all $x \in S$,

$$e \star x = x \star e = x$$

we say that S is a *semigroup with identity* or (more usual) a *monoid*. The element e of S is called *identity*.

Proposition 3.13 *Let e be a left identity of S and e' is a right identity of S, then $e = e'$. Consequently, a semigroup contains at most one identity.*

Proof Since e is a left identity, it follows that $e \star e' = e'$. Since e' is a right identity, it follows that $e = e \star e'$. Hence, we get $e = e \star e' = e'$, as desired. ■

By Proposition 3.13, the identity element is unique and we shall generally denote it by 1.

Example 3.14 Let $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$ be the set of all non-negative integers. Then, $(\mathbb{N}^0, \cdot)$ is a semigroup for the usual multiplication of integers. Also, $(\mathbb{N}^0, +)$ is a semigroup, when $+$ is the ordinary addition of integers. Define $(\mathbb{N}^0, \star)$ by $n \star m = \max\{n, m\}$. Then, $(\mathbb{N}^0, \star)$ is a semigroup, since

$$\begin{aligned} n \star (m \star k) &= \max\{n, \max\{m, k\}\} = \max\{n, m, k\} \\ &= \max\{\max\{n, m\}, k\} = (n \star m) \star k. \end{aligned}$$

Example 3.15 Let S be a non-empty set. There are two simple semigroup structures on S: with the multiplication given by $x \star y = x$, for all $x, y \in S$, in this case, the

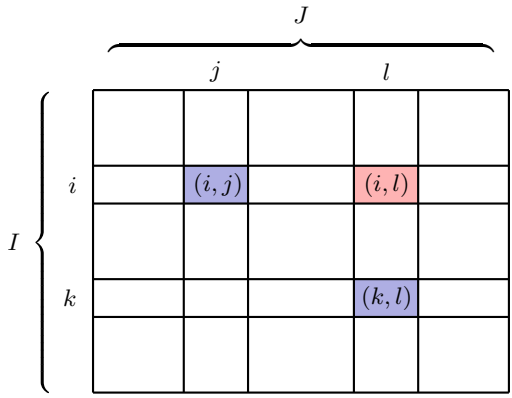


Fig. 3.3 The rectangular band

semigroup $(S, \star)$ is called the *left zero semigroup* over S. Also, fixing an element $a \in S$ and putting $x \star y = a$, for all $x, y \in S$, gives a semigroup structure on S.

Example 3.16 The *opposite semigroup* S^{op} of S is the semigroup with the same set as S but "*reversed multiplication*". That is, for $x, y \in S$, the product $x \star_{op} y$ in S^{op} is equal to the product $y \star x$ in S. It is easy to check that S^{op} is indeed a semigroup. Notice that if S is commutative, then S^{op} and S are the same semigroup.

An element x in a semigroup S is said to be *idempotent* if $x^2 = x$.

Example 3.17 Let I, J be two non-empty sets and set $T = I \times J$ with the binary operation

$$(i, j) \star (k, l) = (i, l).$$

Then, we have

$$\big((i, j) \star (k, l)\big) \star (m, n) = (i, l) \star (m, n) = (i, n),$$
$$(i, j) \star \big((k, l) \star (m, n)\big) = (i, l) \star (k, n) = (i, n),$$

for all (i, j), (k, l) $(m, n) \in T$, and so the multiplication is associative. Hence, $(T, \star)$ is a semigroup called the *rectangular band* on $I \times J$. Note that $(i, j)^2 = (i, j) \star (i, j) = (i, j)$, i.e., every element is an idempotent. The name derives from the observation that if the members of $I \times J$ are pictured in a rectangular grid in the obvious fashion, then the product of two elements lies at the intersection of the row of the first member and the column of the second, see Fig. 3.3.

Example 3.18 The *direct product* $S \times T$ of two semigroups $(S, \cdot)$ and $(T, \circ)$ is defined by

$$(s_1, t_1) \star (s_2, t_2) = (s_1 \cdot s_2, t_1 \circ t_2) \quad (s_1, s_2 \in S,\ t_1, t_2 \in T).$$

It is easy to show that the so defined product is associative and hence the direct product is, indeed, a semigroup. The direct product is a convenient way of combining two semigroup operations. The new semigroup $S \times T$ inherits properties of both S and T.

Example 3.19 On the Cartesian product $\mathbb{Z} \times \mathbb{Z}$ we define a binary operation as follows:

$$(a, b) \star (c, d) = \begin{cases} (a - b + c, d) & \text{if } b < c \\ (a, d) & \text{if } b = c \\ (a, d + b - c & \text{if } b > c, \end{cases}$$

for all $a, b, c, d \in \mathbb{Z}$. The set $\mathbb{Z} \times \mathbb{Z}$ with such defined operation is a semigroup.

Example 3.20 Let $(S, \star)$ be a semigroup, which is not a monoid. Find a symbol 1 such that $1 \notin S$. Now, we extend the multiplication on S to $S \cup \{1\}$ by

$$\begin{aligned} &a \star b = a \star b \qquad \text{if } a, b \in S, \\ &a \star 1 = a = 1 \star a \text{ for all } a \in S, \\ &1 \star 1 = 1. \end{aligned}$$

Then, $\star$ is associative. Thus, we have managed to extend multiplication in S to $S \cup \{1\}$. For an arbitrary semigroup S the monoid S^1 is defined by

$$S^1 = \begin{cases} S & \text{if } S \text{ is a monoid,} \\ S \cup \{1\} & \text{if } S \text{ is not a monoid.} \end{cases}$$

Therefore, S^1 is "S with a 1 *adjoined*" if necessary.

In a semigroup $(S, \star)$ an element z_l such that $z_l \star x = z_l$ for every $x \in S$ is called a *left zero element* of S, and an element z_r such that $x \star z_r = z_r$ for every $x \in S$ is called a *right zero element* of S. If z is both a left and a right zero element of S, then z is called a *two-sided zero element*, or simply a *zero element*, of S. A semigroup S may have any number of left (or of right) zero elements, but if it has a left zero element z_l and a right zero element z_r, then $z_l = z_l \star z_r = z_r$, whence S has a unique two-sided zero element and no other left or right zero element. Usually, we denote zero element by 0.

Example 3.21 Let $(S, \star)$ be a semigroup. Similar to Example 3.20, let 0 be an element not in S and extend the multiplication on S to $S \cup \{0\}$ by

$$0 \star x = x \star 0 = 0 \star 0 = 0,$$

for all $x \in S$. Again, this extended multiplication is associative. Thus, $S \cup \{0\}$ is a semigroup with zero element. We define

$$S^0 = \begin{cases} S & \text{if } S \text{ has a zero,} \\ S \cup \{0\} & \text{otherwise.} \end{cases}$$

Then, S^0 is called the *semigroup obtained by adjoining a zero* to S if necessary.

Theorem 3.22 *If $(S, \star)$ is a finite semigroup, then there is an idempotent element in S.*

Proof Since S is finite, it follows that $a, a^2, a^3, \ldots$ cannot be distinct elements. So, there exist integers i and j with $i < j$ such that $a^i = a^j$. This implies that $a^{i+k} = a^i$, where $k = j - i$. Now, we have

$$a^{2i+k} = a^i \star a^{i+k} = a^{2i}.$$

Next, by induction, we observe that

$$a^{ni+k} = a^{ni},$$

for all positive integer n. Also, we have

$$\begin{aligned} a^{ni+2k} &= a^{ni+k} \star a^k = a^{ni} \star a^k = a^{ni+k} = a^{ni}, \\ a^{ni+3k} &= a^{ni+2k} \star a^k = a^{ni+2k} = a^{ni}, \end{aligned}$$

and so on. Therefore, we deduce that

$$a^{ni+rk} = a^{ni},$$

for all positive integer r. In particular, we have $a^{ki+ki} = a^{ki}$, or $a^{2ki} = a^{ki}$. Now, if we take $m = ki$, then a^m is an idempotent element. ■

Let $(S, \star)$ be a semigroup. An element b of the semigroup S is called a *right divisor* of the element a of the same semigroup if there exists an element $x \in S$ such that $x \star b = a$. An element b is called a *left divisor* of a if there exists an element $y \in S$ such that $b \star y = a$. If b is a right divisor of a, we say that a is *divisible on the right* by b. If b is a left divisor of a, we say that a is *divisible on the left* by b. If the element b of S is a right divisor of the element a of the same semigroup, then the element x satisfying the equation $x \star b = a$ is called a *left inverse* of b with respect to a. The notion of *right inverse* is defined analogously. An element which is both a right inverse and a left inverse of b with respect to a is called a *two-sided inverse*, or shortly an *inverse*, of b with respect to a.

Definition 3.23 Let M be a monoid and $x \in M$. If there exists an element x' such that $x \star x' = 1$, then x' is a *right inverse* for x, and x is *right invertible*. Similarly, suppose that there exists an element x'' such that $x'' \star x = 1$, then x'' is a *left inverse* for x, and x is *left invertible*. If x is both left and right invertible, then x is *invertible*.

Proposition 3.24 *Let M be a monoid, and let $x \in M$. Suppose that x is invertible and let x' be a right inverse of x and x'' be a left inverse of x. Then, $x' = x''$.*

Proof Since x' and x'' are right and left inverses of x, respectively, it follows that $x \star x' = 1$ and $x'' \star x = 1$. Thus, we have

$$x' = 1 \star x' = (x'' \star x) \star x' = x'' \star (x \star x') = x'' \star 1 = x'',$$

as desired. ■

Proposition 3.24 says that right and left inverses coincide when they both exist. The existence of one does not imply the existence of the other. Thus, if x is an invertible element of a monoid M, denote the unique right and left inverse of x by x^{-1}.

Definition 3.25 A *subsemigroup* A of a semigroup S is a non-empty subset of S such that $A \star A \subseteq A$, i.e., $x, y \in A$ implies $x \star y \in A$. A *submonoid* A of a monoid M is a subsemigroup A which contains the identity 1 of M.

Theorem 3.26 *The set of invertible elements of a monoid forms a submonoid.*

Proof Let I be the set of invertible elements of a monoid M. Since $1 \in I$, it follows that I is non-empty. Suppose that x and y are two arbitrary elements of I. Since x and y are invertible, it follows that

$$\begin{aligned}(y^{-1} \star x^{-1}) \star (x \star y) &= y^{-1} \star (x^{-1} \star x) \star y = y^{-1} \star y = 1,\\ (x \star y) \star (y^{-1} \star x^{-1}) &= x \star (y \star y^{-1}) \star x^{-1} = x \star x^{-1} = 1.\end{aligned}$$

Hence, $x \star y$ is invertible and so $x \star y \in I$. Consequently, I is a subsemigroup of M. In addition, $1 \in I$ is an identity for I. Therefore, I is a submonoid of M. ■

Definition 3.27 A semigroup $(S, \star)$ is *left cancellative*, if

$$c \star a = c \star b \Rightarrow a = b,$$

and $(S, \star)$ is *right cancellative*, if

$$a \star c = b \star c \Rightarrow a = b.$$

If $(S, \star)$ is both left and right cancellative, then it is *cancellative*.

Exercises

1. Let $(\mathbb{Q}, \star)$ be a groupoid, where $a \star b = a + b - ab$, for all $a, b \in \mathbb{Q}$.
   (a) Is the groupoid $(\mathbb{Q}, \star)$ a semigroup?
   (b) Is there an identity element in $(\mathbb{Q}, \star)$?
   (c) Which elements of the groupoid have inverses?

2. If $\mathbb{Q}$ is replaced by $\mathbb{Z}$ in Exercise 1, are the solutions the same?
3. A set S has n elements, what is the number of commutative binary operation of S?
4. Prove that if S is a semigroup and $e \in S$ is both a right zero and a right identity, then S is trivial.
5. In the set of all continuous functions of two variables x and y, we define in the square $0 \leq x \leq a, 0 \leq y \leq a$, the following operation, which plays an important role in the theory of integrals. The result of this operation carried out for the functions $K_1(x, y)$ and $K_2(x, y)$ is the function

$$\int_0^a K_1(x,t)K_2(t,y)dt.$$

   By using the simplest properties of integrals, show that we obtain a semigroup.
6. We consider the set of functions of one variable which are absolutely integrable for $0 \leq x < \infty$. In many branches of mathematics, one considers the operation in this set, the result of which for $f_1(x)$ and $f_2(x)$ is the function

$$\int_0^x f_1(t)\, f_2(x-t)dt.$$

   Show that this operation is associative and commutative.
7. Prove that for any commutative monoid M, the set of idempotent elements of M forms a submonoid.
8. Let S be a left cancellative semigroup. Suppose that $e \in S$ is an idempotent. Prove that e is a left identity. Deduce that a cancellative semigroup can contain at most one idempotent, which must be an identity.
9. Give an example of a semigroup containing more than one idempotent but containing no identity.

3.4 Groups and Examples

In this section, we embark on the study of the algebraic object known as a group. We give a few basic definitions and then concentrate on examples of groups.

Definition 3.28 Let G be a non-empty set and $\star$ be a binary operation on G. We say that $(G, \star)$ is a *group* if it satisfies the following conditions:

(1) *Associativity Law:* $a \star (b \star c) = (a \star b) \star c$, for all $a, b, c \in G$;
(2) *Existence of Identity:* There exists an element $e \in G$ called an *identity* such that $a \star e = e \star a = a$, for all $a \in G$;
(3) *Existence of Inverse:* For each $a \in G$, there exists an element $b \in G$ such that $a \star b = b \star a = e$ (we write this element b as a^{-1} and call it the *inverse* of a in G).

Hence, a group G is a monoid G that satisfies the condition (3). In other words, a group G is a semigroup with an identity in which every element has an inverse.

Remark 3.29 In many books, there is an extra condition in the definition of group, that is, "*G is closed under $\star$*". In other words, $x \star y \in G$, for all $a, b \in G$. But according to our definition, this condition is a result of the definition of binary operation.

Corollary 3.30 *If G is a group, then*

(1) The identity element of G is unique;
(2) Every $a \in G$ has a unique inverse in G.

Proof Since any group is a semigroup and a monoid, the result follows from Propositions 3.13 and 3.24. ■

Definition 3.31 The number of elements in a group G is called the *order* of G and is denoted by $|G|$. If $|G|$ is finite, then G is said to be a *finite group*; otherwise G is an *infinite group*.

Before starting to look into the nature of groups, we look at some examples.

Example 3.32 (*Additive Groups*) The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$, and the set of complex numbers $\mathbb{C}$ are all groups under ordinary addition.

Example 3.33 If E is the set of even integers, then E is a group under addition of integers.

Example 3.34 The sets $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ and $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ are groups under ordinary multiplication.

Example 3.35 Let G be the set of real numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$ and are not simultaneously zero. Then, G is a group under the usual multiplication of real numbers.

Example 3.36 Let $\mathbb{C}^*$ be the set of all non-zero complex numbers, i.e.,

$$\mathbb{C}^* = \{a + bi \mid a, b \in \mathbb{R} \text{ and } (a \neq 0 \text{ or } b \neq 0)\}.$$

Recall that $i^2 = -1$. We define multiplication of complex numbers as follows:

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

This is a binary operation on $\mathbb{C}^*$. Note that both $ac - bd$ and $ad + bc$ cannot be zero. Suppose that $a + bi$, $c + di$ and $e + fi$ are arbitrary elements of $\mathbb{C}^*$. Then, we have

$$\begin{aligned}
&\big((a+bi)\cdot(c+di)\big)\cdot(e+fi)\\
&=\big((ac-bd)+(ad+bc)i\big)\cdot(e+fi)\\
&=\big((ac-bd)e-(bc+ad)f\big)+\big((bc+ad)e+(ac-bd)f\big)i\\
&=\big(a(ce-df)-b(de+cf)\big)+\big(b(ce-df)+a(de+cf)\big)i\\
&=(a+bi)\cdot\big((ce-df)+(de+cf)\big)\\
&=(a+bi)\cdot\big((c+di)\cdot(e+fi)\big).
\end{aligned}$$

Hence, the multiplication $\cdot$ is associative on $\mathbb{C}^*$. Clearly, $1 = 1 + 0i \in \mathbb{C}^*$ is the identity element in $\mathbb{C}^*$. Now, we check the existence of inverse. Assume that $a + bi \in \mathbb{C}^*$. Then not both a and b are zero, and so $a^2 + b^2 \neq 0$. Consequently, we have

$$\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \in \mathbb{C}^*.$$

Moreover, we see that

$$\Big(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\Big)(a+bi) = (a+bi)\Big(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\Big) = 1.$$

Therefore, we proved that $(\mathbb{C}^*, \cdot)$ is a group and we call this group the *multiplicative group of non-zero complex numbers*.

Example 3.37 The set $K_4 = \{e,\ a,\ b,\ c\}$ under the binary operation defined by the following Cayley table is a group.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

This group is known as *Klein's four group*.

Definition 3.38 A group G is said to be *abelian* (or *commutative*) if $a \star b = b \star a$, for all $a, b \in G$.

All the previous examples of groups are abelian. Now, we give some examples of non-abelian groups.

Example 3.39 The group D_3 is the *symmetry group of an equilateral triangle* with vertices on the unit circle, at angles 0, $2\pi/3$, and $4\pi/3$, that is, it is the set of all reflection, rotation, and combinations of these, that leave the shape and position of this triangle fixed. Figure 3.4 shows the effect of the sixth element of D_3. Note that r, s and t can be equally well considered as a rotation of $\theta = \pi$ in $\mathbb{R}^3$ about the axes r, s and t. Then, these six operations form a group. The Cayley table for this group is:

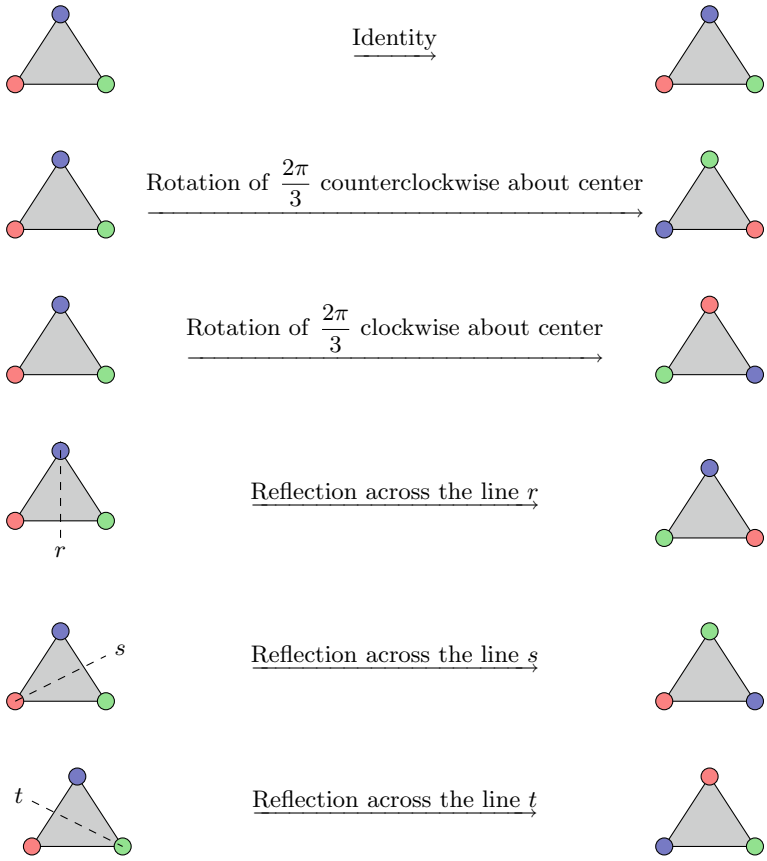


Fig. 3.4 The symmetry group of an equilateral triangle

$\cdot$	R_0	R_1	R_2	S_0	S_1	S_2
R_0	R_0	R_1	R_2	S_0	S_1	S_2
R_1	R_1	R_2	R_0	S_1	S_2	S_0
R_2	R_2	R_0	R_1	S_2	S_0	S_1
S_0	S_0	S_2	S_1	R_0	R_2	R_1
S_1	S_1	S_0	S_2	R_1	R_0	R_2
S_2	S_2	S_1	S_0	R_2	R_1	R_0

Example 3.40 The group D_4 is the *symmetry group of a square* with vertices on the unit circle, at angles 0, $\pi/2$, π, and $3\pi/2$. Figure 3.5 shows the eight symmetries of square. Let

$$D_4 = \{R_0,\ R_1,\ R_2,\ R_3,\ S_0,\ S_1,\ S_2,\ S_3\}$$

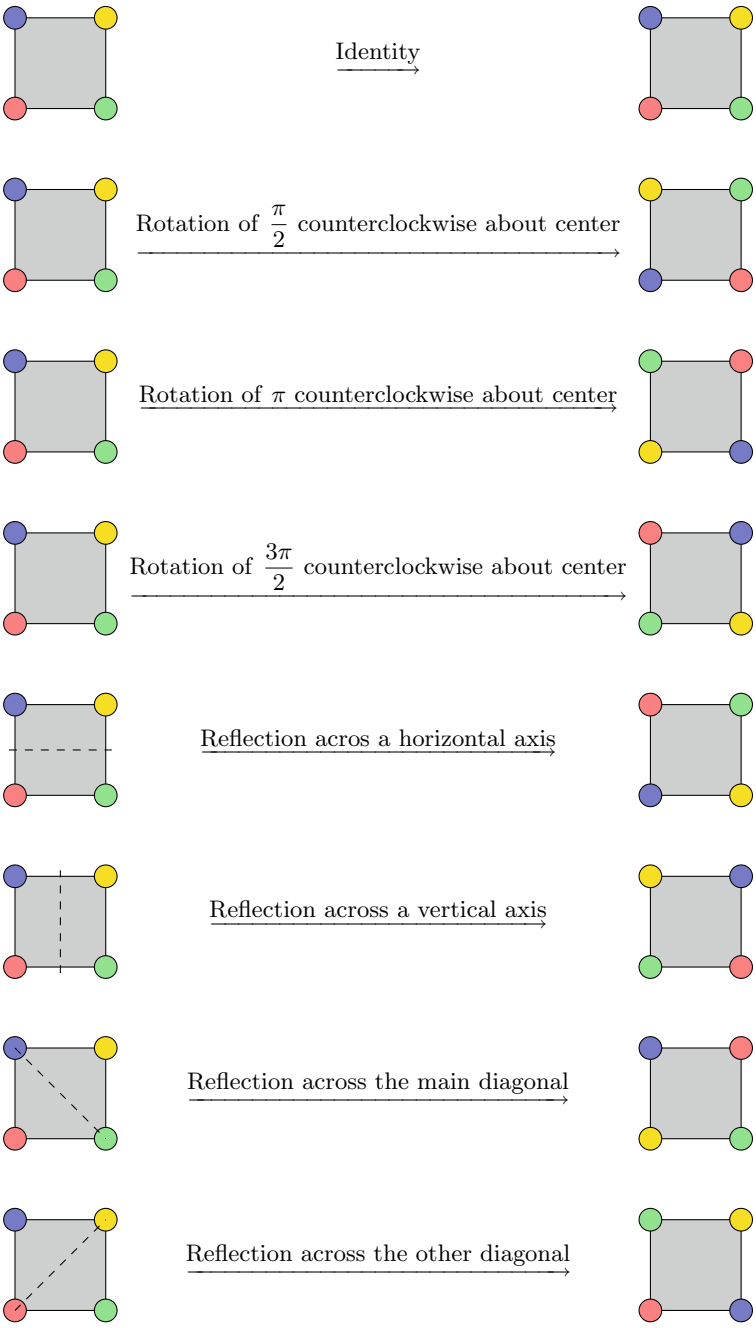


Fig. 3.5 The symmetry group of a square

be the symmetry group of a square. The Cayley table for this group is:

$\cdot$	R_0	R_1	R_2	R_3	S_0	S_1	S_2	S_3
R_0	R_0	R_1	R_2	R_3	S_0	S_1	S_2	S_3
R_1	R_1	R_2	R_3	R_0	S_1	S_2	S_3	S_0
R_2	R_2	R_3	R_0	R_1	S_2	S_3	S_0	S_1
R_3	R_3	R_0	R_1	R_2	S_3	S_0	S_1	S_2
S_0	S_0	S_3	S_2	S_1	R_0	R_3	R_2	R_1
S_1	S_1	S_0	S_3	S_2	R_1	R_0	R_3	R_2
S_2	S_2	S_1	S_0	S_3	R_2	R_1	R_0	R_3
S_3	S_3	S_2	S_1	S_0	R_3	R_2	R_1	R_0

Example 3.41 Let G be the set of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where a, b, c, and d are real numbers such that $ad - bc \neq 0$. For the binary operation in G we use the following multiplication:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}.$$

Clearly, the entries of this 2×2 matrix are real. In order to see that this matrix belongs to G we must show that

$$(aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') \neq 0.$$

A short computation gives that

$$(aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') = (ad - bc)(a'd' - b'c') \neq 0,$$

because both

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$$

are in G. It is not difficult to check that the associative law holds in G. The element $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ belongs to G, and it acts as an identity element relative to the binary operation of G.

Now, suppose that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an arbitrary element of G. Then, we have $ad - bc \neq 0$, and so the matrix

$$\begin{bmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{bmatrix}$$

makes sense. Moreover, we obtain

$$\Big(\frac{d}{ad-bc}\Big)\Big(\frac{a}{ad-bc}\Big)-\Big(\frac{-b}{ad-bc}\Big)\Big(\frac{-c}{ad-bc}\Big)=\frac{ad-bc}{(ad-bc)^2}=\frac{1}{ad-bc}\neq 0.$$

Thus, the matrix

$$\begin{bmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{bmatrix}$$

belongs to G. An easy computation shows that

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

This means that this element of G is the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Therefore, we conclude that G is a group.

Example 3.42 Let $G=\{(a,b)\mid a,b\in\mathbb{R} \text{ and } a>0\}$. We define the following operation on G as follows:

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

for all $(a,b),\ (c,d)\in G$. Obviously, if $b\neq 0$ and $c\neq 0$, then $bc+d\neq 0$. So, $\star$ is a binary operation on G. Now, we verify associativity. Suppose that (a,b), (c,d), and (e,f) are arbitrary elements of G. Then, we have

$$\begin{aligned}\big((a,b)\star(c,d)\big)\star(e,f)&=(ac,bc+d)\star(e,f)\\&=(ace,bce+de+f)\\&=(a,b)\star(ce,de+f)\\&=(a,b)\star\big((c,d)\star(e,f)\big).\end{aligned}$$

Moreover, since $(a,b)\star(1,0)=(1,0)\star(a,b)=(a,b)$, it follows that $(1,0)$ is the identity element. Finally, since

$$(a,b)\star\left(\frac{1}{a},-\frac{b}{a}\right)=\left(\frac{1}{a},-\frac{b}{a}\right)\star(a,b)=(1,0),$$

it follows that $(1/a,-b/a)$ is the inverse of (a,b). Therefore, $(G,\star)$ is a group. But

$$(2,3)\star(1,4)=(2,7) \text{ and } (1,4)\star(2,3)=(2,11).$$

This shows that G is not abelian.

Example 3.43 Let G be the set of all functions $T_{a,b} : \mathbb{R} \to \mathbb{R}$ defined by $T_{a,b}(x) = ax + b$, for each $x \in \mathbb{R}$, where $a, b \in \mathbb{R}$ and $a \neq 0$, i.e.,

$$G = \{T_{a,b} : \mathbb{R} \to \mathbb{R} \mid a, b \in \mathbb{R} \text{ and } a \neq 0\}.$$

Consider the product of elements of G as the compositions of functions. Hence, if $T_{a,b}$ and $T_{c,d}$ are elements in G, then

$$\begin{aligned}\big(T_{a,b} \circ T_{c,d}\big)(x) &= T_{a,b}\big(T_{c,d}(x)\big) = aT_{c,d}(x)b \\ &= a(cx + d) + b = (ac)x + (ad + b) \\ &= T_{ac,ad+b}(x),\end{aligned}$$

for all $x \in \mathbb{R}$. Therefore, we conclude that

$$T_{a,b} \circ T_{c,d} = T_{ac,ad+b}.$$

This yields that $T_{ac,ad+b} \in G$, i.e., G is closed under the composition of functions. For all elements $T_{a,b}$, $T_{c,d}$ and $T_{e,f}$ in G, we see that

$$\begin{aligned}\big(T_{a,b} \circ T_{c,d}\big) \circ T_{e,f} &= T_{ac,ad+b} \circ T_{e,f} \\ &= T_{ace,acf+ad+b} \\ &= T_{a,b} \circ T_{ce,cf+d} \\ &= T_{a,b} \circ \big(T_{c,d} \circ T_{e,f}\big).\end{aligned}$$

So, the associativity law holds. The element $T_{1,0}$ is the identity function and $T_{1,0} \circ T_{a,b} = T_{a,b} \circ T_{1,0} = T_{1,0}$. Finally, what is $T_{a,b}^{-1}$? We must find real numbers $x \neq 0$ and y such that $T_{a,b} \circ T_{x,y} = T_{x,y} \circ T_{a,b} = T_{1,0}$, or equivalently

$$T_{ax,ay+b} = T_{ax,bx+y} = T_{1,0}.$$

This implies that $ax = 1$ and $ay + b = bx + y = 0$. Remember $a \neq 0$, so $a = 1/a$ and $y = -b/a$. Thus, $T_{a^{-1},-a^{-1}b}$ is the inverse of $T_{a,b}$. Consequently, $(G, \circ)$ is a group. Since $T_{1,2} \circ T_{3,4} \neq T_{3,4} \circ T_{1,2}$, it follows that G is not abelian.

It is a little clumsy to keep writing the $\star$ for the product in G, and from now on we shall write the product $a \star b$ simply as ab, for all $a, b \in G$.

Theorem 3.44 *If G is a group, then*

(1) For every $a \in G$, $(a^{-1})^{-1} = a$;
(2) For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof (1) For any $a \in G$, we have

$$aa^{-1} = e = a^{-1}a \text{ and } (a^{-1})^{-1}a^{-1} = e = a^{-1}(a^{-1})^{-1}.$$

Since the inverse of a^{-1} is unique, it follows that $(a^{-1})^{-1} = a$.

(2) This item is proved by the equalities

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$$
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

and the uniqueness of the inverse. ■

In part (2), notice the change in the order of the factors from ab to $b^{-1}a^{-1}$. If in a group the binary operation is written additively, then $a + b$ (for $a, b \in G$) is called the *sum* of a and b, and the identity element is denoted by 0. Also, the inverse of $a \in G$ is denoted by $-a$. We write $a - b$ for $a + (-b)$. Abelian groups are frequently written additively.

Note that $a^n = \underbrace{aa \ldots a}_{n \text{ times}}$. If $n = -m$ is a negative integer, then we define $a^n = (a^{-1})^m$; also, we define $a^0 = e$. The formulas $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ hold for any element a of G and any pair of integers m and n. One must be careful with this notation when dealing with a specific group whose binary operation is addition. In this case, the definitions and group properties expressed in multiplicative notation must be translated to additive notation. Table 3.1 shows the common notation and corresponding terminology for groups under multiplication and groups under addition.

Corollary 3.45 *In any group G both the cancellation laws hold, i.e.,*

(1) $ab = ac$ implies $b = c$;
(2) $ba = ca$ implies $b = c$.

Proof It is enough to multiply a^{-1} on the left or right side. ■

Theorem 3.46 *Any finite semigroup in which both cancellation laws hold is a group.*

Proof Suppose that G is a finite semigroup with n elements in which both cancellation laws hold and let

$$G = \{x_1, x_2, \ldots, x_n\}.$$

Suppose that $a \in G$ is arbitrary and fixed. Then, the elements $ax_1, ax_2, \ldots, ax_n$ are distinct, because $ax_i = ax_j$ (for some i and j) implies that $x_i = x_j$ (the left cancellation law). Consequently, we have

Table 3.1 Notation and corresponding terminology for groups under multiplication and addition

Multiplicative group		Additive group	
$a \cdot b$ or ab	Multiplicative	$a + b$	Addition
e or 1	Identity	0	Zero
a^{-1}	Multiplicative inverse of a	na	Multiple of a
a^n	Power of a	$a - b$	Difference

$$G = \{ax_1,\ ax_2,\ \ldots, ax_n\}.$$

Hence, for each $x_i \in G$, there exists $x_j \in G$ such that

$$x_i = ax_j. \tag{3.1}$$

In particular, there exists $x_k \in G$ such that $a = ax_k$. Then, $ax_i = (ax_k)x_i = a(x_kx_i)$. Now, by the left cancellation law, we conclude that $x_i = x_kx_i$, for each $1 \leq i \leq n$.

Similarly, by considering the elements x_1a, x_2a, …, x_na and using the right cancellation law, we can find an element $x_l \in G$ such that $x_i = x_ix_l$, for each $1 \leq i \leq n$. So, we get $x_l = x_kx_l = x_k$. Therefore, x_k is the identity element in G. As usual, we set $x_k = e$.

Taking $x_i = e$ in (3.1), then we can say that there exists $x_m \in G$ such that

$$e = ax_m.$$

In a similar way, by considering the elements x_1a, x_2a, …, x_na, we can find an element $a_r \in G$ such that

$$e = x_ra.$$

Thus, we can write

$$x_r = x_re = x_r(ax_m) = (x_ra)x_m = ex_m = x_m.$$

Hence, $x_ma = ax_m = e$, which implies that $x^{-1} = x_m$. This shows that every element in G has its inverse in G. Therefore, G is a group. ■

Corollary 3.47 *A finite semigroup G is a group if and only if G satisfies both cancellation laws.*

Proof The proof follows immediately from Corollary 3.45 and Theorem 3.46. ■

Theorem 3.48 *Let G be a non-empty set together with a binary operation. Then, G is a group if and only if*

(1) $a(bc) = (ab)c$, *for all* $a, b \in G$;
(2) *Given any* $a, b \in G$, *the equations* $ax = b$ *and* $ya = b$ *have unique solutions in* G.

Proof Let G be a group. Since $a(a^{-1}b) = (aa^{-1})b = eb = b$, it follows that $x = a^{-1}b$ is a solution of the equation $ax = b$ in G. Similarly, $y = ba^{-1}$ is a solution of the equation $ya = b$ in G. The uniqueness of the solution follows from the cancellation law.

Suppose that G is a non-empty set together with a binary operation satisfying (1) and (2). In order to show that G is a group we need to show that G contains an identity and each element of G has an inverse.

Let $a \in G$ be an arbitrary element. By (2), since $ax = a$ has solution in G, it

follows that there is an element $e \in G$ such that $ae = a$.

Now, given $b \in G$, then by (2) there exists $y \in G$ such that $b = ya$. Then, $be = (ya)e = y(ae) = ya = b$, and so $be = b$, for each $b \in G$. Similarly, since the equation $ya = a$ has solution in G, it follows that there exists $e' \in G$ such that $e'a = a$. Again, given $b \in G$, by (2) there exists $z \in G$ such that $b = az$. Then, $e'b = e'(az) = (e'a)z = az = b$, and so $e'b = b$, for each $b \in G$. In particular, since $be = b$, for each $b \in G$, it follows that $e'e = e'$. Also, since $e'b = b$, for each $b \in G$, it follows that $e'e = e$. Consequently, $e = e'$ and we get $be = b = eb$, for each $b \in G$. This shows that e is the identity element of G.

Next, we prove the existence of inverse. Let $a \in G$. Then, by (2), there exist $a', a'' \in G$ such that $aa' = e$ and $a''a = e$. Hence, we obtain

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

and we conclude that $a'a = e = aa'$. This yields that $a^{-1} = a$. ■

Theorem 3.49 *Let G be a non-empty set together with a binary operation. Then, G is a group if and only if*

(1) $a(bc) = (ab)c$, for all $a, b \in G$;
(2) There exists an element $e \in G$ such that $ae = a$, for all $a \in G$;
(3) For every $a \in G$, there exists $a' \in G$ such that $aa' = e$.

Proof If G is a group, then by Definition 3.28, the statements (1), (2), and (3) hold.

Now, assume that G is a non-empty set together with a binary operation satisfying (1), (2), and (3). Let $a \in G$. Then, by (3), there is $a' \in G$ such that $aa' = e$. Again, by (3), there exists $a'' \in G$ such that $a'a'' = e$. Hence, we get

$$\begin{aligned} a'a &= (a'a)e = (a'a)(a'a'') = a'(a(a'a'')) = a'((aa')a'') \\ &= a'(ea'') = (a'e)a'' = a'a'' = e. \end{aligned}$$

Consequently, we have $aa' = e = a'a$. In addition, we find that

$$ea = (aa')a = a(a')a = a(a'a) = ae = a,$$

and so $ea = ae = a$. Therefore, we deduce that G is a group. ■

Theorem 3.50 *Let G be a non-empty set together with a binary operation. Then, G is a group if and only if*

(1) $a(bc) = (ab)c$, for all $a, b \in G$;
(2) There exists an element $e \in G$ such that $ea = a$, for all $a \in G$;
(3) For every $a \in G$, there exists $a' \in G$ such that $a'a = e$.

Proof The proof is similar to the proof of Theorem 3.49. ■

The following example shows that the conclusion of Theorems 3.49 and 3.50 fails, if a semigroup S contains a right identity e and each element $a \in G$ may possess a left inverse.

Example 3.51 Let S be a set having at least two elements. For any $x, y \in G$, we define $xy = x$. It is easy to check that S together with this binary operation is a semigroup. Let b and c be two distinct elements of S. Then, for each $a \in S$, we have $ab = ac$, while $b \neq c$. Hence, S does not satisfy cancellation law, and so S is not a group. Now, let e be any fixed element of S. We have

(1) For each $a \in S$, $ae = a$. This means that e is a right identity element;
(2) For each $a \in G$, since $ea = e$, it follows that e is a left inverse of a with respect to e.

Consequently, S has the right identity e and each element of S has a left inverse in S but we know that G is not a group.

We leave it to readers to construct a similar example of a semigroup S which has a left identity and right inverse for each of its elements but it fails to be a group.

Definition 3.52 Let a and b be elements of a group G. We say that a and b are *conjugate* in G (and call b a conjugate of a) if there exists $x \in G$ such that $b = x^{-1}ax$.

We write, for this, $a \sim_{Conj} b$ and refer to this relation as conjugacy.

Theorem 3.53 *Conjugacy is an equivalence relation on G.*

Proof Since $a = e^{-1}ae$, for each $a \in G$, it follows that $a \sim_{Conj} a$, i.e., $\sim_{Conj}$ is reflexive.

If $a \sim_{Conj} b$, then there exists $x \in G$ such that $b = x^{-1}ax$. Hence, $a = (x^{-1})^{-1} bx^{-1}$. Since $x^{-1} \in G$, it follows that $b \sim_{Conj} a$, i.e., $\sim_{Conj}$ is symmetric.

Suppose that $a \sim_{Conj} b$ and $b \sim_{Conj} c$, where $a, b, c \in G$. Then, $b = x^{-1}ax$ and $c = y^{-1}by$, for some $x, y \in G$. Substituting for b in the expression for c we obtain $c = y^{-1}x^{-1}axy$. This shows that $c = (xy)^{-1}a(xy)$. Since $xy \in G$, it follows that $a \sim_{Conj} c$, i.e., $\sim_{Conj}$ is transitive. ■

Theorem 3.53 shows that we can divide a group G into equivalence classes under the relation of conjugacy. Each such equivalence class is called a *conjugate class*.

Exercises

1. Prove that the set of all rational numbers of the form $3^m 6^n$, where m and n are integers, is a group under multiplication.
2. Let $G = \{a \in \mathbb{R} \mid -1 < a < 1\}$. Define a binary operation $\star$ on G by

$$a \star b = \frac{a + b}{1 + ab},$$

for all $a, b \in G$. Show that $(G, \star)$ is a group.

3. Let G be the set of all rational numbers except -1. Show that $(G, \star)$ is a group where
$$a \star b = a + b + ab,$$
for all $a, b \in G$.
4. If a and b are elements of a group G, prove that $ab^n a^{-1} = (aba^{-1})^n$, for each integer n.
5. Show that if every element of the group G is its own inverse, then G is abelian.
6. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.
7. Prove that a finite semigroup G with identity is a group if and only if G contains only one idempotent.
8. Let G be a group.
   (a) If G has three elements, then show that it must be abelian;
   (b) Do part (a) if G has four elements;
   (c) Do part (a) if G has five elements.
9. Consider the set $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Suppose that there is a binary operation $\star$ on G that satisfies the following two conditions:
   (a) $a \star b \leq a + b$, for all $a, b \in G$;
   (b) $a \star a = 0$, for all $a \in G$.

   Construct Cayley table for G. (This group sometimes called *Nim group*).
10. Find an example which shows it is impossible to have $(ab)^{-2} \neq b^{-2}a^{-2}$.
11. In a finite group, show that the number of non-identity elements that satisfy the equation $x^5 = e$ is a multiple of 5. If the stipulation that the group be finite is omitted, what can you say about the number of non-identity elements that satisfy the equation $x^5 = e$?
12. For each positive integer n, prove that the number of groups of order n is finite.
13. Let G be a group in which $(ab)^n = a^n b^n$ for some fixed integer $n > 1$ and for all $a, b \in G$. For all $a, b \in G$, prove that
   (a) $(ab)^{n-1} = b^{n-1}a^{n-1}$;
   (b) $a^n b^{n-1} = b^{n-1}a^n$;
   (c) $(aba^{-1}b^{-1})^{n(n-1)} = e$.
14. In Theorem 3.46 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.
15. Show that in Theorem 3.46 infinite examples exist, satisfying the conditions which are not groups.
16. Show that the equation $x^2 ax = a^{-1}$ has a solution for x in a group G if and only if a is the cube of some element in G.

3.5 Turning Groups into Latin Squares (Optional)

The name "Latin square" was inspired by mathematical papers by Leonhard Euler (1707–1783), who used Latin characters as symbols, but any set of symbols can be used.

Definition 3.54 A *Latin square* is an $n \times n$ table filled with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column.

Example 3.55 The following are two examples of Latin squares.

1	2	3
2	3	1
3	1	2

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

Theorem 3.56 *Cayley table of any finite group is a Latin square.*

Proof Take a row indexed by the group element a. Suppose that two elements in this row are equal. In other words, there are two columns c and d such that $ac = ad$. If we multiply by a^{-1} on the left, this gives us $c = d$, i.e., these were in fact the same columns, and therefore, there are no repetitions in this row. The same logic tells us that there are also no repetitions in any column; therefore, this is a Latin square. ■

A natural question is: which Latin squares are Cayley tables of groups?

Many of the group axioms for the operation $\cdot$ of a finite group can be checked by referring to the Cayley table for the group. From the table, one can quite easily check the existence of an identity element and observe that each group element occurs exactly once in each row and each column. The only group property that is difficult to check directly from the properties of the Cayley table is associativity. It must be shown that $(ab)c = a(bc)$ for all elements a, b, and c of the group, and to check this property case by case is quite tedious. If the group contains n elements, there are n^3 ordered triple (a, b, c) that must be considered with $(ab)c$ and $a(bc)$ checked for equality in each case.

The following theorem may simplify the verification of the associative law for multiplication.

Theorem 3.57 *Let G be a finite group. Let r and s be in the array representing the Cayley table for G such that the column containing r and the row containing s intersect at the identity element e. Then, rs is the element at the fourth corner of the rectangle formed by r, s, and e.*

Proof The identity element e occurs exactly once in each row and in each column, so suppose that e of the theorem is in the row headed by q and in the column headed

by b. Then, r occurs exactly once in the column headed by b, say in the row headed by p; so s occurs exactly once in the row headed by q, say in the column headed by a.

$\cdot$	a	b
p		r
q	s	e

Thus, $pb = r$, $qa = s$, and $qb = e$. We wish to show that the fourth corner pa of the rectangle formed by r, s, and e is rs. We have

$$rs = (pb)(qa) = p(bq)a.$$

The last equality is a result of the associativity law present in the group G. However, qb is the identity; thus bq is the identity element.

It follows that $rs = pea = pa$. ■

The rule stated in Theorem 3.57 is called the *rectangle rule*.

Since we wish to emphasize that the rectangle rule follows from the associative law, Theorem 3.57 could be stated as follows:

Suppose that G is a system with identity element e such that each group element occurs exactly once in each row and in each column of the Cayley table; then the rectangle rule is a consequence of Gs having the associative property.

Suppose that we number the rows and columns from 1 to n and let a_{ij} be the element in the ith row and jth column. Suppose that $r = a_{ik}$ and $s = a_{jt}$. Then, $pa = a_{it}$ since pa is the same row as r in the same column as s. Also, $e = a_{jk}$ since e is in the same column as r and in the same row as s. The rectangle rule $pa = rs$ now becomes the following:

If $e = a_{jk}$, then $a_{it} = a_{ik}a_{jt}$, for all i and t. The table

$\cdot$	a	b
p	rs	r
q	s	e

now takes the form

$\cdot$	a	b
p	a_{it}	a_{ik}
q	a_{jt}	a_{jk}

Theorem 3.58 *Suppose that G is a system with identity element e and with the following properties:*

(1) The Cayley table is a Latin square. In other words, each element of G occurs exactly once in each row and in each column;

(2) The rectangle rule holds.

Then, the operation obeys the associative law.

Fig. 3.6 Rectangle A

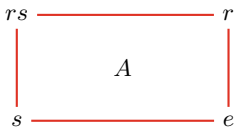


Fig. 3.7 Rectangle B

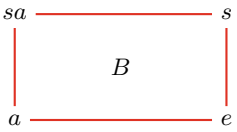


Fig. 3.8 Rectangles A and B together

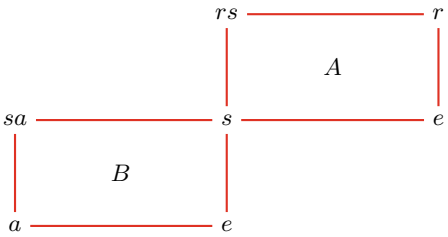
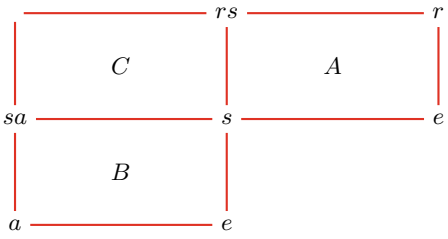


Fig. 3.9 Rectangles A B and C together



Proof Let r, s, and a be elements of G. By (1), e occurs in each column, so pick an e in the table. By (1), we can locate the r in the column containing e and the s in the row containing e. By (2), we know that the element in the fourth corner of the rectangle A is rs, see Fig. 3.6.

By (1), we can find the e in the column containing the above mentioned s. By (1), a can be located in the row containing this e. By (2), the element in the fourth corner of rectangle B is sa, see Fig. 3.7. Rectangles A and B fit together to form Fig. 3.8. We see that a new rectangle C is formed with three of the corners labeled sa, s, and rs, see Fig. 3.9. By (2), the element in the fourth corner of rectangle C union A is $r(sa)$. By (2), the element in the fourth corner of rectangle C union B is $(rs)a$. But these corners are the same. Consequently, we obtain $r(sa) = (rs)a$. ■

Example 3.59 Consider the following table:

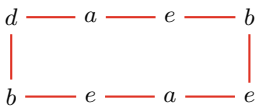


Fig. 3.10 Rectangle related to Example 3.59

·	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

This table is a Latin square, but rectangle rule does not hold as $bb \neq d$ in the rectangle in Fig. 3.10.

The operation does not have the associative property, because $(ab)c = a$ and $a(bc) = c$.

Another method of verifying the associative law is to use permutations. We shall study this method in the future.

Exercises

1. Show that the number of $n \times n$ Latin squares is 1, 2, 12, 576 for $n = 1,\ 2,\ 3,\ 4$, respectively.
2. Which of the following Latin squares are Cayley tables of groups?

1	2	3	4	5
2	5	4	1	3
3	1	2	5	4
4	3	5	2	1
5	4	1	3	2

1	2	3	4	5
2	4	1	5	3
3	1	5	2	4
4	5	2	3	1
5	3	4	1	2

3. Suppose the following is the Cayley table of a group G. Fill in the blank entries.

·	e	a	b	c	d
e	e	–	–	–	–
a	–	b	–	–	e
b	–	c	d	e	–
c	–	d	–	a	b
d	–	–	–	–	–

3.6 Subgroups

In general, we shall not be interested in arbitrary subsets of a group G because they do not reflect that G has an algebraic structure imposed on it. So, we are interested in special subsets of a group, called "subgroups". The concept of subgroup is one of the most basic ideas in group theory.

Definition 3.60 A non-empty subset H of a group G is called a *subgroup* of G if relative to the operation in G, H itself forms a group.

Let e be the identity element of a group G. Then, trivially G and $\{e\}$ are subgroups of G. These subgroups are called *trivial subgroups* of G. A subgroup H of G is called a *proper subgroup* if it is different from G as well as from $\{e\}$. We denote the relation "H is a subgroup of G" by $H \leq G$.

It would be useful to have some criterion for deciding whether a given subset of a group is a subgroup.

Theorem 3.61 (Two-Step Subgroup Test) *A non-empty subset H of the group G is a subgroup if and only if*

(a) $a, b \in H$ *implies* $ab \in H$*;*
(b) $a \in H$ *implies* $a^{-1} \in H$.

Proof If H is a subgroup of G, then it is obvious that (1) and (2) must hold.

Conversely, suppose that H is a subset of G for which (1) and (2) hold. In order to establish that H is a subgroup, all that is needed is to verify that $e \in H$ and that the associative law holds for elements of H. Since the associative law does hold for G, it holds all the more so for H, which is a subset of G. Now, if $a \in H$, then by (2), $a^{-1} \in H$. Next, since $a \in H$ and $a^{-1} \in H$, by (1), it follows that $e = aa^{-1} \in H$. This yields that H is a subgroup of G.. ■

Theorem 3.62 (One-Step Subgroup Test) *A non-empty subset H of the group G is a subgroup if and only if*

$$a, b \in H \text{implies } ab^{-1} \in H.$$

Proof Let H be a subgroup of G and let $a, b \in H$. By Theorem 3.61 (2), we conclude that $b^{-1} \in H$. Now, since $a, b^{-1} \in H$, by Theorem 3.61 (1), it follows that $ab^{-1} \in H$.

Conversely, let H be a non-empty subset of G such that $ab^{-1} \in H$, for all $a, b \in H$. Since H is non-empty, it follows that there exists $x \in H$. So, $e = xx^{-1} \in H$. Now, suppose that a and b are two arbitrary elements of H. As $a, e \in H, ea^{-1} \in H$, i.e., $a^{-1} \in H$. Next, since $a, b \in H$, it follows that $b^{-1} \in H$ and $a(b^{-1})^{-1} \in H$. This implies that $ab \in H$. Therefore, by Theorem 3.61, we conclude that H is a subgroup of G. ■

Theorem 3.63 (Finite Subgroup Test) *If H is a non-empty finite subset of a group G, then H is a subgroup of G if*

$$a, b \in H implies ab \in H.$$

Proof In light of Theorem 3.61, we need to prove that $a^{-1} \in H$ whenever $a \in H$. Assume that a is an arbitrary element of H. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, then the set $\{a,\ a^2,\ a^3, \ldots\}$ is a subset of H. Since H is finite, there must be repetition in this set of elements, i.e., for some positive integers i and j, $a^i = a^j$ with $i > j > 0$. Then, by the cancellation law in G, $a^{i-j} = e$, and since $a \neq e, i - j > 1$. Hence, we can write $a^{i-j} = aa^{i-j-1} = e$, and consequently $a^{i-j-1} = a^{-1}$. But $i - j - 1 \geq 1$ implies $a^{i-j-1} \in H$ and we are done. ■

Example 3.64 Let $\mathbb{R}$ be the group of all real numbers under addition, and let $\mathbb{Z}$ be the set of all integers. Then, $\mathbb{Z}$ is a subgroup of $\mathbb{R}$.

Example 3.65 Let $\mathbb{R}^*$ be the group of all non-zero real numbers under ordinary multiplication, and let $\mathbb{Q}^+$ be the set of positive rational numbers. Then, $\mathbb{Q}^+$ is a subgroup of $\mathbb{R}^*$.

Example 3.66 Let $\mathbb{C}^*$ be the group of all non-zero complex numbers under multiplication, and let $H = \{a + bi \mid a^2 + b^2 = 1\}$. Then, H is a subgroup of $\mathbb{C}^*$.

Example 3.67 Let G be an abelian group. Then, $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

The following remark is clear.

Remark 3.68 If H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.

Example 3.69 Suppose that $H = \{1,\ -1,\ i,,\ -i\}$ and $K = \{1,\ -1\}$, where $i^2 = -1$. Then, H is a subgroup of $\mathbb{C}^*$, the group of non-zero complex numbers under multiplication, and K is a subgroup of H. So, we can say that K is a subgroup of $\mathbb{C}^*$.

Example 3.70 Consider the group of integers $\mathbb{Z}$ with ordinary addition. Then, the set

$$n\mathbb{Z} = \{\ldots,\ -3n,\ -2n,\ -n,\ 0,\ n,\ 2n,\ 3n,\ \ldots\}$$

for each positive integer n is a subgroup of $\mathbb{Z}$.

Example 3.71 Let G be the group defined in Example 3.41. Let H be the subset of G consisting of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $ad - bc = 1$. Then, as easily verified, H is a subgroup of G.

Example 3.72 Let $C_{12} = \{e = a^0,\ a^1,\ a^2,\ \ldots,\ a^{11}\}$. We define a binary operation on C_{12} as follows:

$$a^i a^j = \begin{cases} a^{i+j} & \text{if } i + j < 12 \\ a^{i+j-12} & i + j \geq 12. \end{cases}$$

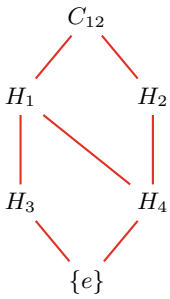


Fig. 3.11 Hasse diagram for the family of subgroups of C_{12}

It is easy to see that C_{12} is a group under the above multiplication. Moreover, all of the subgroups of C_{12} are as follows:

$$\begin{aligned}
&\{e\},\ G,\\
&H_1 = \{e,\ a^2,\ a^4,\ a^6,\ a^8,\ a^{10}\},\\
&H_2 = \{e,\ a^3,\ a^6,\ a^9\},\\
&H_3 = \{e,\ a^4,\ a^8\}\\
&H_4 = \{e, a^6\}.
\end{aligned}$$

In Fig. 3.11, we illustrate Hasse diagram for subgroups of C_{12}.

Example 3.73 Let G be any group and H be a subgroup of G. For $a \in G$, let

$$a^{-1}Ha = \{a^{-1}ha \mid h \in H\}.$$

We assert that $a^{-1}Ha$ is a subgroup of G. Let x and y be two arbitrary elements of $a^{-1}Ha$. Then, $x = a^{-1}ha$ and $y = a^{-1}h'a$, for some $h, h' \in H$. Thus, we obtain

$$xy^{-1} = (a^{-1}ha)(a^{-1}h'a)^{-1} = (a^{-1}ha)(a^{-1}h'^{-1}a) = a^{-1}hh'^{-1}a.$$

Since $h, h' \in H$ and H is a subgroup of G, it follows that $hh'^{-1} \in H$. This shows that $xy^{-1} \in a^{-1}Ha$, and so $a^{-1}Ha$ is a subgroup of G.

Theorem 3.74 *If G is a group and $\{H_i \mid i \in I\}$ is a non-empty family of subgroups of G, then*

$$\bigcap_{i \in I} H_i$$

is a subgroup of G.

Proof Suppose that a and b are two elements of $\bigcap_{i \in I} H_i$. Then, $a, b \in H_i$, for all $i \in I$. Since for each $i \in I$, H_i is a subgroup of G, it follows that $ab^{-1} \in H_i$, for all $i \in I$. Hence, we conclude that $ab^{-1} \in \bigcap_{i \in I} H_i$. This shows that $\bigcap_{i \in I} H_i$ is a subgroup of G. ■

In particular, the intersection of two subgroups of a group is a subgroup. The following example shows that the union of two subgroups of a group is not a subgroup, in general.

Example 3.75 Suppose that $G = \mathbb{Z}$. We know that $H_1 = 2\mathbb{Z}$ and $H_2 = 3\mathbb{Z}$ are subgroups of G. We have

$$2 \in H_1 \subseteq H_1 \cup H_2 \text{ and } 3 \in H_2 \subseteq H_1 \cup H_2,$$

while $2 + 3 = 5 \notin H_1 \cup H_2$. So, $H_1 \cup H_2$ cannot be a subgroup of G.

Definition 3.76 (*Center of a Group*) The *center* $Z(G)$ of a group G is the subset of elements in G that commute with every element of G, i.e.,

$$Z(G) = \{a \in G \mid ax = xa, \text{ for all } x \in G\}.$$

Theorem 3.77 *The center of a group G is a subgroup of G.*

Proof We use Theorem 3.61 to prove this result. Since $e \in Z(G)$, it follows that $Z(G)$ is non-empty. Now, assume that a and b be two arbitrary elements of $Z(G)$. Then, we have

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab),$$

for all $x \in G$. Thus, $ab \in Z(G)$. Also, we have

$$\begin{aligned} xa^{-1} &= exa^{-1} = (a^{-1}a)xa^{-1} = a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \\ &= a^{-1}x(aa^{-1}) = a^{-1}xe = a^{-1}x, \end{aligned}$$

for all $x \in G$. This shows that $a^{-1} \in Z(G)$ whenever $a \in Z(G)$. ■

Corollary 3.78 *If G is an abelian group, then $Z(G) = G$.*

Definition 3.79 Let X be a fixed non-empty subset of a group G. The *centralizer of X in G*, $C_G(X)$, is the set of all elements in G that commute with elements of X, i.e.,

$$C_G(X) = \{a \in G \mid ax = xa, \text{ for all } x \in X\}.$$

Theorem 3.80 *The centralizer of a non-empty subset of a group G is a subgroup of G.*

Proof The proof is similar to the proof of Theorem 3.77 and it is left to the reader. ■

If $X = \{x\}$, then we write $C_G(x)$ instead of $C_G(\{x\})$. In this case, $C_G(x)$ is the set of all elements in G that commute with x.

Corollary 3.81 *We have*

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

Proof It is straightforward. ■

Theorem 3.82 *Let H_1 and H_2 be two subgroups of G. Then, $H_1 \cup H_2$ is a subgroup of G if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.*

Proof If $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$, then it is clear that $H_1 \cup H_2$ is a subgroup of G.

Conversely, let $H_1 \cup H_2$ be a subgroup of G. We prove by contradiction method. Suppose that $H_1 \nsubseteq H_2$ and $H_2 \nsubseteq H_1$. Then, there exist $x \in H_1 - H_2$ and $y \in H_2 - H_1$. So, we conclude that $x^{-1} \in H_1$, $y^{-1} \in H_2$ and $x, y \in H_1 \cup H_2$. Since $H_1 \cup H_2$ is a subgroup, it follows that $xy \in H_1 \cup H_2$. This implies that $xy \in H_1$ or $xy \in H_2$. If $xy \in H_1$, then $y = x^{-1}(xy) \in H_1$, and this is a contradiction. Similarly, if $xy \in H_2$, then $x = (xy)y^{-1} \in H_2$, and this is again a contradiction. Therefore, we deduce that $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$. ■

Corollary 3.83 *If $\{H_i \mid i \in I\}$ is a chain of subgroups of a group G, then $\bigcup_{i \in I} H_i$ is a subgroup of G.*

Exercises

1. If G is an abelian group and if $H = \{a \in G \mid a^2 = e\}$, show that H is a subgroup of G.
2. Give an example of a non-abelian group for which the H in Exercise 1 is not a subgroup.
3. Let G be an abelian group, fix a positive integer n. Let $H = \{a^n \mid a \in G\}$. Show that H is a subgroup of G.
4. In Example 3.43, let $H = \{T_{a,b} \in G \mid a \text{ is rational}\}$. Show that H is a subgroup of G.
5. If H is a subgroup of G, let

$$N = \bigcap_{x \in G} x^{-1} H x.$$

   Prove that N is a subgroup of G such that $a^{-1}Na = N$, for all $a \in G$.
6. If H is a subgroup of G such that $a^{-1}Ha \subseteq H$, for all $a \in G$, prove that actually $a^{-1}Ha = H$.
7. Let H and K be two subgroups of G such that $a^{-1}Ha = H$ and $a^{-1}ka = K$, for all $a \in G$. If $H \cap K = \{e\}$, prove that $hk = kh$, for any $h \in H$ and $k \in K$.
8. For a non-empty subset X of a group G, define

$$X^k = \left\{ \prod_{i=1}^{k} x_i \mid x_i \in X \right\},$$

for any positive integer k. Prove that if G has n element, then X^n is a subgroup of G.

9. Let G be a group, and let $a \in Z(G)$. In a Cayley table for G, how does the row headed by a compare with the column headed by a? Is the converse of your answer true?
10. Show that $x \in Z(G)$ if and only if $C_G(x) = G$.
11. Let $x, y \in G$ and let $xy = z$ if $z \in Z(G)$. Show that x and y commute.
12. If G is a group and $a, c \in G$, prove that

$$C_G(a^{-1}xa) = a^{-1}C_G(x)a.$$

13. Let G be a group and X be a non-empty subset of G. The set

$$N_G(X) = \{a \in G \mid a^{-1}Xa = X\}$$

is called the *normalizer of X in G*. If H is a subgroup of G, prove that

(a) $N_G(H)$ is a subgroup of G;
(b) $H \leq N_G(H)$.

14. Give an example of a group G and a subgroup H such that $N_G(H) \neq C_G(H)$. Is there any relation between $N_G(H)$ and $C_G(H)$?

3.7 Worked-Out Problems

Problem 3.84 Let G be the group defined in Example 3.41. Find the center of G.

Solution Suppose that $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an arbitrary element in the center of G. So, this matrix commutes with all elements of G. Since $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in G$, it follows that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

and so $a = d$ and $b = c$. Similarly, since $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in G$, it follows that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Hence, we get

$$\begin{bmatrix} a & a+b \\ b & b+a \end{bmatrix} = \begin{bmatrix} a+b & b+a \\ b & a \end{bmatrix}.$$

This implies that $b = 0$. Therefore, each element of the center of G is in the form

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix},$$

where $a \neq 0$. On the other hand, it is easy to check that for each non-zero real number a, the matrix $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$ belongs to the center of G. Consequently, we have

$$Z(G) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{R},\ a \neq 0 \right\},$$

and we are done. ■

Problem 3.85 Let $S = \mathbb{N}^0 \times \mathbb{N}^0$. On S we define a binary operation

$$(a, b) \star (c, d) = \big(a - b + \max\{b, c\}, d - c + \max\{b, c\}\big).$$

Prove that $(S, \star)$ is a monoid with identity $(0, 0)$. This monoid is called *Bicycle semigroup/monoid*.

Solution Suppose that $(a, b), (c, d) \in S$. Then, we have $\max\{b, c\} - b \geq 0$ and $\max\{b, c\} - c \geq 0$. So, we get $a - b + \max\{b, c\} \geq a$ and $d - c + \max\{b, c\} \geq d$. Consequently, $(a - b + \max\{b, c\}, d - c + \max\{b, c\} \in S$, and hence the multiplication is closed. Clearly, $(0, 0) \in S$ and for any $(a, b) \in S$ we have

$$\begin{aligned} (0, 0) \star (a, b) &= \big(0 - 0 + \max\{0, a\}, b - a + \max\{0, a\}\big) \\ &= (a, b) = (a, b) \star (0, 0). \end{aligned}$$

Hence, $(0, 0)$ is the identity element of S. Now, we verify the associativity. Assume that (a, b), (c, d) and (e, f) are arbitrary elements of S. Then, we have

$$\begin{aligned} &\big((a, b) \star (c, d)\big) \star (e, f) \\ &= \big(a - b + \max\{b, c\}, d - c + \max\{b, c\}\big) \star (e, f) \\ &= \big(a - b - d + c + \max\{d - c + \max\{b, c\}, e\}, \\ &\quad f - e + \max\{d - c + \max\{b, c\}, e\}, e\}\big) \end{aligned}$$

and

$$\begin{aligned} &(a, b) \star \big((c, d) \star (e, f)\big) \\ &= (a, b) \star \big(c - d + \max\{d, e\},\ f - e + \max\{d, e\}\big) \\ &= \big(a - b + \max\{b, c - d + \max\{d, e\}\}, \\ &\quad f - e - c + d + \max\{b, c - d + \max\{d, e\}\}\big). \end{aligned}$$

Now, we must show that

$$a - b - d + c + \max\{d - c + \max\{b, c\}, e\} = a - b + \max\{b, c - d + \max\{d, e\}\}, \tag{3.2}$$

and

$$f - e + \max\{d - c + \max\{b, c\}, e\} = f - e - c + d + \max\{b, c - d + \max\{d, e\}\}. \tag{3.3}$$

Equations (3.2) and (3.3) are the same, and so we only need to show that

$$-d + c + \max\{d - c + \max\{b, c\}, e\} = \max\{b, c - d + \max\{d, e\}\}.$$

But this equality is equivalent to

$$\max\{\max\{b, c\}, c - d + e\} = \max\{b, c - d + \max\{d, e\}\},$$

and this equality holds, because

$$\begin{aligned}\max\{b, c - d + \max\{d, e\}\} &= \max\{b, \max\{c - d + d, c - d + e\}\} \\ &= \max\{b, \max\{c, c - d + e\}\} \\ &= \max\{b, c, c - d + e\} \\ &= \max\{\max\{b, c\}, c - d + e\}.\end{aligned}$$

Therefore, the multiplication is associative and hence S is a monoid. ■

Problem 3.86 Let G be a group and $a_0 \in G$. Define a new binary operation $*$ on G such that $(G, *)$ is a group with a_0 as its identity.

Solution We define $*$ on G as follows:

$$x * y = x a_0^{-1} y,$$

for all $x, y \in G$. Let x, y, and z be arbitrary elements of G. Then, we can write

$$\begin{aligned}(x * y) * z = (x a_0^{-1} y) * z = x a_0^{-1} y a_0^{-1} z = x a_0^{-1} (y a_0^{-1} z) \\ = x * (y a_0^{-1} z) = x * (y * z).\end{aligned}$$

Hence, the associative law holds.

For any $x \in G, x * a_0 = x a_0^{-1} a_0 = xe = x$, where e is the identity of G. Similarly, $a_0 * x = a_0 a_0^{-1} x = ex = x$. This shows that a_0 is the identity element of G with respect to $*$.

Next, let $x \in G$. Then, we have $x * (a_0 x^{-1} a_0) = x a_0^{-1} a_0 x^{-1} a_0 = a_0$. Also, we have $(a_0 x^{-1} a_0) * x = a_0 x^{-1} a_0 a_0^{-1} x = a_0$. Hence, $a_0 x^{-1} a_0$ is the inverse of x with respect to $*$.

Therefore, $(G, *)$ is a group with a_0 as its identity. ■

Problem 3.87 Let G be a group and m, n be relatively prime positive integers such that

$$a^m b^m = b^m a^m \text{ and } a^n b^n = b^n a^n.$$

for all $a, b \in G$. Prove that G is abelian.

Solution Since $(m, n) = 1$, it follows that there exist integers x and y such that $mx + ny = 1$. Then, we have

$$\begin{aligned}
(a^m b^n)^{mx} &= (a^m b^n)(a^m b^n)\ldots(a^m b^n) \\
&= a^m\big((b^n a^m)(b^n a^m)\ldots(b^n a^m)\big)b^n \\
&= a^m (b^n a^m)^{mx}(b^n a^m)^{-1} b^n \\
&= a^m (b^n a^m)^{mx} a^{-m} b^{-n} b^n \\
&= a^m (b^n a^m)^{mx} a^{-m} \\
&= a^m \big((b^n a^m)^x\big)^m a^{-m} \\
&= \big((b^n a^m)^x\big)^m a^m a^{-m} \\
&= (b^n a^m)^{mx}.
\end{aligned}$$

This shows that

$$(a^m b^n)^{mx} = (b^n a^m)^{mx}. \tag{3.4}$$

In a similar way, we see that

$$(a^m b^n)^{ny} = (b^n a^m)^{ny}. \tag{3.5}$$

From (3.4) and (3.5), we obtain

$$a^m b^n = (a^m b^n)^{mx+ny} = (b^n a^m)^{mx+ny} = b^n a^m.$$

Finally, we can write

$$\begin{aligned}
ab &= a^{mx+ny} b^{mx+ny} = a^{mx}(a^{ny} b^{mx}) b^{ny} \\
&= a^{mx} b^{mx} a^{ny} b^{ny} = b^{mx} a^{mx} b^{ny} a^{ny} \\
&= b^{mx} b^{ny} a^{mx} a^{ny} = b^{mx+ny} a^{mx+ny} = ba.
\end{aligned}$$

This completes the proof. ■

Problem 3.88 If G is a group in which

$$(ab)^k = a^k b^k \tag{3.6}$$

for three constructive integers k and for all $a, b \in G$, show that G is abelian.

Solution Suppose that (3.6) is true for n, $n + 1$, and $n + 2$, where n is an integer, i.e.,

$$\begin{aligned}
(ab)^n &= a^n b^n, \\
(ab)^{n+1} &= a^{n+1} b^{n+1}, \\
(ab)^{n+2} &= a^{n+2} b^{n+2}.
\end{aligned}$$

Then, we obtain

$$a^{n+1}b^{n+1} = (ab)^{n+1} = (ab)^n ab = a^n b^n ab.$$

By cancellation law, we get

$$ab^n = b^n a. \tag{3.7}$$

On the other hand, we have

$$a^{n+2}b^{n+2} = (ab)^{n+2} = (ab)^n (ab)^2 = a^n b^n abab.$$

Again, by cancellation law, we obtain

$$a^2 b^{n+1} = b^n aba. \tag{3.8}$$

From (3.7) and (3.8), we have

$$a^2 b^{n+1} = b^n aba = ab^n ba = ab^{n+1} a.$$

This yields that

$$ab^{n+1} = b^{n+1} a. \tag{3.9}$$

Now, from (3.7) and (3.9), we conclude that $ab^{n+1} = b^{n+1}a = bb^n a = bab^n$. This shows that $ab = ba$. ■

3.8 Supplementary Exercises

1. Let G be the set of all real 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that G forms a group under matrix multiplication.
2. Let G be the set of all real 2×2 matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?
3. Let G be the set of all real 2×2 matrices $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$, where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.
4. A semigroup S is called *regular* if for each $y \in S$ there exists $a \in S$ such that $yay = y$. Let S be a semigroup with at least three elements and $x \in S$ is such that $S \setminus \{x\}$ is a group. Prove that S is regular if and only if $x^2 = x$.
5. Let $x_1, x_2, \ldots, x_n$ be elements of a group G. Prove that there are

$$\frac{(2n-2)!}{n!(n-1)!}$$

ways of evaluating the product of $x_1, x_2, \ldots, x_n$ in that order. All these ways yield the same group element which can thus be denoted unambiguously by $x_1 x_2 \ldots x_n$.

6. Let G be a finite group. Show that there are an odd number of elements x of G such that $x^3 = e$. Show that there are an even number of elements y of G such that $y^2 \neq e$.
7. Let G be a group with an odd number of elements. Prove that for each $a \in G$, the equation $x^2 = a$ has a unique solution.
8. Show that the conclusion of Problem 3.88 does not follow if we assume the relation $(ab)^k = a^k b^k$ for just two constructive integers.
9. Let G be a group, $a, b \in G$ and m, n be two integers.
   (a) If $b^{-1}ab = a^m$, show that $b^{-1}a^n b = a^{mn}$ and $b^{-n}ab^n = a^{m^n}$;
   (b) If $a^{-1}b^2 a = b^3$ and $b^{-1}a^2 b = a^3$, prove that $a = b = e$.
10. Let G be the set of all positive rational numbers of the form

$$\frac{a^2 + b^2}{c^2 + d^2},$$

where a, b, c, and d are integers. Is G a group, being ordinary multiplication?

11. A group G satisfies the *ascending chain condition (ACC) on subgroups* if every ascending sequence

$$H_1 \leq H_2 \leq \ldots$$

of subgroups must eventually be constant, that is, if there is an $n > 0$ such that $H_{n+k} = H_n$ for all $k > 0$. A group G satisfies the *maximal condition on subgroups* if every non-empty family of subgroups has a maximal member. Prove that a group G satisfies the maximal condition on subgroups if and only if it satisfies the ascending chain condition on subgroups.

12. Let G be a group of order n and let m be an integer relatively prime to n. Show that if $x^m = y^m$, then $x = y$. Hence show that for each $z \in G$ there is a unique $x \in G$ such that $x^m = z$.