Chapter 2
Groups: Introductory Concepts

Groups serve as one of the fundamental building blocks for the subject called today modern algebra. This chapter gives an introduction to the group theory and closely related topics. The idea of group theory was used as early as 1770 by J.L. Lagrange (1736–1813). Around 1830, E. Galois (1811–1832) extended Lagrange's work in the investigation of solutions of equations and introduced the term 'group'. At that time, mathematicians worked with groups of transformations. These were sets of mappings that, under composition, possessed certain properties. Originally, group was a set of permutations (i.e., bijections) with the property that the combination of any two permutations again belongs to the set. Felix Klein (1849–1925) adopted the idea of groups to unify different areas of geometry. In 1870, L. Kronecker (1823–1891) gave a set of postulates for a group. Earlier definitions of groups were generalized to the present concept of an abstract group in the first decade of the twentieth century, which was defined by a set of axioms. The theory of abstract groups plays an important role in the present day mathematics and science. Groups arise in a number of apparently unrelated disciplines. They appear in algebra, geometry, analysis, topology, physics, chemistry, biology, economics, computer science etc. So the study of groups is essential and very interesting. In this chapter, we make an introductory study of groups with geometrical applications along with free abelian groups and structure theorem for finitely generated abelian groups. Moreover, semigroups, homology groups, cohomology groups, topological groups, Lie groups, Hopf groups, and fundamental groups are discussed.

2.1 Binary Operations

Operations on the pairs of elements of a non-empty set arise in several contexts, such as the usual addition of two integers, usual addition of two residue classes in $\mathbf{Z}_n$, usual multiplication of two real or complex square matrices of the same order and similar others. In such cases, we speak of a binary operation. The concept of binary operations is essential in the study of modern algebra. It provides algebraic structures on non-empty sets. The concept of binary operations is now introduced.

M.R. Adhikari, A. Adhikari, *Basic Modern Algebra with Applications*,
DOI 10.1007/978-81-322-1599-8_2, © Springer India 2014

Definition 2.1.1 Let S be a non-empty set. A *binary operation* on S is a function $f : S \times S \to S$.

There are several commonly used notations for the image $f(a, b) \in S$ for $a, b \in S$, such as ab or $a \cdot b$ (multiplicative notation), $a + b$ (additive notation), $a * b$ etc. We may therefore think the usual addition in $\mathbf{Z}$, as being a function: $\mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, where the image of every pair of integers $(m, n) \in \mathbf{Z} \times \mathbf{Z}$ is denoted by $m + n$. Clearly, a binary operation '$\cdot$' on S is equivalent to the statement: if $a, b \in S$, then $a \cdot b \in S$ (known as the *closure axiom*). In this event S is said to be closed under '$\cdot$'. There may be several binary operations on a non-empty set S. For example, usual addition $(a, b) \mapsto a + b$; usual multiplication $(a, b) \mapsto ab$; $(a, b) \mapsto$ maximum $\{a, b\}$, minimum $\{a, b\}$, lcm $\{a, b\}$, gcd $\{a, b\}$ for $(a, b) \in \mathbf{N}^+ \times \mathbf{N}^+$ are binary operations on $\mathbf{N}^+$.

A binary operation on a set S is sometimes called a *composition in* S.

Example 2.1.1 Two binary operations, called addition and multiplication are defined on $\mathbf{Z}_n$ (see Chap. 1) by $((a), (b)) \mapsto (a + b)$ and $((a), (b)) \mapsto (ab)$, respectively. Clearly, each of these operations is independent of the choice of representatives of the classes and hence is well defined.

Example 2.1.2 Let S be any non-empty set. Then

(i) both union and intersection of two subsets of S define binary operations on $\mathcal{P}(S)$, the power set of S;

(ii) the usual composition '$\circ$' of two mappings of $M(S)$, the set of all mappings of S into S, is a binary operation on $M(S)$ i.e., $(f, g) \mapsto f \circ g$, $f, g \in M(S)$, defines a binary operation on $M(S)$.

Clearly, $f \circ g \neq g \circ f$, $f, g \in M(S)$ for an arbitrary set S.

For example, if $S = \{1, 2, 3\}$ and $f, g \in M(S)$ are defined by

$$\begin{aligned} f(s) &= 1 \quad \forall s \in S \quad \text{and} \quad g(s) = 2 \quad \forall s \in S, \quad \text{then } (g \circ f)(s) = g\big(f(s)\big) \\ &= g(1) = 2 \quad \text{and} \quad (f \circ g)(s) = f\big(g(s)\big) = f(2) = 1, \quad \forall s \in S \\ &\Rightarrow \quad g \circ f \neq f \circ g. \end{aligned}$$

We may construct a table called the *Cayley table* as a convenient way of defining a binary operation only on a finite set S or tabulating the effect of a binary operation on S. Let S be a set with n distinct elements. To construct a table, the elements of S are arranged horizontally in a row, called initial row or 0-row: these are again arranged vertically in a column, called the initial column or 0-column. The element in the ith position in the 0-column determines a horizontal row across it, called the ith row of the table.

Similarly, the element in the jth position in the 0-row determines a vertical column below it, called the jth column of the table. The (i, j)th position in the table is determined by the intersection of the ith row and the jth column.

The (i, j)th positions $(i, j = 1, 2, \ldots, n)$ are filled up by elements of S in any manner. Accordingly, a binary operation on S is determined.

For two elements $u, v \in S$, where u occupies ith position in the 0-column and v occupies jth position in the 0-row, $(u, v) \mapsto u \circ v$, where $u \circ v$ is the element in the (i, j)th position, $i, j = 1, 2, 3, \ldots, n$.

There is also a reverse procedure: given a binary operation f on a finite set S, we can construct a table displaying the effect of f. For example, let $S = \{1, 2, 3\}$ and f a binary operation on S defined by

$$f(1,1) = 1, \quad f(1,2) = 1, \quad f(1,3) = 2, \quad f(2,1) = 2, \quad f(2,2) = 3,$$
$$f(2,3) = 3, \quad f(3,1) = 1, \quad f(3,2) = 3, \quad f(3,3) = 2.$$

Then the corresponding table is

f :	1	2	3
1	1	1	2
2	2	3	3
3	1	3	2

A table of this kind is termed a *multiplication table or composition table* or *Cayley's table* on S.

Definition 2.1.2 A groupoid is an ordered pair $(S, \circ)$, where S is a non-empty set and '$\circ$' is a binary operation on S and a non-empty subset H of S is said to be a subgroupoid of $(S, \circ)$ iff $(H, \circ_H)$ is a groupoid, where $\circ_H$ is the restriction of '$\circ$' to $H \times H$.

Supplementary Examples (SE-IA)

1 Let $\mathbf{R}$ be the set of all real numbers and $\mathbf{R}^* = \mathbf{R} - \{0\}$.

(i) Define a binary operation $\circ$ on $\mathbf{R}^*$ by $x \circ y = |x|y$. Then $(x \circ y) \circ z = x \circ (y \circ z)$ for all $x, y, z \in \mathbf{R}^*$ but $x \circ y \neq y \circ x$ for some $x, y \in \mathbf{R}^*$.

(ii) Define a binary operation $\circ$ on $\mathbf{R}^*$ by $x \circ y = |x - y|$. Then $(x \circ y) \circ z \neq x \circ (y \circ z)$ for some $x, y, z \in \mathbf{R}^*$ but $x \circ y = y \circ x$ for all $x, y \in \mathbf{R}^*$.

(iii) Define a binary operation $\circ$ on $\mathbf{R}^*$ by $x \circ y = \min\{x, y\}$. Then $(x \circ y) \circ z = x \circ (y \circ z)$ and $x \circ y = y \circ x$ for all $x, y, z \in \mathbf{R}^*$.

2 Let $\mathbf{Q}^*$ be the set of all non-zero rational numbers. Define a binary relation $\circ$ on $\mathbf{Q}^*$ by $x \circ y = x/y$ (usual division).

Then $x \circ y \neq y \circ x$ and $(x \circ y) \circ z \neq x \circ (y \circ z)$ for some $x, y, z \in \mathbf{Q}^*$.

3 A homomorphism f from a groupoid $(G, \circ)$ into a groupoid $(H, *)$ is a mapping $f : G \to H$ such that $f(x \circ y) = f(x) * f(y)$ for all $x, y \in G$. A homomorphism f is said to be a *monomorphism, epimorphism* or *isomorphism* ($\cong$) according as f is injective, surjective or bijective.

(i) Isomorphism relation of groupoids is an equivalence relation.
(ii) If G and H are finite groupoids such that $|G| \neq |H|$. Then G cannot be isomorphic to H.
(iii) The groupoids $(\mathbf{Z}, \circ)$ and $(\mathbf{Z}, *)$ under the compositions defined by $x \circ y = x + y + xy$ and $x * y = x + y - xy$ are isomorphic.
[*Hint*. The function $f : (\mathbf{Z}, \circ) \to (\mathbf{Z}, *)$ defined by $f(x) = -x \ \forall x \in \mathbf{Z}$ is an isomorphism.]
(iv) Let $(\mathbf{C}, +)$ be the groupoid of complex numbers under usual addition and $f : (\mathbf{C}, +) \to (\mathbf{C}, +)$ be defined by $f(a+ib) = a-ib$. Then f is an isomorphism.
(v) Let $(\mathbf{N}^+, \cdot)$ and $(\mathbf{R}, +)$ be groupoids under usual multiplication of positive integers and usual addition of real numbers. Then $f : (\mathbf{N}^+, \cdot) \to (\mathbf{R}, +)$ defined by $f(n) = \log_{10} n$ is a monomorphism but not an epimorphism.
[*Hint*. $0 = \log_{10} 1 < \log_{10} 2 < \log_{10} 3 < \cdots \Rightarrow$ there is no integer $n \in \mathbf{N}^+$ such that $\log_{10} n = -1 \in \mathbf{R} \Rightarrow f$ is not an epimorphism.]

2.2 Semigroups

Our main interest in this chapter is in groups. Semigroups and monoids are convenient algebraic systems for stating some theorems on groups. Semigroups play an important role in algebra, analysis, topology, theoretical computer science, and in many other branches of science. Semigroup actions unify computer science with mathematics.

Definition 2.2.1 A *semigroup* is an ordered pair $(S, \cdot)$, where S is non-empty set and the dot '.' is a binary operation on S, i.e., a mapping $(a, b) \mapsto a \cdot b$ from $S \times S$ to S such that for all $a, b, c \in S$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*associative law*).

For convenience, $(S, \cdot)$ is abbreviated to S and $a \cdot b$ to ab. The associative property in a semigroup ensures that the two products $a(bc)$ and $(ab)c$ are same, which can be denoted as abc.

Definition 2.2.2 A semigroup S is said to be *commutative* iff $ab = ba$ for all $a, b \in S$; otherwise S is said to be non-commutative.

Example 2.2.1 (i) $(\mathbf{Z}, +)$ and $(\mathbf{Z}, \cdot)$ are commutative semigroups, where the binary operations on $\mathbf{Z}$ are usual addition and multiplication of integers.
(ii) $(\mathcal{P}(S), \cap)$ and $(\mathcal{P}(S), \cup)$ (cf. Example 2.1.2(i)) are commutative semigroups.
(iii) $(M(S), \circ)$ (cf. Example 2.1.2(ii)) is a non-commutative semigroup.

Definition 2.2.3 Let S be a semigroup. An element $1 \in S$ is called a *left* (*right*) *identity* in S iff $1a = a$ ($a1 = a$) for all $a \in S$ and 1 is called an *identity* iff it is a both left and right identity in S.

Proposition 2.2.1 *If a semigroup S contains a left identity e and a right identity f, then $e = f$ is an identity and there is no other identity.*

Proof $ef = f$, as e is a left identity and also $ef = e$, as f is a right identity. Consequently, $e = f$ is an identity. Next let $1 \in S$ is also an identity. Then 1 is both a left and a right identity. Consequently, $e = 1$ and $f = 1$. □

This proposition shows that a semigroup has at most one identity element and we denote the identity element (if it exists) of a semigroup by 1.

Definition 2.2.4 Let S be a semigroup. An element $0 \in S$ is called a *left* (*right*) *zero* in S iff $0a = 0$ ($a0 = 0$) for all $a \in S$ and 0 is called a *zero* iff it is a both left and right zero in S.

If an element $a \in S$ is such that $a \neq 0$, then a is called a non-zero element of S.

Proposition 2.2.2 *If a semigroup S contains a left zero z and also a right zero w, then $z = w$ is a zero and there is no other zero.*

Proof Similar to proof of Proposition 2.2.1. □

Definition 2.2.5 A semigroup S with the identity element is called a *monoid*.

Example 2.2.2 (i) $(\mathbf{Z}, \cdot)$ is a monoid under usual multiplication, where 1 is the identity.

(ii) The set of even integers is not a monoid under usual multiplication.

If a semigroup S has no identity element, it is easy to adjoin an extra element 1 to the set S. For this we extend the given binary operation '$\cdot$' on S to $S \cup \{1\}$ by defining $1 \cdot a = a \cdot 1 = a$ for all $a \in S$ and $1 \cdot 1 = 1$. Then $S \cup \{1\}$ becomes a semigroup with identity element 1.

Analogously, it is easy to adjoin an element 0 to S and extend the given binary operation on S to $S \cup \{0\}$ by defining $0 \cdot a = a \cdot 0 = 0$ for all $a \in S$ and $0 \cdot 0 = 0$. Then $S \cup \{0\}$ becomes a semigroup with zero element 0.

Definition 2.2.6 Let S be a semigroup with zero element 0. If for two non-zero elements $a, b \in S$, $ab = 0$, then a and b are called respectively a *left* and a *right divisor of zero*.

Example 2.2.3 $M_2(\mathbf{Z})$, the set of 2×2 matrices over $\mathbf{Z}$ is semigroup (non-commutative) under usual multiplication of matrices with $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ as zero element. Clearly, $\left(\begin{smallmatrix} 2 & 0 \\ 3 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 5 \end{smallmatrix}\right)$ are non-zero elements of $M_2(\mathbf{Z})$ such that $\left(\begin{smallmatrix} 2 & 0 \\ 3 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 0 \\ 1 & 5 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. As a result, $\left(\begin{smallmatrix} 2 & 0 \\ 3 & 0 \end{smallmatrix}\right)$ is a left divisor of zero, having $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 5 \end{smallmatrix}\right)$ the corresponding right divisor of zero. Again $\left(\begin{smallmatrix} -3 & 2 \\ -6 & 4 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 0 \\ 3 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ shows that $\left(\begin{smallmatrix} 2 & 0 \\ 3 & 0 \end{smallmatrix}\right)$ is also a right divisor of zero, having a different matrix $\left(\begin{smallmatrix} -3 & 2 \\ -6 & 4 \end{smallmatrix}\right)$ the corresponding left divisor of zero.

If $a_1, a_2, \ldots, a_n$ are elements of a semigroup S, we define the product $a_1a_2 \cdots a_n$ inductively, as $(a_1\, a_2 \cdots a_{n-1})a_n$.

Theorem 2.2.1 *Let S be a semigroup. Then all the products obtained by insertion of parentheses in the sequence $a_1, a_2, \ldots, a_n, a_{n+1}, a_{n+2}$ of elements of S are equal to the product $a_1a_2 \cdots a_na_{n+1}a_{n+2}$.* (Generalized associative law.)

Proof By associative property in S, the theorem holds for $n = 1$. Let the theorem hold for all values of n such that $1 \leq n \leq r$ and let p and p' be the product of an ordered set of $2 + r + 1$ elements $a_1, a_2, \ldots, a_{2+r+1}$, for two different modes of association obtained by insertion of parentheses. Since the theorem holds for all values of $n \leq r$, the parentheses can all be deleted up to the penultimate stage. Then we have $p = (a_1a_2 \cdots a_t)(a_{t+1} \cdots a_{2+r+1})$, where $1 \leq t \leq 2 + r$, and $p' = (a_1 \cdots a_i)(a_{i+1} \cdots a_{2+r+1})$, where $1 \leq i \leq 2 + r$. If $i = t$, then $p = p'$. Otherwise, we can assume without loss of generality that $i > t$. Then

$$\begin{aligned} p' &= \big((a_1a_2 \cdots a_t)(a_{t+1} \cdots a_i)\big)(a_{i+1} \cdots a_{2+r+1}) \\ &= (a_1 \cdots a_t)\big((a_{t+1} \cdots a_i)(a_{i+1} \cdots a_{2+r+1})\big), \quad \text{by associativity in } S \\ &= (a_1 \cdots a_t)(a_{t+1} \cdots a_ia_{i+1} \cdots a_{2+r+1}) = p. \end{aligned}$$

Thus $p = p'$ in either case, and the theorem holds for $n = r + 1$ also. Hence by the principle of mathematical induction the theorem holds for all positive integral values of n. □

Powers of an Element Let S be a semigroup and $a \in S$. Then the powers of a are defined recursively:

$$a^1 = a, \qquad a^{n+1} = a^n \cdot a \quad \text{for } n = 1, 2, 3, \ldots;$$

n is called the index of a^n. Thus the powers of a are defined for all positive integral values of n.

Proposition 2.2.3 *Let S be a semigroup. Then for any element $a \in S$, $a^r a^t = a^{r+t}$ and $(a^r)^t = a^{rt}$, r, t are positive integers.*

Proof The proof follows from Theorem 2.2.1. □

Definition 2.2.7 Let S be a semigroup with identity 1 and $a \in S$. An element $a' \in S$ is said to be a left inverse of a with respect to 1 iff $a'a = 1$. Similarly, an element $a^* \in S$ is a right inverse of a iff $aa^* = 1$. An element, which is both a left and right inverse of an element a, with respect to 1, is called a two-sided inverse or an inverse of a.

Theorem 2.2.2 *Let G be a semigroup with an identity element* 1. *If $a \in G$ has an inverse, then it is unique.*

Proof Let b and b' be inverses of a in G. Then

$$\begin{aligned} b &= b1 \\ &= b(ab'), \quad \text{since } b' \text{ is an inverse of } a. \\ &= (ba)b' \quad \text{(by associativity in } G) \\ &= 1b', \quad \text{since } ba = 1 \\ &= b'. \end{aligned}$$

□

We denote by a^{-1} the unique inverse (if it exists) of an element a of a semigroup.

The set $M(X)$ of all mappings of a given non-empty set X into itself, where the binary operation is the usual composition '$\circ$' of mappings, forms an important semigroup.

Proposition 2.2.4 *If X is a non-empty set, $M(X)$ is a monoid.*

Proof Clearly, $(M(X), \circ)$ is a semigroup under usual composition of mappings. Let $1_X : X \to X$ be the identity map defined by $1_X(x) = x$ for all $x \in X$. Then for any $f \in M(X)$, $(1_X \circ f)(x) = 1_X(f(x)) = f(x)$ and $(f \circ 1_X)(x) = f(1_X(x)) = f(x)$ for all $x \in X$ imply $1_X \circ f = f \circ 1_X = f$. Consequently, $M(X)$ is a monoid with 1_X as its identity element. □

Remark Every element in $M(X)$ may not have an inverse.

For example, if $X = \{1, 2, 3\}$, then $f \in M(X)$ defined by $f(1) = f(2) = f(3) = 1$ has no inverse in $M(X)$. Otherwise, there exists an element $g \in M(X)$ such that $f \circ g = g \circ f = 1_X$. Then $1 = 1_X(1) = (g \circ f)(1) = g(f(1)) = g(1)$ and $2 = 1_X(2) = (g \circ f)(2) = g(f(2)) = g(1)$ imply that $g(1)$ has two distinct values. This contradicts the assumption that g is a map.

We now characterize the elements of $M(X)$ which have inverses.

Theorem 2.2.3 *An element f in the monoid $M(X)$ has an inverse iff f is a bijection.*

Proof The proof follows from Corollary of Theorem 1.2.7 of Chap. 1 (by taking $X = Y$ in particular). □

Let X be a non-empty set and $B(X)$ denote the set of all binary relations on X. Define a binary operation '$\circ$' on $B(X)$ as follows:

If $\rho, \sigma \in B(X)$, then $\sigma \circ \rho = \{(x, y) \in X \times X : \text{if } \exists z \in X \text{ such that } (x, z) \in \rho \text{ and } (z, y) \in \sigma\}$.

Then $B(X)$ is a semigroup with identity element $\Delta = \{(x, x) : x \in X\}$.

Definition 2.2.8 A relation ρ on a semigroup S is called a *congruence relation* on S iff

(i) ρ is an equivalence relation on S;
(ii) $(a, b) \in \rho \Rightarrow (ca, cb) \in \rho$ and $(ac, bc) \in \rho$ for all $c \in S$.

Let ρ be a congruence relation on a semigroup S and S/ρ the set of all ρ-equivalence classes $a\rho, a \in S$. Define a binary operation '$\circ$' on S/ρ by $a\rho \circ b\rho = (ab)\rho$, for all $a, b \in S$. Clearly, the operation '$\circ$' is well defined.

Then $(S/\rho, \circ)$ becomes a semigroup.

Definition 2.2.9 A mapping f from a semigroup S into a semigroup T is called a homomorphism iff for all $a, b \in S$,

$$f(ab) = f(a)f(b).$$

Let S and T be semigroups. Then a homomorphism $f : S \to T$ is called

(i) an *epimorphism* iff f is surjective;
(ii) a *monomorphism* iff f is injective; and
(iii) an *isomorphism* iff f is bijective.

If $f : S \to T$ is an isomorphism, we say that S is isomorphic to T denoted $S \cong T$.

Proposition 2.2.5 *Let S be a semigroup and ρ a congruence relation on S. Then the map $p : S \to S/\rho$ defined by $p(a) = a\rho$ for all $a \in S$ is a homomorphism from S onto S/ρ (p is called* natural homomorphism).

Proof Trivial. □

Definition 2.2.10 Let S and T be two semigroups and $f : S \to T$ a homomorphism from S onto T. The kernel of f denoted by $\ker f$ is defined by $\ker f = \{(a, b) \in S \times S : f(a) = f(b)\}$.

Clearly, $\rho = \ker f$ is a congruence relation on S. Then S/ρ is a semigroup.

Proposition 2.2.6 *Let f be a homomorphism from a semigroup S onto a semigroup T. Then the semigroup $S/\ker f$ is isomorphic to T.*

Proof Suppose $\rho = \ker f$. Define $g : S/\rho \to T$ by $g(a\rho) = f(a)$ for all $a \in S$. Clearly, g is an isomorphism. □

Definition 2.2.11 A non-empty subset I of a semigroup S is called a *left* (*right*) *ideal* of S iff $xa \in I$ ($ax \in I$) for all $x \in S$, for all $a \in I$ and I is called an *ideal* of S iff I is both a left ideal and a right ideal of S.

Example 2.2.4 Let S be a semigroup. Then

(i) S is an ideal of S;

(ii) for each $a \in S$, $Sa = \{sa : s \in S\}$ is a left ideal and $aS = \{as : s \in S\}$ is a right ideal of S.

Definition 2.2.12 A semigroup S is called *left* (*right*) *simple* iff S has no left (right) ideals other than S.

Definition 2.2.13 Let S be a semigroup. An element $a \in S$ is called an *idempotent* iff $aa = a^2 = a$.

Clearly if 1 or $0 \in S$, they are idempotents. The set of idempotents of S is denoted by $E(S)$.

If a semigroup S contains 0, then an element $c \in S$ is said to be a *nilpotent* element of rank n for $n \geq 2$ iff $c^n = 0$, but $c^{n-1} \neq 0$ and hence $(c^{n-1})^2 = 0$, since $2(n-1) \geq n$, so that c^{n-1} is a nilpotent element of rank 2. Thus the following proposition is immediate.

Proposition 2.2.7 *If a semigroup S contains any nilpotent element, then there also exists a nilpotent element of rank 2 in S.*

Definition 2.2.14 A semigroup S is called a *band* iff $S = E(S)$, i.e., iff every element of S is idempotent. S is called a right (left) group, iff S is right (left) simple and left (right) cancellative.

Let S be a band. Define a relation '$\leq$' on S by $e \leq f$, iff $ef = fe = e$. Then clearly, $\leq$ is a partial order on S. A band S is said to be commutative, iff S is a commutative semigroup.

Let X and Y be two sets and define a binary operation on $S = X \times Y$ as follows: $(x, y)(z, t) = (z, t)$, where $x, z \in X$ and $y, t \in Y$. Then S is a non-commutative band. We call S the rectangular band on $X \times Y$.

Definition 2.2.15 Let S be a semigroup. An element $a \in S$ is called *regular* iff $a \in aSa$, i.e., iff $a = axa$ for some $x \in S$. A semigroup S is called regular iff every element of S is regular.

Clearly, if $axa = a$, then $e = ax$ and $f = xa$ are idempotents in S.

Let $a \in S$. An element $b \in S$ is said to be an inverse of a iff $aba = a$ and $bab = b$. Clearly, if a is a regular element of S, then a has at least one inverse.

Example 2.2.5 (i) Every right group is a regular semigroup.

(ii) Every band is a regular semigroup.

(iii) $M(X)$ (cf. Proposition 2.2.4) is a regular semigroup under usual composition of mappings.

(iv) Let $M_2(\mathbf{Q})$ be the set of all 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ over $\mathbf{Q}$, the set of rationals. Then $M_2(\mathbf{Q})$ is a regular semigroup with respect to the usual matrix multiplication.

Definition 2.2.16 A regular semigroup S is called an *inverse semigroup* iff for every element a of S there exists a unique element a^{-1} such $aa^{-1}a = a$ and $a^{-1}aa^{-1} = a^{-1}$.

Clearly, every inverse semigroup is a regular semigroup, but there are regular semigroups which are not inverse semigroups. For example, a rectangular band is a regular semigroup, but it is not an inverse semigroup.

Let $(S, \circ)$ be a semigroup. A non-empty subset T of S is called a sub-semigroup of S iff $\forall a, b \in T$, $a \circ b \in T$ i.e., iff $(T, \circ)$ is also a semigroup where the latter operation '$\circ$' is the restriction of '$\circ$' to $T \times T$.

For example, $(\mathbf{N}, \cdot)$ is a sub-semigroup of $(\mathbf{Z}, \cdot)$, where '$\cdot$' denotes the usual multiplication. Clearly, for any semigroup S, S is a sub-semigroup of itself.

Example 2.2.6 Let $S = M_2(\mathbf{R})$ be the multiplicative semigroup of all 2×2 real matrices and T the subset of all matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $a \in \mathbf{R}$. Then T is a sub-semigroup of S.

S has an identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and T has an identity $I' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ but $I \neq I'$.

This example shows that a semigroup S with an identity 1 may have a sub-semigroup with an identity e such that $e \neq 1$.

Proposition 2.2.8 *If $\{A_i\}$ is any collection of sub-semigroups of a semigroup S, then $\bigcap_i A_i$ is also a sub-semigroup of S, provided $\bigcap_i A_i \neq \emptyset$.*

Proof Let $M = \bigcap_i A_i$ $(\neq \emptyset)$ and $a, b \in M$. Then $a, b \in A_i \Rightarrow ab \in A_i$ for each sub-semigroup $A_i \Rightarrow ab \in M \Rightarrow M$ is a sub-semigroup of S, as associative property is hereditary. □

If X is a non-empty subset of a semigroup S, then $\langle X \rangle$, the sub-semigroup of S generated by X defined by the intersection of all sub-semigroups of S containing X, is the smallest sub-semigroup of S. We say that X generates S iff $\langle X \rangle = S$. Clearly $\langle S \rangle = S$.

Let $a \in S$, then $\langle \{a\} \rangle = \langle a \rangle$ is called the cyclic sub-semigroup of S generated by a. A semigroup S is called *cyclic* iff there exists an element $a \in S$ such that $S = \langle a \rangle$.

Let S be an inverse semigroup and $a, b \in S$. Then the relation '$\leq$' defined by $a \leq b$ iff there exists an idempotent $e \in S$ such that $a = eb$ is a partial order relation.

Let $E(S)$ be the set of all idempotents of an inverse semigroup S. Then $E(S)$ is a sub-semigroup of S. Moreover, $E(S)$ is a semilattice, called the *semilattice* of *idempotents* of S.

Some Other Semigroups A semigroup S is called fully idempotent iff each ideal I of S is idempotent, i.e., iff $I^2 = I$.

The following statements for a semigroup S are equivalent:

(a) S is fully idempotent;

(b) for each pair of ideals, I, J of S, $I \cap J = IJ$;
(c) for each right ideal R and two-sided ideal I, $R \cap I \subseteq IR$;
(d) for each left ideal L and two-sided ideal I, $L \cap I \subseteq LI$.

Definition 2.2.17 A function $l(r)$ on a semigroup S is said to be *left* (*right*) *translation* on S iff $l(r)$ is written as a left (right) operator and satisfies

$$l(xy) = (lx)y\big((xy)r = x(yr)\big) \quad \forall x, y \in S.$$

The pair (l, r) is said to be *linked* iff $x(ly) = (xr)y$ $\forall x, y \in S$ and is then called a bitranslation on S.

The set $L(S)$ of all left translations ($R(S)$ of all right translations) on S with the operation of multiplication defined by $(ll_1)x = l(l_1x)(x(rr_1) = (xr)r_1)$ $\forall x \in S$ is a semigroup.

The set $B(S)$ of all bitranslations on S with the operation defined by $(l, r)(l_1, r_1) = (ll_1, rr_1)$ is a semigroup and it called the *translational hull* of S.

Two bitranslations (l, r) and (l_1, r_1) are said to be equal iff $l = l_1$ and $r = r_1$.

For any $s \in S$, the functions l_s and r_s given by $l_sx = sx, xr_s = xs$ $\forall x \in S$ are called respectively the *inner left and inner right translation* on S induced by s; the pair $T_s = (l_s, r_s)$ is called the *inner bitranslation* on S induced by s.

The set $T(S)$ of all inner bitranslations on S is called the inner part of $B(S)$. If $L_i(S)$ and $R_i(S)$ are two sets of all *inner left* and *inner right translations* on S respectively, then $T(S) \subset B(S)$, $L_i(S) \subset L(S)$, and $R_i(S) \subset R(S)$.

Lemma 2.2.1 *If* $l \in L(S), r \in R(S), l_s \in L_i(S), r_s \in R_i(S), T_s \in T(S), w = (l, r) \in B(S)$, *then for every* $s \in S$,

(i) $ll_s = l_{ls}, l_sl = l_{sr}$;
(ii) $r_sr = r_{sr}, rr_s = r_{ls}$ *and*
(iii) $wT_s = T_{ls}, T_sw = T_{sr}$.

Proof (i) $(ll_s)x = l(l_sx) = l(sx) = (ls)x = l_{ls}x$ $\forall x \in S \Rightarrow ll_s = l_{ls} \in L_i(S)$.
Again $(l_sl)x = l_s(lx) = s(lx) = (sr)x = l_{sr}x$ $\forall x \in S \Rightarrow l_sl = l_{sr} \in L_i(S)$.
(ii) $x(r_sr) = (xr_s)r = (xs)r = x(sr) = xr_{sr}$ $\forall x \in S \Rightarrow r_sr = r_{sr} \in R_i(S)$.
Similarly, $rr_s = r_{ls} \in R_i(S)$.
By using (i) and (ii) it follows that
(iii) $wT_s = (l, r)(l_s, r_s) = (ll_s, rr_s) = (l_{ls}, r_{ls}) = T_{ls} \in T(S)$.
Similarly, $T_sw = T_{sr} \in T(S)$. □

Corollary 1 *For a semigroup* S,

(i) $L_i(S)$ *is an ideal of* $L(S)$;
(ii) $R_i(S)$ *is an ideal of* $R(S)$; *and*
(iii) $T(S)$ *is an ideal of* $B(S)$.

Corollary 2 *For a semigroup* S,

(i) $L_i(S)$ *is a sub-semigroup of* $L(S)$;

(ii) $R_i(S)$ *is a sub-semigroup of* $R(S)$; *and*
(iii) $T(S)$ *is a sub-semigroup of* $B(S)$.

Definition 2.2.18 A semigroup S is said to be left (right) *reductive*, iff $xa = xb$ $(ax = bx)$ $\forall x \in S \Rightarrow a = b$. If S is both left and right reductive, then S is said to be *reductive*. If $xa = xb$ and $ax = bx$ $\forall x \in S \Rightarrow a = b$, then S is said to be *weakly reductive*.

Clearly, a reductive semigroup is also weakly reductive.

For the application of *category theory* we follow the terminology of Appendix B. It is easy to check that semigroups and their homomorphisms form a category denoted by S_G.

We note that for a semigroup $S \in S_G$, $T(S)$ is also a semigroup $\in S_G$. For $f : S \to W$ in S_G, define $f_* = T(f) : T(S) \to T(W)$ by $f_*((l_r, r_s)) = (l_{f(s)}, r_{f(s)})$. Then for $g : W \to X$ in S_G, $(gf)_* : T(S) \to T(X)$ in S_G is such that

$$(gf)_*((l_s, r_s)) = (l_{(gf)(s)}, r_{(gf)(s)}) = (l_{g(f(s))}, r_{g(f(s))}) = g_*((l_{f(s)}, r_{f(s)}))$$
$$= g_*\big(f_*((l_s, r_s))\big) \quad \forall (l_s, r_s) \in T(S) \quad \Rightarrow \quad (gf)_* = g_* f_*.$$

Also for the identity homomorphism $I_S : S \to S$ in S_G, $I_{S*} : T(S) \to T(S)$ in S_G is such that $I_{S*}((l_s, r_s)) = (l_{I_S(s)}, r_{I_S(s)}) = (l_s, r_s)$ $\forall (l_s, r_s) \in T(S) \Rightarrow I_{S*}$ is the identity homomorphism. The following theorem is immediate from the above discussions.

Theorem 2.2.4 $T : S_G \to S_G$ *is a covariant functor* (*see Appendix B*).

Lemma 2.2.2 *For a semigroup* S, *the function* $f : S \to T(S)$ *defined by* $f(s) = T_s$ $\forall s \in S$ *is a homomorphism from* S *onto* $T(S)$.

Proof $f(st) = T_{st} = T_s T_t = f(s) f(t)$ $\forall s, t \in S \Rightarrow f$ is a homomorphism. Moreover, for any $T_s \in T(S)$, we can find $s \in S$ such that $f(s) = T_s$. □

Theorem 2.2.5 *The function* $f : S \to T(S)$ *defined by* $f(s) = T_s$ *is an isomorphism iff* S *is reductive.*

Proof Suppose S is reductive and $f(s) = f(t)$ for some $s, t \in S$. Then $T_s = T_t \Rightarrow (l_s, r_s) = (l_t, r_t) \Rightarrow l_s = l_t$ and $r_s = r_t \Rightarrow sx = tx$ and $xs = xt$ $\forall x \in S \Rightarrow s = t \Rightarrow f$ is injective. Hence by Lemma 2.2.2, f is an isomorphism.

Conversely, let f be an isomorphism and $ax = bx, xa = xb$ hold $\forall a, b \in S$ and $\forall x \in S$. Then $l_a x = l_b x$ and $x r_a = x r_b$ hold $\forall x \in S$. This shows that $l_a = l_b$ and $r_a = r_b$ yielding $f(a) = T_a = (l_a, r_a) = (l_b, r_b) = T_b = f(b)$. Hence $a = b \Rightarrow S$ is reductive. □

Corollary *If* S *is a cancellative semigroup, then the function* $f : S \to T(S)$ *defined by* $f(s) = T_s$ *is an isomorphism.*

For a given semigroup $S \in S_G$, the set $F_S(X)$ of all semigroup homomorphisms from S to X in S_G forms a semigroup under usual multiplication of functions.

We also define for each homomorphism $f : X \to Y$ in S_G, the semigroup homomorphism $f_* = F_S(f) : F_S(X) \to F_S(Y)$ by $f_*(g) = f \circ g \ \forall g : S \to X$ in S_G. Hence the following lemma is immediate

Lemma 2.2.3 *$F_S : S_G \to S_G$ is a covariant functor.*

Let (F_S, T) denote the set of all natural transformations from the covariant functor F_S to the covariant functor $T : S_G \to S_G$ (see Appendix B).

Theorem 2.2.6 *For each semigroup $S \in S_G$, the set (F_S, T) admits a semigroup structure such that (F_S, T) is isomorphic to $T(S)$.*

Proof Using the Yoneda Lemma (see Appendix B) for covariant functors F_S and T we find that there is a bijection $f_S : T(S) \to (F_S, T)$ for every $S \in S_G$. As $T(S)$ is a semigroup, f_S induces composition on the set (F_S, T) admitting it a semigroup structure such that (F_S, T) is isomorphic to $T(S)$. □

Theorem 2.2.7 *A semigroup S is isomorphic to the semigroup (F_S, T) iff S is reductive.*

Proof The theorem is immediate by using Theorems 2.2.5 and 2.2.6. □

Remark Theorem 2.2.6 yields a representation of the covariant functor $T : S_G \to S_G$. In this way the problem of classifying semigroups, i.e., of computing $T(S)$ has been reduced to the determination of the set of natural transformations (F_S, T).

Let S be a semigroup. T a sub-semigroup of S and $w \in B(T)$. Then a bitranslation $\tilde{w} \in B(S)$ is said to be an extension of w to S iff $\tilde{w}x = wx$ and $x\tilde{w} = xw \ \forall x \in T$ and we write $\tilde{w}|T = w$.

Theorem 2.2.8 *Let S be a semigroup, T a reductive semigroup, $f : S \to T$ an epimorphism and let $w \in B(S)$. Then there exists a unique element $w' \in B(T)$ such that for each $x \in S$, $w' f(x) = f(wx)$ and $f(x)w' = f(xw)$.*

Proof For $t \in T, \exists s \in S$ such that $f(s) = t$. Now define $w't = f(ws)$ and $tw' = f(xw)$. Then the theorem follows. □

Theorem 2.2.9 *Let S be a reductive semigroup and $l, r : S \to S$ are such that the pair (l, r) is linked, then $(l, r) \in B(S)$.*

Proof It is sufficient to show that $l \in L(S)$ and $r \in R(S)$. Let $x, y \in S$. Then for each $t \in S, t(lx)(y) = (t(lx))y = (tr)(x)y = (tr)(xy) = t(l(xy))$. Since S is reductive, $(lx)y = l(xy) \Rightarrow l \in L(S)$. Similarly, $r \in R(S)$. □

2.2.1 Topological Semigroups

Let S be a semigroup. If A and B are subsets of S, we define $AB = \{ab : a \in A \text{ and } b \in B\}$. If a subgroup S is a Hausdorff space such that the multiplication function $(x, y) \mapsto xy$ is continuous with the product topology on $S \times S$, then S is called a topological semigroup. The condition that the multiplication on S is continuous is equivalent to the condition that for each $x, y \in S$ and each open set W in S with $xy \in W$, $\exists$ open sets U and V such that $x \in U$, $y \in V$ and $UV \subset W$.

Note that any semigroup can be made into a topological semigroup by endowing it the discrete topology and hence a finite semigroup is a compact semigroup.

Let $\mathbf{C}$ be the space of complex numbers with complex multiplication. Then $\mathbf{C}$ becomes a topological semigroup with a zero and an identity and no other idempotents. The unit disk $D = \{z \in \mathbf{C} : |z| \leq 1\}$ is a complex sub-semigroup of $\mathbf{C}$. The circle $S^1 = \{z \in \mathbf{C} : |z| = 1\}$ is also a sub-semigroup of $\mathbf{C}$.

Problems

A *Let A and B be subsets of a topological semigroup S.*

(a) *If A and B are compact, then AB is compact.*
(b) *If A and B are connected, then AB is connected.*
(c) *If B is closed, then $\{x \in S : xA \subset B\}$ is closed.*
(d) *If B is closed, then $\{x \in S : A \subset xB\}$ is closed.*
(e) *If B is compact, then $\{x \in S : xA \subset Bx\}$ is closed.*
(f) *If A is compact and B is open, then $\{x \in S : xA \subset B\}$ is open.*
(g) *If A is compact and B is closed, then $\{x \in S : xA \cap B \neq \emptyset\}$ is closed.*

Proof [See Carruth et al. (1983, 1986)]. □

B *If S is a topological semigroup which is a Hausdorff space, then the set $E(S)$ of all idempotents of S is a closed subset of S.*

Proof $E(S)$ is the set of fixed points of the continuous function $f : S \to S$ defined by $x \mapsto x^2$.

Define $g : S \to S \times S$ by $g(x) = (f(x), x) = (x^2, x)$. Then g is continuous. Since the diagonal of a Hausdorff space is closed in $S \times S$, $g^{-1}(\Delta(S)) = \{x \in S : x^2 = x\}$ is closed. □

Semigroups of Continuous Self Maps Let $S(X)$ denote the semigroup of all continuous maps from a topological space X into itself under composition of maps.

At present there are at least four *broad areas* where active researches on $S(X)$ are going on.

These are:

(1) homomorphisms from $S(X)$ into $S(Y)$;
(2) finitely generated sub-semigroups of $S(X)$;

(3) Green's relations and related topics for $S(X)$;
(4) congruences on $S(X)$.

We list some problems:

Problem 1 (a) If X and Y are homeomorphic spaces, then $S(X)$ and $S(Y)$ are isomorphic semigroups. Is its converse true?

[*Hint*. Let X be a discrete space with more than one element and Y be the same set, but endowed with the indiscrete topology. Then X and Y are not homeomorphic but $S(X)$ and $S(Y)$ are isomorphic under identity map.]

(b) If X and Y are two compact 0-dimensional metric spaces, then X and Y are homeomorphic $\Leftrightarrow$ the semigroups $S(X)$ and $S(Y)$ are isomorphic.

Problem 2 Determine Green's relations for elements of $S(X)$ which are not necessarily regular.

Remark Some work has been done in this direction but there is much yet to do.

Problem 3 Determine all congruences on $S(X)$.

Remark If X is discrete, this was solved. For the case when X is not discrete [see Magil Jr. (1982)].

Problem 4 If X is Hausdorff and locally compact, then $S(X)$ endowed with compact open topology is a topological semigroup. Is the converse true?

Remark The converse is not true [see De Groot (1959)].

2.2.2 *Fuzzy Ideals in a Semigroup*

Let S be a non-empty set. Consider the closed interval $[0, 1]$. Any mapping from $S \to [0, 1]$ is called a fuzzy subset of S. It is a generalization of the usual concept of a subset of S in the following sense.

Let A be a subset of S. Define its characteristic function κ_A by

$$\begin{aligned} \kappa_A(x) &= 1 \quad \text{when } x \in A \\ &= 0 \quad \text{when } x \notin A. \end{aligned}$$

So for each subset A of S there corresponds a fuzzy subset κ_A.

Conversely, suppose $\tilde{A} : S \to [0, 1]$ is a mapping such that $\operatorname{Im} \tilde{A} = \{0, 1\}$.

Let $A = \{x \in S : \tilde{A}(x) = 1\}$.

Now A is a subset of S and $\tilde{A}$ is the characteristic function of A.

Definition 2.2.19 Let S be a semigroup. A fuzzy subset $\tilde{A}$ (that is, a mapping from $S \to [0, 1]$) is called a *left* (*right*) *fuzzy ideal* iff

$$\tilde{A}(xy) \geq \tilde{A}(y)\big(\tilde{A}(xy) \geq \tilde{A}(x)\big).$$

Definition 2.2.20 Let $\tilde{A}, \tilde{B}$ be two fuzzy subsets in a semigroup S. Define $\tilde{A} \cup \tilde{B}$, $\tilde{A} \cap \tilde{B}$, $\tilde{A} \circ \tilde{B}$ by

$$\begin{aligned}
(\tilde{A} \cup \tilde{B})(x) &= \max\big(\tilde{A}(x), \tilde{B}(x)\big), \quad \forall x \in S;\\
(\tilde{A} \cap \tilde{B})(x) &= \min\big(\tilde{A}(x), \tilde{B}(x)\big), \quad \forall x \in S;\\
(\tilde{A} \circ \tilde{B})(x) &= \max\big\{\min\big(\tilde{A}(u), \tilde{B}(v)\big)\big\}, \quad \text{if } x = uv,\ u, v \in S\\
&= 0, \quad \text{if } x \text{ cannot be expressed in the form } x = uv.
\end{aligned}$$

2.2.3 Exercises

Exercises-IA

1. Verify that the following '$*$' are binary operations on the Euclidean plane $\mathbf{R}^2$: For $(x, y), (x', y') \in \mathbf{R}^2$,
   (i) $(x, y) * (x', y') = (x, y)$ [if $(x, y) = (x', y')$] = midpoint of the line joining the point (x, y) to the point (x', y') if $(x, y) \neq (x', y')$;
   (ii) $(x, y) * (x', y') = (x + x', y + y')$, where $+$ is the usual addition in $\mathbf{R}$;
   (iii) $(x, y) * (x', y') = (x \cdot x', y \cdot y')$, where '$\cdot$' is the usual multiplication in $\mathbf{R}$.
2. Verify that the following '$\circ$' are binary operations on $\mathbf{Q}$:
   (i) $x \circ y = x - y - xy$;
   (ii) $x \circ y = \frac{x+y+xy}{2}$;
   (iii) $x \circ y = \frac{x+y}{3}$.

   Determine which of the above binary operations are associative and commutative.
3. Determine the number different binary operations which can be defined on a set of three elements.
4. Let S be the set of the following six mappings $f_i : \mathbf{R}\backslash\{0, 1\} \to \mathbf{R}$, defined by

$$f_1 : x \mapsto x; \qquad f_2 : x \mapsto \frac{1}{1-x}; \qquad f_3 : x \mapsto \frac{x-1}{x}; \qquad f_4 : x \mapsto \frac{1}{x};$$

$$f_5 : x \mapsto \frac{x}{x-1}; \qquad f_6 : x \mapsto 1 - x.$$

   Verify that usual composition of mappings is a binary operation on S and construct the corresponding multiplicative table.

Exercises-IB

1. A binary operation $*$ is defined on $\mathbf{Z}$ by $x * y = x + y - xy$, $x, y \in \mathbf{Z}$. Show that $(\mathbf{Z}, *)$ is a semigroup. Let $A = \{x \in \mathbf{Z}; x \leq 1\}$. Show that $\{A, *\}$ is a subsemigroup of $(\mathbf{Z}, *)$.
2. Let A be a non-empty set and $S = \mathcal{P}(A)$ its power set. Show that $(S, \cap)$ and $(S, \cup)$ are semigroups. Do these semigroups have identities? If so, find them.
3. Show that for every element a in a finite semigroup, there is a power of a which is idempotent.
4. Let $(\mathbf{Z}, +)$ be the semigroup of integers under usual addition and $(\mathbf{E}, +)$ be the semigroup of even integers with integer 0 under usual addition. Then the mapping $f : \mathbf{Z} \to \mathbf{E}$ defined by $z \mapsto 2z \ \forall z \in \mathbf{Z}$ is a homomorphism. Find a homomorphism $g : \mathbf{Z} \to \mathbf{E}$ such that $g \neq f$.
5. Show that the following statements are equivalent:

   (i) S is an inverse semigroup;
   (ii) S is regular and its idempotents commute.

6. Prove the following:

   (a) Let I be a left ideal of a semigroup S. Then its characteristic function κ_I is a fuzzy left ideal. Conversely, if for any subset I of S its characteristic function κ_I is a fuzzy left ideal, then I is a left ideal of S;
   (b) If $\tilde{A}$, $\tilde{B}$ are fuzzy ideals of a semigroup S, then $\tilde{A} \cap \tilde{B}$, $\tilde{A} \cup \tilde{B}$, $\tilde{A} \circ \tilde{B}$ are fuzzy ideals of S.

7. Let S be an inverse semigroup and $E(S)$ the semilattice of idempotents of S. Prove that

   (i) $(a^{-1})^{-1} = a, \ \forall a \in S$
   (ii) $e^{-1} = e, \ \forall e \in E(S)$
   (iii) $(ab)^{-1} = b^{-1}a^{-1}, \ \forall a, b \in S$
   (iv) $aea^{-1} \in E(S) \ \forall a \in S$ and $e \in E(S)$.

8. Let '$\leq$' be a partial order on S such that $(S, \circ, \leq)$ is a partially ordered (p.o.) semigroup. Define the set $P_l^0(S) = \{p \in S : a \leq p \circ a \ \forall a \in S\}$ of all left positive elements of $(S, \circ, \leq)$ and correspondingly the set $P_r^0(S)$ of all right positive ones, and $P^0(S) = P_l^0(S) \cap P_r^0(S)$. Let $E^0(S)$ denote the set of all idempotents of (S, o). Prove the following:

   (i) If the p.o. semigroup $(S, \circ, \leq)$ has a least element u, i.e., $u \leq a \ \forall a \in S$, then u is idempotent, iff $u = x \circ y$ holds for some $x, y \in S$;
   (ii) If $P^0(S) = S$ and $f \in E^0(S)$, then $x \leq f \Leftrightarrow x \circ f = f \Leftrightarrow f \circ x = f$ holds $\forall x \in S$.
   (iii) If $P^0(S) = S$ holds and u is the least element of $(S, \leq)$, then $S \backslash \{u\}$ is an ideal of (S, o), which is a maximal one. The converse holds if $(S, \leq)$ is a fully ordered set, and if, for $a < b \Rightarrow a \circ x = b$ for some $x \in S$.

9. A non-empty subset A of a semigroup S is called a generalized left semi-ideal (gls ideal), iff $x^2 A \subseteq A$ for every $x \in S$.

(a) Let $\mathbf{Z}^*$ denote the set of all non-negative integers. Then $\mathbf{Z}^*$ is a semigroup under usual multiplication. Show that $A = \{x \in \mathbf{Z}^* : x \geq 6\}$ is a gls ideal.
(b) In an idempotent semigroup S, prove that A is a left ideal of $S \Leftrightarrow A$ is a gls ideal.
(c) Let S be a semigroup prove that S is regular iff for each generalized left semi-ideal A of S and for each right ideal B of S, $B \cap A = B^*A$, where $B^* = \{b^2 : b \in B\}$.

2.3 Groups

Historically, the concept of a group arose through the study of bijective mappings $A(S)$ on a non-empty set S. Any mathematical concept comes naturally in a very concrete form from specific sources. We start with two familiar algebraic systems: $(\mathbf{Z}, +)$ (under usual addition of integers) and $(\mathbf{Q}^+, \cdot)$ (under usual multiplication of positive rational numbers). We observe that the system $(\mathbf{Z}, +)$ possesses the following properties:

1. '$+$' is a binary operation on $\mathbf{Z}$;
2. '$+$' is associative in $\mathbf{Z}$;
3. $\mathbf{Z}$ contains an additive identity element, i.e., there is a special element, namely 0, such that $x + 0 = 0 + x = x$ for every x in $\mathbf{Z}$;
4. $\mathbf{Z}$ contains additive inverses, i.e., to each $x \in \mathbf{Z}$, there is an element $(-x)$ in $\mathbf{Z}$, called its negative, such that $x + (-x) = (-x) + x = 0$.

We also observe that the other system $(\mathbf{Q}^+, \cdot)$ possesses similar properties:

1. multiplication '$\cdot$' is a binary operation on $\mathbf{Q}^+$;
2. multiplication '$\cdot$' is associative in $\mathbf{Q}^+$;
3. $\mathbf{Q}^+$ contains a multiplicative identity element, i.e., there is a special element, namely 1, such that $x \cdot 1 = 1 \cdot x = x$ for every x in $\mathbf{Q}^+$;
4. $\mathbf{Q}^+$ contains multiplicative inverses, i.e., to each $x \in \mathbf{Q}^+$, there is an element x^{-1} which is the reciprocal of x in $\mathbf{Q}^+$, such that $x \cdot (x^{-1}) = (x^{-1}) \cdot x = 1$.

If we consciously ignore the notation and terminology, the above four properties are identical in the algebraic systems $(\mathbf{Z}, +)$ and $(\mathbf{Q}^+, \cdot)$. The concept of a group may be considered as a distillation of the common structural forms of $(\mathbf{Z}, +)$ and $(\mathbf{Q}^+, \cdot)$ and of many other similar algebraic systems.

Remark The algebraic system $(A(S), \circ)$ of bijective mappings $A(S)$ on a non-empty set S(under usual composition of mappings) satisfies all the above four properties. This group of transformations is not the only system satisfying all the above properties. For example, the non-zero rationals, reals or complex numbers also satisfy above four properties under usual multiplication. So it is convenient to introduce an abstract concept of a group to include these and other examples.

The above properties lead to introduce the abstract concept of a group. We define a group as a monoid in which every element has an inverse. We repeat the definition in more detail.

Definition 2.3.1 A group G is an ordered pair $(G, \cdot)$ consisting of a non-empty set G together with a binary operation '$\cdot$' defined on G such that

(i) if $a, b, c \in G$, then $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associative law);
(ii) there exists an element $1 \in G$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in G$ (identity law);
(iii) for each $a \in G$, there exists $a' \in G$ such that $a' \cdot a = a \cdot a' = 1$ (inverse law).

Clearly, the identity element 1 is unique by Proposition 2.2.1. The element a' called an inverse of a is unique by Theorem 2.2.2 and is denoted by a^{-1}.

A group G is said to be *commutative* iff its binary operation '$\cdot$' is commutative: $a \cdot b = b \cdot a$, for all $a, b \in G$, otherwise G is said to be non-commutative.

The definition of a group may be re-written using additive notation: We write $a + b$ for $a \cdot b$, $-a$ for a^{-1}, and 0 for 1; $a + b$, $-a$, and 0 are, respectively, called the sum of a and b, negative of a, additive identity or zero and $(G, +)$ is called an additive group.

The binary operation in a group need not be commutative. Sometimes a commutative group is called an *Abelian group* in honor of Niels Henrick Abel (1802–1829); one of the pioneers in the study of groups.

Throughout this section a group G will denote an arbitrary multiplicative group with identity 1 (unless stated otherwise).

Proposition 2.3.1 *If G is a group, then*

(i) *$a \in G$ and $aa = a$ imply $a = 1$;*
(ii) *for all $a, b, c \in G$, $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$* (left *and* right cancellation laws);
(iii) *for each $a \in G$, $(a^{-1})^{-1} = a$;*
(iv) *for $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$;*
(v) *for $a, b \in G$, each of the equations $ax = b$ and $ya = b$ has a unique solution in G.*

Proof (i) $aa = a \Rightarrow a^{-1}(aa) = a^{-1}a \Rightarrow (a^{-1}a)a = 1 \Rightarrow a = 1$.

(ii) $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow 1b = 1c \Rightarrow b = c$. Similarly, $ba = ca \Rightarrow b = c$.

(iii) $aa^{-1} = a^{-1}a = 1 \Rightarrow (a^{-1})^{-1} = a$.

(iv) $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(1b) = b^{-1}b = 1$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1 \Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

(v) $a^{-1}b = a^{-1}(ax) = (a^{-1}a)x = 1x = x$ and $ba^{-1} = (ya)a^{-1} = y(aa^{-1}) = y1 = y$ are solutions of the equations $ax = b$ and $ya = b$, respectively.

Uniqueness of the two solutions follow from the cancellation laws (ii). □

Corollary *If* $a_1, a_2, \ldots, a_n \in G$, *then* $(a_1 a_2 a_3 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$.

Proposition 2.3.2 *Let* G *be a semigroup. Then* G *is a group iff the following conditions hold*:

(i) *there exists a left identity* e *in* G;
(ii) *for each* $a \in G$, *there exists a left inverse* $a' \in G$ *of* a *with respect to* e, *so that* $a'a = e$.

Proof If G is a group, then conditions (i) and (ii) follow trivially. Next let a semigroup G satisfy conditions (i) and (ii). As $e \in G$, $G \neq \emptyset$. If $a \in G$, then by using (ii) it follows that $aa' = e$. Thus $a' = a^{-1}$ is an inverse of a with respect to e, where $ae = a(a^{-1}a) = (aa^{-1})a = ea = a \ \forall a \in G \Rightarrow e$ is an identity. Therefore G is a group. □

Proposition 2.3.3 *Let* G *be a semigroup. Then* G *is a group iff for all* $a, b \in G$ *the equations* $ax = b$ *and* $ya = b$ *have solutions in* G.

Proof If G is a group, then by Proposition 2.3.1(v), the equations $ax = b$ and $ya = b$ have solutions in G. Conversely, let the equation $ya = a$ have a solution $e \in G$. Then $ea = a$. For any $b \in G$, if t (depending on a and b) be a solution of the equation $ax = b$, then $at = b$.

Now, $eb = e(at) = (ea)t = at = b$.

Consequently, $eb = b$, $\forall b \in G \Rightarrow e$ is a left identity in G.

Next a left inverse of an element $a \in G$ is given by the solution $ya = e$ and the solution belongs to G. Consequently, for each $a \in G$, there exists a left inverse in G. As a result G is a group by Proposition 2.3.2. □

Corollary *A semigroup* G *is a group iff* $aG = G$ *and* $Ga = G$ *for all* $a \in G$, *where* $aG = \{ax : x \in G\}$ *and* $Ga = \{xa : x \in G\}$.

Definition 2.3.2 The order of a group G is the cardinal number $|G|$ and G is said to be finite (infinite) according as $|G|$ is finite (infinite).

Example 2.3.1 $(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$ and $(\mathbf{R}, +)$ are infinite abelian groups, where $+$ denotes ordinary addition. They are called *additive group of integers*, *additive group of rational numbers* and *additive group of real numbers,* respectively.

Example 2.3.2 $(\mathbf{Q}^*, \cdot)$, $(\mathbf{R}^*, \cdot)$ and $(\mathbf{C}^*, \cdot)$, $(S^1, \cdot)$ $(S^1 = \{z \in \mathbf{C} : |z| = 1\})$ form groups under usual multiplication, where $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ and $\mathbf{C}$ denote respectively the set of all non-zero rational numbers, non-zero real numbers, non-zero complex numbers and all complex numbers. They are called *multiplicative groups of non-zero rationals, multiplicative group of non-zero reals* and *multiplicative group of non-zero complex numbers,* respectively. $(S^1, \cdot)$ is called *circle group* in $\mathbf{C}$.

We now present vast sources of interesting groups.

Example 2.3.3 (Permutation group) Let S be a non-empty set and $A(S)$ be the set of all bijective mappings from S onto itself. Let $f, g \in A(S)$.

Define

$$fg \quad \text{by } (fg)(x) = f\big(g(x)\big), \quad \text{for all } x \in S. \tag{2.1}$$

First we show that $fg \in A(S)$. Suppose $x, y \in S$ and $(fg)(x) = (fg)(y)$. Then $f(g(x)) = f(g(y))$. Since f is injective, it follows that $g(x) = g(y)$. Again this implies $x = y$ as g is injective. Consequently, fg is an injective mapping. Now let $x \in S$. Since f is surjective, there exists $y \in S$ such that $f(y) = x$. Again g is surjective. Hence $g(z) = y$ for some $z \in S$. Then $(fg)(z) = f(g(z)) = f(y) = x$. This implies that fg is surjective and hence $fg \in A(S)$. Since every element of $A(S)$ has an inverse, we find that $A(S)$ is a group under the composition defined by (2.1) This group is called the *permutation group* or the *group of all permutations* on S.

Example 2.3.4 (Symmetric group) In Example 2.3.3, if S contains only n $(n \geq 1)$ elements, say $S = I_n = \{1, 2, \ldots n\}$, then the group $A(S)$ is called the *symmetric group* S_n on n elements. If $f \in A(S)$, then f can be described by listing the elements of I_n on a row and the image of each element under f directly below it. According to this assumption we write

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \quad \text{where } f(t) = i_t \in I_n,\ t \in I_n.$$

Suppose now $i_1, i_2, \ldots, i_r$ $(r \leq n)$ are r distinct elements of I_n. If $f \in A(S)$ be such that f maps $i_1 \mapsto i_2, i_2 \mapsto i_3, \ldots, i_{r-1} \mapsto i_r, i_r \mapsto i_1$ and maps every other elements of I_n onto itself, then f is also written as $f = (i_1 i_2 \cdots i_r)$. This is called an *r-cycle*. A 2-cycle is called a transposition. The permutations $\alpha_1, \alpha_2, \ldots, \alpha_t$ in S_n are said to be disjoint iff for every i, $1 \leq i \leq t$ and every k in I_n, $\alpha_i(k) \neq k$ imply $\alpha_j(k) = k$ for every j, $1 \leq j \leq t$. A permutation $\alpha \in S_n$ is said to be even or odd according as α can be expressed as a product of even or odd number of transpositions. The set of all even permutations in S_n forms a group, called the alternating group of degree n, denoted by A_n. For $n \geq 3$, it is a normal subgroup of S_n (see Ex. 14 of SE-II).

The groups S_n are very useful to the study of finite groups. As n increases the structure of S_n becomes complicated. But we can work out the case $n = 3$ comfortably. The symmetric group S_3 has six elements and is the smallest group whose law of composition is not commutative.

Because of importance of this group, we now describe this group as follows:

For $n = 3$, $I_3 = \{1, 2, 3\}$ and $A(S) = S_3$. This *symmetric groups* S_3 consists of exactly six elements:

$$\begin{array}{llllll} e: 1 \mapsto 1, & f_1: 1 \mapsto 2, & f_2: 1 \mapsto 3, & f_3: 1 \mapsto 1, & f_4: 1 \mapsto 3, & f_5: 1 \mapsto 2 \\ \quad 2 \mapsto 2 & \quad 2 \mapsto 3 & \quad 2 \mapsto 1 & \quad 2 \mapsto 3 & \quad 2 \mapsto 2 & \quad 2 \mapsto 1 \\ \quad 3 \mapsto 3 & \quad 3 \mapsto 1 & \quad 3 \mapsto 2 & \quad 3 \mapsto 2 & \quad 3 \mapsto 1 & \quad 3 \mapsto 3. \end{array}$$

We can describe these six mappings in the following way:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1), \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 \quad 2 \quad 3),$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2), \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3),$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3), \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1 \quad 2).$$

In

$$S_3, e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

is the identity element.

Now

$$f_1 f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = f_5 \quad \text{and} \quad f_3 f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_4.$$

Hence $f_1 f_3 \neq f_3 f_1$. Consequently S_3 is not a commutative group.

Example 2.3.5 (General linear group) Let $GL(2, \mathbf{R})$ denote the set of all 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where a, b, c, d are real numbers and $ad - bc \neq 0$. Taking usual multiplication of matrices as the group operation, we can show that $GL(2, \mathbf{R})$ is a group where $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the identity element and the element

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

is the inverse of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $GL(2, \mathbf{R})$.

This is a non-commutative group, as $\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right) \in GL(2, \mathbf{R})$ and $\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)\left(\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 19 & 22 \\ 43 & 50 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 5 & 6 \\ 7 & 8 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 23 & 34 \\ 31 & 46 \end{smallmatrix}\right)$.

This group is called the *general linear group* of order 2 over the set of all real numbers $\mathbf{R}$.

Remark The group $GL(2, \mathbf{C})$ defined in a similar way is called *general linear group of order 2 over* $\mathbf{C}$. In general, $GL(n, \mathbf{R})$ ($GL(n, \mathbf{C})$), the group of all invertible $n \times n$ real (complex) matrices is called *general linear group of order n* over $\mathbf{R}$ ($\mathbf{C}$).

The concept of congruence of integers (see Chap. 1) is essentially due to Gauss. This is one of the most important concepts in number theory. This suggests the concept of congruence relations on groups, which is important in modern algebra, because every congruence relation on a group produces a new group.

We now introduce the concept of congruence relation on a group. An equivalence relation ρ on a group G is said to be a *congruence* relation on G iff $(a, b) \in \rho$ implies $(ca, cb) \in \rho$ and $(ac, bc) \in \rho$, for all $c \in G$. Let a be an element of a group G and ρ be a congruence relation on G. Then the subset $\{x \in G : (a, x) \in \rho\}$ is called a *congruence class* for the element a. This subset is denoted by (a). The following theorem lists some properties of congruence classes.

Theorem 2.3.1 *Let ρ be a congruence relation on a group G. Then*

(i) $a \in (a)$;
(ii) $(a) = (b)$ *iff* $(a, b) \in \rho$;
(iii) *if* $a, b \in G$, *then either* $(a) = (b)$ *or* $(a) \cap (b) = \emptyset$;
(iv) *If* $(a) = (b)$ *and* $(c) = (d)$, *then* $(ac) = (bd)$ *and* $(ca) = (db)$.

Proof (i) Left as an exercise.

(ii) Left as an exercise.

(iii) Suppose $(a) \cap (b) \neq \emptyset$. Let $c \in (a) \cap (b)$. Then $(a, c) \in \rho$ and $(b, c) \in \rho$. Let $x \in (a)$. Then $(a, x) \in \rho$. From the symmetric and transitive property of ρ and from $(a, c) \in \rho$ and $(a, x) \in \rho$ we find that $(c, x) \in \rho$. Hence $(b, c) \in \rho$ and $(c, x) \in \rho$ imply that $(b, x) \in \rho$. As a result $x \in (b)$ and hence $(a) \subseteq (b)$. Similarly, we can show that $(b) \subseteq (a)$. Consequently $(a) = (b)$.

(iv) From the assumption, $(a, b) \in \rho$ and $(c, d) \in \rho$. Now ρ is a congruence relation. Hence $(ca, cb) \in \rho$ and $(cb, db) \in \rho$. The transitive property of ρ implies that $(ca, db) \in \rho$. Hence $(ca) = (db)$. Similarly $(ac) = (bd)$. □

The following theorem will show how one can construct a new group from a given group G if a congruence relation ρ on G is given.

Theorem 2.3.2 *Let ρ be a congruence relation on a group G. If G/ρ is the set of all congruence classes for ρ on G, then G/ρ becomes a group under the binary operation given by $(a)(b) = (ab)$.*

Proof Let $(a), (b) \in G/\rho$. Suppose $(a) = (c)$ and $(b) = (d)$ $(c, d \in G)$. Then $(a, c) \in \rho$ and $(b, d) \in \rho$. Hence from (iv) of Theorem 2.3.1, we find that $(ab, cd) \in \rho$. This shows that $(ab) = (cd)$. Therefore the operation defined by $(a)(b) = (ab)$ is well defined. Now, let (a), (b) and (c) be three elements of G. Then $((a)(b))(c) = (ab)(c) = ((ab)c) = (a(bc)) = (a)(bc) = (a)((b)(c))$. Therefore G/ρ is a semigroup. We can show that the congruence class (1) containing the identity element 1 of G is the identity element of G/ρ. If $(a) \in G/\rho$, then $a \in G$ and hence $a^{-1} \in G$ implies $(a^{-1}) \in G/\rho$. Now $(a^{-1})(a) = (a^{-1}a) = (1) = (aa^{-1}) = (a)(a^{-1})$. Hence the inverse of (a) exists in G/ρ. Consequently G/ρ is a group. □

Corollary 1 *If G is a commutative group and ρ is a congruence on G, then G/ρ is a commutative group.*

Example 2.3.6 (Additive group of integers modulo m) Let $(\mathbf{Z}, +)$ be the additive group of integers. Let m be a fixed positive integer. Define a relation ρ on $\mathbf{Z}$ by

$$\rho = \{(a, b) \in \mathbf{Z} \times \mathbf{Z} : a - b \text{ is divisible by } m\}.$$

Clearly, ρ is a congruence relation. This relation is usually called *congruence relation modulo* m. Two integers a and b are said to be congruent modulo m, written $a \equiv b \pmod{m}$, iff $a - b$ is divisible by m. For each integer a, the congruence class to which a belongs is $(a) = \{x \in \mathbf{Z} : x \equiv a \pmod{m}\} = \{a + km : k \in \mathbf{Z}\}$. Let $\mathbf{Z}/\rho$ denote the set of all congruence classes modulo m.

From Theorem 2.3.2, we find that $\mathbf{Z}/\rho$ is a group where the group operation + is defined by

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

This group is a commutative group. In this group the identity element is the congruence class (0) and $(-a)$ is the inverse of (a). Generally we denote this group by $\mathbf{Z}_m$ and this group is said to be the *additive group of integers modulo* m. $(0), (1), \ldots, (m-1)$ exhaust all the elements of $\mathbf{Z}_m$. Given an arbitrary integer a, the division algorithm implies that there exist unique integers q nd r such that

$$a = mq + r, \quad 0 \leq r < m.$$

From the definition of congruence $a \equiv r \pmod{m}$, it follows that $(a) = (r)$. Clearly, there are m possible remainders: $0, 1, \ldots, m-1$. Consequently, every integer belongs to one and only one of the m different congruence classes: $(0), (1), \ldots, (m-1)$ and $\mathbf{Z}_m$ consists of exactly these elements.

Remark The above example shows that for every positive integer m, there exists an abelian group G such that $|G| = m$.

Note 1 $\mathbf{Z}_m$ may be considered to be a group consisting of m integers $0, 1, \ldots, m-1$ together with the binary operation $*$ given by the rule:

$$\begin{aligned} \text{for } t, s \in \mathbf{Z}, \quad t * s &= t + s, && \text{if } t + s < m \\ &= r, && \text{if } t + s \geq m, \text{ where } r \text{ is the remainder} \\ & && \text{when } t + s \text{ is divided by } m. \end{aligned}$$

One of the basic problems in group theory is to classify groups up to isomorphisms. For such a classification, we have to either construct an explicit expression for an isomorphism or we have to show that no such isomorphism exists. An isomorphism is a special homomorphism and it identifies groups for their classifications. The concept of a homomorphism is itself very important in modern algebra.

In the context of group theory (like semigroup), the word homomorphism means a mapping from a group to another, which respects binary operations defined on the two groups: If $f : G \to G'$ is a mapping between groups G and G', then f is called

a homomorphism iff $f(ab) = f(a)f(b)$ for all $a, b \in G$. The *kernel* of the homomorphism f denoted by $\ker f$ is defined by $\ker f = \{a \in G : f(a) = 1_{G'} = 1'\}$.

Remark Taking $a = b = 1$, the identity element in G, we find $f(1) = f(1)f(1)$, which shows that $f(1)$ is the identity element $1'$ of G'. Again taking $b = a^{-1}$, we find $f(1) = f(a)f(a^{-1})$. This implies $f(a^{-1}) = [f(a)]^{-1}$. Thus a homomorphism of groups maps identity element into identity element and the inverse element into the inverse element.

Note 2 If $f : G \to G'$ is a homomorphism of groups, then

$$f\left(a^n\right) = \left(f(a)\right)^n, \quad a \in G,\ n \in \mathbf{Z}\ \left(a^n \text{ is defined in Definition 2.3.4}\right).$$

Proof It follows by induction on n that for $n = 1, 2, 3, \ldots,$

$$f\left(a^n\right) = \left(f(a)\right)^n.$$

Again $f(a^{-1}) = (f(a))^{-1}$ shows that for $n = -k, k = 1, 2, 3, \ldots,$

$$f\left(a^n\right) = f\left(\left(a^{-1}\right)^k\right) = \left(f\left(a^{-1}\right)\right)^k = \left(f(a)\right)^{-k} = \left(f(a)\right)^n$$

Finally, $f(a^0) = f(1) = 1' = (f(a))^0$. □

Definition 2.3.3 A homomorphism $f : G \to G'$ between groups is called

(i) an *epimorphism* iff f is surjective (i.e., onto);
(ii) a *monomorphism* iff f is injective (i.e., 1–1);
(iii) an *isomorphism* iff f is an epimorphism and a monomorphism;

An isomorphism of a group onto itself is called an *automorphism* and a homomorphism of a group G into itself is called an *endomorphism*.

Remark Since two isomorphic groups have the identical properties, it is convenient to identify them to each other. They may be considered as replicas of each other.

If $f : G \to H$ and $g : H \to K$ are homomorphisms of groups, then their usual composition $g \circ f : G \to K$ defined by $(g \circ f)(a) = g(f(a)), a \in G$, is again a homomorphism. Because if $a, b \in G$, then $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$.

Theorem 2.3.3 *Let $f : G \to G'$ be a homomorphism of groups. Then*

(i) *f is a monomorphism iff* $\ker f = \{1\}$;
(ii) *f is an epimorphism iff* $\operatorname{Im} f = G'$;
(iii) *f is an isomorphism iff there is a homomorphism $g : G' \to G$ such that $g \circ f = I_G$ and $f \circ g = I_{G'}$, where I_G is the identity homomorphism of G.*

Proof (i) Let f be a monomorphism. Then f is injective and hence $\ker f = \{1\}$. Conversely, let $\ker f = \{1\}$. Now if $f(a) = f(b)$, then $f(ab^{-1}) = f(a)f(b)^{-1} = 1$ shows that $ab^{-1} \in \ker f = \{1\}$, and hence $a = b$. Consequently, f is injective.

(ii) and (iii) follow trivially. □

Theorem 2.3.4 *Let G be a group and* Aut G *be the set of all automorphisms of G. Then* Aut G *is a group, called the automorphism group of G.*

Proof For $f, g \in \text{Aut}\, G$, define $f \circ g$ to be the usual composition. Clearly, $f \circ g \in \text{Aut}\, G$. Then Aut G becomes a group with identity homomorphism I_G of G as identity and f^{-1} as the inverse of $f \in \text{Aut}\, G$. □

Example 2.3.7 (i) Let $(\mathbf{R}^*, \cdot)$ be the multiplicative group of non-zero reals and $GL(2, \mathbf{R})$ be the general linear group defined in Example 2.3.5. Consider the map $f : GL(2, \mathbf{R}) \to \mathbf{R}^*$ defined by $f(A) = \det A$. Then for $A, B \in GL(2, \mathbf{R})$, $AB \in GL(2, \mathbf{R})$ and $f(AB) = \det(AB) = \det A \det B = f(A)f(B)$. This shows that f is a homomorphism. As $1 \in \mathbf{R}^*$ is the identity element of $(\mathbf{R}^*, \cdot)$, $\ker f = \{A \in GL(2, \mathbf{R}) : f(A) = \det A = 1\}$.

(ii) Let G be the group under binary operation on $\mathbf{R}^3$ defined by $(a, b, c) * (x, y, z) = (a + x, b + y, c + z + ay)$ and H be the group of matrices

$$\left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{R} \right\}$$

under usual matrix multiplication. Then the map $f : G \to H$ defined by

$$f(a, b, c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

is an isomorphism.

(iii) Let G be an abelian group and $f : G \to G$ be the map defined by $f(a) = a^{-1}$. Then f is an automorphism of G. This automorphism is different from the identity automorphism.

(iv) Let $(\mathbf{R}, +)$ and $(\mathbf{R}^+, \cdot)$ denote the additive group of reals and multiplication group of positive reals, respectively. Then the map $f : \mathbf{R} \to \mathbf{R}^+$ defined by $f(x) = e^x$ is an isomorphism.

(v) Let $(\mathbf{Q}, +)$ and $(\mathbf{Q}^+, \cdot)$ denote the additive group of rationals and multiplicative group of positive rationals, respectively. Then these groups cannot be isomorphic. To prove this, let $\exists$ an isomorphism $f : (\mathbf{Q}, +) \to (\mathbf{Q}^+, \cdot)$. Then for $2 \in \mathbf{Q}^+$, $\exists$ a unique element $x \in \mathbf{Q}$ such that $f(x) = 2$. Now $x = \frac{x}{2} + \frac{x}{2}$ and $\frac{x}{2} \in \mathbf{Q}$ show that $2 = f(x) = f(\frac{x}{2} + \frac{x}{2}) = f(\frac{x}{2})f(\frac{x}{2}) = [f(\frac{x}{2})]^2$. This cannot hold as $f(\frac{x}{2})$ is a positive rational. Hence f cannot be an isomorphism.

In any group, the integral powers a^n of a group element a play an important role to study finitely generated groups, in particular, cyclic groups.

Powers of an element have been defined in a semigroup, for positive integral indices. In a group, however, powers can be defined for all integral values of the index, i.e., positive, negative, and zero.

Definition 2.3.4 Let a be an element of a group G. Define

(i) $a^0 = 1$ and $a^1 = a$;
(ii) $a^{n+1} = a^n a$ for any non-negative integer n;

If $n = -m$ $(m > 0)$ be a negative integer, then define $a^{-m} = (a^m)^{-1} = (a^{-1})^m$; a^n is said to be the nth power of a.

The exponents so defined have the following properties:

$$a^m a^n = a^{m+n} \quad \text{and} \quad \left(a^m\right)^n = a^{mn}.$$

Definition 2.3.5 Let G be a group. An element $a \in G$ is said to be of *finite order* iff there exists a positive integer n such that $a^n = 1$. If a is an element of finite order, then the smallest positive integer of the set $\{m \in \mathbf{N}^+ : a^m = 1\}$ (existence of the smallest positive integer is guaranteed by the well-ordering principle) is called the *order* or *period* of a (denoted by $O(a)$). An element $a \in G$ is said to be of infinite order, iff there is no positive integer n such that $a^n = 1$.

Example 2.3.8 Let $G = \{1, -1, i, -i\}$. Then G is a group under usual multiplication of complex numbers. In the group, -1 is an element of order 2 and i is an element of order 4.

Remark An element a of a group G is of infinite order iff $a^r \neq a^t$ whenever $r \neq t$. This is so because $a^r = a^t \Leftrightarrow a^{r-t} = 1$; that is, a is of finite order, unless $r = t$.

Theorem 2.3.5 *Let G be a group and $a \in G$ such that $O(a) = t$. Then*

(i) *the elements* $1 = a^0, a, \ldots, a^{t-1}$ *are all distinct*;
(ii) $a^n = 1$, *iff* $t|n$;
(iii) $a^n = a^m$, *iff* $n \equiv m \pmod{t}$;
(iv) $O(a^r) = t/\gcd(t, r)$, $(r, m, n \in \mathbf{Z})$.

Proof (i) If for $0 < n < m < t$, $a^m = a^n$, then $a^{m-n} = a^m(a^n)^{-1} = 1$. This contradicts the property of the order of a, since $o < m - n < t$ and $O(a) = t$.

(ii) If $n = tm$, then $a^n = a^{tm} = (a^t)^m = 1$. Conversely, if $a^n = 1$, taking $n = tm + r$, where $0 \leq r < t$, we have $1 = a^n = a^{tm+r} = (a^t)^m a^r = a^r$. This implies $r = 0$, since t is the smallest positive integer for which $a^t = 1$ and $0 \leq r < t$. Therefore $n = tm$, and hence t is a factor of n.

(iii) $a^m = a^n \Leftrightarrow a^{n-m} = 1 \Leftrightarrow t$ is a factor of $n - m$ by (ii) $\Leftrightarrow n \equiv m \pmod{t}$.

(iv) Let $\gcd(t, r) = m$ and $t/\gcd(t, r) = n$. Then $t = nm$.

Let $r = ms$, where $\gcd(n, s) = 1$. Now $(a^r)^q = a^{rq} = 1 \Leftrightarrow t|rq$ by (ii) $\Leftrightarrow nm|msq \Leftrightarrow n|sq \Leftrightarrow n|q$, since $\gcd(n, s) = 1$. Thus the smallest positive integer q

for which $(a^r)^q = 1$ holds is given by $q = n$. This implies $n = t/\gcd(t, r)$ is the order of a^r. □

Remark Any power a^n is equal to one of the elements given in (i).

Definition 2.3.6 A group G is called a

(i) *torsion group* or a *periodic group* iff every element of G is of finite order;
(ii) *torsion-free* group iff every element of G except the identity element is of infinite order;
(iii) *mixed group* iff some elements of G are of infinite order and some excepting 1 are of finite order.

Example 2.3.9 (i) (Finite torsion group) Consider the multiplicative group $G = \{1, -1, i, -i\}$. Then G is a *torsion group*.

(ii) (Group of rationals modulo 1) Consider the additive group $\mathbf{Q}$ of all rational numbers. Let $\rho = \{(a, b) \in \mathbf{Q} \times \mathbf{Q} : a - b \in \mathbf{Z}\}$. Then ρ is a congruence relation on $\mathbf{Q}$ and hence $\mathbf{Q}/\rho$ is a group under the composition $(a) + (b) = (a + b)$. Now $(\frac{1}{n})$, $n = 1, 2, 3, \ldots$, are distinct elements of $\mathbf{Q}/\rho$. Then $\mathbf{Q}/\rho$ contains infinite number of elements. Let p/q be any rational number such that $q > 0$. Now $q(p/q) = (p) = (0)$ shows that (p/q) is an element of finite order. Consequently, $\mathbf{Q}/\rho$ is a *torsion group*. This is an infinite abelian group, called the group of rationals modulo 1, denoted by $\mathbf{Q}/\mathbf{Z}$.

Example 2.3.10 (Torsion-free group) The positive rational numbers form a multiplicative group $\mathbf{Q}^+$ under usual multiplication. The integer 1 is the identity element of this group and it is the only element of finite order. Consequently, $\mathbf{Q}^+$ is a *torsion-free group*.

Example 2.3.11 (Mixed group) The multiplicative group of non-zero complex numbers $\mathbf{C}^*$ contains infinitely many elements of finite order, viz. every nth root of unity, for $n = 1, 2, \ldots$. It also contains infinitely many elements $re^{i\theta}$, with $r \neq 1$, of infinite order. Consequently, $\mathbf{C}^*$ is a mixed group.

2.4 Subgroups and Cyclic Groups

Arbitrary subsets of a group do not generally invite any attention. But subsets forming groups contained in larger groups create interest. For example, the group of even integers with 0, under usual addition is contained in the larger group of all integers and the group of positive rational numbers under usual multiplication is contained in the larger group of positive real numbers. Such examples suggest the concept of a subgroup, which is very important in the study of group theory. The cyclic subgroup is an important subgroup and is generated by an element g of a group G. It is the smallest subgroup of G which contains g. In this section we study subgroups and cyclic groups.

Let $(G, \circ)$ be a group and H a non-empty subset of G. If for any two elements $a, b \in H$, it is true that $a \circ b \in H$, then we say that H is closed under this group operation of G. Suppose now H is closed under the group operation '$\circ$' on G. Then we can define a binary operation $\circ_H : H \times H \to H$ by $a \circ_H b = a \circ b$ for all $a, b \in H$. This operation $\circ_H$ is said to be the restriction of '$\circ$' to $H \times H$. We explain this with the help of the following example.

Example 2.4.1 Consider the additive group $(\mathbf{R}, +)$ of real numbers. If $\mathbf{Q}^*$ is the set of all non-zero rational numbers, then $\mathbf{Q}^*$ is a non-empty subset of $\mathbf{R}$. Now for any two $a, b \in \mathbf{Q}^*$, we find that ab (under usual product of rational numbers) is an element of $\mathbf{Q}^*$. But we cannot say that $\mathbf{Q}^*$ is closed under the group operation '$+$' on $\mathbf{R}$. Consider now the set $\mathbf{Z}$ of integers. We can show easily that $\mathbf{Z}$ is closed under the group operation '$+$' on $\mathbf{R}$.

Definition 2.4.1 A subset H of a group $(G, \circ)$ is said to be a subgroup of the group G iff

(i) $H \neq \emptyset$;
(ii) H is closed under the group operation '$\circ$' on G and
(iii) $(H, \circ_H)$ is itself a group, where $\circ_H$ is the restriction of '$\circ$' to $H \times H$.

Obviously, every subgroup becomes automatically a group.

Remark $(\mathbf{Q}^*, \cdot)$ is not a subgroup of the additive group $(\mathbf{R}, +)$. But $(\mathbf{Z}, +)$ is a subgroup of the group $(\mathbf{R}, +)$.

The following theorem makes it easier to verify that a particular subset H of a group G is actually a subgroup of G. In stating the theorem we again use the multiplicative notation.

Theorem 2.4.1 *Let G be a group and H a subset of G. Then H is a subgroup of G iff $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.*

Proof Let H be a subgroup of G and $a, b \in H$. Then $b^{-1} \in H$ and hence $ab^{-1} \in H$. Conversely, let the given conditions hold in H. Then $aa^{-1} = 1 \in H$ and $1a^{-1} = a^{-1} \in H$ for all $a \in H$. Clearly, associative property holds in H (as it is hereditary). Finally, for all $a, b \in H$, $ab = a(b^{-1})^{-1} \in H$, since $b^{-1} \in H$. Consequently, H is a subgroup of G. □

Corollary *A subset H of a group G is a subgroup of G iff $H \neq \emptyset$ and $ab \in H$, $a^{-1} \in H$ for all $a, b \in H$.*

Proof It follows from Theorem 2.4.1. □

Using the above theorem we can prove the following:

(i) G is a subgroup of the group G.
(ii) $H = \{1\}$ is a subgroup of the group G.

Hence we find that every group G has at least two subgroups: G and $\{1\}$. These are called *trivial subgroups.* Other subgroups of G (if they exist) are called proper subgroups of G.

We now give an interesting example of a subgroup.

Definition 2.4.2 The *center* of a group G, written $Z(G)$ is the set of those elements of G which commute with every element in G, that is, $Z(G) = \{a \in G : ab = ba \text{ for all } b \in G\}$.

This set is extremely important in group theory. In an abelian group G, $Z(G) = G$. The center is in fact a subgroup of G. This follows from the following theorem.

Theorem 2.4.2 *The center $Z(G)$ of a group G is a subgroup of G.*

Proof Since $1b = b = b1$ for all $b \in G, 1 \in Z(G)$. Hence $Z(G) \neq \emptyset$. Let $a, b \in Z(G)$. Then for all $x \in G, ax = xa$ and $bx = xb$. Hence $ax = xa$ and $xb^{-1} = b^{-1}x$. Now $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$ for all $x \in G$. Hence $ab^{-1} \in Z(G)$. Consequently $Z(G)$ is a subgroup of G. □

We now introduce the concepts of conjugacy class and conjugate subgroup.

Let G be a group and $a \in G$. An element $b \in G$ is said to be a *conjugate* of a in G iff $\exists g \in G$, such that $b = gag^{-1}$. Then the relation ρ on G defined by $\rho = \{(a, b) \in G \times G : b \text{ is a conjugate of } a\}$ is an equivalence relation, called *conjugacy* on G; the equivalence class (a) of the relation ρ is called a *conjugacy class* of a in G. Two subgroups H and K of G are said to be conjugate subgroups iff there exists some g in G such that $K = gHg^{-1}$. Clearly, conjugacy is an equivalence relation on the collection of subgroups of G. The equivalence class of the subgroup H is called the conjugacy class or the conjugate class of H.

Theorem 2.4.3 *Let H be a subgroup of a group G and $g \in G$. Then gHg^{-1} is a subgroup of G such that $H \cong gHg^{-1}$.*

Proof Since $1 = g1g^{-1} \in gHg^{-1}$, $gHg^{-1} \neq \emptyset$. For $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, we have $(gh_1g^{-1})(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1} \in gHg^{-1}$. Hence gHg^{-1} is a subgroup of G. Consider the map $f : H \to gHg^{-1}$ defined by $f(h) = ghg^{-1}$ $\forall h \in H$. For $h_1, h_2 \in H, h_1 = h_2 \Rightarrow gh_1g^{-1} = gh_2g^{-1} \Rightarrow f$ is well defined. Also for $a \in gHg^{-1}$, there exists $h = g^{-1}ag \in H$ such that $f(h) = ghg^{-1} = gg^{-1}agg^{-1} = a$. Moreover, $f(h_1) = f(h_2) \Rightarrow gh_1g^{-1} = gh_2g^{-1} \Rightarrow h_1 = h_2$. Finally, $f(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = f(h_1)f(h_2)$ $\forall h_1, h_2 \in H$. Consequently, f is an isomorphism. □

Let H and K be two subgroups of a group G. Now both subgroups H and K contain the identity 1 of G. Hence $H \cap K \neq \emptyset$. Let $a, b \in H \cap K$. Then $a, b \in H$ and also $a, b \in K$. Since H and K are both subgroups, $ab^{-1} \in H$ and $ab^{-1} \in K$. Hence $ab^{-1} \in H \cap K$ for all $a, b \in H \cap K$. Consequently, $H \cap K$ in a subgroup of G. The more general theorem follows:

Theorem 2.4.4 *Let $\{H_i : i \in I\}$ be a family of subgroups of a group G. Then $\bigcap_{i\in I} H_i$ is a subgroup of G.*

Proof Trivial. □

Theorem 2.4.5 *Let $f : G \to K$ be a homomorphism of groups. Then*

(i) $\text{Im } f = \{f(a) : a \in G\}$ *is a subgroup of* K;
(ii) $\ker f = \{a \in G : f(a) = 1_K\}$ *is a subgroup of* G, *where* 1_K *denotes the identity element of* K.

Proof It follows by using Theorem 2.4.1. □

Remark Let $\mathcal{C}$ be a given collection of groups. Define a relation '$\sim$' on $\mathcal{C}$ by $G_1 \sim G_2$ iff $\exists$ an isomorphism $f : G_1 \to G_2$. Then '$\sim$' is an equivalence relation which partitions $\mathcal{C}$ into mutually disjoint classes of isomorphic groups. Two isomorphic groups are abstractly indistinguishable. The main problem of group theory is: given a group G, how is one to determine the above equivalence class containing G, i.e., to determine the class of all groups which are isomorphic to G? In other words, given two groups G_1 and G_2, the problem is to determine whether G_1 is isomorphic to G_2 or not i.e., either to determine an isomorphism $f : G_1 \to G_2$ or to show that there does not exist such an isomorphism. We can solve such problems partially by using the concept of generator, which is important for a study of certain classes of groups, such as cyclic groups, finitely generated groups which have applications to number theory and homological algebra.

Finitely Generated Groups and Cyclic Groups There are some groups G which are generated by a finite set of elements of G. Such groups are called finitely generated and are very important in mathematics. A cyclic group is, in particular, generated by a single element.

Let G be a group and A be a non-empty subset of G. Consider the family $\mathcal{C}$ of all subgroups of G containing A. This is a non-empty family, because $G \in \mathcal{C}$. Now the intersection of all subgroups of this family is again a subgroup of G. This subgroup contains A and this subgroup is denoted by $\langle A\rangle$.

Definition 2.4.3 If A is a non-empty subset of a group G, then $\langle A\rangle$ is called the *subgroup generated* by A in the group G. If $\langle A\rangle = G$, then G is said to be generated by A, and if, A contains finite number of elements, then G is said to be *finitely generated*.

If A contains a finite number of elements, say $A = \{a_1, a_2, \ldots, a_n\}$, then we write $\langle a_1, a_2, \ldots a_n\rangle$ in place of $\langle\{a_1, a_2, \ldots, a_n\}\rangle$.

The particular case when A consists of a single element of the group is of immense interest. For example, for the circle S of radius 1 in the Euclidean plane, if r is a rotation through an angle $2\pi/n$ radians about the origin, then $r^n = r \circ r \circ \cdots \circ r$ (n times) is the identity. This example leads to the concept of cyclic groups.

Definition 2.4.4 A subgroup H of a group G is called a *cyclic subgroup* of G iff $\exists$ an element $a \in G$ such that $H = \langle a \rangle$ and G is said to be cyclic iff $\exists$ an element $a \in G$ such that $G = \langle a \rangle$, a is called a *generator* of G.

Theorem 2.4.6 *Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^n : n \in \mathbf{Z}\}$.*

Proof Let $T = \{a^n : n \in \mathbf{Z}\}$. Then for $c, d \in T$, there exist $r, t \in \mathbf{Z}$ such that $c = a^r$ and $d = a^t$. Now $cd^{-1} = a^r(a^t)^{-1} = a^r a^{-t} = a^{r-t} \in T \Rightarrow T$ is subgroup of G. Clearly, $\{a\} \subseteq T$. Let H be a subgroup of G such that $\{a\} \subseteq H$. Then $a \in H$ and hence $a^{-1} \in H$. As a result $a^n \in H$ for any $n \in \mathbf{Z}$ and then $T \subseteq H$. Hence T is the intersection of all subgroups of G containing $\{a\}$. This shows that $\langle a \rangle = T = \{a^n : n \in \mathbf{Z}\}$. □

Remark If a group G is cyclic, then there exists an element $a \in G$ such that any $x \in G$ is a power of a, that is, $x = a^n$ for some $n \in \mathbf{Z}$. Then the mapping $f : \mathbf{Z} \to G$ defined by $f(n) = a^n$ is an epimorphism. Moreover, if $\ker f = \{0\}$, f is a monomorphism by Theorem 2.3.3(i), and hence f is an isomorphism, and such G is called an infinite cyclic group or a free cyclic group. For example, $\mathbf{Z}$ is an infinite additive cyclic group with generator 1. Clearly, -1 is also a generator.

Remark Every cyclic group is commutative. Its converse is not true. For example, the Klein four-group (see Ex. 22 of Exercises-III) is a finite commutative group which is not cyclic and $(\mathbf{Q}, +)$ is an infinite commutative group which is not finitely generated (see Ex. 1 of SE-I) and hence not cyclic.

Theorem 2.4.7 *An infinite cyclic group is torsion free.*

Proof Let G be an infinite cyclic group and $1 \neq a \in G$. Then $G = \langle g \rangle$ for some $g \in G$. Consequently, $a = g^t$, where t is a non-zero integer. If a is of finite order $r > 0$, then $g^{tr} = a^r = 1$, a contradiction. Consequently, a is of infinite order. □

Let G be a group. If G contains a finite number of elements, then the group G is said to be a *finite group*, otherwise, the group G is called an *infinite group*. The number of elements of a finite group is called the order of the group. We write $|G|$ or $O(G)$ to denote the *order* of a group G.

Theorem 2.4.8 *Let G be a group and $a \in G$. Then the order of the cyclic subgroup $\langle a \rangle$ is equal to $O(a)$, when it is finite, and is infinite when $O(a)$ is infinite.*

Proof It follows from Theorem 2.3.5, and Remark of Definition 2.3.5. □

In particular, if $\gcd(t, r) = 1$ in Theorem 2.3.5(iv), then $O(a) = O(a^r)$ and therefore each of a and a^r generates the same group G. This proves the following theorem.

Theorem 2.4.9 *If G is a cyclic group of order n, then there are $\phi(n)$ distinct elements in G, each of which generates G, where $\phi(n)$ is the number of positive integers less than and relatively prime to n.*

The function $\phi(n)$ is called the Euler ϕ-function *in honor of Leonhard Euler* (1707–1783).

For example, for $\mathbf{Z}_{14}$, $\phi(14) = 6$ and $\mathbf{Z}_{14}$ can be generated by each of the elements (1), (3), (5), (9), (11) and (13), since $r(1)$ is a generator iff gcd $(r, 14) = 1$, where $0 < r < 14$.

Remark If a, b are relatively prime positive integers then $\phi(ab) = \phi(a)\phi(b)$. Moreover, for any positive prime integer p, $\phi(p) = p - 1$, $\phi(p^n) = p^n - p^{n-1}$ for all integers $n \geq 1$ and if $n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r}$, then $\phi(n) = p_1^{n_1-1}(p_1 - 1)p_2^{n_2-1}(p_2 - 1) \dots p_r^{n_r-1}(p_r - 1)$ (see Chap. 10).

Theorem 2.4.10 *Every non-trivial subgroup of the additive group $\mathbf{Z}$ is cyclic.*

Proof Let H be a subgroup of $\mathbf{Z}$, and $H \neq \{0\}$. Then H contains a smallest positive integer a (say). To prove the theorem it is sufficient to show that any integer $x \in H$ is of the form na for some $n \in \mathbf{Z}$. If $x = na + r$ where $0 \leq r < a$, then $r = x - na \in H$ as H is a group. Consequently, $r = 0$, so $x = na$. □

Theorem 2.4.11 *If G is a cyclic group, then every subgroup of G is cyclic.*

Proof If G is infinite cyclic, then by definition $G \cong \mathbf{Z}$. Then the proof follows from Theorem 2.4.10. Next suppose that G is a finite cyclic group generated by a and H a subgroup of G. Let t be the smallest positive integer such that $a^t \in H$. We claim that a^t is a generator of H. Let $a^m \in H$. If $m = tq + r$, $0 \leq r < t$, then $a^r = a^{m-tq} = a^m(a^t)^{-q} \in H$, since $a^m, a^t \in H$. Since $0 \leq r < t$, it follows by the property of t that $r = 0$. Therefore $m = tq$ and hence $a^m = (a^t)^q$. Thus every element $a^m \in H$ is some power of a^t. Again, since $a^t \in H$, every power of a^t is in H. Hence $H = \langle a^t \rangle$. Thus H is cyclic. □

The following theorem gives a characterization of the cyclic groups.

Theorem 2.4.12 *Let $(G, \cdot)$ be a cyclic group. Then*

(i) *$(G, \cdot)$ is isomorphic to $(\mathbf{Z}, +)$ iff G is infinite;*
(ii) *$(G, \cdot)$ is isomorphic to $(\mathbf{Z}_n, +)$ iff G is finite and $|G| = n$.*

Proof (i) Let $(G, \cdot)$ be an infinite cyclic group. Then the group $(G, \cdot)$ is isomorphic to $(\mathbf{Z}, +)$. Conversely, suppose $(G, \cdot)$ is isomorphic to $(\mathbf{Z}, +)$. In this case, since $(\mathbf{Z}, +)$ is infinite, $(G, \cdot)$ is also infinite, as an isomorphism is a bijection.

(ii) Suppose $(G, \cdot)$ is a finite cyclic group. Then the case (i) cannot arise and therefore the case (ii) must occur. In this case $(G, \cdot)$ is isomorphic to $(\mathbf{Z}_n, +)$, where

$n = |G|$. Conversely, suppose $(G, \cdot)$ is isomorphic to $(\mathbf{Z}_n, +)$. Then $|\mathbf{Z}_n| = n \Rightarrow |G| = n \Rightarrow G$ is finite. □

Remark Let G and K be finite cyclic groups such that $|G| = m \neq n = |K|$. Then G and K cannot be isomorphic, i.e., there cannot exist an isomorphism $f : G \to K$.

Theorem 2.4.13 *Let G be a cyclic group of order n and H a cyclic group of order m such that* $\gcd(m, n) = 1$. *Then $G \times H$ is a cyclic group of order mn. Moreover, if a is a generator of G and b a generator of H, then (a, b) is a generator of $G \times H$.*

Proof Clearly, $G \times H$ is a group under pointwise multiplication defined by $(g, h)(g', h') = (gg', hh')$ for all g, g' in G and h, h' in H. If e_1 and e_2 be identity elements of G and H respectively, then $a^n = e_1$ and $1 \leq r < n \Rightarrow a^r \neq e_1$, $b^m = e_2$ and $1 \leq r < m \Rightarrow b^r \neq e_2$. Let $x = (a, b) \in G \times H$. Then $x^{mn} = (a^{mn}, b^{mn})$ by definition of multiplication (i.e., pointwise multiplication) in

$$G \times H \quad \Rightarrow \quad x^{mn} = (e_1, e_2) \quad \Rightarrow \quad \text{order } x \leq mn \tag{2.2}$$

Again

$$\begin{aligned} x^t = (e_1, e_2) \quad &\Rightarrow \quad \left(a^t, b^t\right) = (e_1, e_2) \\ &\Rightarrow \quad a^t = e_1 \quad \text{and} \quad b^t = e_2 \\ &\Rightarrow \quad n|t \quad \text{and} \quad m|t \\ &\Rightarrow \quad mn|t \quad \left(\text{since } \gcd(m, n) = 1\right) \\ &\Rightarrow \quad t \geq mn \\ &\Rightarrow \quad \text{order } x \geq mn \end{aligned} \tag{2.3}$$

Consequently, (2.2) and (2.3) $\Rightarrow$ order x = order $(a, b) = mn$. Since $|G \times H| = mn$ and the order of the element $(a, b) = mn$, it follows that (a, b) generates $G \times H$ i.e., $G \times H$ is a cyclic group of order mn. □

Remark The converse of the last part of Theorem 2.4.13 is also true. Suppose (u, v) is a generator of $G \times H$. Let a be a fixed generator of G and b a fixed generator of H. Then since $\langle (u, v) \rangle = G \times H$, $\exists$ positive integers n and r such that $(u, v)^n = (a, e_2) \in G \times H$ and $(u, v)^r = (e_1, b) \in G \times H$. Then $u^n = a$ and $v^r = b \Rightarrow G = \langle a \rangle \subseteq \langle u \rangle \subseteq G$ and $H = \langle b \rangle \subseteq \langle v \rangle \subseteq H \Rightarrow \langle u \rangle = G$ and $\langle v \rangle = H \Rightarrow u$ is a generator of G and v is a generator of H.

Problems

Problem 1 Let G ($\neq \{1\}$) be a group which has no other subgroup except G and $\{1\}$. Show that G is isomorphic to $\mathbf{Z}_p$ for some prime p.

Solution Let $a \in G - \{1\}$ (since $G \neq \{1\}$). If $T = \langle a \rangle$, then $T = G$ (since $a \in T$ and $a \neq 1$) $\Rightarrow G$ is a cyclic group generated by a. If possible, let G be infinite cyclic.

Then $G = \{a^n : n \in \mathbf{Z}\}$, $a^m \neq a^n$ for $n \neq m$ and $a^0 = 1$. Consider $H = \{a^{2n} : n \in \mathbf{Z}\}$. Then H is proper subgroup of G (as $a \notin H$) and $H \neq \{1\}$. This contradicts the fact that only subgroups of G are G and $\{1\}$. So, G cannot be infinite cyclic. In other words, G must be finite cyclic. Let $|G| = n$. If possible, let $n = rs$, $1 < r < n$, $1 < s < n$. Since $r||G|$ and G is cyclic, G has a cyclic subgroup H of order r. This contradicts the fact that only subgroups of G are G and $\{1\}$. So, n cannot be composite, i.e., n is some prime p, since $G \neq \{1\}$. Thus $(G, \cdot)$ is a cyclic group of order p and hence isomorphic to $(\mathbf{Z}_p, +)$ by Theorem 2.4.12(ii).

Problem 2 Let G be a group which is isomorphic to every proper subgroup H of G with $H \neq \{1\}$ and assume that there exists at least one such proper subgroup $H \neq \{1\}$. Show that G is infinite cyclic. Conversely, if G is an infinite cyclic group, show that G is isomorphic to every proper subgroup H of G such that $H \neq \{1\}$.

Solution There exists an element $a \in G$ such that $a \neq 1$. Let P be the cyclic subgroup generated by a. So, by hypothesis, P is isomorphic to G as $P \neq \{1\}$. Since P is cyclic, G must be also cyclic. Consequently, G is infinite.

Conversely, let G be an infinite cyclic group and H a proper subgroup of G such that $H \neq \{1\}$. Then $H = \langle a^r \rangle (r \geq 1)$, where a is a generator of G. Consider a function $f : G \to H$ by $f(a) = a^r$. Then $f(a^n) = a^{rn}$. Clearly, f is an isomorphism.

2.5 Lagrange's Theorem

One of the most important invariants of a finite group is its order. While studying finite groups Lagrange established a relation between the order of a finite group and the order of its any subgroup. He proved that the order of any subgroup H of a finite group G divides the order of G. This is established by certain decompositions of the underlying set G into a family of subsets $\{aH : a \in G\}$ or $\{Ha : a \in G\}$, called cosets of H.

Let G be a group and H subgroup of G. If $a \in G$, then aH denotes the subset $\{ah \in G : h \in H\}$ and Ha denotes the subset $\{ha \in G : h \in H\}$ of G. Now $a = a1 = 1a$ shows that $a \in aH$ and $a \in Ha$. The set aH is called the *left coset* of H in G containing a and Ha is called the *right coset* of H in G containing a. A subset A of G is called a left (right) coset of H in G iff $A = aH$ $(= Ha)$ for some $a \in G$.

Lemma 2.5.1 *If H is a subgroup of a group G and $a, b \in G$, then each of the following statements is true.*

(i) $aH = H$ *iff* $a \in H$;
(i)' $Ha = H$ *iff* $a \in H$;
(ii) $aH = bH$ *iff* $a^{-1}b \in H$;
(ii)' $Ha = Hb$ *iff* $ab^{-1} \in H$;
(iii) *Either* $aH = bH$ *or* $aH \cap bH = \emptyset$;
(iii)' *Either* $Ha = Hb$ *or* $Ha \cap Hb = \emptyset$;

(iv) $G = \bigcup_{\langle a \in G \rangle} aH$;
(iv)' $G = \bigcup_{\langle a \in G \rangle} Ha$;
(v) *There exists a bijection* $aH \to H$ *for each* $a \in G$;
(v)' *There exists a bijection* $Ha \to H$ *for each* $a \in G$;
(vi) *If* $\mathcal{L}$ *is the set of all left cosets of* H *in* G *and* $\mathcal{R}$ *is the set of all right cosets of* H *in* G, *then there exists a bijection from* $\mathcal{L}$ *onto* $\mathcal{R}$.

Proof (i)–(iv) follow trivially.

(v) If $x \in aH$, then there exists $h \in H$ such that $x = ah$.

Suppose $x = ah_1 = ah_2$ $(h_1, h_2 \in H)$. Then $h_1 = a^{-1}(ah_1) = a^{-1}(ah_2) = h_2$. Hence for each $x \in aH$ there exists a unique $h \in H$ such that $x = ah$. Define $f : aH \to H$ by $f(x) = h$ when $x = ah \in aH$. Now one can show that f is a bijective mapping from aH onto H.

(vi) Define $f : \mathcal{L} \to \mathcal{R}$ by $f(aH) = Ha^{-1}$. One can show that f is a well defined bijective mapping. □

Example 2.5.1 (i) Consider the group S_3 on the set $I_3 = \{1, 2, 3\}$. In S_3, $H = \{e, (12)\}$ is a subgroup. For this subgroup $eH = \{e, (12)\}$, $(13)H = \{(13), (123)\}$ and $(23)H = \{(23), (132)\}$ are three distinct left cosets and $S_3 = eH \cup (13)H \cup (23)H$. Again $He = \{e, (12)\}$, $H(13) = \{(13), (132)\}$, $H(23) = \{(23), (123)\}$ are three distinct right cosets of H and

$$S_3 = He \cup H(13) \cup H(23).$$

Hence the number of left cosets of H is three and the number of right cosets of H is also three. But $\mathcal{L} \neq \mathcal{R}$.

(ii) Consider the group $\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ (see Example 2.3.6). In $\mathbf{Z}_6$, $H = \{0, 3\}$ is a subgroup. Using additive notation, the left cosets $H = \{0, 3\}$, $1 + H = \{1, 4\}$, $2 + H = \{2, 5\}$ partition $\mathbf{Z}_6$.

We now prove several interesting results about finite groups.

One of the most important invariance of a finite group is its order.

Let G be a finite group. Any subgroup H of G is also a finite group. Lagrange's Theorem (Theorem 2.5.1) establishes a relation between the order of H and the order of G. It plays a very important role in the study of finite groups.

Theorem 2.5.1 (Lagrange's Theorem) *The order of a subgroup of a finite group divides the order of the group.*

Proof Let G be a finite group of order n and H a subgroup of G. Let $|H| = m$. Now $1 \leq m \leq n$. We can write $G = \bigcup_{a \in G} aH$. Since any two left cosets of H are either identical or disjoint, there exist elements $a_1, a_2, \ldots, a_t$ $(t \leq n)$ such that left cosets $a_1H, a_2H, \ldots, a_tH$ are all distinct and $G = a_1H \cup a_2H \cdots \cup a_tH$. Hence $|G| = |a_1H| + |a_2H| + \cdots + |a_tH|$ ($|a_iH|$ denotes the number of elements in a_iH).

Let $H = \{h_1, h_2, \ldots, h_m\}$. Then $aH = \{ah_1, ah_2, \ldots, ah_m\}$. The cancellation property of a group implies that $ah_1, ah_2, \ldots, ah_m$ are m distinct elements, so that

$|H| = |aH|$ ($|aH|$ denotes the number of elements in aH). Therefore $n = |G| = |a_1H| + |a_2H| + \cdots + |a_tH| = |H| + |H| + \cdots + |H|$ (t times) $= t|H| = tm$. Hence m divides n, where $n = |G|$. □

Corollary 1 *The order of an element of a finite group divides the order of the group.*

Proof Let G be a finite group and $a \in G$. Then $O(a) = |\langle a \rangle|$ by Theorem 2.4.8. Hence the corollary follows from Lagrange's Theorem 2.5.1. □

Corollary 2 *A group of prime order is cyclic.*

Proof Let G be a group of prime order p and $1 \neq a \in G$. Then $O(a)$ is a factor of p by Corollary 1. As p is prime, either $O(a) = p$ or $O(a) = 1$. Now $a \neq 1 \Rightarrow O(a) = p \Rightarrow |\langle a \rangle| = p = |G| \Rightarrow G$ is a cyclic group, since $\langle a \rangle \subseteq G$. □

Remark The converse of the Lagrange Theorem asserts that if a positive integer m divides the order n of a finite group G, then G contains a subgroup of order m. But it is not true in general. For example, the alternating group A_4 of order 12 has no subgroup of order 6 (see Ex. 4 of SE-I). However, the following properties of special finite groups show that the partial converse is true.

1. If G is a finite abelian group, then corresponding to every positive divisor m of n, there exists a subgroup of order m (see Corollary 2 of Cauchy's Theorem in Chap. 3).
2. If $m = p$, a prime integer, then G has a subgroup of order p (see Cauchy's Theorem in Chap. 3).
3. If m is a power of a prime p, then G has a subgroup of order m (see Sylow's First Theorem in Chap. 3).

Let G be a group and H be a subgroup of G. We have proved that there exists a bijective mapping $f : \mathcal{L} \to \mathcal{R}$, where $\mathcal{L}$ is the set of all left cosets of H in G and $\mathcal{R}$ is the set of all right cosets of H in G. Then the cardinal number of $\mathcal{L}$ is the same as the cardinal number of $\mathcal{R}$. This cardinal number is called the index of H in G and is denoted by $[G : H]$. If $\mathcal{L}$ is a finite set, then the cardinal number of $\mathcal{L}$ is the number of left cosets of H in G. Hence in this case the number of left cosets of H (equivalently the number of right cosets of H) in G is the index of H in G.

Theorem 2.5.2 *If H is a subgroup of a finite group G, then*

$$[G : H] = \frac{|G|}{|H|}.$$

Proof Let G be a finite group of order n. Then a subgroup H of G must also be of finite order, r (say). Every left coset of H contains exactly r distinct elements. If $[G : H] = i$, then $n = ri$, since the cosets are disjoint. This proves the theorem. □

Given two finite subgroups H and K of a group G, $HK = \{hk : h \in H \text{ and } k \in K\}$ may not be a subgroup of G. Hence $|HK|$ may not divide $|G|$. However, Theorem 2.5.3 determines $|HK|$.

Theorem 2.5.3 *If H and K are two finite subgroups of a group G, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof Let $A = H \cap K$. Then A is a subgroup of G such that $A \subseteq H$ and $A \subseteq K$. Now A is a subgroup of the finite group H. Hence $[H : A]$ is finite. Let $[H : A] = t$. Then there exist elements $x_1, x_2, \ldots, x_t$ in H such that $x_1A, x_2A, \ldots, x_tA$ are distinct left cosets of A in H and $H = \bigcup_{i=1}^{t} x_iA$. Now $HK = (\bigcup_{i=1}^{t} x_iA)K = \bigcup_{i=1}^{t} x_iK$, since $A \subseteq K$. We claim that $x_1K, x_2K, \ldots, x_tK$ are t distinct left cosets of K.

Suppose $x_iK = x_jK$ for some i and j, where $1 \leq i \neq j \leq t$. Then $x_j^{-1}x_i \in K$. But $x_j^{-1}x_i \in H$. Hence $x_j^{-1}x_i \in H \cap K = A$. This shows that $x_iA = x_jA$; this is not true as $x_1A, \ldots, x_tA$ are distinct. As a result $|HK| = |x_1K| + |x_2K| + \cdots + |x_tK|$. Also, by Lemma 2.5.1(v) it follows that $|x_iK| = |K|$. Consequently,

$$|HK| = t|K| = [H : A]|K| = \frac{|H||K|}{|A|} = \frac{|H||K|}{|H \cap K|}. \qquad \square$$

Corollary *If H and K are finite subgroups of a group G such that $H \cap K = \{1\}$, then $|HK| = |H||K|$.*

2.6 Normal Subgroups, Quotient Groups and Homomorphism Theorems

In this section we make the study of normal subgroups and develop the theory of quotient groups with the help of homomorphisms. We show how to construct isomorphic replicas of all homomorphic images of a specified abstract group. For this purpose we introduce the concept of normal subgroups. For some subgroups of a group, every left coset is a right coset and conversely, which implies that for some subgroups, the concepts of a left coset and a right coset coincide. Such subgroups are called normal subgroups. Galois first recognized that those subgroups for which left and right cosets coincide are a distinguished one. We shall now study those subgroups H of a group G such that $aH = Ha$ for all $a \in G$. Such subgroups play an important role in determining both the structure of a group and the nature of the homomorphisms with domain G.

Definition 2.6.1 Let H be a subgroup of a group G and $a, b \in G$. Then a is said to be *right* (*left*) *congruent* to b modulo H, denoted by $a\rho_r b \pmod{H}$ ($a\rho_l b \pmod{H}$) iff $ab^{-1} \in H$ ($a^{-1}b \in H$).

Theorem 2.6.1 *Let H be a subgroup of a group H. Then the relation ρ_r (ρ_l) on G is an equivalence relation and the corresponding equivalence class of $a \in G$ is the right (left) coset Ha (aH). ρ_r (ρ_l) is called the right (left) congruence relation on G modulo H.*

Proof We write $a\rho b$ for $a\rho_r b \pmod H$ and then prove the theorem only for right congruence ρ and right cosets.

$aa^{-1} = 1 \in H \Rightarrow a\rho a \ \forall a \in G$. Again $a\rho b \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow b\rho a$. Finally, $a\rho b$ and $b\rho c \Rightarrow ab^{-1} \in H$ and $bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H \Rightarrow ac^{-1} \in H \Rightarrow a\rho c$. Consequently, ρ is an equivalence relation. Now for each $a \in G$, $a\rho = \{x \in G : x\rho a\} = \{x \in G : xa^{-1} \in H\} = \{x \in G : xa^{-1} = h \text{ for some } h \in H\} = \{x \in G : x = ha, h \in H\} = \{ha \in G : h \in H\} = Ha$. □

Theorem 2.6.2 *If H is a subgroup of a group G, then the following conditions are equivalent.*

(i) *Left congruence ρ_l and right congruence ρ_r on G modulo H coincide*;
(ii) *every left coset of H in G is also a right coset of H in G*;
(iii) *$aH = Ha$ for all $a \in G$*;
(iv) *for all $a \in G$, $aHa^{-1} \subseteq H$, where $aHa^{-1} = \{aha^{-1} : h \in H\}$.*

Proof (i) $\Leftrightarrow$ (iii) $\rho_l = \rho_r \Leftrightarrow a\rho_l = a\rho_r \ \forall a \in G \Leftrightarrow aH = Ha \ \forall a \in G$ by Theorem 2.6.1.

(iii) $\Leftrightarrow$ (iv) Suppose $aH = Ha \ \forall a \in G$. Then for each $h \in H$, $ah = h'a$ for some $h' \in H$. Consequently, $aha^{-1} = h' \in H \ \forall h \in H$. This shows that $aHa^{-1} \subseteq H$ for every $a \in G$. Again let for every $a \in G$, $aHa^{-1} \subseteq H$. Then $H = a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1}$, since $a^{-1}Ha \subseteq H$ (by hypothesis). Consequently, $aHa^{-1} = H$ for every $a \in G$. This shows that $aH = Ha \ \forall a \in G$.

(ii) $\Leftrightarrow$ (iii) Suppose $aH = Hb$ for $a, b \in G$. Then $a \in Ha \cap Hb$. Since two right cosets of H in G are either disjoint or equal, it follows that $Ha = Hb$ and hence (ii) $\Rightarrow$ (iii). Its converse is trivial. □

Definition 2.6.2 Let G be a group and H a subgroup of G. Then H is said to be a *normal subgroup* of G denoted by $H \triangle G$ iff H satisfies any one of the equivalent conditions of Theorem 2.6.2.

Thus for a normal subgroup, we need not distinguish between the left and right cosets.

In any group G, G and $\{1\}$ are normal subgroups, called trivial normal subgroups. Every subgroup of a commutative group is a normal subgroup.

Example 2.6.1 If S_3 is the symmetric group of order 6, then $H = \{e, (123), (132)\}$ is a subgroup of S_3. Now for any $a \in H$, $aH = H = Ha$. The elements (12), (23), and (13) $\notin H$. Now $(12)H = \{(12), (23), (13)\} = H(12)$. Similarly, $(13)H = H(13)$ and $(23)H = H(23)$. Consequently, H is a normal subgroup of S_3. Clearly, $K = \{e, (12)\}$ is not a normal subgroup of S_3.

Theorem 2.6.3 *Let A and B be two subgroups of a group G.*

(i) *If A is a normal subgroup of a group G, then $AB = BA$ is a subgroup of G.*
(ii) *If A and B are normal subgroups of G, then $A \cap B$ is a normal subgroup of G.*
(iii) *If A and B are normal subgroups of G such that $A \cap B = \{1\}$, then $ab = ba$ $\forall a \in A$ and $\forall b \in B$.*

Proof (i) Let $x = ab \in AB$. Now $bA = Ab \Rightarrow ab = ba_1$ for some $a_1 \in A \Rightarrow x = ba_1 \in BA \Rightarrow AB \subseteq BA$. Similarly, $BA \subseteq AB$. Consequently, $AB = BA$. Again for $b, b' \in B$ and $a, a' \in A$, $(ba)(b'a')^{-1} = ba(a'^{-1}b'^{-1}) = b(aa'^{-1})b'^{-1} = ba_1b'^{-1}(a_1 \in A) = b_1a_2$, where $a_2 \in A$, $b_1 \in B$. This implies $BA = AB$ is a subgroup of G.

(ii) Clearly, $H = A \cap B$ is a normal subgroup of G, since if $h \in H$ and $g \in G$, then ghg^{-1} belongs to both A and B and hence is in H.

(iii) Consider the element $x = aba^{-1}b^{-1}(a \in A, b \in B)$. Now $x = (aba^{-1})b^{-1} \in (aBa^{-1})b^{-1} \subseteq Bb^{-1} = B$ and again $x = a(ba^{-1}b^{-1}) \in a(bAb^{-1}) \subseteq aA = A$. Hence $x \in A \cap B = \{1\}$. Consequently, $aba^{-1}b^{-1} = 1$. This shows that $ab = ba$ $\forall a \in A$ and $\forall b \in B$. □

We now show how to make the set of cosets into a group, called a quotient group.

Theorem 2.6.4 *Let H be a normal subgroup of a group G and G/H the set of all cosets of H in G. Then G/H is a group.*

Proof Define multiplication of cosets by $(aH) \cdot (bH) = (ab)H$, $\forall a, b \in G$. We show that the multiplication is well defined. Let $aH = xH$ and $bH = yH$. Then $a \in aH$ and $b \in bH$ are such that $a = xh_1$ and $b = yh_2$ for some $h_1, h_2 \in H$. Now, $(xy)^{-1}(ab) = y^{-1}x^{-1}ab = y^{-1}x^{-1}xh_1yh_2 = y^{-1}h_1yh_2 \in H$, since $y^{-1}h_1y \in H$ as H is a normal subgroup of G. Consequently, by Lemma 2.5.1, it follows that $(ab)H = (xy)H \Rightarrow (aH) \cdot (bH) = (xH) \cdot (yH)$. Then G/H is a group where the identity element is the coset H, and the inverse of aH is $a^{-1}H$. □

Corollary *If H is a normal subgroup of a finite group G then $|G/H| = |G|/|H|$.*

Proof It follows from Theorem 2.5.2. □

Definition 2.6.3 If H is a normal subgroup of a group G, then group G/H is called the *factor group* (or quotient group) of G by H.

Remark If G is an additive abelian group, the group operation on G/H is defined by

$$(a + H) + (b + H) = (a + b) + H$$

and the corresponding quotient group G/H is sometimes called difference group.

We now show that the construction of quotient groups is closely related to homomorphisms of groups and prove a natural series of theorems.

Theorem 2.6.5 *If $f : G \to T$ is a homomorphism of groups, then the kernel of f is a normal subgroup of G. Conversely, if H is a normal subgroup of G, then the map*

$$\pi : G \to G/H, \quad \text{given by } \pi(g) = gH, \quad g \in G$$

is an epimorphism with kernel H.

Proof Clearly, $1 \in \ker f$. So, $\ker f \neq \emptyset$. Let $x, y \in \ker f$. Then $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = 1 \cdot 1 = 1 \ \forall x, y \in \ker f \Rightarrow \ker f$ is a subgroup of G by Theorem 2.4.1. Again if $g \in G$, then $f(gxg^{-1}) = f(g)f(x)(f(g))^{-1} = f(g) \cdot 1 \cdot (f(g))^{-1} = 1 \Rightarrow gxg^{-1} \in \ker f \Rightarrow \ker f$ is a normal subgroup of G.

The map $\pi : G \to G/H$ given by $\pi(g) = gH$ is clearly surjective. Moreover, $\pi(gg') = gg'H = gHg'H = \pi(g)\pi(g') \ \forall g, g' \in G \Rightarrow \pi$ is an epimorphism, called the canonical epimorphism or projection or natural homomorphism. Now $\ker \pi = \{g \in G : \pi(g) = H\} = \{g \in G : gH = H\} = \{g \in G : g \in H\} = H$. □

Remark Let G be a group and H a subgroup of G. Then H is a normal subgroup of G iff H is the kernel of some homomorphism.

Theorem 2.6.6 (Fundamental Homomorphism Theorem for groups) *Let $f : G \to H$ be a homomorphism of groups and N a normal subgroup of G such that $N \subseteq \ker f$. Then there is a unique homomorphism $\tilde{f} : G/N \to H$ such that $\tilde{f}(gN) = f(g) \ \forall g \in G, \operatorname{Im} \tilde{f} = \operatorname{Im} f$ and $\ker \tilde{f} = \ker f/N$. Moreover, $\tilde{f}$ is an isomorphism iff f is an epimorphism and $\ker f = N$.*

Proof If $x \in gN$, then $x = gn$ for some $n \in N$ and $f(x) = f(gn) = f(g)f(n) = f(g)1 = f(g)$, since by hypothesis $N \subseteq \ker f$. This shows that the effect of f is the same on every element of the coset gN. Thus the map $\tilde{f} : G/N \to H$, $gN \mapsto f(g)$ is well defined. Now $\tilde{f}(gN \cdot hN) = \tilde{f}(ghN) = f(gh) = f(g)f(h) = \tilde{f}(gN)\tilde{f}(hN) \ \forall g, h \in G \Rightarrow \tilde{f}$ is a homomorphism. From the definition of $\tilde{f}$, it is clear that $\operatorname{Im} \tilde{f} = \operatorname{Im} f$. Moreover, $gN \in \ker \tilde{f} \Leftrightarrow f(g) = 1 \Leftrightarrow g \in \ker f$. Consequently, $\ker \tilde{f} = \{gN : g \in \ker f\} = \ker f/N$. Since $\tilde{f}$ is completely determined by f, $\tilde{f}$ is unique. Clearly, f is a monomorphism iff $\ker \tilde{f} = \ker f/N$ is a trivial subgroup of G/N. The latter holds iff $\ker f = N$. Moreover, $\tilde{f}$ is an epimorphism iff f is an epimorphism. Consequently, $\tilde{f}$ is an isomorphism iff f is an epimorphism and $\ker f = N$. □

Corollary 1 (First Isomorphism Theorem) *If $f : G \to H$ is a homomorphism of groups, then f induces an isomorphism $\tilde{f} : G/\ker f \to \operatorname{Im} f$.*

Corollary 2 *If G and H are groups and $f : G \to H$ is an epimorphism, then the group $G/\ker f$ and H are isomorphic.*

Remark The homomorphic images of a given abstract group G are the quotient groups G/N by its different normal subgroups N.

Proposition 2.6.1 *If G and H are groups and $f : G \to H$ is a homomorphism of groups, N is a normal subgroup of G, and T is a normal subgroup of H such that $f(N) \subseteq T$, then there is a homomorphism $\tilde{f} : G/N \to H/T$.*

Proof Define $\tilde{f} : G/N \to H/T$ by $\tilde{f}(gN) = f(g)T$. □

Corollary *If $f : G \to H$ is a homomorphism of groups with* ker $f = N$, *then there is a monomorphism $\tilde{f} : G/N \to H$.*

Proof We have $f(N) = \{1\}$ and $\{1\}$ is a trivial normal subgroup of H. Then by Proposition 2.6.1, f induces a homomorphism $\tilde{f} : G/N \to H$ given by $\tilde{f}(gN) = f(g)\ \forall g \in G$. This shows that $\tilde{f}$ is a monomorphism. Moreover, if $f : G \to H$ is an epimorphism, then $\tilde{f} : G/N \to H$ is also an epimorphism. □

Remark These results also prove the *First Isomorphism Theorem*.

Theorem 2.6.7 (Subgroup Isomorphism Theorem or the Second Isomorphism Theorem) *Let N be a normal subgroup of a group G and H a subgroup of G. Then $H \cap N$ is a normal subgroup of H, HN is a subgroup of G and $H/H \cap N \cong HN/N$ (or NH/N), where $HN = \{hn : h \in H, n \in N\}$.*

Proof Suppose $x \in H \cap N$ and $h \in H$. Then $h^{-1}xh \in N$ as N is a normal subgroup of G. Moreover, $h^{-1}xh \in H$ as $x \in H$. Consequently, $h^{-1}xh \in H \cap N \Rightarrow H \cap N$ is a normal subgroup of H. Clearly, $HN \neq \emptyset$. Now $x, y \in HN \Rightarrow x = hn$ and $y = h'n'$ for some $n, n' \in N, h, h' \in H \Rightarrow xy^{-1} = hn(h'n')^{-1} = hnn'^{-1}h'^{-1} = hn_1h'^{-1}$ (for some $n_1 \in N$)$= hh'^{-1}h'n_1h'^{-1} = h_1n_2$ (where $hh'^{-1} = h_1 \in H$ and $h'n_1h'^{-1} = n_2 \in N$ as N is a normal subgroup of G) $\in HN \Rightarrow HN$ is a subgroup of G.

Define $f : H \to HN/N$ by $h \mapsto hN$. Then f is an epimorphism. By using First Isomorphism Theorem, $H/\ker f \cong f(H) = HN/N$.

Now ker $f = \{x \in H : f(x) = N\} = \{x : x \in H$ and $xN = N\} = \{x : x \in H$ and $x \in N\} = H \cap N$. Consequently, $H/H \cap N \cong HN/N$. □

Theorem 2.6.8 (Factor of a Factor Theorem or Third Isomorphism Theorem) *If both H and K are normal subgroups of a group G and $K \subseteq H$, then H/K is a normal subgroup of G/K and $G/H \cong (G/K)/(H/K)$.*

Proof Clearly, G/K, G/H and H/K are groups.

Consider the map $f : G/K \to G/H$ given by

$$f(aK) = aH, \quad \forall a \in G.$$

As $aK = bK \Rightarrow a^{-1}b \in K \subseteq H \Rightarrow aH = bH$, the map f is well defined.

Again,

$$f(aK \cdot bK) = f(abK) = abH = aHbH$$
$$= f(aK)f(bK), \quad \text{for all } aK, bK \in G/K$$

shows that f is a homomorphism.

Clearly, f is an epimorphism. We have

$$\ker f = \{aK \in G/K : f(aK) = aH = H\}$$
$$= \{aK : a \in H\} = H/K.$$

Consequently, by the First Isomorphism Theorem, $(G/K)/(H/K) \cong G/H$. □

Theorem 2.6.9 *Let $f : G \to K$ be an epimorphism of groups and S a subgroup of K. Then $H = f^{-1}(S)$ is a subgroup of G such that* $\ker f \subseteq H$. *Moreover, if S is normal in K, then H is normal in G. Furthermore, if $H_1 \supseteq \ker f$ is any subgroup of G such that $f(H_1) = S$, then $H_1 = H$.*

Proof It is clear that, as $1 \in H$, $H \neq \emptyset$. For $g, h \in H$, $f(gh^{-1}) = f(g)f(h^{-1}) = f(g)f(h)^{-1} \in S \Rightarrow gh^{-1} \in H \Rightarrow H$ is a subgroup of G. Now $\ker f = \{g \in G : f(g) = 1_K \in S\} \Rightarrow \ker f \subseteq H$. Next let S be normal in K, $g \in G$ and $h \in H$. Then $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} \in S \Rightarrow ghg^{-1} \in H \Rightarrow H$ is normal in G.

Finally, let $H_1 \supseteq \ker f$ be a subgroup of G such that $f(H_1) = S$. We claim that $H_1 = H$. Now $h_1 \in H_1 \Rightarrow f(h_1) \in S \Rightarrow H_1 \subseteq H$. Again $h \in H \Rightarrow f(h) = s \in S$. Choose $h_1 \in H_1$ such that $f(h_1) = s$. Then $f(hh_1^{-1}) = f(h)f(h_1)^{-1} = ss^{-1} = 1_K \Rightarrow hh_1^{-1} \in \ker f \subseteq H_1 \Rightarrow h \in H_1 \Rightarrow H \subseteq H_1$. Consequently, $H = H_1$. □

Corollary 1 (Correspondence Theorem) *If $f : G \to K$ is an epimorphism of groups, then the assignment $H \mapsto f(H)$ defines an one-to-one correspondence between the set $S(G)$ of all subgroups H of G which contain* $\ker f$ *and the set $S(K)$ of all subgroups of K such that normal subgroups correspond to normal subgroups.*

Proof The assignment $H \mapsto f(H)$ defines a map $\psi : S(G) \to S(K)$. By Theorem 2.6.9 it follows that ψ is a bijection. Moreover, the last part also follows from this theorem. □

Corollary 2 *If N is a normal subgroup of a group G, then every subgroup of G/N is of the form T/N, where T is a subgroup of G that contains N.*

Proof Apply Corollary 1 (Theorem 2.6.9) to the natural epimorphism $\pi : G \to G/N$. □

By using the First Isomorphism Theorem, the structure of certain quotient groups is determined.

Example 2.6.2 (i) Let $G = GL(n, \mathbf{R})$ be the group of all non-singular $n \times n$ matrices over $\mathbf{R}$ under usual matrix multiplication and H the subset of all matrices

$X \in GL(n, \mathbf{R})$ such that $\det X = 1$, i.e., $H = \{X \in GL(n, \mathbf{R}) : \det X = 1\}$. Since the identity matrix $I_n \in H$, $H \neq \emptyset$. Let $X, Y \in H$, so that $\det X = \det Y = 1$. By using the properties of determinants, we have $\det(XY^{-1}) = \det X \cdot \det(Y^{-1}) = \det X \cdot (1/\det Y) = 1$. Thus $X, Y \in H \Rightarrow XY^{-1} \in H \Rightarrow H$ is a subgroup of G by Theorem 2.4.1. Moreover, H is a normal subgroup of G by Theorem 2.6.5, because H is the kernel of the determinant function $\det : GL(n, \mathbf{R}) \to \mathbf{R}^*$ given by $X \mapsto \det X$, where $\mathbf{R}^*$ is the multiplicative group of non-zero reals. As the image set of this homomorphism is $\mathbf{R}^*$, we have $GL(n, \mathbf{R})/H \cong \mathbf{R}^*$.

Remark A similar result holds for $GL(n, \mathbf{C})$ with complex entries.

(ii) Let $f : (\mathbf{R}, +) \to (\mathbf{C}^*, \cdot)$ be the homomorphism defined by $f(x) = e^{2\pi i x} = \cos 2\pi x + i \sin 2\pi x \ \forall x \in \mathbf{R}$. Then $\ker f$ is the additive group $(\mathbf{Z}, +)$ and $\operatorname{Im} f$ is the multiplicative group H of all complex numbers with modulus 1. Hence the additive quotient group $\mathbf{R}/\mathbf{Z}$ is isomorphic to the multiplicative group H.

Problem If H is a non-normal subgroup of a group G, is it possible to make the set $\{aH\}$ of left cosets of H in G a group with the rule of multiplication $aH \cdot bH = abH \ \forall a, b \in G$?

Solution (*The answer is no.*) If it was possible, then the mapping $f : G \to G'$, the group formed by the cosets, given by $x \mapsto xH$, would be a homomorphism with H as kernel. But this is not possible unless H is normal in G.

We now study a very important subgroup defined below which is closely associated with given subgroup.

Definition 2.6.4 If H is a subgroup of a group G, then the set $N(H) = \{a \in G : aHa^{-1} = H\} = \{a \in G : aH = Ha\}$ is called the normalizer of H and H is said to be *invariant* under each $a \in N(H)$.

Proposition 2.6.2 *If $N(H)$ is the normalizer of a subgroup H of a group G, then*

(i) *$N(H)$ is a subgroup of G;*
(ii) *H is a normal subgroup of $N(H)$;*
(iii) *if H and K are subgroups of G, and H is a normal subgroup of K, then $K \subseteq N(H)$;*
(iv) *H is a normal subgroup of $G \Leftrightarrow N(H) = G$.*

Proof (i) Since $1 \in N(H)$, $N(H) \neq \emptyset$. Now $x \in N(H) \Rightarrow xH = Hx \Rightarrow x^{-1}(xH) = x^{-1}(Hx) \Rightarrow H = (x^{-1}H)x \Rightarrow Hx^{-1} = x^{-1}H$.

Then $a, x \in N(H) \Rightarrow aH = Ha$ and $x^{-1}H = Hx^{-1} \Rightarrow (ax^{-1})H = a(x^{-1}H) = a(Hx^{-1}) = (aH)x^{-1} = Hax^{-1} \Rightarrow N(H)$ is a subgroup of G.

(ii) and (iii) follow trivially.

(iv) H is a normal subgroup of $G \Rightarrow$ for each $g \in G$, $gH = Hg \Rightarrow G \subseteq N(H)$. Consequently, $G = N(H)$. The converse part follows from (ii). □

In abelian groups every subgroup is normal but it is not true in an arbitrary non-abelian group. There are some groups in which no normal subgroup exists except its trivial subgroups. Such groups are called simple groups.

Definition 2.6.5 A group G is said to be simple iff G and $\{1\}$ are its only normal subgroups.

Definition 2.6.6 A normal subgroup H of a group G is said to be a maximal normal subgroup iff $H \neq G$ and there is no normal subgroup N of G such that $H \subsetneqq N \subsetneqq G$.

Theorem 2.6.10 *If H is a normal subgroup of a group G, then G/H is simple iff H is a maximal normal subgroup of G.*

Proof Let H be a maximal normal subgroup of G. Consider the canonical homomorphism $f : G \to G/H$. As f is an epimorphism, f^{-1} of any proper normal subgroup of G/H would be a proper normal subgroup of G containing H, which contradicts the maximality of H. Consequently G/H must be simple. Conversely, let G/H be simple. If N is a normal subgroup of G properly containing H, then $f(N)$ is a normal subgroup of G/H and if also $N \neq G$, then $f(N) \neq G/H$ and $f(N) \neq H$, which is not possible. So no such N exists and hence H is maximal. □

Remark There was a long-standing conjecture that a non-abelian simple group of finite order has an even number of elements. This conjecture has been proved to be true by Walker Feit and John Thompson.

2.7 Geometrical Applications

2.7.1 Symmetry Groups of Geometric Figures in Euclidean Plane

The study of symmetry gives the most appealing applications in group theory. While studying symmetry we use geometric reasoning. Symmetry is a common phenomenon in science. In general a symmetry of a geometrical figure is a one-one transformation of its points which preserves distance. Any symmetry of a polygon of n sides in the Euclidean plane is uniquely determined by its effect on its vertices, say $\{1, 2, \ldots, n\}$. The group of symmetries of a regular polygon of n sides is called the *dihedral group* of degree n denoted by D_n which is a subgroup of S_n and contains $2n$ elements. D_n is generated by rotation r of the regular polygon of n sides through an angle $2\pi/n$ radians in its own plane about the origin in anti-clockwise direction and certain reflections s satisfying some relations (see Ex. 19 of Exercises-III).

(a) *Isosceles triangle*. Figure 2.1 is symmetric about the perpendicular bisector 1D. So the symmetry group consists of identity and reflection about the line 1D. In

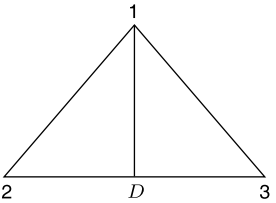


Fig. 2.1 Group of symmetries of isosceles triangle (S_2)

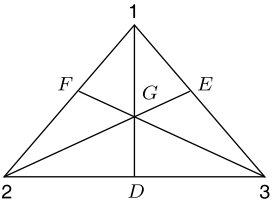


Fig. 2.2 Group of symmetries of equilateral triangle (S_3)

terms of permutations of vertices this group is

$$\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\} \cong S_2.$$

(b) *Equilateral triangle*. In Fig. 2.2, the symmetry consists of three rotations of magnitudes $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, $\frac{6\pi}{3} = 2\pi$ about the center G denoted by r_1, r_2 and r_3, respectively, together with three reflections about the perpendicular lines $1D, 2E, 3F$ denoted by t_1, t_2, and t_3, respectively. So in terms of permutations of vertices the symmetry group is

$$\left\{r_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, r_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, r_3 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\right.$$
$$\left. t_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, t_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, t_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\} \cong S_3.$$

(c) *Rectangle* (not a square). In this case, the symmetry group consists of the identity I, reflections r_1, r_2 about DE, FG (lines joining the midpoints of opposite sides), respectively, and reflection r_3 about O (which is actually a rotation about O through an angle π). In terms of permutations of vertices this group is

$$\left\{I = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, r_1 = \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\right.$$
$$\left. r_2 = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, r_3 = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\},$$

which is Klein's 4-group (see Ex. 22 of Exercises-III).

(d) *Square*. In Fig. 2.3, the symmetry group consists of four rotations r_1, r_2, r_3, r_4 (= Identity I) of magnitudes $\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi$ about the circumcenter O respectively and four reflections t_1, t_2, t_3, t_4 about DE, FG, 13, 24.

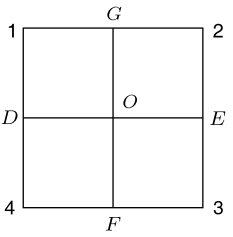


Fig. 2.3 Group of symmetries of the square (D_4)

In terms of permutations of vertices involved here, this group is

$$\left\{r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\right.$$
$$r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = I, t_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, t_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$
$$\left. t_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, t_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}\right\}.$$

This group is called the group of symmetries of the square (also called *octic* group) and is the dihedral group D_4 (see Ex. 19 of Exercises-III).

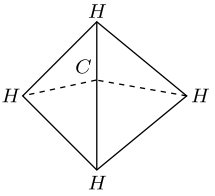
Remark In this group D_4 there are eight (hence octic) mappings of a square into itself that preserve distance between points and distance between their images, map adjacent vertices into adjacent vertices, center into center so that the only distance preserving mappings are rotations of the square about its center, reflections (flips) about various bisectors, and the identity map.

2.7.2 Group of Rotations of the Sphere

A sphere with a fixed center O can be brought from a given position into any other position by rotating the sphere about an axis through O. Clearly, the rotations about the same axis have the same result iff they differ by a multiple of 2π. Thus if $r(S)$ denotes the set of all rotations about the same axis, then we call the rotations r and r' in $r(S)$ equal or different iff they differ by a multiple of 2π or not. Clearly, the result of two successive rotations in $r(S)$ can also be obtained by a single rotation in $r(S)$. It follows that $r(S)$ forms a group. (The identity is a rotation in $r(S)$ through an angle 0 and the inverse of a rotation r in $r(S)$ has the same angle but in the opposite direction of r). Thus if any rotation r in $r(S)$ has the angle of rotation θ about the axis, then the map $f : r(S) \to S^1$ defined by $f(r) = e^{i\theta}$ is a group isomorphism from the group $r(S)$ onto the circle group S^1 (see Example 2.3.2).

Remark The rotations of $\mathbf{R}^2$ or $\mathbf{R}^3$ about the origin are the linear operators whose matrices with respect to the natural basis are orthogonal and have determinant 1 (see Chap. 8).

Fig. 2.4 Structure of CH_4



2.7.3 Clock Arithmetic

On a 24-hour clock, let the cyclic group $\langle a \rangle$ of order 24 represent hours. Then each of 24 numerals of the dial serves as representatives of a coset of hours. Here we use the fact that a 10 hour journey starting at 20 hrs (8 o'clock) ends at 30 hrs, i.e., $10 + 20 = 30 \equiv 6$ o'clock (the following day). In shifting from a 24-hour clock to a 12 hour clock, we take the 24 hours modulo the normal subgroup $H = \{1, a^{12}\}$. Then the quotient group $\langle a \rangle / H$ is a group of 12 cosets or a group of representatives: $\{a, a^2, a^3, a^{11}, a^{12}\}$, where $(a) = \{a, a^{13}\}$, $(a^2) = \{a^2, a^{14}\}$, $(a^3) = \{a^3, a^{15}\}$, $(a^{11}) = \{a^{11}, a^{23}\}$ and $(a^{12}) = \{a^{12}, a^{24}\}$. A seven hour journey starting at 9 AM (9 PM) ends at 4 PM (4 AM). On the 12-hour clock we do not distinguish between the congruent elements in the same coset {4 AM, 4 PM}.

A Note on Symmetry Group Group theory is an ideal tool to study symmetries. In this note we call any subset of $\mathbf{R}^2$ or $\mathbf{R}^3$ an object. We study orthogonal maps from $\mathbf{R}^2$ to $\mathbf{R}^2$ or from $\mathbf{R}^3$ to $\mathbf{R}^3$ and these are rotations or reflections or rotation-reflections. As orthogonal maps are only those linear maps which keep lengths and angles invariant, they do not include translations.

Let X be an object in $\mathbf{R}^2$ or $\mathbf{R}^3$. Then the set $S(X)$ of all orthogonal maps g with $g(X) = X$ is a group with respect to the usual composition of maps. This group is called the symmetry group of X. The elements of $S(X)$ are called symmetry operations on X. Let $S_2(X)$ (or $S_3(X)$) correspond to the symmetric group of X in $\mathbf{R}^2$ (or $\mathbf{R}^3$).

Examples (a) If $X =$ regular n-gon in $\mathbf{R}^2$ with center at (0, 0), then $S_2(X) = D_n$, the dihedral group with $2n$ elements and for $S_3(X)$, we also get the reflection about the xy-plane and its compositions with all $g \in S_2(X)$, i.e., $S_3(X) = D_n \times \mathbf{Z}_2$.

(b) If $X =$ regular tetrahedron with center at (0, 0, 0), then $S_3(X) \cong S_4$.

(c) If $X =$ cube, then $S_3(X) = S_4 \times \mathbf{Z}_2$.

(d) If $X =$ the letter M, then $S_2(X) \cong \mathbf{Z}_2$ and $S_3(X) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

(e) If $X =$ a circle, then $S_2(X) = O_2(\mathbf{R})$, the whole orthogonal group of all orthogonal maps from $\mathbf{R}^2$ to $\mathbf{R}^2$.

For applications to chemistry and crystallography, X is considered a molecule and $S(X)$ depends on the structural configuration of the molecule X.

For example, methane CH_4 (see Fig. 2.4) has the shape of a regular tetrahedron with H-atoms at the vertices and C-atom at its center (0, 0, 0). Then by (b), $S_3(CH_4) \cong S_4$.

Weyl (1952) first realized the importance of group theory to study symmetry in nature and the application of group theory was boosted by him. Molecules, crystals, and elementary particles are different, but they have very similar theories of symmetry.

Applications of groups to physics are described in Elliot and Dawber (1979) and Sternberg (1994) and those to Chemistry in Cotton (1971) and Farmer (1996).

2.8 Free Abelian Groups and Structure Theorem

If we look at the dihedral group D_n (see Ex. 19 of SE-III) we see that D_n has two generators r and s satisfying some relations other than the associative property. But we now consider groups which have a set of generators satisfying no relations other than associativity which is implied by the group axioms. Such groups are called free groups. In this section we study free abelian groups and prove the 'Fundamental Theorem of Finitely Generated Abelian Groups' which is a structure theorem. This theorem gives notions of 'Betti numbers' and 'invariant factors'. We also introduce the concept of 'homology and cohomology groups' which are very important in homological algebra and algebraic topology.

A free abelian groups is a direct sum of copies of additive abelian group of integers $\mathbf{Z}$. It has some properties similar to vector spaces. Every free abelian group has a basis and its rank is defined as the cardinality of a basis. The rank determines the groups up to isomorphisms and the elements of such a group can be written as finite formal sums of the basis elements.

The concept of free abelian groups is very important in mathematics. It has wide applications in homology theory. Algebraic topology is also used to prove some interesting properties of free abelian groups [see Rotman (1988)].

We consider in this section an additive abelian group G.

Definition 2.8.1 Let G be an additive abelian group and $\{G_i\}_{i\in I}$ be a family of subgroups of G. Then G is said to be generated by $\{G_i\}$ iff every element $x \in G$ can be expressed as

$$x = x_{i_1} + \cdots + x_{in}, \quad \text{where the additive indices } i_t \text{ are distinct.}$$

We sometimes use the following notation:

$$x = \sum_{i\in I} x_i, \quad \text{where we take } x_i = 0, \text{ if } i \text{ is not one of the indices } i_1, i_2, \ldots, i_n.$$

If the subgroups $\{G_i\}$ generate G, we write

$$G = \sum_{i\in I} G_i, \quad \text{in general,} \quad \text{and} \quad G = \sum_{i=1}^{n} G_i, \quad \text{when } I = \{1, 2, \ldots, n\}.$$

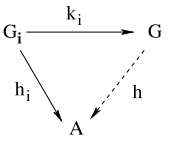


Fig. 2.5 Commutativity of the triangle

Definition 2.8.2 If a group G is generated by the groups $\{G_i\}_{i\in I}$ and every element $x \in G$ has the unique representation as $x = \sum_{i\in I} x_i$, where $x_i = 0$ for all but finitely many i, then G is said to be *direct sum of the groups* G_i, written

$$G = \bigoplus_{i\in I} G_i, \quad \text{in general} \quad \text{and} \quad G = \sum_{i=1}^{n} G_i, \quad \text{if } I = \{1, 2, \ldots, n\}.$$

Remark For $n = 2$, see Ex. 21 of Exercises-III.

A Characterization of Direct Sums Let G be an abelian group and $\{G_i\}$ be a family of subgroups of G. We say that G satisfies the extension condition (EC) for direct sums iff given any abelian group A and any family of homomorphisms $h_i : G_i \to A$, there exists a unique homomorphism $h : G \to A$ extending h_i, for each i, i.e., $h|G_i = h_i$, i.e., making the diagram in Fig. 2.5 commutative, where $k_i : G_i \hookrightarrow G$ is an inclusion map for each i.

Proposition 2.8.1 *Let G be an abelian group and $\{G_i\}$ be a family of subgroups of G.*

(a) *If $G = \bigoplus G_i$, then G satisfies the condition (EC);*
(b) *if G is generated by $\{G_i\}$ and G satisfies the condition (EC), then $G = \bigoplus G_i$.*

Proof (a) Let $G = \oplus G_i$. Then for the given homomorphisms $h_i = G_i \to A$, we define a homomorphism $h : G \to A$ as follows.

If $x = \sum x_i$ (unique finite), then the homomorphism h given by $h(x) = \sum h_i(x_i)$ is well defined and is our required homomorphism.

(b) Let $x = \sum x_i = \sum y_i$. Given an index j, let $A = G_j$.

Define $h_i : G_i \to G_j$ as follows:

$$\begin{aligned} h_i &= id, \quad \text{if } i = j; \\ &= 0, \quad \text{if } i \neq j. \end{aligned}$$

Let $h : G \to G_j$ be the homomorphism extending each h_i by the condition (EC). Then

$$h(x) = \sum_{i\in I} h_i(x_i) = x_j \quad \text{and} \quad h(x) = \sum_{i\in I} h_i(y_i) = y_j.$$

Hence $x_j = y_j \Rightarrow x$ has a unique representation $\Rightarrow G = \bigoplus G_i$. □

Corollary 1 *Let $G = H \oplus K$, where H and K are subgroups of G such that $H = \bigoplus_{i\in I} G_i$ and $K = \bigoplus_{j\in J} G_j$ and $I \cap J = \emptyset$. Then $G = \bigoplus_{t\in I\cup J} G_t$.*

Proof Let A be an abelian group. If $h_i : G_i \to A$ and $h_j : G_j \to A$ are families of homomorphisms, then by Proposition 2.8.1, they can be extended to homomorphisms $f : H \to A$ and $g : K \to A$, respectively. Again f and g can be extended to a homomorphism $h : G \to A$ by Proposition 2.8.1. Hence $G = \bigoplus_{t \in I \cup J} G_t$. □

Corollary 2 $(G_1 \oplus G_2) \oplus G_3 = G_1 \oplus (G_2 \oplus G_3) = G_1 \oplus G_2 \oplus G_3$ *for any subgroups* G_1, G_2 *and* G_3 *of a group* G.

Corollary 3 *For any group* G *and subgroups* G_1 *and* G_2, $G = G_1 \oplus G_2 \Rightarrow G/G_2 \cong G_1$.

Proof Let $A = G_1$ and $h_1 : G_1 \to A = G_1$ be the identity homomorphism and $h_2 : G_2 \to A$ be the zero homomorphism. If $h : G \to A$ is the homomorphism extending h_1 and h_2, then h is an epimorphism with $\ker h = G_2$. Hence $G/G_2 \cong G_1$. □

We are now in a position to study free abelian groups. Let G be an additive group. Then $(m + n)x = mx + nx \ \forall x \in G$ and $\forall m, n \in \mathbf{Z}$.

If the group G is abelian, then $n(x + y) = nx + ny, \ \forall x, y \in G$ and $\forall n \in \mathbf{Z}$.

If S $(\neq \emptyset)$ is a subset of G, then the subgroup $\langle S \rangle$ generated by S is given by

$$\langle S \rangle = \{n_1 s_1 + n_2 s_2 + \cdots + n_t s_t : n_i \in \mathbf{Z}, s_i \in S\}.$$

In particular, if $S = \{s\}$, then $\langle s \rangle = \{ns : n \in \mathbf{Z}\}$ is the cyclic group generated by s and if $S = \emptyset$, then $\langle S \rangle = \{0\}$. The subset S is said to be independent iff $\sum n_i s_i = 0 \Rightarrow n_i = 0, \ \forall i$.

Definition 2.8.3 Let G be an additive abelian group. The group G is said to be a free *abelian group* with a basis B iff

(i) for each $b \in B$, the cyclic subgroup $\langle b \rangle$ is infinite cyclic; and
(ii) $G = \bigoplus_{b \in B} \langle b \rangle$ (direct sum).

Remark A free abelian group G is a direct sum of copies of $\mathbf{Z}$ and every element $x \in G$ can be expressed uniquely as $x = \sum n_b b$, where $n_b \in \mathbf{Z}$ and almost all n_b (i.e., all but a finite number of n_b) are zero.

Using the extension condition (EC) for direct sums, the following characterization of free abelian groups follows.

Proposition 2.8.2 *Let* G *be an abelian group and* $\{b_i\}$ *be a family of elements of* G *that generates* G. *Then* G *is a free abelian group with a basis* $\{b_i\}$ *iff for any abelian group* A *and any family* $\{a_i\}$ *of elements of* A, *there is a unique homomorphism* $h : G \to A$ *such that* $h(b_i) = a_i$ *for each* i.

Proof Let $G_i = \langle b_i \rangle$. Then $\{G_i\}$ is a family of subgroups of G. First suppose that the condition (EC) holds. We claim that each G_i is infinite cyclic. If for some index j, the element b_j generates a finite cyclic subgroup of G, then taking $A = \mathbf{Z}$,

there exists no homomorphism $h : G \to A$, mapping each b_i to the number 1. This is so because b_j is of finite order but 1 is not of finite order in $\mathbf{Z}$. Hence by Proposition 2.8.1(b), $G = \bigoplus G_i$.

Conversely, let G be a free group with a basis $\{b_i\}$. Then given elements $\{a_i\}$ of A, $\exists$ homomorphisms $h_i : G_i \to A$ such that $h_i(b_i) = a_i$, because G_i is infinite cyclic. Hence the proof is completed by using Proposition 2.8.1(a). □

Theorem 2.8.1 *If G is a free abelian group with a basis $B = \{b_1, b_2, \ldots, b_n\}$, then n is uniquely determined by G.*

Proof By hypothesis, $G = \mathbf{Z} \oplus \mathbf{Z} + \cdots \oplus \mathbf{Z}$ (n summands). Then $2G$ is a subgroup of G such that

$$2G \cong 2\mathbf{Z} \oplus 2\mathbf{Z} + \cdots + 2\mathbf{Z} \quad (n \text{ summands}).$$

Hence $G/2G \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/2\mathbf{Z}$ (n summands) shows that card $(G/2G) = 2^n$. □

Definition 2.8.4 An abelian group G is said to be a finitely generated free abelian group iff G has a finite basis.

Remark The basis of a finitely generated free abelian group is not unique. For example, $\{(1, 0), (0, 1)\}$ and $\{(-1, 0), (0, -1)\}$ are two different bases of $G = \mathbf{Z} \oplus \mathbf{Z}$.

Corollary 1 *Let G be a finitely generated abelian group. Then any two bases of G have the same cardinal number.*

Proof Let $B = \{b_1, b_2, \ldots, b_n\}$ and $X = \{x_1, x_2, \ldots x_r\}$ be two bases of G. Then by Theorem 2.8.1, card $(G/2G) = 2^n$ and also card $(G/2G) = 2^r$. Hence $n = r$. □

For more general result, like vector spaces, we prove the following theorem.

Theorem 2.8.2 *Any two bases of a free abelian group F have the same cardinality.*

Proof Let B and C be two bases of F. Given a prime integer $p > 1$, the quotient group F/pF is a vector space over the field $\mathbf{Z}_p$ (see Chap. 8 and Example 4.1.5 of Chap. 4). Hence the cosets $\{b + pF : b \in B\}$ form a basis $\Rightarrow \dim_{\mathbf{Z}_p}(F/pF) =$ card B. Similarly, $\dim_{\mathbf{Z}_p}(F/pF) =$ card C. Hence card $B =$ card C. □

Remark If $V = F/pF$ is infinite dimensional, Zorn's Lemma is used to prove the existence of a basis of V and then using the result that the family of all finite subsets of an infinite set B has the same cardinality as B the invariance of the cardinality of a basis is proved.

Definition 2.8.5 Let F be a free abelian group with a basis B. The cardinality of B is called the rank of F, denoted rank F. In particular, if F is finitely generated, then the number of elements in a basis of F is the rank F.

Remark Rank F is well defined by Theorem 2.8.2.

Like vector spaces free abelian groups are characterized by their ranks. More precisely, two free abelian groups are isomorphic iff they have the same rank. Let G be an arbitrary abelian group. We define its rank as follows:

Definition 2.8.6 An abelian group G has rank r (possibly infinite) iff $\exists$ a free abelian subgroup F of G such that

(a) rank $F = r$;
(b) G/F is a torsion group (i.e., every element of G/F is of finite order).

Existence of F: Let B be an independent subset of G. Then the subgroup $\langle B\rangle$ generated by B is abelian and free with a basis B. Let S be a maximal independent subset of G, which exists by Zorn's Lemma. Then $F = \langle S\rangle$ is a free abelian group and G/F is a torsion group.

Remark Rank F precisely depends on G, since rank $G = \dim_{\mathbf{Q}}(\mathbf{Q} \otimes G)$, where $\mathbf{Q} \otimes G$ is a vector space over $\mathbf{Q}$ [see Chaps. 8 and 9]. Hence rank G is well defined.

Sometimes, given an arbitrary family of abelian groups $\{G_i\}$, we can find a group G that contains subgroups H_i isomorphic to the group G_i, such that G is isomorphic to the direct sum of these groups. This leads to the concept of the external direct sum of groups.

Definition 2.8.7 Let $\{G_i\}$ be a family of abelian groups. If G is an abelian group and $f_i : G_i \to G$ is a family of monomorphisms, such that G is the direct sum of the groups $f_i(G_i)$. Then we say that G is the *external direct sum* of the groups G_i, relative to the monomorphisms $f_i : G_i \to G$.

We prescribe a construction of G.

Theorem 2.8.3 *Given a family of abelian groups* $\{G_i\}_{i\in I}$, *there exists an abelian group* G *and a family of monomorphisms* $f_i : G_i \to G$ *such that* $G = \bigoplus f_i(G_i)$.

Proof We consider the cartesian product $\prod_{i\in I} G_i$. It is an abelian group under componentwise addition. Let G be the subgroup of the cartesian product consisting of those tuples $(x_i)_{i\in I}$ such that $x_i = o_i$, for all but a finitely many values of i. Given an index j, define $f_j : G_j \to G$ by $f_j(x)$ be the tuple that has x at its jth coordinate and 0 at its ith coordinate for $i \neq j$. Then f_j is a monomorphism. Since each element $x \in G$ has only finitely many non-zero coordinates, x can be expressed uniquely as a finite sum of elements from the groups $f_j(G_j)$. □

A Characterization of External Direct Sums of Groups Like extension condition (EC) of direct sums, extension condition (ED) for external direct sums is defined.

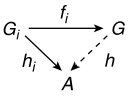


Fig. 2.6 Commutativity of the triangle for external direct sum

Let $\{G_i\}_{i\in I}$ be a family of abelian groups, G be an abelian group and $f_i : G_i \to G$ be a family of homomorphisms. Then G is said to satisfy the condition (ED) iff given any abelian group A and a family of homomorphisms $h_i : G_i \to A$, $\exists$ a unique homomorphism $h : G \to A$ making the diagram in Fig. 2.6 commutative, i.e., $h \circ f_i = h_i,\ \forall i$.

Proposition 2.8.3 *Let $\{G_i\}$ be a family of abelian groups and A be an abelian group.*

(a) *If each $f_i : G_i \to G$ is a monomorphism and $G = \bigoplus_{i\in I} f_i(G_i)$, then G satisfies the condition (ED).*
(b) *Conversely, if $\{f_i(G_i)\}$ generates G and G satisfies the condition (ED), then each $f_i : G_i \to G$ is a monomorphism and $G = \bigoplus_{i\in I} f_i(G_i)$.*

Proof Left as an exercise. □

We now prove the following *structure theorem* for finitely generated abelian groups and also prove as its corollary the structure theorem of an arbitrary finite abelian group (also known as fundamental theorem of finite abelian groups).

Theorem 2.8.4 (Fundamental theorem for finitely generated abelian groups) *Every finitely generated abelian group can be expressed uniquely as*

$$G \cong \overbrace{\mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}}^{r \text{ summands}} \oplus \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_t}$$

for some integers $r, n_1, n_2, \ldots n_t$ such that

(i) *$r \geq 0$ and $n_j \geq 2,\ \forall j$; and*
(ii) *$n_i | n_{i+1}$, for $1 \leq i \leq t-1$.*

Proof As finitely generated $\mathbf{Z}$-modules are finitely generated abelian groups, the theorem follows from Theorem 9.6.5 of Chap. 9 by taking $R = \mathbf{Z}$. □

Definition 2.8.8 The integer r in Theorem 2.8.4 is called the *free rank* or *Betti number* of the group G and the integers $n_1, n_2, \ldots, n_i$ are called the *invariant factors of G*.

Remark Betti numbers are very important in mathematics. For example, two closed surfaces are homeomorphic iff their homology groups have the same Betti numbers in all dimensions [see Massey (1991)].

Theorem 2.8.5 *Two finitely generated abelian groups are isomorphic iff they have the same rank and the same invariant factors* (*up to units*).

Proof It follows from Theorem 9.6.11 of Chap. 9 by taking $R = \mathbf{Z}$. □

Remark If we write $F(G) = \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$ (r summands) and $T(G) = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_t}$ in Theorem 2.8.4, then $G \cong F(G) \oplus T(G)$. $F(G)$ is called a *free subgroup* of G and $T(G)$ is called a *torsion subgroup* of G.

Corollary 1 (Structure Theorem for finite abelian groups) *Any finite abelian group G can be expressed uniquely as $G \cong \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_t}$ such that $n_i | n_{i+1}$, for $1 \leq i \leq t-1$.*

Proof The finite abelian group G is certainly finitely generated (which is generated by the finite set consisting of all its elements). Hence, in this case, $F(G) = 0$. □

Corollary 2 *Two finite abelian groups are isomorphic iff they have the same invariant factors.*

Supplementary Examples (SE-IB)

1 For any abelian group G, the following statements are equivalent:

(a) G has a finite basis;
(b) G is the internal direct sum of a family of infinite cyclic groups;
(c) G is isomorphic to a finite direct sum of finite copies of $\mathbf{Z}$.

[*Hint*. (a) $\Rightarrow$ (b). Let $B = \{b_1, b_2, \ldots, b_t\}$ be a basis of G. Let $nb_i = 0$ for some $n \in \mathbf{Z} \Rightarrow ob_1 + \cdots + nb_i + \cdots ob_t = 0 \Rightarrow n = 0 \Rightarrow b_i$ is of infinite order $\Rightarrow \langle b_i \rangle$ is an infinite cyclic group for $1 \leq i \leq t \Rightarrow G = \bigoplus_{i=1}^{t} \langle b_i \rangle$.
(b) $\Rightarrow$ (c). Let $G = \bigoplus_{i=1}^{t} G_i$, where each $G_i \cong \mathbf{Z}$. This implies (c).
(c) $\Rightarrow$ (a). Let $G \cong \mathbf{Z} \oplus \mathbf{Z} + \cdots + \oplus \mathbf{Z} = \mathbf{Z}^t$ (say) be a finite direct sum of t copies of $\mathbf{Z}$ and $f : G \to \mathbf{Z}^t$ be an isomorphism.
Let $e_i = (0, \ldots, 0, 1, 0 \ldots, 0) \in \mathbf{Z}^t$, where 1 is at the i the place.
Then $\exists b_i \in G$, such that $f(b_i) = e_i$ for each i.
Clearly, $B = \langle b_1, b_i, \ldots, b_t \rangle$ forms a basis of G.]

2 Let F be a free abelian group with a basis B and G be an abelian group.

(a) For every group $f : B \to G$, $\exists$ a unique group homomorphism $\tilde{f} : F \to G$ such that $\tilde{f}(b) = f(b)$, $\forall b \in B$.
(b) For every abelian group G, $\exists$ a free abelian group F such that G is isomorphic to a quotient group of F.

[*Hint*. (a) $x \in F \Rightarrow \exists n_b \in \mathbf{Z}$ such that $x = \sum n_b b$.
Define $\tilde{f} : F \to G$, by $\tilde{f}(x) = \sum n_b f(b)$. Unique expression of $x \Rightarrow \tilde{f}$ is well defined.

Clearly, $\tilde{f}$ is a homomorphism such that $\tilde{f}$ is unique, because homomorphisms agreeing on the set of basis are equal (like linear transformations of vector spaces).

(b) For each $g \in G$, take an infinite cyclic group generated by b_g (say). Then $F = \bigoplus_{g\in G}\langle b_g\rangle$ is a free abelian group with a basis $B = \{b_g : g \in G\}$. Define a map $f : B \to G$, $b_g \mapsto g$ and extend it by linearity.

Then by (a), $\exists$ a unique homomorphism $\tilde{f} : F \to G$ such that $\tilde{f}(b_g) = f(b_g) = g$. Hence $\tilde{f}$ is an epimorphism $\Rightarrow G \cong F/\ker \tilde{f}$.]

3 Every finitely generated abelian group G is the homomorphic image of a finitely generated free abelian group F.

[*Hint*. Let $G = \langle X\rangle$, where $X = \{x_1, x_2, \ldots, x_t\}$ and $B = \{b_1, b_2, \ldots, b_t\}$ be a basis of F.

Define a map $f : F \to G$, $b_i \mapsto x_i$ and extend it by linearity. Then f is well defined and an epimorphism $\Rightarrow G = f(F)$].

4 Let $F = \langle x\rangle$ be a free abelian group. Then $F/\langle nx\rangle \cong \mathbf{Z}_n$, for all integers $n \geq 0$.

[*Hint*. Define map $f : F \to \mathbf{Z}_n$, $mx \mapsto [m]$, $\forall m \in \mathbf{Z}$. Then f is an epimorphism with $\ker f = \langle nx\rangle \Rightarrow F/\langle nx\rangle \cong \mathbf{Z}_n$.]

2.8.1 Exercises

Exercises-II

1. For a given non-empty set S, define a word to be a finite product $x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}$, where $x_i \in S$ and $n_i \in \mathbf{Z}$. The word is said to be reduced iff $x_i \neq x_{i+1}$ and n_i's are non-zero. We can make a given word reduced by collecting up powers of the adjacent elements x_i and omitting the zero powers and continue the process according to the necessity.

   We consider the word x_1^0 as the empty word. Let $F(S)$ denote the set of all reduced words on S. If $S = \emptyset$, $F(S)$ is taken to be the trivial group. If $S \neq \emptyset$, we define a binary operation on $F(S)$ by concatenation of reduced words, i.e., $(x_1^{n_1}\cdots x_t^{n_t})(y_1^{m_1}\cdots y_r^{m_r}) = x_1^{n_1}\cdots x_t^{n_t}y_1^{m_1}\cdots y_r^{m_r} = w$ (say) (making the word reduced).

   Show that

   (a) $F(S)$ becomes a group under this operation with the empty word as its identity element and $x_t^{-n_t}\cdots x_1^{-n_1}$ as the inverse of the reduced word $x_1^{n_1}\cdots x_t^{n_t}$;
   (b) $|X| = |S| \Rightarrow F(X) \cong F(S)$;
   (c) The free group $F(\{x\})$ is the infinite cyclic group having only possible non-empty reduced words are the powers x^r;
   (d) If S consists of more than one element, then $F(S)$ is not abelian.

2. Show that the following statements on an abelian group G are equivalent:

   (a) G has a non-empty basis;
   (b) G is the internal direct sum of a family of infinite cyclic subgroups;

(c) G is isomorphic to a direct sum of copies of $\mathbf{Z}$;
(d) for a subset S and a map $g : S \to G$ such that given an abelian group A and a map $h : S \to A$, $\exists$ a unique homomorphism $f : G \to A$ satisfying $f \circ g = h$.

3. Show that given an abelian group A, $\exists$ a free abelian group G and an epimorphism $f : G \to A$.

[*Hint*. Show that any abelian group is the homomorphic image of a free abelian group.]

4. Let G and H be free abelian groups on the set S w.r.t. maps $g : S \to G$ and $h : S \to H$ respectively. Show that $\exists$ a unique isomorphism $f : G \to H$ such that $f \circ g = h$.

5. If A is a free abelian group of rank n, then any subgroup B of A is a free abelian group of rank at most n.

[*Hint*. Let $A = \mathbf{Z} \oplus \mathbf{Z} \oplus \cdots \oplus \mathbf{Z}$ (n summands) and $\pi_i : A \to \mathbf{Z}$ be the projection on the ith coordinate.

Given $t \leq n$, let $B_t = \{b \in B : \pi_i(b) = 0,\ \forall i > t\}$. Then B_t is a subgroup of $B \Rightarrow \pi_t(B_t)$ is a subgroup of $\mathbf{Z}$. If $\pi_t(B_t) \neq 0$, take $x_t \in B_t$ such that $\pi_t(x_t)$ is a generator of this group. Otherwise, take $x_t = 0$. Then

(i) $B_t = \langle x_1, x_2, \ldots, x_t \rangle$, for each t;
(ii) the non-zero elements of $\{x_1, x_2, \ldots, x_t\}$ form a basis of B_t, for each t;
(iii) $B_t = B$ is a free abelian group with rank B at most n.]

6. *Homology* and *cohomology groups* (see Sect. 9.11 of Chap. 9). A sequence $\{C_n\}$ of abelian groups and a sequence $\{\partial_n\}$ of homomorphisms $\partial_n : C_n \to C_{n-1}$ such that $\partial_{n-1} \circ \partial_n = 0,\ \forall n \in \mathbf{Z}$, are called a *chain complex* $C = (C_n, \partial_n)$ of abelian groups. Given two chain complexes $C = (C_n, \partial_n)$ and $C' = (C'_n, \partial'_n)$, a sequence $f = \{f_n\}$ of homomorphisms $f_n : C_n \to C'_n$ such that $f_{n-1} \circ \partial_n = \partial'_n \circ f_n,\ \forall n \in \mathbf{Z}$, is called a *chain map* $f : C \to C'$. The elements of $Z_n = \ker \partial_n$ are called *n-cycles*, elements of $B_n = \operatorname{Im} \partial_{n+1}$ are called *n-boundaries*. $f = \{f_n\}$ is said to be an isomorphism iff each f_n is an isomorphism of groups. Then the quotient group Z_n/B_n, denoted $H_n(C)$ exists and is called the nth homology group of C. Moreover each f_n induces a group homomorphism $f_n* : H_n(C) \to H_n(C')$ defined by $f_n * ([z]) = [f(z)],\ \forall [\mathbf{z}] \in H_n(C)$ and $f_* = \{f_n*\}$ is said to be an isomorphism iff each f_n* is an isomorphism.

The nth cohomology group $H^n(C)$ is defined dually.

(a) (*Eilenberg–Steenrod*). Let the groups in the chain complexes C and C' be free and $f : C \to C'$ be a chain map. Let $K = \{K_n = \ker f_n\}$. Show that f_* is an isomorphism iff $H_n(K) = 0\ \forall n \in \mathbf{Z}$.
(b) Show that the complex C is exact (see Sect. 9.7 of Chap. 9) iff $H(C) = 0$.
(c) Establish the dual results of (a) and (b) for $H^n(C)$.

7. Using the techniques of algebraic topology, the following results of free groups can be proved [see Rotman (1988, p. 305)]:

(a) Every subgroup G of a free group F is itself free;
(b) a free group F of rank 2 contains a subgroup that is not finitely generated;

(c) let F be a free group of finite rank n, and let G be a subgroup of finite index j. Then G is a free group of finite rank; indeed rank $G = jn - j + 1$.

2.9 Topological Groups, Lie Groups and Hopf Groups

An abstract group endowed with an additional structure having its group operations (multiplication and inversion) compatible with the additional structure, invites further attraction. Some of such groups are studied in this section. For example, we study topological groups, Lie groups and Hopf groups which are very important in topology, geometry, and physics. Topological groups were first considered by S. Lie (1842–1899). A topological group is a topological space whose elements form an abstract group such that the group operations are continuous with respect to the topology of the space. A Lie group is a topological group having the structure of a smooth manifold for which the group operations are smooth functions. On the other hand, a Hopf group (H-group) is a pointed topological space with a continuous multiplication such that it satisfies all the axioms of a group up to homotopy. The concept of an H-group is a generalization of the concept of topological groups. Lie groups are an important branch of group theory. The importance of Lie groups lies in the fact that Lie groups include almost all important groups of geometry and analysis. The theory of Lie groups stands at the crossing point of the theories of differential manifolds, topological groups, and Lie algebras.

2.9.1 Topological Groups

Definition 2.9.1 A *topological group* G is a non-empty set with a group structure and a topology on G such that the function $f : G \times G \to G$, $(x, y) \mapsto xy^{-1}$ is continuous.

The above condition of continuity is equivalent to the statement:

The functions $G \times G \to G$, $(x, y) \mapsto xy$ and $G \to G$, $x \mapsto x^{-1}$ are both continuous.

Some important examples of topological groups.

Example 2.9.1 (i) $(\mathbf{R}, +)$, under usual addition of real numbers and with the topology induced by the Euclidean metric $d(x, y) = |x - y|$.

(ii) The circle group $(S^1, \cdot)$ in $\mathbf{C}$, topologized by considering it as a subset of $\mathbf{R}^2$.

(iii) $(\mathbf{R}^n, +)$, under usual coordinatewise addition and with product topology.

(iv) $(GL(n, \mathbf{R}), \cdot)$, under usual multiplication of real matrices and with the Euclidean subspace topology of $\mathbf{R}^{n^2}$ $(n > 1)$.

(v) The orthogonal group $(O(n), \cdot)$ of real matrices with the Euclidean subspace topology $(n > 1)$. It is a subgroup of $GL(n, \mathbf{R})$.

(vi) The general linear group $(GL(n, \mathbf{C}), \cdot)$ over $\mathbf{C}$ topologized by considering it as a subspace of $\mathbf{R}^{2n^2}$.

(vii) $(U(n), \cdot)$ of all $n \times n$ complex matrices A such that $A\bar{A}^T = I$. It is a subgroup of $GL(n, \mathbf{C})$.

2.9.2 Lie Groups

A Lie group is a topological group which is also a manifold with some compatibility conditions. Lie groups have algebraic structures and they are also subsets of well known spaces and have a geometry, moreover, they are locally Euclidean in the sense that a small portion of them looks like a Euclidean space making it possible to do analysis on them. Thus Lie groups and other topological groups lie at the crossing of different areas of mathematics. Representations of Lie groups and Lie algebras have revealed many beautiful connections with other branches of mathematics, such as number theory, combinatorics, algebraic topology as well as mathematical physics.

Definition 2.9.2 A topological group G is called a *real Lie group* iff

(i) G is a differentiable manifold;
(ii) the group operations $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are both differentiable.

Definition 2.9.3 A topological G is called a *complex Lie group* iff

(i) G is a complex manifold;
(ii) the group operations $(x, y) \mapsto xy$ and $x \mapsto x^{-1}$ are both holomorphic.

The name Lie group is in honor of Sophus Lie. The dimension of a Lie group is defined as its dimension as a manifold.

Some Important Examples of Lie Groups

Example 2.9.2 (i) $(\mathbf{R}^n, +)$ is an n-dimensional Lie group over $\mathbf{R}$.

(ii) $(\mathbf{C}^n, +)$ is an n-dimensional Lie group over $\mathbf{C}$, but it is a $2n$-dimensional Lie group over $\mathbf{R}$.

(iii) $GL(n, \mathbf{R})$ is a real Lie group of dimension n^2.

(iv) $GL(n, \mathbf{C})$ is a complex Lie group of dimension n^2.

(v) $SL(n, \mathbf{R})$ is a real Lie group of dimension $n^2 - 1$.

(vi) $SL(n, \mathbf{C})$ is a complex Lie group of dimension $n^2 - 1$.

2.9.3 Hops's Groups or H-Groups

A pointed topological space is a non-empty topological space with a distinguished element.

Let P and Q be pointed topological spaces and $f, g : P \to Q$ be base point preserving continuous maps. Then f and g are said to be homotopic relative to the base point $p_0 \in P$, denoted by $f \simeq g \operatorname{rel} p_0$, iff there exists a continuous one-parameter family of maps

$$f_t : P \to Q,$$

such that $f_0 = f$, $f_1 = g$ and $f_t(p_0) = f(p_0) = g(p_0)$ for all $t \in I = [0, 1]$. f_t is called a *homotopy* between f and g relative to p_0, denoted by $f_t : f \simeq g \operatorname{rel} p_0$.

Since '$\simeq$' is an equivalence relation; one can speak of homotopy class of maps between two spaces. Thus $[P; Q]$ usually denotes the set of all homotopy classes of base point preserving continuous maps $P \to Q$ (all homotopies are relative to the base point).

Definition 2.9.4 A pointed topological space P is called a *Hopf group* or *H-group* iff $\exists$ a continuous multiplication $\mu : P \times P \to P$ such that

(i) $\mu(c, 1_P) \simeq 1_p \simeq \mu(1_P, c)$;
(ii) $\mu(\mu \times 1_P) \simeq \mu(1_P \times \mu)$;
(iii) $\mu(1_P, \phi) \simeq c \simeq \mu(\phi, 1_P)$,

where $c : P \to p_0 \in P$ is the constant map (p_0 is the base point of P), $1_P : P \to P$ is the identity map and $\phi : P \to P$ is a continuous map and ϕ is called a *homotopy inverse* for P and μ. Then the homotopy class $[c]$ of c is a homotopy identity and $[\phi]$ is homotopy inverse for P and μ.

Clearly, any topological group is an H-group with identity element e as a base point.

Theorem 2.9.1 *Let X be an arbitrary pointed topological space and P be an H-group. Then $[X; P]$ is a group.*

Proof Define for every pair of maps $g_1, g_2 : X \to P$, the product $g_1 g_2 : X \to P$ by $(g_1 g_2)(x) = \mu(g_1(x), g_2(x)) = g_1(x) g_2(x)$; where the right hand multiplication is the multiplication μ in the H-group P. This law of composition carries over to give an operation on homotopy classes such that $[g_1][g_2] = [g_1 g_2]$. As the two homotopic maps determine the same homotopy class, the group axioms for $[X; P]$ follow from (i)–(iii) of Definition 2.9.4. □

Theorem 2.9.2 *If $f : X \to Y$ is a base point preserving continuous map, then f induces a group homomorphism*

$$f^* : [Y; P] \to [X; P] \quad \textit{for each } H\textit{-group } P.$$

Proof Define f^* by $f^*[h] = [h \circ f]$. This map is well defined, since $h_0 \simeq h_1 \Rightarrow h_0 of \simeq h_1 of$ (cf. Spanier 1966, Th. 6, p. 24). Verify that f^* is a group homomorphism. □

Let P and P' be H-groups with multiplications μ and μ', respectively. Then a continuous map $\alpha : P \to P'$ is called a *homomorphism* of H-groups, iff $\alpha\mu \simeq \mu'(\alpha \times \alpha)$.

Theorem 2.9.3 *If $\alpha : P \to P'$ is a homomorphism between H-groups, then α induces a group homomorphism $\alpha_* : [X; P] \to [X; P']$.*

Proof Define $\alpha_* : [X; P] \to [X; P']$ by $\alpha_*[f] = [\alpha \circ f]$. Then α_* is well defined and a homomorphism. □

Remark For further results, see Appendix B.

2.10 Fundamental Groups

Homotopy theory plays an important role in mathematics. In this section, we define fundamental group of a topological space X based at a point x_0 in X. This group is an algebraic invariant in the sense that the fundamental groups of two homeomorphic spaces are isomorphic. By using the fundamental groups many problems of algebra, topology, and geometry are solved by reducing them into algebraic problems. For example, the fundamental theorem of algebra is proved in Chap. 11 by homotopy theory and the Brouwer Fixed Point Theorem for dimension 2 is proved in Appendix B by the fundamental group.

Definition 2.10.1 Let X be a topological space and x_0 be a fixed point of X, called a base point of X. A continuous map $f : I \to X$ (where $I = [0, 1]$) is called a *path* in X; $f(0)$ and $f(1)$ are called the initial point and the terminal point of the path f, respectively. If $f(0) = f(1) = x_0$, the path f is called a *loop* in X based at x_0. A space X is said to be *path connected*, iff any two points of X can be joined by a path. Let $f, g : I \to X$ be two loops based at x_0. Then they are called *homotopic* relative to 0 and 1, denoted by $f \simeq g \,\mathrm{rel}\{0, 1\}$ iff $\exists$ a continuous map $F : I \times I \to X$ such that

$$F(t, 0) = f(t), \qquad F(t, 1) = g(t), \qquad F(0, s) = F(1, s) = x_0 \quad \forall t, s \in I.$$

The above homotopy relation between loops is an equivalence relation, and this gives the set of homotopy classes relative to 0 and 1 of the loops based at x_0 and this is denoted by $\pi_1(X, x_0)$. Given loops $f, g : I \to X$ based at x_0, their product $f * g$ is a loop $f * g : I \to X$ at x_0 defined by

$$(f * g)(t) = \begin{cases} f(2t), & 0 \le t \le \frac{1}{2}, \\ g(2t - 1), & \frac{1}{2} \le t \le 1. \end{cases}$$

If $[f]$ and $[g]$ are two elements of $\pi_1(X, x_0)$, define their product $[f] \circ [g] = [f * g]$. This product is well defined and $\pi_1(X, x_0)$ is group under this composition. This group is called the *fundamental group* of X based at x_0.

Clearly, if X is path connected, $\pi_1(X, x_0)$ is independent of its base point x_0.

We now find geometrically the fundamental group of the unit circle S^1 which is the boundary of the unit ball or disc E^2 in $\mathbf{R}^2$. Since S^1 is path connected, its fundamental group $\pi_1(S^1, x_0)$ is independent of its base point x_0. A loop f in S^1 based at x_0 is a closed path starting at x_0 and ending at x_0. Then f is either a null-path (constant path) or f is given by one or more complete description (clockwise or anti-clockwise) around the circle. Let f and g be two loops in S^1 based at the same point x_0 such that f describes S^1, m times and g describes S^1, n times. If $m > n$, then $f * g^{-1}$ is a path describing $(m - n)$ times the circle S^1 and such that it is not homotopic to a null path. Thus the homotopy classes of loops in S^1 based at x_0 are in bijective correspondence with $\mathbf{Z}$. Hence $\pi_1(S^1, x_0)$ is isomorphic to $\mathbf{Z}$.

Proceeding as above, for a solid disc E^2 the fundamental $\pi_1(E^2, x_0) = 0$, since the space E^2 is a convex subspace of $\mathbf{R}^2$.

For an analytical proof use the degree function d defined in (v) below or [see Rotman (1988)].

Let $\dot{I} = \{0, 1\}$ be the end point of the closed interval $I = [0, 1]$. Then a loop in S^1 based at 1 is a continuous map $f : (I, \dot{I}) \to (S^1, 1)$. Let $p : (\mathbf{R}, r_0) \to (S^1, 1)$ be the exponential map defined by $p(t) = e^{2\pi i t}$, $\forall t \in \mathbf{R}$, where $r_0 \in \mathbf{Z}$. We now present some interesting properties of fundamental groups (see Rotman (1988)).

(i) There exists a unique continuous map $\tilde{f} : I \to \mathbf{R}$ such that $p \circ \tilde{f} = f$ and $\tilde{f}(0) = 0$.
(ii) If $g : (I, \dot{I}) \to (S^1, 1)$ is continuous and $f \simeq g$ relative to $\dot{I}$, then $\tilde{f} \simeq \tilde{g}$ relative to $\dot{I}$ and $\tilde{f}(1) = \tilde{g}(1)$, where $p \circ \tilde{g} = g$ and $\tilde{g}(0) = 0$.
(iii) If $f : (I, \dot{I}) \to (S^1, 1)$ is continuous, the degree of f denoted by deg f is defined by deg $f = \tilde{f}(1)$, where $\tilde{f}$ is the unique lifting of f with $\tilde{f}(0) = 0$. Then deg f is an integer.
(iv) If $f(x) = x^n$, then deg $f = n$ and the degree of a constant loop is 0.
(v) The function $d : \pi_1(S^1, 1) \to \mathbf{Z}$, defined by $d([f]) = \deg f$, is an isomorphism of groups.
(vi) Two loops in S^1 at the base point 1 are homotopic relative to $\dot{I}$ if and only if they have the same degree.

2.10.1 A Generalization of Fundamental Groups

Rodes (1966) introduced the fundamental group $\sigma(X, x_0, G)$ of a *transformation group* (X, G, σ) (see Definition 3.1.1), where X is a path connected space with x_0 as base point. Given an element $g \in G$, a path α of order g with base point x_0 is a continuous map $\alpha : I \to X$ such that $\alpha(0) = x_0$, $\alpha(1) = gx_0$. A path α_1 of order g_1 and a path α_2 of order g_2 give rise to a path $\alpha_1 + g\alpha_2$ of order $g_1 g_2$ defined by the equations

$$(\alpha_1 + g\alpha_2)(s) = \begin{cases} \alpha_1(2s), & 0 \le s \le \frac{1}{2}, \\ g_1\alpha_2(2s-1), & \frac{1}{2} \le s \le 1. \end{cases}$$

Two paths α and β of the same order g are said to be homotopic iff $\exists$ a continuous map $F : I \times I \to X$ such that

$$\begin{aligned} F(s,0) &= \alpha(s), \quad 0 \le s \le 1; \\ F(s,1) &= \beta(s), \quad 0 \le s \le 1; \\ F(0,t) &= x_0, \quad 0 \le t \le 1; \\ F(1,t) &= gx_0, \quad 0 \le t \le 1. \end{aligned}$$

The homotopy class of a path α of order g is denoted by $[\alpha; g]$. Prove that the set of homotopy classes of paths of prescribed order with rule of composition '$\circ$' form a group where $\circ$ is defined by

$$[\alpha; g_1] \circ [\beta; g_2] = [\alpha + g_1\beta; g_1 g_2].$$

This group denoted by $\sigma(X, x_0, G)$ is called the *fundamental group* of (X, G, σ) with base point x_0.

Problems and Supplementary Examples (SE-I)

1 Show that $(\mathbf{Q}, +)$ is not finitely generated ($+$ denotes usual addition of rational numbers).

Solution If possible, suppose $(\mathbf{Q}, +)$ is finitely generated. Then there exists a finite set

$$S = \left\{ \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_n}{q_n} \right\}$$

of rational numbers such that $\mathbf{Q} = \langle S \rangle$. Now we can find a prime p such that p does not divide $q_1, q_2, \ldots, q_n$. Let $x \in \mathbf{Q}$. Then there exist integers $m_1, m_2, \ldots, m_n$ such that

$$x = m_1 \frac{p_1}{q_1} + m_2 \frac{p_2}{q_2} + \cdots + m_n \frac{p_n}{q_n} = \frac{m}{q_1 q_2 \cdots q_n}$$

for some integer m. Since p does not divide $q_1, q_2, \ldots, q_n$, p does not divide $q_1 q_2 \ldots q_n$. Hence p does not divide the denominator of any rational number (expressed in lowest terms) of $\langle S \rangle$. This shows that $\frac{1}{p} \notin \langle S \rangle = \mathbf{Q}$. This yields a contradiction. Hence $(\mathbf{Q}, +)$ is not finitely generated.

2 Let S_n be the symmetric group on $\{x_1, x_2, \ldots, x_n\}$ with identity e. For $i = 1, 2, \ldots, n-1$, write σ_i for the permutation of S which transposes x_i and x_{i+1} and keep the remaining elements fixed. Then show that

(i) $\sigma_i^2 = e$ for $i = 1, 2, \ldots, n-1$;
(ii) $\sigma_i \sigma_j = \sigma_j \sigma_i$ if $|i - j| > 2$;
(iii) $(\sigma_i \sigma_{i+1})^3 = e$ for $1 \le i \le n-2$;
(vi) $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ generate the group S_n.
(v) The relations (i)–(iii) between the generators determine the Cayley table of S_n completely (these relations are called the defining relations of S_n).

3 Consider as a conjecture. "Let H be a subgroup of a finite group G. If H is abelian, then H is normal in G." Disprove the conjecture by reference to the Octic group and one of its subgroups.

4 Show by an example that the converse of Lagrange's Theorem is not true for arbitrary finite groups.

Solution We show that the alternating group A_4 of order 12 has no subgroup H of order 6. If possible, let $|H| = 6$. All the following eight 3-cycles (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3) are in A_4. As $|H| = 6$, H cannot contain all these elements. Let $\beta = (x\ y\ z)$ be a 3-cycle in A_4 such that $\beta \notin H$. Let $K = \{\beta, \beta^2, \beta^3 = 1\}$. Then K is a subgroup of A_4. Hence $H \cap K = \{1\}$ shows that $HK = \frac{|H||K|}{|H \cap K|} = 18$. But $HK \subseteq A_4$ implies a contradiction.

Problems and Supplementary Examples (SE-II)

1 Let G be a group and H be a subgroup of G. Show that $\forall g \in G$, $gH = H \Leftrightarrow g \in H$.

Solution Let $g \in G$ and $gH = H$. Then $g = g \cdot 1 \in gH = H \Rightarrow g \in H$. Thus $\forall g \in G$, $gH = H \Rightarrow g \in H$. Conversely, suppose $g \in H$. Then for $\forall h \in H$, $gh \in H \Rightarrow gH \subseteq H$. Again $g, h \in H \Rightarrow g^{-1}h \in H \Rightarrow h = g(g^{-1}h) \in gH \Rightarrow H \subseteq gH$. Thus for any $g \in H$, $gH = H$.

2 Show that any factor group of a cyclic group is cyclic.

Solution Let $G = \langle a \rangle$ be a cyclic group and N be a normal subgroup of G. Then computation of all powers of aN amounts to computing in G, all powers of the representative a and these powers give all the elements of G. Hence the powers of aN give all the cosets of N and thus $G/N = \langle aN \rangle \Rightarrow G/N$ is cyclic.

3 Find the kernel of the homomorphism: $f : (\mathbf{R}, +) \to (C^*, \cdot)$ defined by $f(x) = e^{ix}$ and hence find the factor group $\mathbf{R}/\ker f$.

Solution

$$\ker f = \left\{x \in \mathbf{R} : e^{ix} = 1\right\} = \{x \in \mathbf{R} : \cos x + i \sin x = 1\}$$
$$= \{x \in \mathbf{R} : x = 2\pi n, n \in \mathbf{Z}\} = \langle 2\pi \rangle.$$

Thus $\mathbf{R}/\ker f = \mathbf{R}/\langle 2\pi \rangle \cong \text{Im } f = S^1$ (circle group in C^*, see Example 2.3.2).

4 Show that a group having only a finite number of subgroups is finite.

Solution If $G = \{1\}$, then G is finite. Suppose $G \neq \{1\}$. Then $\exists$ an element $a\ (\neq 1) \in G$. Thus $H = \langle a \rangle$ is a finite subgroup of G.

Otherwise, $(H, \cdot) \cong (\mathbf{Z}, +)$ and $(\mathbf{Z}, +)$ has infinite number of subgroups viz. $\langle n \rangle$ (by Theorem 2.4.10), $n = 0, 1, 2, \ldots$ would imply that H has an infinite number of subgroups contradicting our hypothesis. Thus $O(a)$ is also finite. If $G = \langle a \rangle$, the proof ends. If $G \neq \langle a \rangle$, then $\exists$ only a finite number of elements in $(G - \langle a \rangle)$. Otherwise, for each $g \in (G - \langle a \rangle)$, $\langle g \rangle$ is a subgroup of $G \Rightarrow \exists$ an infinitely many non-trivial subgroups of $G \Rightarrow$ a contradiction of hypothesis. Consequently, G is finite.

5 Let G be a finite group and H be a proper subgroup of G such that for $x, y \in G - H, xy \in H$. Prove that H is a normal subgroup of G such that $|G|$ is an even integer.

Solution $g \in H \Rightarrow ghg^{-1} \in H, \ \forall h \in H$. Again $g \notin H \Rightarrow hg^{-1} \notin H, \ \forall h \in H$. This is so because $hg^{-1} \in H$ and $h, h^{-1} \in H \Rightarrow h^{-1}(hg^{-1}) \in H \Rightarrow g^{-1} \in H \Rightarrow g \in H \Rightarrow$ a contradiction. Thus $g, hg^{-1} \in G - H \Rightarrow g(hg^{-1}) \in H$ by hypothesis $\Rightarrow ghg^{-1} \in H$. Hence it follows that H is a normal subgroup of G. Thus G/H is a group. We now show that $|G|$ is of even order. By hypothesis, $\exists x \in G$ such that $x \notin H$ but $x^2 \in H$. Hence $x^2 H = H \Rightarrow (xH)^2 = eH$. Again $x \notin H \Rightarrow xH \neq eH$. Thus $O(xH) = |xH| = 2$. Now $|xH|$ divides $|G/H| \Rightarrow 2$ divides $|G/H|$. Hence $|G/H|$ is an even integer $\Rightarrow |G| = |G/H| \cdot |H|$ is an even integer.

6 Let G be a finite group and H, K be subgroups of G such that $K \subseteq H$. Then $[G : K] = [G : H][H : K]$.

Solution $H = \bigcup_i x_i K$ and $G = \bigcup_j y_j H$, where both are disjoint union $\Rightarrow \ G = \bigcup_{i,j} y_j x_i K$ is also a disjoint union $\Rightarrow \ [G : K] = [G : H][H : K]$.

7 Let G be a finite cyclic group of order n. Show that corresponding to each positive divisor d of n, $\exists$ a unique subgroup of G of order d.

Solution Let $G = \langle g \rangle$ for some $g \in G$ and d a positive divisor of n. Then $n = md$ for some $m \in \mathbf{Z}$.

Now $g^m \in G \Rightarrow O(g^m) = \frac{O(g)}{\gcd(m,n)} = \frac{n}{m} = d$ by Theorem 2.3.5.

Let $H = \langle g^m \rangle$. Then H is subgroup of G of order d.

Uniqueness of H: Let K be a subgroup of G of order d. Let t be the smallest positive integer such that $g^t \in K$. Then $K = \langle g^t \rangle$. Now $|K| = d \Rightarrow O(g^t) = d \Rightarrow d = \frac{O(g)}{\gcd(t,n)} = \frac{n}{\gcd(t,n)}$ by Theorem 2.3.5 $\Rightarrow \gcd(t, n) = \frac{n}{d} = m \Rightarrow m|t$. If $t = ml$ for some $l \in \mathbf{Z}$, then $g^t = g^{ml} = (g^m)^l \in H \Rightarrow K \subseteq H \Rightarrow K = H$, since $|H| = |K|$.

8 Let G be a finite group and $f : G \to \mathbf{Z}_{15}$ be an epimorphism. Show that G has normal subgroups with indices 3 and 5.

Solution $G/\ker f \cong \mathbf{Z}_{15}$ by the First Isomorphism Theorem. Then $\mathbf{Z}_{15}$ being a cyclic group of order 15, $G/\ker f$ is a cyclic group of order 15 $\Rightarrow G/\ker f$ has

a normal subgroup N_1 of order 5 and a normal subgroup N_2 of order 3 $\Rightarrow \exists$ normal subgroups H_1 and H_2 of G such that $\ker f \subseteq H_1$, $\ker f \subseteq H_2$, $H_1/\ker f = N_1$ and $H_2/\ker f = N_2$ by the Correspondence Theorem. Hence $15 = |G/\ker f| = [G : \ker f] = [G : H_1][H_1 : \ker f]$ (by Ex. 6 of SE-II) $= [G : H_1] \cdot 5 \Rightarrow [G : H_1] = 3$. Similarly, $[G : H_1] = 5$.

9 Prove that the group $\mathbf{Z}_m \times \mathbf{Z}_n$ is isomorphic to the group $\mathbf{Z}_{mn} \Leftrightarrow \gcd(m, n) = 1$ i.e., $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn} \Leftrightarrow m, n$ are relatively prime.

Solution $\mathbf{Z}_m$ and $\mathbf{Z}_n$ are cyclic groups of order m and n, respectively. If $\gcd(m, n) = 1$, then $\mathbf{Z}_m \times \mathbf{Z}_n$ is a cyclic group of order mn and hence isomorphic to $\mathbf{Z}_{mn}$ (see Theorems 2.4.12 and 2.4.13). Conversely, let $\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n$. If $\gcd(m, n) = d > 1$, then $mn = d \cdot l\,\mathrm{cm}(m, n) \Rightarrow \frac{mn}{d} = l\,\mathrm{cm}(m, n) \Rightarrow \frac{mn}{d} = t$ is divisible by both m and n. Now for $(x, y) \in \mathbf{Z}_m \times \mathbf{Z}_n$, $(x, y) + (x, y) + \cdot + (x, y)$ (t summand) $= (0, 0) \Rightarrow$ no element $(x, y) \in \mathbf{Z}_m \times \mathbf{Z}_n$ can generate the entire group $\mathbf{Z}_m \times \mathbf{Z}_n$. Hence $\mathbf{Z}_m \times \mathbf{Z}_n$ cannot be cyclic and therefore cannot be isomorphic to $\mathbf{Z}_{mn}$. So we reach a contradiction. Hence $\gcd(m, n) = 1$.

10 If $n = p_1^{n_1} p_2^{n_2} \cdots p_n^{n_r}$, where p_i's are distinct primes, $n_i \geq 0$, show that $\mathbf{Z}_n$ is isomorphic to $\mathbf{Z}_{p_1}^{n_1} \times \mathbf{Z}_{p_2}^{n_2} \times \cdots \times \mathbf{Z}_{p_r}^{n_r}$.

Solution The result follows from Ex. 9 of SE-II by an induction argument.

11 Prove that a finitely generated group cannot be expressed as the union of an ascending sequence of its proper subgroups.

Solution Let G be a finitely generated group $G = \langle a_1, a_2, \ldots, a_n \rangle$. If possible, let $G = \bigcup_i A_i$, where $A_1 \subseteq A_2 \subseteq \cdots$ and each A_i is a proper subgroup of $G, i = 1, 2, \ldots$. Then $\exists$ a positive integer t such that $a_1, a_2, \ldots, a_n \in A_t$. Then $G = \langle a_1, a_2, \ldots, a_n \rangle \subseteq A_t$. Again $A_t \subseteq G$. Hence $G = A_t \Rightarrow$ a contradiction, since A_t is a proper subgroup of G.

12 Show that every finitely generated subgroup of $(\mathbf{Q}, +)$ is cyclic.

Solution Let H be a finitely generated subgroup of $(\mathbf{Q}, +)$. Then any element x of H is of the form

$$x = \frac{m}{q_1 q_2 \cdots q_n} \text{ for some integer } m \text{ (proceed as Ex. 1 of SE-I)}$$

$$\Rightarrow \quad H \subseteq \left\langle \frac{1}{q_1 q_2 \cdots q_n} \right\rangle = K \text{ (say)}$$

$$\Rightarrow \quad K \text{ is a cyclic group generated by } \frac{1}{q_1 q_2 \cdots q_n} \in \mathbf{Q}$$

$$\Rightarrow \quad H \text{ is a cyclic group.}$$

13 Prove that every finite subgroup of $(\mathbf{C}^*, \cdot)$ is cyclic.

Solution Let $(H, \cdot)$ be a finite subgroup of $(\mathbf{C}^*, \cdot)$. Let $|H| = n$ and $x \in H$. Then $x^n = 1$.

The nth roots of $x^n = 1$ are given by

$$1, w, w^2, \ldots, w^{n-1}, \quad \text{where } w = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ k = 0, 1, 2, \ldots, n-1.$$

Then each of the roots belongs to H and $O(w) = n = |H|$. Hence $H = \langle w\rangle \Rightarrow H$ is cyclic.

14 Prove that the alternating group A_n of order n ($\geq$3) is a normal subgroup of S_n (see Ex. 58 of Exercises-III).

Solution Consider the subgroup $G = (\{1, -1\}, \cdot)$ of $(\mathbf{R}^*, \cdot)$. Define a mapping $\psi : S_n \to G$ by

$$\psi(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

Then ψ is an epimorphism such that $\ker\psi = \{\sigma \in S_n : \psi(\sigma) = 1\} = A_n$.

Hence A_n is a normal subgroup of S_n by Theorem 2.6.5.

15 Let H be a normal subgroup of a group G such that H and G/H are both cyclic. Show that G is not in general cyclic.

Solution Take $G = S_3$ and $H = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

Then $|G/H| = 2 \Rightarrow H$ is a normal subgroup of G. Hence G/H is also a group. Since $|G/H| = 2$ and $|H| = 3$, which are both prime, G/H and H are both cyclic groups. But G is not commutative $\Rightarrow S_3$ is not cyclic.

16 Let G be a non-cyclic group of order p^2 (p is a prime integer) and $g(\neq e) \in G$. Show that $O(g) = p$.

Solution $O(g)||G| = p^2 \Rightarrow O(g) = 1, p$ or p^2. Now $g \neq e \Rightarrow O(g) \neq 1$. If $O(g) = p^2$, then G contains an element g such that $O(g) = |G|$. Hence G is cyclic $\Rightarrow$ a contradiction of hypothesis $\Rightarrow O(g) \neq p^2$. Thus $O(g) \neq 1$, $O(g) \neq p^2 \Rightarrow O(g) = p$.

2.11 Exercises

Exercises-III

1. Prove that a semigroup S is a group iff for each $a \in S$, $aS = Sa = S$.

2. Let S be a semigroup. A non-empty subset A of S is called a pseudo-ideal (left, right) iff $ab \in A\ \forall a, b \in A$; $x^2A \subseteq A$ and $Ax^2 \subseteq A (x^2A \subseteq A, Ax^2 \subseteq A)$ for every $x \in S$. Show that a semigroup S is a group iff $x(A\backslash B)x \subseteq A\backslash B$ for every $x \in S$ when $A\backslash B \neq \emptyset$, where A, B are either both left pseudo-ideals or both right pseudo-ideals of S.
3. Show that (a) in the semigroup $(\mathbf{Z}^*, \cdot)$ (of all non-zero integers under usual multiplication), $A = \{a \in \mathbf{Z}^* : a \geq 6\}$ is a pseudo-ideal but not an ideal of $\mathbf{Z}^*$.

   In the multiplicative group $(\mathbf{Q}^*, \cdot)$ of all non-zero rational numbers, $A = \{r^2 : r \in \mathbf{Q}^*\}$ is a proper pseudo-ideal of $\mathbf{Q}^*$.

   (This example shows that a group may contain a proper pseudo-ideal.)
4. Define a binary operation o on $\mathbf{Z}$ by $a \circ b = a + b - 2$. Show that $(\mathbf{Z}, \circ)$ is a commutative group.
5. Let G be the set of all rational numbers excepting -1. Define a binary operation '$\circ$' on G by $a \circ b = a + b + ab$. Show that $(G, \circ)$ is a group.
6. Define a binary operation '$\circ$' on the set of non-zero rational numbers by $a \circ b = |a|b$. Is $(\mathbf{R}^*, \circ)$ a group? Justify your answer.
7. Let

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbf{R} \text{ (or } \mathbf{Z}) \text{ and } ad - bc = 1 \right\}.$$

   Show that G is a group under usual multiplication. Is this group commutative?
8. (i) A semigroup (X, o) is said to be cancellative iff for each $x, y, z \in X, x \circ y = x \circ z \Rightarrow y = z$ and $y \circ x = z \circ x \Rightarrow y = z$. Show that a finite cancellative semigroup $(X, \circ)$ is a group.

   Does this result hold if the semigroup is not finite?

   (ii) Show that a cancellative semigroup can be extended to a group iff it is commutative.
9. Let $SL(n, \mathbf{R})$ $(SL(n, \mathbf{C}))$ be the set of all $n \times n$ $(n > 1)$ unimodular matrices A (i.e., $\det A = 1$) with real (complex) entries. Show that $(SL(n, \mathbf{R}), \cdot)$ $((SL(n, \mathbf{C}), \cdot))$ is a group under usual multiplication.
10. Let U_n $(n > 1)$ denote the set of all $n \times n$ complex matrices A such that $A\bar{A}^T = I$. Show that $(U_n, \cdot)$ is a non-commutative group and is a subgroup of $GL(n, \mathbf{C})$ (under usual multiplication). $((U_n, \cdot)$ is called *unitary group*.)

    [*Hint*. $A\bar{A}^T \Rightarrow I \Rightarrow |\det A|^2 = 1$.] Show that in particular, the set SU_n of all unitary matrices A with $\det A = 1$ is a non-commutative group (known as *special unitary group*).
11. Let O_n $(n > 1)$ denote the set of all orthogonal $n \times n$ real matrices A (i.e., $AA^T = I$). Show that $(O_n, \cdot)$ is a non-commutative group (under usual multiplication).
12. Let SO_n be the special *orthogonal group* consisting of all orthogonal matrices A such that $\det A = 1$. Show that $(SO_n, \cdot)$ is a non-commutative group but $(SO_n, +)$ is not a group (where '$\cdot$' and '$+$' denote usual multiplication and addition of matrices respectively).

    [*Hint*. $(SO_n, +)$ does not contain identity.]

13. Let $(G, \cdot)$ be a group and S, T subsets of G. Then define the product $S \circ T$ as

$$S \circ T = \begin{cases} z \in G : z = xy & \text{for some } x \in S, y \in T \\ \emptyset & \text{if either } S \text{ or } T \text{ is empty.} \end{cases}$$

Then the inverse of the set S denoted by S^{-1} is defined by

$$S^{-1} = \begin{cases} z \in G : z = x^{-1} & \text{for some } x \in S \\ \emptyset & \text{iff } S = \emptyset. \end{cases}$$

Show that if S, T, W are subsets of G, then

(a) $(S \circ T) \circ W = S \circ (T \circ W)$;
(b) $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$;
(c) $S \circ T \neq T \circ S$ (in general).

14. Show that a non-empty subset T of a group $(G, \cdot)$ is a subgroup of G iff $T \circ T \subseteq T$ and $T^{-1} \subseteq T$ or equivalently, $T \circ T^{-1} \subseteq T$.
15. Let S, T be subgroups of a group $(G, \cdot)$. Show that $S \circ T$ is a subgroup of G iff $S \circ T = T \circ S$.
16. Let G be a group and T_1, T_2 two proper subgroups of G.

    Show that $T_1 \cup T_2$ is a subgroup of G iff $T_1 \subseteq T_2$ or $T_2 \subseteq T_1$. Hence show that a group cannot be the union of two proper subgroups.
17. Let $(G, \cdot)$ be a group and S a non-empty subset of G.

    Show that the subgroup $\langle S \rangle$ generated by S consists of all elements of the form $x_1 x_2 \cdots x_n$, where $x_i \in S \cup S^{-1}$ for all integers $n \geq 1$ and, moreover, if S is a countable subset of G, then $\langle S \rangle$ is countable.

    [*Hint*. T be the set of all finite products of the given form $x_1 x_2 \cdots x_n$. Taking $n = 1$ and allowing x_1 run over S, it follows that $S \subseteq T$. Suppose $a = x_1 x_2 \cdots x_n$ and $b = y_1 y_2 \cdots y_m \in T$. Now $ab^{-1} = x_1 x_2 \cdots x_n x_{n+1} x_{n+2} \cdots x_{n+m}$, where $x_{n+i} = (y_{m-i+1})^{-1}$.

    But $y_j \in S \cup S^{-1} \Rightarrow y_{j^{-1}} \in S \cup S^{-1}$. Consequently, $x_{n+i} \in S \cup S^{-1} \Rightarrow x_i \in S \cup S^{-1}, i = 1, 2, \ldots, m + n \Rightarrow ab^{-1} \in T \Rightarrow T$ is a subgroup of G. Now $S \subseteq T \Rightarrow \langle S \rangle \subseteq T$. Since $S \subseteq \langle S \rangle$ and $\langle S \rangle$ is a subgroup, $S^{-1} \subseteq \langle S \rangle$.

    $S \cup S^{-1} \subseteq \langle S \rangle$. By closure property and induction, it follows that any finite product of elements of $S \cup S^{-1}$ is also contained in $\langle S \rangle$ i.e., $T \subseteq \langle S \rangle$.]
18. Show that $(\mathbf{R}, +)$ is not finitely generated (+ denotes usual addition of reals).

    [*Hint*. If possible, $\exists$ a finite subset $S \subset \mathbf{R}$ such that $\langle S \rangle = \mathbf{R}$. Then S is countable $\Rightarrow \mathbf{R}$ is countable $\Rightarrow$ a contradiction.]
19. The *dihedral group* D_n: The group D_n is completely determined by two generators s, t; and the defining relations $t^n = 1, s^2 = 1, (ts)^2 = 1$, and $t^k \neq 1$ for $0 < k < n$, where 1 denotes the identity element. Find $|D_n|$. Construct the Cayley table for the group D_3. Interpret D_n as a group of symmetries of a regular n-gon.
20. *The quaternion group* H. This group is completely determined by two generators s, t; and the defining relations $s^4 = 1, t^2 = s^2, ts = s^3 t$. Construct its Cayley table.

21. (a) *External direct product of groups*. Let H and K be groups. Show that

(i) $H \times K$ is a group under binary operation: $(h, k)(h', k') = (hh', kk')$ $\forall h, h' \in H$ and $k, k' \in K$;
(ii) If $H \neq \{1\}$ and $K \neq \{1\}$, $H \times K$ is neither isomorphic to H nor to K;
(iii) $H \times K$ is an abelian group iff H and K are both abelian groups.

(b) *Internal direct product of subgroups*. Let G be a group and H, K be normal subgroups of G such that $G = HK$ and $H \cap K = \{1\}$. Then G is called the internal direct product of H and K. If G is an additive abelian group, then it is called the internal direct sum of H and K and denoted by $G = H \oplus K$.

Prove the following:

(i) $G = H \oplus K$ iff every element $x \in G$ can be expressed uniquely as $x = h + k$ for some $h \in H$ and $k \in K$.
(ii) Let G be the internal direct product of normal subgroups H and K. Then G is isomorphic to $H \times K$.
(iii) If $G = H \times K$, then H and K are isomorphic to suitable subgroups $\bar{H}$ and $\bar{K}$ of G respectively, such that G is the internal direct product of $\bar{H}$ and $\bar{K}$.
(iv) Let $f : G \to H$ and $g : H \to K$ be homomorphisms of abelian groups such that $g \circ f$ is an isomorphism. Then $H = \text{Im } f \oplus \ker f$.

22. *Klein four-group* $C \times C$: If C is the cyclic group of order 2 generated by g, show by using Ex. 21 that $C \times C$ is a group of order 4. Work out the multiplication table for $C \times C$. Show that the cyclic group of order 4, $C_4 = \{1, a, a^2, a^3\}$, where $a^4 = 1$ and the group $C \times C$ are not isomorphic.

[*Hint*. All elements other than (1, 1) of $C \times C$ are of order 2 but it is not true for C_4.]

Remark The Klein 4-group is named after Felix Klein (1849–1925). This group may also be defined as the set $\{1, a, b, c\}$ together with the multiplication defined by the following table:

$\bullet$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

23. (a) Show that a finite group G of order r is cyclic iff it contains an element g of order r.

(b) Let $\langle a \rangle$ be a finite cyclic group of order n. Show that $\langle a \rangle = \{a, a^2, \ldots, a^{n-1}\}$.

24. Show that every element a ($\neq 1$) in a group of prime order p has period p.
25. Show that a group in which every element a ($\neq 1$) has period 2 is abelian.
26. Show that every group of order <6 is abelian.

27. Let G be a non-abelian group of order 10. Prove that G contains at least one element of period 5.
28. If G is a group of order p^2 (p is prime >1), show that G is abelian (see Ex. 3 of Exercises-I, Chap. 3).
29. Let A and B be different subgroups of a group G such that both A and B are of prime order p. Show that $A \cap B = \{1\}$.
30. Let G be a group of order 27. Prove that G contains a subgroup of order 3.
31. Let G be a finite group and A, B subgroups of G such that $B \subseteq A$. Show that $[G : A]$ is a factor of $[G : B]$.
32. Let f be a homomorphism from G to G', where G and G' are finite groups. Show that $|\operatorname{Im} f|$ divides $|G'|$ and $\gcd(|G|, |G'|)$.
    [*Hint*. Use Theorem 2.4.5(i) and Theorem 2.5.1.]
33. Show that
    (i) two cyclic groups of the same order are isomorphic;
    (ii) every cyclic group of order n is isomorphic to $\mathbf{Z}_n$ (cf. Theorem 2.4.12);
    (iii) $\mathbf{Z}_4$ is cyclic and both 1 and 3 are generators;
    (iv) $\mathbf{Z}_p$ has no proper subgroup if p is a prime integer;
    (v) an infinite cycle group has exactly two generators.
34. Find all the subgroups of $\mathbf{Z}_{18}$ and give their lattice diagram.
35. (a) Let G be a group of order pq, where p and q are primes. Verify that every proper subgroup of G is cyclic.
    (b) Prove that finite groups of rotations of the Euclidean plane are cyclic.
36. Let G be a finite group of order 30. Can G contain a subgroup of order 9? Justify your answer.
37. If the index of a subgroup H in a group G is 2, prove that $aH = Ha \ \forall a \in G$ and G/H is isomorphic to a cyclic group of order 2.
38. Give an example of a subgroup H in a group G satisfying $aH = Ha \ \forall a \in H$ but $[G : H] > 2$.
39. If H is a subgroup of finite index in G, prove that there is only a finite number of distinct subgroups of G of the form aHa^{-1}.
40. Show that the order of an element of finite group G divides the order of G.
    [*Hint*. The order of an element $a \in G$ is the same as the order of $\langle a \rangle$ (by Theorem 2.4.8) and then apply Lagrange's Theorem.]
41. Let G be a group and $x \in G$ be such that x is of finite order m. If $x^r = 1$, show that $m|r$.
42. (i) Let G be a cyclic group of prime order p. Show that G has no proper subgroups.
    (ii) Show that the only non-trivial groups which have no proper subgroups are the cyclic groups of prime order p.
43. Let $(G, \cdot)$, $(H, \cdot)$ and $(K, \cdot)$ be groups and $f : G \to H$ and $g : H \to K$ be group homomorphisms. Show that
    (i) $g \circ f : G \to K$ is also a homomorphism. Further, if f, g are both monomorphisms (epimorphisms), then $g \circ f$ is also a monomorphism (epimorphism);

(ii) in particular, if f and g are both isomorphisms, then $g \circ f$ is also an isomorphism;
(iii) further, if $f : G \to H$ is an isomorphism, then $f^{-1} : H \to G$ is also an isomorphism.

44. Let P be the set of all polynomials with integral coefficients. Show that $(P, +)$ is an abelian group isomorphic to the multiplicative group $(\mathbf{Q}^+, .)$ of positive rationals.

[*Hint*. Let $\{p_n\}_{n=0}^{\infty}$ be an *enumeration of* positive rationals *in increasing order*: $p_0 < p_1 < p_2 < \cdots < p_n < \cdots$.

Define $f : P \to \mathbf{Q}^+$ as follows: for $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in P$, $f(p(x)) = p_0^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \in \mathbf{Q}^+$.

Verify that f is a homomorphism with $\ker f = \{a_0 + a_1 x + \cdots + a_n \in P : p_0^{a_0} p_1^{a_1} \cdots p_n^{a_n} = 1\} = \{0\}$. Check that f is an *isomorphism*.]

45. A homomorphism of a group into itself is called an endomorphism. Let $(\mathbf{C}^*, \cdot)$ be the multiplicative group of non-zero complex numbers. Define $f : (\mathbf{C}^*, \cdot) \to (\mathbf{C}^*, \cdot)$ by $f(z) = z^n$ (n is a positive integer). Show that f is an endomorphism. Find $\ker f$.
46. Let G be a group. Show that a mapping $f : G \to G$ defined by $x \mapsto x^{-1}$ is an automorphism of G iff G is abelian.
47. Let G be a group and $a \in G$. Then the mapping $f_a : G \to G$ defined by $f_a(x) = a^{-1}xa$ $(\forall x \in X)$ is an automorphism of G (called an inner automorphism induced by a) and $f_1 = 1_G$ is an inner automorphism (called a trivial automorphism). Show that for an abelian group G, the only inner automorphism is 1_G but for a non-abelian group there exist non-trivial automorphisms.
48. Show that

(a) the map $f : (\mathbf{R}^+, \cdot) \to (\mathrm{R}, +)$ defined by $f(x) = \log_e x$ is an isomorphism;
(b) the map $g : (\mathbf{R}, +) \to (\mathbf{R}^+, \cdot)$ defined by $g(x) = e^x$ is an isomorphism.

[*Hint*. Check that f and g are homomorphisms such that $g \circ f = 1$ and $f \circ g = 1$].

49. Show that every homomorphic image of an abelian group is abelian but the converse is not true.
50. Show that

(a) a homomorphism from any group to a simple group is either trivial or surjective;
(b) a homomorphism from a simple group is either trivial or one-to-one.

51. Prove the following:

$$\mathrm{Aut}\,\mathbf{Z}_6 \cong \mathbf{Z}_2 \quad \text{and} \quad \mathrm{Aut}\,\mathbf{Z}_5 \cong \mathbf{Z}_4$$

(see Theorem 2.3.4).

52. (a) If G is a cyclic group and $f : G \to G'$ is a homomorphism of groups, show that $\mathrm{Im}\, f$ is cyclic.

(b) Let G be a group such that every cyclic subgroup of G is normal in G. Show that every subgroup of G is a normal subgroup of G.

53. If G is a cyclic group and a, b are generators of G. Show that there is an automorphism of G which maps a onto b and also any automorphism of G maps a generator onto a generator.
54. Let $A(S)$ be the permutation group on $S(\neq\emptyset)$. If two permutations $f, g \in A(S)$ are such that for any $x \in S$, $f(x) \neq x \Rightarrow g(x) = x$ and for any $y \in S$, $g(y) \neq y \Rightarrow f(y) = y$, (then f and g are called disjoint), examine the validity of the equality $fg = gf$.
55. Show that every permutation can be expressed as a product of disjoint cycles (the number of cycle may be 1), where the component cycles are uniquely determined except for their order of combination.
56. Show that a permutation σ can be expressed as a product of transpositions (i.e., cycles of order 2) in different ways but the number of transpositions in such a decomposition is always odd or always even.

    (σ is said to be an odd or even permutation according as r is odd or even, where r is the number of transpositions in a decomposition.)
57. Show that in a permutation group G, either all permutations are even or exactly half the permutations are even, which form a subgroup of G.
58. Show that all even permutations of a set of n distinct elements ($n \geq 3$) form a normal subgroup A_n of the symmetric group S_n (A_n is called the *alternating group* of degree n).

    Find its order (see Ex. 14 of SE-II).
59. (i) Show that the alternating group A_n is generated by the following cycles of degree 3: $(123), (124), \ldots, (12n)$.

    (ii) If a normal subgroup H of the alternating group A_n contains a cycle of degree 3, show that $H = A_n$.

    (iii) Show that the groups S_3 and $\mathbf{Z}_6$ are not isomorphic but for every proper subgroup G of S_3, there exists a proper subgroup H of $\mathbf{Z}_6$ such that $G \cong H$.
60. Let G be a group and $a, b \in G$. The element $aba^{-1}b^{-1}$ denoted by $[a, b]$ is called a commutator of G. The subgroup of G whose elements are finite products of commutators of G is called the commutator subgroup of G. Denote this subgroup by $C(G)$. Show that

    (i) $[a, b][b, a] = 1$;
    (ii) G is an abelian group iff $C(G) = \{1\}$;
    (iii) $C(G)$ is a normal subgroup of G;
    (iv) the quotient group $G/C(G)$ is abelian;
    (v) if H is any normal subgroup of G such that G/H is abelian, then $C(G) \subset H$;
    (vi) $C(S_3) = A_3$.

61. A group G is called a *quaternion* group iff G is generated by two elements $a, b \in G$ satisfying the relations:

$$O(a) = 4, \qquad a^2 = b^2 \quad \text{and} \quad ba = a^3 b \quad \text{(see Ex. 20)}.$$

    Let G be a subgroup of the General Linear group $GL(2, \mathbf{C})$ of order 2 over $\mathbf{C}$, generated by $A = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. Show that G is a quaternion group.

62. Prove the following:

    (a) A semigroup S is a semilattice of groups iff S is a regular semigroup, all of whose one sided ideals are two sided.
    (b) A semigroup S is a semilattice of left groups iff S is a regular semigroup, all of whose left ideals are two sided.
    (c) (i) A semigroup S is a semilattice of left groups iff the condition $I \cap L \cap R = RLI$ holds for any two-sided ideal I, every ideal left L and right ideal R of S;
        (ii) a semigroup S is a semilattice of right groups iff the condition $I \cap L \cap R = IRL$ holds for every two-sided ideal I, every left ideal L and every right ideal R of S.

63. A *Clifford* semigroup is a regular semigroup S in which the idempotents are central i.e., in which $ex = xe$ for every idempotent $e \in S$ and every $x \in S$.

    Prove that a semigroup S is a Clifford semigroup iff S is a semilattice of groups.

64. Prove the following:

    (i) Finite groups of rotations of Euclidean plane are cyclic; any such group of order n consists of all rotations about a fixed point through angles of $2\frac{r\pi}{n}$ for $r = 0, 1, 2, \ldots, n-1$.
    (ii) The cyclic and dihedral groups and the *groups of tetrahedron, octahedron* and *icosahedron* are all the finite subgroups of the group of rotations of Euclidean 3-dimensional space.

        The latter three groups are called the *tetrahedral group* of 12 rotations carrying a regular tetrahedron to itself, the *octahedral group* of order 24 of rotations of a regular octahedron and the *icosahedral group* of 60 rotations of a regular icosahedron, respectively.

65. *Series of Subgroups*. A subnormal (or subinvariant) series of subgroups of a group G is a finite sequence $\{H_i\}$ of subgroups of G such that

$$\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$$

    and H_i is a normal subgroup of H_{i+1} for each $i = 0, 1, \ldots, n-1$.

    In addition, if each H_i is a normal subgroup of G, then $\{H_i\}$ is called a *normal* (or *invariant series*) series of G:

    Two subnormal (normal) series $\{H_i\}$ and $\{T_j\}$ of the same group G are isomorphic iff $\exists$ a one-to-one correspondence between the factor groups $\{H_{i+1}/H_i\}$ and $\{T_{j+1}/T_j\}$ such that the corresponding factor groups are isomorphic.

    A subnormal series (normal series) $\{T_j\}$ is a refinement of a subnormal series (normal series) $\{H_i\}$ of a group G iff $\{H_i\} \subseteq \{T_j\}$, i.e., iff each H_i is one of the T_j.

    A subnormal series $\{T_j\}$ of a group G is a composition series iff all the factors groups T_{j+1}/T_j are simple. A normal series $\{N_i\}$ of G is a *principal series* iff all the factor groups N_{i+1}/N_i are simple.

A group G is solvable iff it has a composition series $\{T_j\}$ such that all factor groups T_{j+1}/T_j are abelian.

Prove the following:

(a) (i) *Schreier's Theorem*: Two subnormal (normal)series of a group G have isomorphic refinements.
(ii) $\mathbf{Z}$ has neither a composition series nor a principal series.
(iii) *Jordan–Hölder's Theorem*. Any two composition (principal) series of group G are isomorphic.
(iv) If G has a composition (principal) series, and if N is a proper normal subgroup of G, then $\exists$ a composition (principal) series containing N.
(v) A subgroup of a solvable group and the homomorphic image of a solvable group are solvable.
(vi) If G is a group and N is a normal subgroup of G such that both N and G/N are solvable, then G is solvable.

(b) Let G be a group and A a pseudo-ideal of G. Then G is solvable $\Leftrightarrow$ A is solvable.

66. An abelian group A is said to an *injective group* iff wherever $i : G' \subset G$ (G' is a subgroup of G), for any homomorphism $f : G' \to A$, of abelian groups $\exists$ a homomorphism $\tilde{f} : G \to A$ such that $\tilde{f} \circ i = f$ and A is said to be a *projective group* iff for any epimorphism $\alpha : G \to G''$ of abelian groups, and any homomorphism $f : A \to G''$, $\exists$ a homomorphism $\tilde{f} : A \to G$ such that $\alpha \circ \tilde{f} = f$. An abelian group A is said to be a *divisible group* iff for any element $a \in A$, and any non-zero integer n, $\exists$ an element $b \in A$ such that $nb = a$. Show that

(i) an abelian group A is injective $\Leftrightarrow$ A is divisible;
(ii) any abelian group is a subgroup of an injective group.

2.12 Exercises (Objective Type)

Exercises A *Identify the correct alternative*(*s*) (*there may be more than one*) *from the following list*:

1. Let G be a group and $a, b \in G$ such that $O(a) = 4$, $O(b) = 2$ and $a^3b = ba$. Then $O(ab)$ is
   (a) 2 (b) 3 (c) 4 (d) 8.
2. Let G be a cyclic group of infinite order. Then the number of elements of finite order in G is
   (a) 1 (b) 2 (c) infinitely many (d) 4.
3. Let G be an infinite cyclic group. Then the number of generators of G is
   (a) 1 (b) 3 (c) 2 (d) infinitely many.
4. The number of subgroups of S_3 is
   (a) 4 (b) 5 (c) 6 (d) 3.
5. The order of the permutation (1 2 4) (3 5 6) in S_6 is
   (a) 2 (b) 4 (c) 3 (d) 9.

6. Let G be a finite group and H, K be two finite subgroups of G such that $|H| = 7$ and $|K| = 11$. Then $|H \cap K|$ is
   (a) 1 (b) 7 (c) 11 (d) 77.
7. Let G be a finite group and H, K be two subgroups of G such that $|H| = 7$, $|K| = 11$. Then $|HK|$ is
   (a) 77 (b) 1 (c) 7 (d) 11.
8. Let G be a finite group of order ≤ 400. If G has subgroups of order 45 and 75, then $|G|$ is
   (a) 400 (b) 225 (c) 300 (d) 75.
9. Let G be a finite group having two subgroups H and K and such that $|H| = 45$, $|K| = 75$. If $|G|$ is n, where $225 < n < 500$, then n is given by
   (a) 230 (b) 475 (c) 450 (d) 460.
10. Let G be a cyclic group of order 25. Then the number of elements of order 5 in G is
    (a) 1 (b) 3 (c) 4 (d) 20.
11. Let G be a non-trivial group of order n. Then G has

    (a) always an element of order 5;
    (b) no element of order 5;
    (c) an element of order 5 if 5 divides n;
    (d) an element of order 30 if 30 divides n.

12. The number of elements of order 5 in the group $\mathbf{Z}_{25} \times \mathbf{Z}_5$ is
    (a) 1 (b) 16 (c) 24 (d) 20.
13. The number of subgroups of order 5 in the group $\mathbf{Z}_5 \times \mathbf{Z}_9$ is
    (a) 1 (b) 2 (c) 24 (d) 5.
14. Automorphism group $\mathrm{Aut}(\mathbf{Z}_5)$ of $\mathbf{Z}_5$ is isomorphic to
    (a) $\mathbf{Z}_5$ (b) $\mathbf{Z}_3$ (c) $\mathbf{Z}_4$ (d) $\mathbf{Z}_2$.
15. Let p be a prime integer. Then $|\mathrm{Aut}(\mathbf{Z}_p)|$ is
    (a) p (b) $p - 1$ (c) 1 (d) $p(p - 1)$.
16. Let $f : \mathbf{Z} \to \mathbf{Z}$ be a group homomorphism such that $f(1) = 1$. Then

    (a) f is an isomorphism;
    (b) f is a monomorphism but not an isomorphism;
    (c) f is not a monomorphism;
    (d) f is not an epimorphism.

17. Let G be an arbitrary group and $f : G \to G$ be an epimorphism. Then

    (a) f is always an isomorphism;
    (b) f is not always an isomorphism;
    (c) f is not always a monomorphism;
    (d) $\ker f$ contains more than one element.

18. The number of subgroups of $4\mathbf{Z}/16\mathbf{Z}$ is
    (a) 5 (b) 3 (c) 4 (d) 2.
19. The number of subgroups of $(\mathbf{Z}, +)$ which contains $10\mathbf{Z}$ as a subgroup is
    (a) 4 (b) 10 (c) infinite (d) 3.

20. Consider the groups $G = \mathbf{Z}_2 \times \mathbf{Z}_3$, and $K = \mathbf{Z}_6$. Then

    (a) $\exists$ no homomorphism from G onto K;
    (b) $\exists$ no monomorphism from G onto K;
    (c) $\exists$ an isomorphism from G onto K;
    (d) $\exists$ an epimorphism from G onto K.

21. Let A_n be the set of all even permutations of the symmetric group S_n. Then

    (a) A_n is a subgroup of S_n but not normal;
    (b) A_n is not a subgroup of S_n;
    (c) A_n is a normal subgroup of S_n;
    (d) A_n is always a non-commutative subgroup of S_n.

22. The group $\mathbf{Z}_3 \times \mathbf{Z}_3$ is

    (a) cyclic;
    (b) not isomorphic to $\mathbf{Z}_9$;
    (c) isomorphic to $\mathbf{Z}_9$;
    (d) simple.

23. The group $\mathbf{Z}_2 \times \mathbf{Z}_2$ is

    (a) cyclic;
    (b) isomorphic to Klein's 4-group;
    (c) not isomorphic to Klein 4-group;
    (d) simple.

24. The group $\mathbf{Z}_8 \times \mathbf{Z}_9$ is

    (a) not cyclic;
    (b) isomorphic to $\mathbf{Z}_8 \times \mathbf{Z}_3 \times \mathbf{Z}_3$;
    (c) isomorphic to $\mathbf{Z}_{72}$;
    (d) simple.

25. The number of homomorphisms from the group $(\mathbf{Q}, +)$ into the group $(\mathbf{Q}^+, \cdot)$ is

    (a) one (b) two (c) infinitely many (d) zero.

26. The number of generators of the group $\mathbf{Z}_p \times \mathbf{Z}_q$, where p, q are relatively prime to each other, is

    (a) pq (b) $(p-1)(q-1)$ (c) $p(q-1)$ (d) $q(p-1)$.

27. Given a group G, let $Z(G)$ be its center. For $n \in \mathbf{N}^+$ (the set of positive integers) define $G_n = \{(g_1, \ldots, g_n) \in Z(G) \times \cdots \times Z(G) : g_1 \cdots g_n = 1\}$. As a subset of the direct product group $G \times \cdots \times G$ (n times direct product of the group G), G_n is

    (a) isomorphic to the direct product $Z(G) \times \cdots \times Z(G)$ ($(n-1)$ times);
    (b) a subgroup but not necessarily a normal subgroup;
    (c) a normal subgroup;
    (d) not necessarily a subgroup.

28. Let G be a group of order 77. Then its center $Z(G)$ is isomorphic to
    (a) $\mathbf{Z}_7$ (b) $\mathbf{Z}_1$ (c) $\mathbf{Z}_{11}$ (d) $\mathbf{Z}_{77}$.
29. The number of group homomorphisms from the symmetric group S_3 to the group $\mathbf{Z}_6$ is
    (a) 2 (b) 3 (c) 6 (d) 1.
30. Let G be the group given by $G = \mathbf{Q}/\mathbf{Z}$ and n be a positive integer. Then the statement that there exists a cyclic subgroup of G of order n is

    (a) never true;
    (b) not necessarily true;
    (c) true but not necessarily a unique one;
    (d) true but a unique one.

31. Let $H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ and $K = \{e, (1\ 2)(3\ 4)\}$ be subgroups of S_4, where e denote the identity element of S_4. Then

    (a) H and K are both normal subgroups of S_4;
    (b) K is normal in A_4 but A_4 is not normal in S_4;
    (c) H is normal in S_4, but K is not;
    (d) K is normal in H and H is normal in A_4.

32. Let n be the orders of permutations σ of 11 symbols such that σ does not fix any symbol. Then n is
    (a) 18 (b) 15 (c) 28 (d) 30.
33. Which of the following groups is (are) cyclic?
    (a) $\mathbf{Z}_8 \oplus \mathbf{Z}_8$ (b) $\mathbf{Z}_8 \oplus \mathbf{Z}_9$ (c) $\mathbf{Z}_8 \oplus \mathbf{Z}_{10}$ (d) a group of prime order.
34. Let G be a finite group and H be a subgroup of G. Let $O(G) = m$ and $O(H) = n$. Which of the following statements is (are) correct?

    (a) If m/n is a prime number, then H is normal in G;
    (b) if $m = 2n$, then H is normal in G;
    (c) if there exist normal subgroups A and B of G such that $H = \{ab \mid a \in A, b \in B\}$, then H is normal in G;
    (d) if $[G : H] = 2$, then H is normal in G.

35. Let G be a finite abelian group of odd order. Which of the following maps define an automorphism of G?

    (a) The map $x \mapsto x^{-1}$ for all $x \in G$;
    (b) the map $x \mapsto x^2$ for all $x \in G$;
    (c) the map $x \mapsto x$ for all $x \in G$;
    (d) the map $x \mapsto x^{-2}$ for all $x \in G$.

36. Let $GL(n, \mathbf{R})$ denote the group of all $n \times n$ matrices with real entries (with respect to matrix multiplication) which are invertible. Which of the following subgroups of $GL(n, \mathbf{R})$ is (are) normal?

    (a) The subgroup of all real orthogonal matrices;
    (b) the subgroup of all matrices whose trace is zero;

(c) the subgroup of all invertible diagonal matrices;
(d) the subgroup of all matrices with determinant equal to unity.

37. Which of the following subgroups of $GL(2, \mathbf{C})$ is (are) abelian?

(a) The subgroup of invertible upper triangular matrices;
(b) the subgroup A defined by $A = \left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] : a, b \in \mathbf{R} \text{ and } |a|^2 + |b|^2 = 1\right\}$;
(c) the subgroup $G = \{M \in GL_2(C) : \det M = 1\}$;
(d) the subgroup B defined by $B = \left\{\left[\begin{smallmatrix} a & b \\ -\bar{b} & \bar{a} \end{smallmatrix}\right] : a, b \in \mathbf{C} \text{ and } |a|^2 + |b|^2 = 1\right\}$.

38. Let $f : (\mathbf{Q}, +) \to (\mathbf{Q}, +)$ be a non-zero homomorphism. Then

(a) f is always bijective;
(b) f is always surjective;
(c) f is always injective;
(d) f is not necessarily injective or surjective.

39. Consider the element

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

of the symmetric group S_5 on five elements. Then

(a) α is conjugate to $\left(\begin{smallmatrix} 4 & 5 & 2 & 3 & 1 \\ 5 & 4 & 3 & 1 & 2 \end{smallmatrix}\right)$;
(b) the order of α is 5;
(c) α is the product of two cycles;
(d) α commutes with all elements of S_5.

40. Let G be a group of order 60. Then

(a) G has a subgroup of order 30;
(b) G is abelian;
(c) G has subgroups of order 2, 3, and 5;
(d) G has subgroups of order 6, 10, and 15.

41. Let G be an abelian group of order n. Then
(a) $n = 36$ (b) $n = 65$ (c) $n = 15$ (d) $n = 21$.

42. Which of the following subgroups are necessarily normal subgroups?

(a) The kernel of a group homomorphism;
(b) the center of a group;
(c) a subgroup of a commutative group;
(d) the subgroup consisting of all matrices with positive determinant in the group of all invertible $n \times n$ matrices with real entries (under matrix multiplication).

43. Which of the given subgroup H of a group G is a normal subgroup of G?

(a) G is the group of all 2×2 invertible upper matrices with real entries under matrix multiplication and H is the subgroup of all such matrices (a_{ij}) such that $a_{11} = 1$;

(b) G is the group of all $n \times n$ invertible matrices with real entries under matrix multiplication and H is the subgroup of such matrices with determinant 1;
(c) G is the group of all 2×2 invertible upper matrices with real entries under matrix multiplication and H is the subgroup of all such matrices (a_{ij}) such that $a_{11} = a_{22}$;
(d) G is the group of all $n \times n$ invertible matrices with real entries under matrix multiplication and H is the subgroup of such matrices with positive determinant.

44. Let S_7 denote the symmetric group of all permutations of the symbols $\{1, 2, 3, 4, 5, 6, 7\}$. Then

(a) S_7 has an element of order 10;
(b) S_7 has an element of order 7;
(c) S_7 has an element of order 15;
(d) the order of any element of S_7 is at most 12.

Exercises B (True/False Statements) Determine which of the following statements are true or false. Justify your answers with a proof or give counter-examples accordingly.

1. The set of all Möbius transformations $S : \mathbf{C} \to \mathbf{C}$, $z \mapsto \frac{az+b}{cz+d}$, $ad - bc \neq 0$; $a, b, c, d \in \mathbf{C}$ form a group under usual composition of maps.
2. The set $SL(2, \mathbf{R}) = \{X \in GL(2, \mathbf{R}) : \det X = 1\}$ is a normal subgroup of the group $GL(2, \mathbf{R})$ of all real non-singular matrices of order 2.
3. The set $G = \{x \in \mathbf{Q} : 0 < x \leq 1\}$ is a group under the usual multiplication.
4. If each element of a group G, except its identity element is of order 2, then the group is abelian.
5. A cyclic group can have more than one generator.
6. Let G be a group of infinite order. Then all the elements of G, which are of the form $a^n, n \in \mathbf{Z}$, for a given $a \neq 1$, are distinct.
7. The octic group D_4 is cyclic.
8. If every proper subgroup of group G is cyclic, then G is also cyclic.
9. Let G be a cyclic group of order n. Then G has $\phi(n)$ distinct generators.
10. If G is an abelian group, then the only inner automorphism of G is the identity automorphism.
11. Let G be the internal direct product of its normal subgroups H and K. Then the groups G/H and K are isomorphic.
12. If g and g^2 are both generators of a cyclic group G of order n, then n is prime.
13. Let G be a finite group of odd order. If $H = \{x^2 : x \in G\}$, then H is a subgroup of G only if G is cyclic.
14. Two permutations in S_n are conjugate to each other $\Leftrightarrow$ they have the same cycle decomposition.
15. $Z(A_4)$, the center of the alternating group A_4 is $\{e\}$.
16. Let H be a normal subgroup of a group G. If H and G/H are both cyclic, then G is cyclic.
17. Every group of order 4 is commutative.

18. Every finitely generated group G can be expressed as the union of an ascending sequence of proper subgroups of G.
19. Let G be a finite group and H be a proper subgroup of G such that $x, y \in G$ and $x, y \notin H \Rightarrow xy \in H$. Then $|G|$ is an even integer.
20. The group $(\mathbf{Q}, +)$ is cyclic.
21. The group $(\mathbf{R}, +)$ is cyclic.
22. Any finitely generated subgroup of $(\mathbf{Q}, +)$ is cyclic.
23. In the group $(\mathbf{Q}, +)$, there exists an ascending sequence of cyclic groups G_n such that $\mathbf{Q} = \bigcup G_n$.
24. Let $(H, \cdot)$ be a subgroup of $(\mathbf{C}^*, \cdot)$ such that $[\mathbf{C}^* : H] = n$ (finite). Then $H \subsetneqq \mathbf{C}^*$.
25. Every finite subgroup $(H, \cdot)$ of $(\mathbf{C}^*, \cdot)$ is cyclic.
26. The groups $(\mathbf{Z}, +)$ and $(\mathbf{R}, +)$ are isomorphic.
27. The groups $(\mathbf{R}^*, \cdot)$ and $(\mathbf{R}, +)$ are isomorphic.
28. The groups $(\mathbf{Z}, +)$ and $(\mathbf{Q}, +)$ are isomorphic.
29. Every proper subgroup of a non-cyclic abelian group is non-cyclic.
30. A group G cannot be isomorphic to a proper subgroup H of G.
31. A group G is commutative $\Leftrightarrow (ab)^n = a^n b^n,\ \forall a, b \in G$ and for any three consecutive integers n.
32. $\mathbf{Z}_9$ is a homomorphic image of $\mathbf{Z}_3 \times \mathbf{Z}_3$.
33. The groups $\mathbf{Z}_6 \times \mathbf{Z}_8$ and $\mathbf{Z}_{48}$ are isomorphic.
34. Let G be a group. For a fixed $a \in G$, a mapping $\psi_a : G \to G$ is defined by $\psi_a(x) = ax, \forall x \in G$. Then ψ_a is a permutation of G.

2.13 Additional Reading

We refer the reader to the books (Adhikari and Adhikari 2003, 2004; Artin 1991; Birkoff and Mac Lane 1965; Chatterjee 1964; Herstein 1964; Howie 1976; Hungerford 1974; Jacobson 1974, 1980; Lang 1965; Mac Lane 1997; Malik et al. 1997; Shafarevich 1997; van der Waerden 1970) for further details.

References

Adhikari, M.R., Adhikari, A.: Groups, Rings and Modules with Applications, 2nd edn. Universities Press, Hyderabad (2003)
Adhikari, M.R., Adhikari, A.: Text Book of Linear Algebra: An Introduction to Modern Algebra. Allied Publishers, New Delhi (2004)
Artin, M.: Algebra. Prentice-Hall, Englewood Cliffs (1991)
Birkoff, G., Mac Lane, S.: A Survey of Modern Algebra. Macmillan, New York (1965)
Carruth, J.H., Hildebrant, J.A., Koch, R.J.: The Theory of Topological Semigroups I. Dekker, New York (1983)
Carruth, J.H., Hildebrant, J.A., Koch, R.J.: The Theory of Topological Semigroups II. Dekker, New York (1986)
Chatterjee, B.C.: Abstract Algebra I. Dasgupta, Kolkata (1964)

Cotton, F.A.: Chemical Application to Group Theory. Wiley, New York (1971)
Elliot, J.P., Dawber, P.G.: Symmetry in Physics. Macmillan, New York (1979)
Farmer, D.W.: Groups and Symmetry. Mathematics World Series, vol. 5, Am. Math. Soc., Providence (1996)
De Groot, J.: Groups represented by Homomorphic Groups I. Math. Ann. **138**, 80–102 (1959)
Herstein, I.: Topics in Algebra. Blaisdell, New York (1964)
Howie, I.M.: An Introduction to Semigroup Theory. Academic Press, New York (1976)
Hungerford, T.W.: Algebra. Springer, New York (1974)
Jacobson, N.: Basic Algebra I. Freeman, San Francisco (1974)
Jacobson, N.: Basic Algebra II. Freeman, San Francisco (1980)
Lang, S.: Algebra, 2nd edn. Addison-Wesley, Reading (1965)
Mac Lane, S.: Category for the Working Mathematician. Springer, Berlin (1997)
Magil, K.D. Jr: Some open problems and directions for further research in semigroups of continuous selfmaps. In: Universal Algebra and Applications, Banach Centre Publications, pp. 439–454. PWN, Warsaw (1982)
Malik, S., Mordeson, J.N., Sen, M.K.: Abstract Algebra, Fundamentals of Abstract Algebra. McGraw Hill, New York (1997)
Massey, W.S.: A Basic Course in Algebraic Topology. Springer, New York (1991)
Rodes, F.: On the fundamental group of a transformation group. Proc. Lond. Math. Soc. **16**, 635–650 (1966)
Rotman, I.J.: An Introduction to Algebraic Topology. Springer, New York (1988)
Shafarevich, I.R.: Basic Notions of Algebra. Springer, Berlin (1997)
Spanier, E.H.: Algebraic Topology. McGraw-Hill, New York (1966)
Sternberg, S.: Group Theory and Physics. Cambridge University Press, Cambridge (1994)
van der Waerden, B.L.: Modern Algebra. Ungar, New York (1970)
Weyl, H.: Symmetry. Princeton University Press, Princeton (1952)

http://www.springer.com/978-81-322-1598-1

Basic Modern Algebra with Applications

Adhikari, M.R.; Adhikari, A.

2014, XIX, 637 p. 48 illus., Hardcover
ISBN: 978-81-322-1598-1