Chapter 4

Group Theory

INTRODUCTION

In this chapter, we shall first define general algebraic systems and discuss some of their basic properties and concepts that will be later applied to particular algebraic systems such as semigroups, monoids, groups and rings. Semigroups find their applications in computer arithmetic such as multiplication, theory of sequential machines and formal languages. Monoids are used in the study of syntactic analysis and formal languages. Group theory is useful in the design of fast adders and error-correcting codes. Towards the end of the chapter, basic notions of error-detecting and error-correcting codes are introduced.

ALGEBRAIC SYSTEMS

Definition

A system consisting of a non-empty set and one or more n-ary operations on the set is called an *algebraic system*. An algebraic system will be denoted by $\{S, f_1, f_2, \ldots\}$, when S is the non-empty set and $f_1, f_2, \ldots$ are n-ary operations on S. We will mostly deal with algebraic systems, with $n = 0$, 1 and 2, containing one or two operations only. Though we will mostly deal with one algebraic system only, we may occassionally consider two or more systems which are of the same 'type' in some sense.

General Properties of Algebraic Systems

Let $\{S, *, \oplus\}$ be an algebraic system, where $*$ and $\oplus$ are binary operations on S.

1. Closure Property

For any $a, b \in S$, $\quad a * b \in S$.

For example, if $a, b \in Z$, $a + b \in Z$ and $a \times b \in Z$, where + and × are the operations of addition and multiplication.

2. Associativity

For any $a, b, c \in S$, $(a * b) * c = a * (b * c)$.

For example, if $a, b, c \in Z$,

$$(a + b) + c = a + (b + c) \text{ and } (a \times b) \times c = a \times (b \times c).$$

3. Commutativity

For any $a, b \in S$, $a * b = b * a$.

For example, if $a, b \in Z$, $a + b = b + a$ and $a \times b = b \times a$

4. Identity Element

There exists a distinguished element $e \in S$, such that for any $a \in S$,

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

The element $e \in S$ is called the identity element of S with respect to operation $*$. For example, 0 and 1 are the identity elements of Z with respect to the operations of addition and multiplication respectively, since, for any $a \in Z$.

$$a + 0 = 0 + a = a$$

and

$$a \times 1 = 1 \times a = a$$

5. Inverse Element

For each $a \in S$, there exists an element $a^{-1} \in S$ such that $a * a^{-1} = a^{-1} * a = e$. The element $a^{-1} \in S$ is called the inverse of a under the operation $*$.

For example, for each $a \in Z$, $-a$ is the inverse of a under the operation of addition, since, $a + (-a) = (-a) + a = 0$, where 0 is the identity element of Z under addition.

6. Distributivity

For any $a, b, c \in S$, $a * (b \oplus c) = a * b \oplus a * c$

In this case the operation $*$ is said to be distributive over the operation $\oplus$.

For example, the usual multiplication is distributive over addition, since $a \times (b + c) = a \times b + a \times c$.

7. Cancellation Property

For any $a, b, c \in S$ and $a \neq 0$,

$$a * b = a * c \Rightarrow b = c$$

and

$$b * a = c * a \Rightarrow b = c$$

For example, cancellation property holds good for any $a, b, c \in Z$ under addition and multiplication.

8. Idempotent Element

An element $a \in S$ is called an idempotent element with respect to the operation $*$, if $a * a = a$.

For example, $0 \in Z$ is an idempotent element under addition, since, $0 + 0 = 0$ and 0 and $1 \in Z$ are idempotent elements under multiplication, since,

$$0 \times 0 = 0 \text{ and } 1 \times 1 = 1$$

9. Homomorphism

If $\{X, \bullet\}$ and $\{Y, *\}$ are two algebraic systems, where $\bullet$ and $*$ are binary (n-ary) operations, then a mapping $g: X \to Y$ is called a *homomorphism* or simply *morphism* from $\{X, \bullet\}$ to $\{Y, *\}$, if for any $x_1, x_2 \in X$,

$$g(x_1 \bullet x_2) = g(x_1) * g(x_2).$$

If a function g satisfying the above condition exists, then $\{Y, *\}$ is called the *homomorphic image* of $\{X, \bullet\}$, even though $g(X) \subseteq Y$.

The concept of homomorphism holds good for algebraic systems with more than one binary operations. Also more than one homomorphic mapping is possible from one algebraic system to another.

9(a) Epimorphism

If the homomorphism $g: \{X, \bullet\} \to \{Y *\}$ is onto, the g is called an *epimorphism*.

9(b) Monomorphism

If the homomorphism $g: \{X, \bullet\} \to \{Y, *\}$ is one-to-one, then g is called a *monomorphism*.

9(c) Isomosphism

If $g: \{X, \bullet\} \to \{Y, *\}$ is one-to-one onto, then g is called an *isomorphism*. In this case the algebraic systems $\{X, \bullet\}$ and $\{Y, *\}$ are said to be *isomorphic* or to be of the same type.

9(d) Endomorphism

A homomorphism $g: \{X, \bullet\} \to \{Y, *\}$ is called an *endomorphism*, if $Y \subseteq X$.

9(e) Automorphism

An isomorphism $g: \{X, \bullet\} \to \{Y, *\}$ is called an *automorphism*, if $Y = X$.

Example

Let $\{X, \bullet\}$, where $X = \{a, b, c\}$ and $\bullet$ is a binary operation on X be represented by the *composition table* or *Cayley's representation table* [Table 4.1(a)]. Let $\{Y, *\}$, where $Y = \{1, 2, 3\}$ and $*$ is a binary operation on Y be represented by Table 4.1(b). If g is defined by $g(a) = 3$, $g(b) = 1$ and $g(c) = 2$, then $\{X, \bullet\}$ and $\{Y, *\}$ are isomorphic.

Note If the set $S = \{a_1, a_2, \ldots, a_n\}$ has only a finite number of elements, then the results of applying the binary operation $\bullet$ on its elements may be represented in a table such that $a_i \bullet a_j \in S$ is entered in the point of intersection of the i^{th} row headed by a_i and the j^{th} column headed by a_j [Refer to Table 4.1(a)]. The resulting table is called the Cayley's table or operation table or composition table.

Table 4.1(a)

$\bullet$	a	b	c
a	a	b	c
b	b	b	c
c	c	b	c

Table 4.1(b)

$*$	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

From the definition of g, we see that it is one-to-one onto.
Also

$$g(a \bullet b) = g(b) = 1 = 3 * 1 = g(a) * g(b)$$
$$g(b \bullet c) = g(c) = 2 = 1 * 2 = g(b) * g(c)$$
$$g(c \bullet a) = g(c) = 2 = 2 * 3 = g(c) * g(a)$$

and so on for other combinations.
Thus g: $\{X, \bullet\} \rightarrow \{Y, *\}$ is an isomorphism.

10. Subalgebra

If $\{X, \bullet\}$ is an algebraic system and Y is a non empty set such that $Y \subseteq X$ is closed under the operation $\bullet$, then $\{Y, \bullet\}$ is called a *sub-algebraic system* or a subalgebra of $\{X, \bullet\}$.

For example, $\{Z^+, \times\}$ is a subalgebra of the algebra $\{Z, \times\}$, where X is the multiplication operator.

11. Direct Product

If $\{X, \bullet\}$ and $\{Y, *\}$ are two algebraic systems of the same type, then the algebraic system $\{X \times Y, \oplus\}$ is called the *direct product* of the algebras $\{X, \bullet\}$ and $\{Y, *\}$, provided the operation $\oplus$ is defined for any $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ as $(x_1, y_1) \oplus (x_2, y_2) = \{x_1 \bullet x_2, y_1 * y_2\}$.

The original algebraic systems are called the *factor algebras* of $\{X \times Y, \oplus\}$.

SEMIGROUPS AND MONOIDS

Definition of a Semigroup

If S is a nonempty set and $*$ be a binary operation on S, then the algebraic system $\{S, *\}$ is called a *semigroup*, if the operation $*$ is associative.
viz., if for any $a, b, c \in S$,

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

Note Since the characteristic property of a binary operation on a set S is the closure property, it is not necessary to mention it explicity when algebraic systems are defined.

For example, if E is the set of positive even numbers, then $\{E, +\}$ and $\{E, \times\}$ are semigroups.

Definition of a Monoid

If a semigroup $\{M, *\}$ has an identity element with respect to the operation $*$, then $\{M, *\}$ is called a *monoid*.
viz., if for any $a, b, c \in M$,

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

and if there exists an element $e \in M$ such that for any $a \in M$, $e * a = a * e = a$, then the algebraic system $\{M, *\}$ is called a monoid.

For example, if N is the set of natural numbers, then $\{N, +\}$ and $\{N, \times\}$ are monoids with the identity elements 0 and 1 respectively.

Note The semigroups $\{E, +\}$ amd $\{E, \times\}$ are not monoids.

HOMOMORPHISM OF SEMIGROUPS AND MONOIDS

Definition

If $\{S, *\}$ and $\{T, \Delta\}$ are any two semigroups, then a mapping $g: S \to T$ such that, for any two elements $a, b \in S$,

$$g(a * b) = g(a) \Delta g(b) \tag{1}$$

is called a *semigroup homomorphism*. As defined in general algebraic system, a semigroup homomorphism is called a semigroup epimorphism, monomorphism or isomorphism, according as the mapping g is onto, one-to-one or one-to-one onto. Similarly two semigroups $\{S, *\}$ and $\{T, \Delta\}$ are said to be isomorphic if there exists a semigroup isomorphic mapping from S to T.

Definition

If $\{M, *, e_M\}$ and $\{T, \Delta, e_T\}$ are any two monoids, where e_M and e_T are identity elements of M and T with respect to the corresponding binary operations $*$ and Δ respectively, then a mapping $g: M \to T$ such that, for any two elements $a, b \in M$,

$$g(a * b) = g(a) \Delta g(b) \tag{2}$$

and

$$g(e_M) = e_T \tag{3}$$

is called a *monoid homomorphism*. As before monoid epimorphism, monomorphism and isomorphism are defined.

Note

1. Even if $\{T, \Delta\}$ is any arbitrary algebraic system, it can be proved to be a semigroup, provided (1) is satisfied, where g is onto as given below:

   $$g\{(a * b) * c\} = g(a * b) \Delta g(c), \text{ by (1)}$$
   $$= \{g(a) \Delta g(b)\} \Delta g(c), \text{ by (1)}$$

   Similarly $g\{a * (b * c)\} = g(a) \Delta \{g(b) \Delta g(c)\}$

   Thus Δ is associative. i.e., $\{T, \Delta\}$ is a semigroup.
2. When g is a semigroup homomorphism from $\{S, *\}$ to $\{T, \Delta\}$ and if $a \in S$ is an idempotent element, then $g(a) \in T$ will also be an idempotent element, for

   $g(a * a) = g(a)$, since a is idempotent.

   Also $g(a * a) = g(a) \Delta g(a)$, since g is homomorphism.

   $\therefore$ $g(a) \Delta g(a) = g(a)$

   i.e., $g(a)$ is idempotent.
3. As can be easily proved, commutativity is also preserved by semigroup and monoid homomorphisms.
4. If $\{S, *\}$ is a monoid or semigroup with an identity e and g is a epimorphism from $\{S, *\}$ to $\{T, \Delta\}$, then the semigroup $\{T, \Delta\}$ is also a monoid, for,

   if $a \in S$, $g(a * e) = g(e * a) = g(a)$, since e is the identity of $\{S, *\}$

   i.e., $g(a) \Delta g(e) = g(e) \Delta g(a)$, by epimorphism.

   $\therefore$ $g(a) \Delta g(e) = g(e) \Delta g(a) = g(a)$

   i.e., $g(e)$, the image of e, is the identity element of $\{T, \Delta\}$

   i.e., $\{T, \Delta\}$ is also a monoid.
5. Even if $\{T, \Delta, e_T\}$ is an arbitrary algebraic system, it can be proved to be a monoid, provided condition (2) is satisfied where g is onto, by using the arguments in notes (1) and (4).

6. The monoid homomorphism preserves the property of invertibility as explained below.

Let $a^{-1} \in M$ be the inverse of $a \in M$

Then $g(a * a^{-1}) = g(e_M) = e_T$, by (3)

Also $g(a * a^{-1}) = g(a) \Delta g(a^{-1})$, by homomorphism

$\therefore$ $g(a) \Delta g(a^{-1}) = e_T$

Similarly, using $g(a^{-1} * a)$, we can prove that $g(a^{-1}) \Delta g(a) = e_T$

Hence the inverse of $g(a) = g(a^{-1})$

i.e., $[g(a)]^{-1} = g(a^{-1})$.

Properties of Homomorphism

Property 1

Composition of two homomorphisms is also a homomorphism.

viz., if $\{S, *\}$, $\{T, \Delta\}$ and $\{V, \oplus\}$ are semigroups and if $g: S \to T$ and $h: T \to V$ are homomorphisms, then $(h \bullet g): S \to V$ is also a homomorphism.

Proof

Let $a, b \in S$. Then

$$\begin{aligned}(h \bullet g)\ (a * b) &= h\{g(a * b)\} \\ &= h\{g(a) \Delta g(b)\} \\ &= h\{g(a)\} \oplus h\{g(b)\} \\ &= (h \bullet g)\ (a) \oplus (h \bullet g)\ (b)\end{aligned}$$

i.e., $(h \bullet g): S \to V$ is also a homomorphism.

Property 2

The set of all semigroup endomorphisms (automorphisms) of a semigroup is a semigroup under the operation of (left) composition.

Proof

Let $g: X \to Y$ be a semigroup endomorphism. Then $Y \subseteq X$.

Let $g_1: X \to Y$, $g_2: X \to Y$ and $g_3: X \to Y$ be any 3 elements of the set E of all endomorphisms of the semigroup.

Then $(g_1 \bullet g_2): X \to Y$, since $Y \subseteq X$

Now $$\begin{aligned}(g_1 \bullet g_2)\ (a * b) &= g_1\{g_2(a * b)\} \\ &= g_1\{g_2(a) \Delta g_2(b)\} \\ &= (g_1 \bullet g_2)(a) \Delta (g_1 \bullet g_2)(b)\end{aligned}$$

$\therefore$ $g_1 \bullet g_2$ is a homomorphism (1)

Also $$\begin{aligned}\{(g_1 \bullet g_2) \bullet g_3\}\ (a * b) &= (g_1 \bullet g_2)\ \{g_3(a * b)\} \\ &= (g_1 \bullet g_2)\ \{g_3(a) \Delta g_3(b)\} \\ &= g_1[g_2\{g_3(a)\}] \Delta g_1[g_2\{g_3(b)\}] \\ &= g_1 \bullet \{(g_2 \bullet g_3)\}(a) \Delta g_1 \bullet \{(g_2 \bullet g_3)\}(b)\end{aligned}$$

$\therefore$ $(g_1 \bullet g_2) \bullet g_3 = g_1 \bullet (g_2 \bullet g_3)$ (2)

From (1) and (2), it follows that E is a semigroup.

Property 3

If $\{S, *\}$ is a semigroup, there exists a homomorphism g: $S \to S^S$, where $\{S^S, \bullet\}$ is a semigroup of functions from S to S under the operation of (left) composition.

Proof

For any element $a \in S$, let $g(a) = f_a$, where $f_a \in S^S$ is defined by

$$f_a(b) = a * b, \text{ for any } b \in S \quad (1)$$

Now $$g(a * b) = f_{a*b} \quad (2)$$

where $$f_{a*b}(c) = (a * b) * c = a * (b * c),$$

by the associativity of the semigroup $\{S, *\}$

$$= f_a\{(f_b(c)\}, \text{ by } (1)$$
$$= (f_a \bullet f_b)(c)$$
$$= \{g(a) \bullet g(b)\}(c)$$

i.e., $$f_{a*b} = g(a) \bullet g(b) \quad (3)$$

From (2) and (3), we get

$$g(a * b) = g(a) \bullet g(b)$$

i.e., g: $S \to S^S$ is a homomorphism.

SUBSEMIGROUPS AND SUBMONOIDS

Definition

If $\{S, *\}$ is a semigroup and $T \subseteq S$ is closed under the operation $*$, then $\{T, *\}$ is called a *subsemigroup* of $\{S, *\}$.

For example, if the set E of all even non negative integers, then $\{E, +\}$ is a subsemigroup of the semigroup $\{N, +\}$, where N is the set of natural numbers.

If $\{M, *, e\}$ is a monoid, $T \subseteq M$ is closed under the operation $*$ and $e \in T$, then $\{T, *, e\}$ is called a *submonoid* of $\{M, *, e\}$.

For example, if E is the set of all non-negative even integers, then $\{E, +, 0\}$ is a submonoid of $\{N, +, 0\}$, where N is the set of natural numbers.

Property

The set of idempotent elements of a commutative monoid $\{M, *, e\}$ forms a submonoid of M.

Proof

Let S be the set of idempotent elements of M. Since $e * e = e$, e is an idempotent element of M and hence $e \in S$.

Let $a, b \in S$. Then $a * a = a$ and $b * b = b$.

Now $$(a * b) * (a * b) = a * (b * a) * b$$
$$= a * (a * b) * b, \text{ since, } M \text{ is commutative}$$
$$= (a * a) * (b * b)$$
$$= a * b$$

Hence, $a * b$ is also an idempotent element.

$\therefore$ $a * b \in S$ and $\{S, *\}$ is a submonoid.

GROUPS

Definition

If G is a non empty set and $*$ is a binary operation of G, then the algebraic system $\{G, *\}$ is called a *group* if the following conditions are satisfied:

1. For all $a, b, c \in G$,
   $$(a * b) * c = a * (b * c) \text{ (Associativity)}$$
2. There exists an element $e \in G$ such that, for any $a \in G$,
   $$a * e = e * a = a \text{ (Existence of identity)}$$
3. For every $a \in G$, there exists an element $a^{-1} \in G$ such that
   $$a * a^{-1} = a^{-1} * a = e \text{ (Existence of inverse)}$$

Note The algebraic system $\{S, *\}$ is a semigroup, if $*$ is associative. If there exists an identity element $e \in S$, then $\{S, *\}$ is a monoid. Further if there exists an inverse for each element of S, then $\{S, *\}$ is a group.

For example, $\{Z, +\}$ is a group under the usual addition.

Definitions

When G is finite, the numbers of elements of G is called *the order* of G and denoted by $O(G)$ or $|G|$. If the element $a \in G$, where G is a group with identity element e, then the least positive integer m for which $a^m = e$ is called the *order of the element a* and denoted as $O(a)$. If no such integer exists, then a is of infinity order. A group $\{G, *\}$, in which the binary operation $*$ is commutative, is called a *commutative group* or *abelian group*.

For example, the set of rational numbers excluding zero is an abelian group under the usual multiplication.

Properties of a Group

1. The identity element of a group $(G, *)$ is unique.
2. The inverse of each element of $(G, *)$ is unique.
3. The cancellation laws are true in a group
   viz., $a * b = a * c \Rightarrow b = c$
   and $b * a = c * a \Rightarrow b = c$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$, for any $a, b \in G$.
5. If $a, b \in G$, the equation $a * x = b$ has the unique solution $x = a^{-1} * b$. Similarly the equation $y * b$ has the unique solution $y = b * a^{-1}$.
6. $(G, *)$ cannot have an idempotent element except the identity element.

Proof

1. If possible, let there be two identity elements in the group $\{G, *\}$, say e_1 and e_2. Since, e_2 is an identity and $e_1 \in G$, we have
   $$e_2 * e_1 = e_1 * e_2 = e_1 \quad (1)$$
   Since e_1 is an identity and $e_2 \in G$, we have
   $$e_1 * e_2 = e_2 * e_1 = e_2 \quad (2)$$

From (1) and (2), we have

$$e_1 = e_1 * e_2$$
$$= e_2$$

Hence, the identity element of a group is unique.

2. If possible, let b and c be two inverses of the element $a \in G$.
Then, by axiom (3) in the definition of a group,

$$a * b = b * a = e, \text{ where } e \text{ is the identity of } G \quad (1)$$

Similarly $a * c = c * a = e$ (2)

Now
$$b = e * b$$
$$= (c * a) * b, \text{ by (2)}$$
$$= c * (a * b), \text{ by axiom (1)}$$
$$= c * e, \text{ by (1)}$$
$$= c$$

Hence, the inverse of an element of $(G, *)$ is unique.

3. (i) Given $a * b = a * c$

$\therefore$ $a^{-1} * (a * b) = a^{-1} * (a * c)$, where a^{-1} is the inverse of a

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

i.e., $e * b = e * c$, where e is the identity

i.e., $b = c$

$\therefore$ $a * b = a * c \Rightarrow b = c$

i.e., the left cancellation is valid in a group.

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

$\therefore$ $(b * a) * a^{-1} = (c * a) * a^{-1}$

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

i.e., $b * e = c * e$

i.e., $b = c$

$\therefore$ $b * a = c * a \Rightarrow b = c$

i.e., the right cancellation is valid in a group.

4.
$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1}$$
$$= a * e * a^{-1}$$
$$= a * a^{-1} = e$$

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

Thus the inverse of $(a * b)$ is $b^{-1} * a^{-1}$

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

5. Let $c = a^{-1} * b$.

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

$a * c = b$ means $x = c$ is a solution of the equation $a * x = b$.

If possible, let $x = d$ be another solution of the equation $a * x = b$.

Then $a * c = a * d = b$

By left cancellation, we get $c = d$.
i.e., $x = a^{-1} * b$ is the unique solution of the equation $a * x = b$.
Similarly we can prove that $y = b * a^{-1}$ is the unique solution of the equation $y * a = b$.

6. If possible, let a be an idempotent element of $(G, *)$ other than e.
Then $a * a = a$ (1)
Now $e = a * a^{-1}$
$= (a * a) * a^{-1}$, by (1)
$= a * (a * a^{-1})$
$= a * e$
$= a$
Hence the only idempotent element of G is its identity element.

PERMUTATION

Definition

A bijective mapping of a non-empty set $S \to S$ is called a *permutation* of S. For example, if $S = \{a, b\}$, the two possible permutations of $\{a, b\}$ are $\{a, b\}$ and $\{b, a\}$. In this section, we will represent the two permutations as

$$p_1 = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \quad \text{and} \quad p_2 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

where the first row of p contains the elements of S in the given order and the second row gives their images.

Now the set $S_2 = \{p_1, p_2\}$ is the set of all possible permutations of the elements of S.

Let $*$ denote a binary operation on S_2 representing the *right composition of permutations*, viz., when $i, j, = 1, 2$, $p_i * p_j$ means the permutation obtained by permuting the elements of S by the application of p_i, followed by the application of p_j.

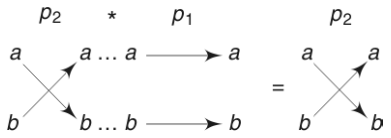
In other words, if p_i and p_j are treated as functions and $\bullet$ denotes the usual left composition of functions, then $p_i * p_j = p_j \bullet p_i$, for $i, j = 1, 2$.
For example,

$$p_2 * p_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} a & b \\ a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ b & a \end{pmatrix} * \begin{pmatrix} b & a \\ b & a \end{pmatrix}$$

$$= \begin{pmatrix} a & b \\ b & a \end{pmatrix} = p_2$$

Pictorially, $p_2 * p_1$ is found as follows:



PERMUTATION GROUP

Definition

The set G of all permutations on a non-empty set S under the binary operation $*$ of right composition of permutations is a group $\{G, *\}$ called *the permutation group*.

If $S = \{1, 2, \ldots, n\}$, the permutation group is also called *the symmetric group* of degree n and denoted by S_n. The number of elements of S_n or $|S_n| = n!$, since there are $n!$ permutations of n elements.

Now let us verify that $\{S_3, *\}$, where $S = \{1, 2, 3\}$ is a group under the operation of right composition of permutations.

There will be $3! = 6$ permutations of the elements 1, 2, 3 of S.

i.e., $S_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, where

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix};$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

The Cayley's composition table of permutations on S_3 is given below in Table 4.2.

Table 4.2

*	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_4	p_3	p_6	p_5
p_3	p_3	p_6	p_5	p_2	p_1	p_4
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_1	p_6	p_3	p_2
p_6	p_6	p_3	p_2	p_5	p_4	p_1

Note To obtain $p_i * p_j$, it will be convenient if we rewrite the first row of p_j so as to coincide with the second row of p_i

Using Table 4.2, all the three axioms of a group are easily verified.

For example, $(p_2 * p_4) * p_6 = p_3 * p_6 = p_4$

Also $p_2 * (p_4 * p_6) = p_2 * p_3 = p_4$

Thus associativity is satisfied.

Now $p_1 * p_i = p_i * p_1 = p_i$, for $i = 1, 2, \ldots, 6$.

Thus the existence of the identity element (in this example, $e = p_1$) is verified.

Also $p_1^{-1} = p_1$, $p_2^{-1} = p_1$, $p_3^{-1} = p_5$, $p_4^{-1} = p_4$, $p_5^{-1} = p_3$, and $p_6^{-1} = p_6$.

Thus the existence of inverse of each element is verified.

Hence $\{S_3, *\}$ is a group.

However this symmetric group is not abelian, since, for example, $p_2 * p_3 = p_4$, whereas $p_3 * p_2 = p_6$.

DIHEDRAL GROUP

Definition

The set of transformations due to all rigid motions of a regular polygon of n sides resulting in identical polygons but with different vertex names under the binary operation of right composition $*$ is a group called *dihedral group*, denoted by $\{D_n, *\}$.

By rigid motion, we mean the rotation of the regular polygon about its centre through angles $1 \times \frac{360}{n}$, $2 \times \frac{360}{n}$, …, $n \times \frac{360}{n}$ in the anticlockwise direction and reflection of the regular polygon about its lines of symmetry.

For example, let us consider a three sided regular polygon, viz., an equilateral triangle whose vertices are 1, 2, 3.

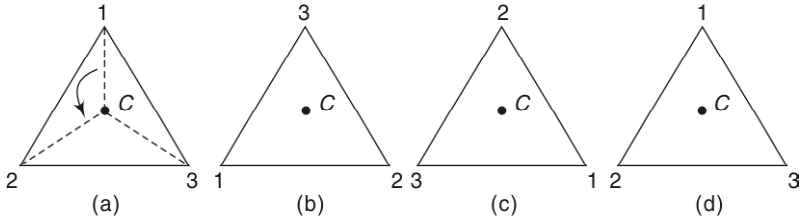


Fig. 4.1

When we rotate the triangle [Fig. 4.1(a)] through $1 \times \frac{360}{3} = 120°$ in the anticlockwise direction about the centre C (i.e., about an axis perpendicular to its plane through C), we get the triangle in Fig. 4.1(b). We note that the vertices originally labeled as 1, 2, 3 have now become 3, 1, 2 respectively. We will denote this transformation, which is the result of rotation through 120° by

$$r_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Note The notation r_5 corresponds to p_5 of the previous example.

Similarly, when we rotate the triangle in Fig. 4.1(a) through $2 \times \frac{360}{3} = 240°$ and through $3 \times \frac{360}{3} = 360°$, we get the triangles in Fig. 4.1(c) and Fig. 4.1(d) respectively. The corresponding transformations are

$$r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{and} \quad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Now let us consider the reflections of the equilateral triangle about its lines of symmetry, namely $1A$, $2B$ and $3C$.

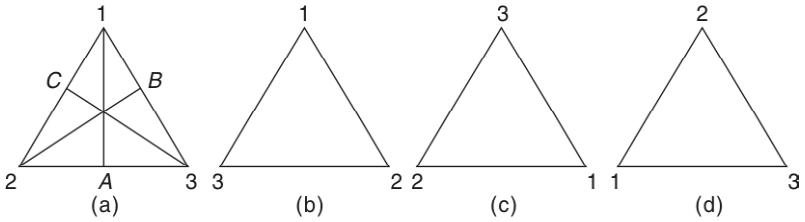


Fig. 4.2

When the triangle in Fig. 4.2(a) is reflected about the line $1A$, the vertex 1 remains in the original position and the other two vertices 2 and 3 interchange their positions and result in the triangle in Fig. 4.2(b). Similarly the reflections of the original triangle about the lines $2B$ and $3C$ result in the triangles in Fig. 4.2(c) and 4.2(d) respectively.

The corresponding transformations are given by

$$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad r_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \text{and} \quad r_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Now the set $\{r_1, r_2, r_3, r_4, r_5, r_6\}$ is the same as the permutation set $\{p_1, p_2, \ldots, p_6\}$ of the previous example.

Hence the set $\{r_1, r_2, \ldots r_6\}$ is a group under the right composition $*$ and called dihedral group $\{D_3, *\}$, which is of order 6 and degree 3 and which is the same as $\{S_3, *\}$.

Note In general, the dihedral group $\{D_n, *\}$ is of order $2n$ and is a permutation group of degree n. Also $\{D_n, *\}$ is a subgroup of $\{S_n, *\}$. For $n = 3$, the orders of both $\{S_3, *\}$ and $\{D_3, *\}$ are 6, but for $n = 4$, the order of S_4 is 4! whereas the order of D_4 is 8. (See worked example (4.13) in this section).

CYCLIC GROUP

Definition

A group $\{G, *\}$ is said to be *cyclic*, if there exists an element $a \in G$ such that every element x of G can be expressed as $x = a^n$ for some integer n.

In such a case, the cyclic group is said to be generated by a or a is a *generator* of G. G is also denoted by $\{a\}$.

For example, if $G = \{1, -1, i, -i\}$, then $\{G, \times\}$ is a cyclic group with the generator i, for $1 = i^4$, $-1 = i^2$, $i = i^1$ and $-i = i^3$.

For this cyclic group, $-i$ is also a generator.

Properties of a Cyclic Group

1. A cyclic group is abelian.

Proof

Let $\{G, *\}$ be a cyclic group with $a \in G$ as generator.

Let $b, c \in G$. Then $b = a^m$ and $c = a^n$, where m and n are integers.

Now $$b * c = a^m * a^n = a^{m+n}$$
$$= a^{n+m}$$
$$= a^n * a^m$$
$$= c * b$$

Hence $\{G, *\}$ is an abelian group.

2. If a is a generator of a cyclic group $\{G, *\}$, a^{-1} is also a generator of $\{G, *\}$.

Proof

Let $b \in G$. Then $b = a^m$, where m is an integer.

Now $b = (a^{-1})^{-m}$ where $-m$ is an integer.

$\therefore$ a^{-1} is also a genarator of $\{G, *\}$.

3. If $\{G, *\}$ is a finite cyclic group generated by an element $a \in G$ and is of order n, then $a^n = e$ so that $G = \{a, a^2, \ldots, a^n(= e)\}$. Also n is the least positive integer for which $a^n = e$.

Proof

If possible let there exist a positive integer $m < n$ such that $a^m = e$.

Since G is cyclic, any element of G can be expressed as a^k, for some $k \in Z$.

When k is divided by m, let q be the quotient and r be the remainder, where $0 \le r < m$.

Then $$k = mq + r$$

$\therefore$ $$a^k = a^{mq+r} = a^{mq} * a^r$$
$$= (a^m)^q * a^r$$
$$= e^q * a^r$$
$$= e * a^r$$
$$= a^r$$

This means that every element of G can be expressed as a^r, where $0 \le r < m$.

This implies that G has at most m elements or order of $G = m < n$, which is a contradiction.

i.e., $a^m = e$, for $m < n$ is not possible.

Hence $a^n = e$, where n is the least positive integer. Now let us prove that the elements $a, a^2, a^3, \ldots, a^n (= e)$ are distinct.

If it is not true, let $a^i = a^j$, for $i < j \le n$

Then $$a^{-i} * a^i = a^{-i} * a^j$$

i.e., $e = a^{j-i}$, where $j - i < n$,

which again is a contradiction.

Hence $a^i \ne a^j$, for $i < j \le n$.

4. If $\{G, *\}$ is a finite cyclic group of order n with a as a generator, then a^m is also a generator of $\{G, *\}$, if and only if the greatest common divisor of m and n is 1, where $m < n$.

Proof

Let us assume that a^m is a generator of $\{G, *\}$.

Then, for some integer r,

$$a = (a^m)^r = a^{mr}$$

i.e., $a = a^{mr} * e = a^{mr} * e^s$, where s is an integer

$= a^{mr} \cdot (a^n)^s$, since, $a^n = e$, by property (3)

$= a^{mr + ns}$

$\therefore \quad mr + ns = 1$

$\therefore \quad$ GCD $(m, n) = 1$

To prove the converse, let us assume that GCD $(m, n) = 1$

$\therefore$ There exists two integers p and q such that

$$mp + nq = 1 \qquad (1)$$

Let H be the set generated by a^m.

Since, each integral power of a^m will also be an integral power of a,

$$H \subseteq G \qquad (2)$$

Now $a^{mp + nq} = a$, by (1)

i.e., $a^{mp} * a^{nq} = a$

i.e., $(a^m)^p * (a^n)^q = a$

i.e., $(a^m)^p * e = a$, since $a^n = e$

i.e., $(a^m)^p = a$

This means that each integral power of a will also be an integral power a^m

i.e., $G \subseteq H \qquad (3)$

From (2) and (3), we have $H = G$

i.e., a^m is a generator of G.

WORKED EXAMPLES 4(A)

Example 4.1 If $*$ is the binary operation on the set R of real numbers defined by $a * b = a + b + 2ab$,

(a) Find if $\{R, *\}$ is a semigroup. Is it commutative?

(b) Find the identity element, if exists.

(c) Which elements have inverses and what are they?

(a) $(a * b) * c = (a + b + 2ab) + c + 2(a + b + 2ab)c$

$= a + b + c + 2(ab + bc + ca) + 4abc$

$a * (b * c) = a + (b + c + 2bc) + 2a(b + c + 2bc)$

$= a + b + c + 2(ab + bc + ca) + 4abc$

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

i.e., $*$ is associative.

Hence, $(R, *)$ is a semigroup.

Also $b * a = b + a + 2ba$

$= a + b + 2ab = a * b$

Hence, $(R, *)$ is commutative.

(b) If the identity element exists, let it be e.
Then for any $a \in R$,
$a * e = a$
i.e., $a + e + 2ae = a$
i.e., $e(1 + 2a) = 0$
$\therefore$ $e = 0$, since $1 + 2a \neq 0$, for any $a \in R$.

(c) Let a^{-1} be the inverse of an element $a \in R$. Then $a * a^{-1} = e$
i.e., $a + a^{-1} + 2a \cdot a^{-1} = 0$
i.e., $a^{-1} \cdot (1 + 2a) = -a$
$\therefore$ $a^{-1} = -\frac{a}{1+2a}$
$\therefore$ If $a \neq -\frac{1}{2}$, a^{-1} exists and $= -\frac{a}{1+2a}$.

Example 4.2 If $*$ is the operation defined on $S = Q \times Q$, the set of ordered pairs of rational numbers and given by $(a, b) * (x, y) = (ax, ay + b)$,

(a) Find if $(S, *)$ is a semigroup. Is it commutative?
(b) Find the identity element of S.
(c) Which elements, if any, have inverses and what are they?

(a) $\{(a, b) * (x, y)\} * (c, d)$
$= (ax, ay + b) * (c, d)$
$= (acx, adx + ay + b)$
Now, $(a, b) * \{(x, y) * (c, d)\}$
$= (a, b) * (cx, dx + y)$
$= (acx, adx + ay + b)$
Hence, $*$ is associative on S.
$\therefore$ $\{S, *\}$ is a semigroup.
Now $(x, y) * (a, b) = (ax, bx + y) \neq (a, b) * (x, y)$
$\therefore$ $\{S, *\}$ is not commutative.

(b) Let (e_1, e_2) be the identity element of $(S, *)$. Then for any $(a, b) \in S$,
$(a, b) * (e_1, e_2) = (a, b)$
i.e., $(ae_1, ae_2 + b) = (a, b)$
$\therefore$ $ae_1 = a$ and $ae_2 + b = b$
i.e. $e_1 = 1$ and $e_2 = 0$, since, $a \neq 0$
$\therefore$ The identity element is (1, 0).

(c) Let the inverse of (a, b) be (c, d), if it exists.
Then $(a, b) * (c, d) = (1, 0)$
i.e., $(ac, ad + b) = (1, 0)$
$\therefore$ $ac = 1$ and $ad + b = 0$
i.e., $c = \frac{1}{a}$ and $d = -\frac{b}{a}$, if $a \neq 0$.
Thus the element (a, b) has an inverse if $a \neq 0$ and its inverse is $\left(\frac{1}{a}, -\frac{b}{a}\right)$.

Example 4.3 If Z_6 is the set of equivalence classes generated by the equivalence relation "congruence modulo 6", prove that $\{Z_6, \times_6\}$ is a monoid where the operation $\times_6$ and Z_6 is defined as

$$[i] \times_6 [j] = [(i \times j)(\text{mod } 6)], \text{ for any } [i], [j] \in Z_6$$

Which elements of the monoid are invertible?

[For the definition of Z_6, the congruence classes modulo 6, refer to example 13(ii) in worked example set 4(b) of Chapter 4.]

The composition table $\{Z_6, \times_6\}$ is given below in Table 4.3. For convenience of notation we have written $[i]$ as simply i in the body of the Table 4.3.

Table 4.3

$\times_6$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	0	0	0	0	0	0
[1]	0	1	2	3	4	5
[2]	0	2	4	0	2	4
[3]	0	3	0	3	0	3
[4]	0	4	2	0	4	2
[5]	0	5	4	3	2	1

The operation $\times_6$ is associative.

For example, $\{[2] \times_6 [4]\} \times_6 [5] = [2] \times_6 [5] = [4]$

Also $[2] \times_6 \{[4] \times_6 [5]\} = [2] \times_6 [2] = [4]$

From the second row and the second column of Table 4.3, we see that [1] is the identity element of $\{Z_6, \times_6\}$

Hence $\{Z_6, \times_6\}$ is a monoid.

From the Table 4.3, we see that

$$[1] \times [1] = [1] \text{ and } [5] \times [5] = [1]$$

$\therefore$ The elements [1] and [5] alone are invertible and their inverses are [1] and [5] respectively.

Example 4.4 If $S = N \times N$, the set of ordered pairs of positive integers with the operation $*$ defined by

$$(a, b) * (c, d) = (ad + bc, bd)$$

and if $f : (S, *) \to (Q, +)$ is defined by $f(a, b) = \frac{a}{b}$, show that f is a semigroup homomorphism.

$$\begin{aligned} \{(a, b) * (c, d)\} * (e, f) &= (ad + bc, bd) * (e, f) \\ &= \{(ad + bc)f + bde, bdf\} \\ &= (adf + bcf + bde, bdf) \end{aligned}$$

Also
$$\begin{aligned} (a, b) * \{(c, d) * (e, f)\} &= (a, b) * (cf + de, df) \\ &= \{adf + b(cf + de), bdf\} \\ &= (adf + bcf + bde, bdf) \end{aligned}$$

i.e., $(S, *)$ is associative and hence a semigroup.

Now $f\{(a, b) * (c, d)\} = f(ad + bc, bd)$

$$= \frac{ad + bc}{bd} \quad \left[\because \ f(a, b) = \frac{a}{b}\right]$$

$$= \frac{a}{b} + \frac{c}{d}$$

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

$\therefore$ $f : (S, *) \to (Q, +)$ is a semigroup homomorphism.

Example 4.5 If $f : X \to X$, where $X = \{1, 2, 3, 4\}$ is defined by $f = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$, prove that $\{F, \bullet\}$, where $F = \{f^0, f^1, f^2, f^3\}$ is a monoid under the operation ($\bullet$) of function composition, if $f^0 = \{(1, 1), (2, 2), (3, 3), (4, 4)$ and $f^1 \bullet f^1 = f \bullet f = f^2$; $f^2 \bullet f = f^3$, $f^3 \bullet f = f^4 = f^0$.

Show also that the mapping g: $(F, \bullet) \to (Z_4, +_4)$ given by $g(f^i) = [i]$, for $i = 0, 1, 2, 3$ is a monoid homomorphism. Is it an isomorphism?

The Cayley Table 4.3 for $\{F, \bullet\}$ is given in Table 4.4.

Table 4.4

$\bullet$	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2

The operation, $\bullet$ is commutative, since, for example,

$$f^2 \bullet f^3 = f^1 = f^3 \bullet f^2$$

Also for example

$$(f^1 \bullet f^2) \bullet f^3 = f^3 \bullet f^3 = f^2$$

and $f^1 \bullet (f^2 \bullet f^3) = f^1 \bullet f^1 = f^2$

i.e., $(f^1 \bullet f^2) \bullet f^3 = f^1 \bullet (f^2 \bullet f^3)$

Thus, $\bullet$ is associative.

Also it is easily seen that f^0 is the identity element of F with respect to $\bullet$.

Hence, $\{F, \bullet\}$ is a commutative monoid. If we define the operation $+_4$ on Z_4 as

$$[i] +_4 [j] = [(i + j) \pmod 4],$$

for any $[i], [j] \in Z_4$,

Table 4.5

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The Cayley table for $\{Z_4, +_4\}$ will be as given in Table 4.5.

It is easily verified that $+_4$ is both commutative and associative. Also [0] is the identity element of Z_4 with respect to $+_4$.

Hence $\{Z_4, +_4\}$ is a commutative monoid.

Note $\{Z_4, +_4\}$ is in fact a commutative group, as the inverse of every element of Z_4 exists.

From Table 4.4 and 4.5, it is easily verified that $g(f^i \bullet f^j) = g(f^i) +_4 g(f^j)$ For example,

$$g(f^2 \bullet f^3) = g(f^1)$$
$$= [1]$$
$$= [2] +_4 [3]$$
$$= g(f^2) +_4 g(f^3)$$

Thus g: $(F, \bullet) \to (Z_4, +_4)$ is a monoid homomorphism. Since $g(f^i) = [i]$ for $i = 0, 1, 2, 3$, g is one-to-one. Also for every element in Z_4, there is a preimage in F. Hence g is onto.

$\therefore$ g is an isomorphism.

Example 4.6 If $S = \{0, 1, 2, 3\}$ is a subset of the semigroup $\{Z_4, +_4\}$, $T = \{1, 3, 7, 9\}$ is a subset of the semigroup $\{Z_{10}, \times_{10}\}$ with the Cayley Tables 4.6(a) and 4.6(b) and if a function g: $S \to T$ is defined by $g(0) = 1$, $g(1) = 3$, $g(2) = 9$ and $g(3) = 7$, show that g is an isomorphism.

Table 4.6(a)

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

Table 4.6(b)

$\times_{10}$	[1]	[3]	[7]	[9]
[1]	1	3	7	9
[3]	3	9	1	7
[7]	7	1	9	3
[9]	9	7	3	1

The Cayley table for $\{g(S), \times_{10}\}$ is obtained from Table 4.6(a) by replacing the elements in S by their images by g and the operation $+_4$ $\times_{10}$. It is given in Table 4.6(c).

Table 4.6(c)

X_{10}	[1]	[3]	[9]	[7]
[1]	1	3	9	7
[3]	3	9	7	1
[9]	9	7	1	3
[7]	7	1	3	9

Interchanging the last two rows in Table 4.6(c) and the interchanging the last two columns, we get exactly the same table as Table 4.6(b), which is the Cayley table for $\{T, \times_{10}\}$.

Hence, the mapping g: $S \to T$ is a homomorphism. Also g is one-to-one onto.

Hence g is an isomorphism.

Note We have used an alternative method for proving that g: $S \to T$ is a homomorphism. This method is equivalent to the proof by the definition of homomorphism, as for example,

$$g(2 +_4 3) = g(1) = 3$$

and $$g(2) \times_{10} g(3) = 9 \times_{10} 7 = 3$$

i.e., $$g(2 +_4 3) = g(2) \times_{10} g(3)$$

When the composition tables of S and T are given, this method may be preferred.

Example 4.7 If $\{S, *\}$ is a monoid, where $S = \{a, b, c\}$ is given by the composition Table 4.7(a) and if a mapping g: $S \to S^S$ is defined by $g(a) = f_a$, $g(b) = f_b$ and $g(c) = f_c$, where $f_a, f_b, f_c \in S^S$ and $f_x(y) = x * y$; $x, y \in S$, show that $\{S^S, \bullet\}$ is a monoid under function composition and g is a monoid isomorphism.

Since $f_x(y) = x * y$, we get $f_a(a) = a * a = a$, $f_a(b) = a * b = b$, $f_a(c) = a * c = c$ etc.

Table 4.7(a)

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

Table 4.7(b)

$\bullet$	f_a	f_b	f_c
f_a	f_a	f_b	f_c
f_b	f_b	f_c	f_a
f_c	f_c	f_a	f_b

The composition table for $\{S^S, \bullet\}$ is given in Table 4.7(b). The entries of this table are obtained as follows:

$$f_a \bullet f_a = f_a(f_a) = f(a)$$
$$f_a \bullet f_b = f_a(f_b) = f(b)$$
$$f_a \bullet f_c = f_a(f_c) = f(c) \text{ etc.}$$

From Table 4.7(b), it is easily seen that $\bullet$ satisfies associativity and f_a is the identity element of S^S.

Hence $\{S^S, \bullet\}$ is a monoid.

The composition Table 4.7(b) can be obtained from Table 4.7(a) by replacing a, b, c respectively by $g(a) = f_a$, $g(b) = f_b$ and $g(c) = f_c$.

Hence $g : S \to S^S$ is a monoid homomorphism. Obviously g is one-to-one onto. Hence, g is a monoid isomorphism.

Example 4.8 Show that the set Q^+ of all positive rational numbers forms an abelian group under the operation $*$ defined by $a * b = \frac{1}{2}ab$; $a, b \in Q^+$.

When $a, b \in Q^+$, $\quad \frac{ab}{2} \in Q^+$

$\therefore$ $\quad Q^+$ is closed under the operation $*$

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

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{1}{2}a \cdot \frac{bc}{2} = \frac{abc}{4}$$

$\therefore$ $\quad (a * b) * c = a * (b * c)$

Hence $*$ is associative.

Let e be the identity element of Q^+ under $*$

$\therefore$ $\quad a * e = e * a = a$, for $a \in Q^+$

i.e., $\quad \frac{1}{2}ae = a$ $\quad$ i.e., $\quad a(e - 2) = 0$

Since $a > 0$, we get $\quad e = 2 \in Q^+$

Hence identity element exists.

Let b be the inverse of the element $a \in G$

Then $\quad a * b = b * a = e = 2$

i.e., $\quad \frac{1}{2}ab = 2$

$\therefore$ $\quad b = \frac{4}{a} \in Q^+$

Thus, every element of Q^+ is invertible

$\therefore$ $(Q^+, *)$ is a group.

Also $b * a = a * b \ \frac{1}{2}ab$

$\therefore$ $(Q^+, *)$ is an abelian group.

Example 4.9 Show that the set $\{Z_m\}$ of equivalence classes modulo m is an abelian group under the operation $+_m$ of addition modulo m.

$$Z_m = \{[0], [1], [2], \ldots, [m-1]\}.$$

If $a, b, \in Z$, such that $a + b = q_1 m + r_1$, (1)

$0 \le r_1 < m$, then

$$[a] +_m [b] = [r_1] \in Z_m \quad (1)'$$

$\therefore$ Z_m is closed under $+_m$.

If $c \in Z$, let $b + c = q_2 m + r_2$ (2)

and $r_1 + c = q_3 m + r_3$ (3)

Then $[b] + [c] = [r_2]$ (2)′

and $[r_1] + [c] = [r_3]$ (3)′

Now $a + r_2 = a + b + c - q_2 m$, by (2)

$= q_1 m + r_1 + c - q_2 m$, by (1)

$= q_1 m + q_3 m + r_3 - q_2 m$, by (3)

$= (q_1 + q_3 - q_2)\, m + r_3$ (4)

$\therefore$ $[a] +_m [r_2] = [r_3]$ (4)′

Now $\{[a] +_m [b]\} +_m [c] = [r_1] +_m [c]$, by (1)′

$= [r_3]$, by (3)′, (5)

Also $[a] +_m \{[b] +_m [c]\} = [a] +_m [r_2]$, by (2)′

$= [r_3]$, by (4)′, (6)

From (5) and (6), we see that $+_m$ is associative.

For every $[a] \in Z_m$,

$$[a] +_m [0] = [0] +_m [a] = [a]$$

$\therefore$ [0] is the identity element of Z_m with respect to $+_m$.

Now $[0] +_m [0] = [0]$. $\therefore$ $[0]^{-1} = [0]$

If $[a] \ne [0] \in Z_m$, then $[m - a] \in Z_m$ such that

$$[a] +_m [m - a] = [m] = [0], \quad \text{since} \quad m = 1 \cdot m + 0.$$

Also $[m - a] +_m [a] = [0]$

$\therefore$ $[a]^{-1} = [m - a]$. i.e., Inverse of $[a]$ exists.

Now $[a] +_m [b] = [b] +_m [a] = [r_1]$, by (1)

$\therefore$ Z_m is commutative with respect to the operation $+_m$.

Thus, $\{Z_m, +_m\}$ is an abelian group.

Example 4.10 If M_2 is the set of 2×2 non-singular matrices over R, viz.,

$$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in R \text{ and } ad - bc \ne 0 \right\},$$

prove that M_2 is a group under the operation of usual matrix multiplication. Is it abelian?

If $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$, then

$$AB = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$$

Also $|AB| = |A| \cdot |B|$

$\therefore$ If A and B are non-singular, AB is also non-singular.
Also if $A, B \in M_2$, then $AB \in M_2$
$\therefore$ Matrix multiplication is closed.

Now if $I = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, then $AI = IA = A$.

Hence I is the identity element of M_2 with respect to matrix multiplication.

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $A^{-1} = \begin{bmatrix} \frac{1}{|A|}d & -\frac{1}{|A|}b \\ -\frac{1}{|A|}c & \frac{1}{|A|}a \end{bmatrix}$, $A^{-1} \in M_2$.

$\therefore$ Inverse of every $A \in M_2$ exists.
Hence, $\{M_2, \times\}$ is a group.
Since, $AB \neq BA$ in general, $\{M_2, \times\}$ is not abelian.

Example 4.11 If $\{G, *\}$ is an abelian group, show that $(a * b)^n = a^n * b^n$, for all $a, b \in G$, where n is a positive integer.

Since, $\{G, *\}$ is an abelian group,

$$a * b = b * a \tag{1}$$

For $a, b \in G$, we have $(a * b)^1 = (b * a)^1$, by (1)

and
$$\begin{aligned} (a * b)^2 &= (a * b) * (a * b) \\ &= a * (b * a) * b, \text{ by associativity} \\ &= a * (a * b) * b, \text{ by (1)} \\ &= (a * a) * (b * b), \text{ by associativity} \\ &= a^2 * b^2 \end{aligned}$$

Thus, the required result is true for $n = 1, 2$. Let us assume that the result is valid for $n = m$.

i.e., $$(a * b)^m = a^m * b^m \tag{2}$$

Now
$$\begin{aligned} (a * b)^{m+1} &= (a * b)^m * (a * b) \\ &= (a^m * b^m) * (a * b), \text{ by (2)} \\ &= a^m * (b^m * a) * b, \text{ by associativity} \\ &= a^m * (a * b^m) * b, \text{ since } G \text{ is abelian} \end{aligned}$$

$= (a^m * a) * (b^m * b)$, by associativity
$= a^{m+1} * b^{m+1}$

Hence, by induction, the result is true for positive integral values of n.

Example 4.12 If the permutations of the elements of {1, 2, 3, 4, 5} are given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}$, $\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$, find $\alpha\beta$, $\beta\alpha$, α^2, $\gamma\beta$, δ^{-1} and $\alpha\beta\gamma$. Also solve the equation $\alpha x = \beta$.

$$\alpha: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 & 5 \end{matrix} \qquad \beta: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 5 & 4 \end{matrix}$$

$$\beta: \begin{matrix} 2 & 3 & 1 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} \qquad \alpha: \begin{matrix} 1 & 2 & 3 & 5 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix}$$

$\therefore \quad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$; $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

$$\alpha: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 4 & 5 \end{matrix} \qquad \gamma: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 4 & 3 & 1 & 2 \end{matrix}$$

$$\alpha: \begin{matrix} 2 & 3 & 1 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 & 5 \end{matrix} \qquad \beta: \begin{matrix} 5 & 4 & 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 5 & 3 & 1 & 2 \end{matrix}$$

$\therefore \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$; $\gamma\delta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$

δ^{-1} is obtained by interchanging the two rows of δ and then rearranging the elements of the first row so as to assume the natural order.

Thus $\quad \delta^{-1} = \begin{pmatrix} 3 & 2 & 1 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$

Note While rearranging the elements of the first row, the correspondence between the corresponding elements of the two rows is maintained).

$$\alpha\beta: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{matrix} \qquad \gamma: \begin{matrix} 2 & 3 & 1 & 5 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 5 & 2 & 1 \end{matrix}$$

$\therefore \quad \alpha\beta\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix}$

Solving the equation $\alpha x = \beta$ means finding the value of x that satisfies the equation. Premultiplying by α^{-1}, the given equation becomes $\alpha^{-1}\,\alpha\, x = \alpha^{-1}\,\beta$

i.e., $\quad ex = \alpha^{-1}\,\beta$, where e is the identity permutation.

$\therefore \quad x = \alpha^{-1}\beta$

Now $$\alpha^{-1} = \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

$$\alpha^{-1}: \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 & 5 \end{matrix} \qquad \beta: \begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 5 & 4 \end{matrix}$$

$$\therefore \quad x = \alpha^{-1}\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

Example 4.13 Define the dihedral group $(D_4, *)$ and give its composition table.

The set of transformations due to all rigid motions of a square resulting in identical squares but with different vertex names under the binary operation of right composition $*$ is a group, called dihedral group of order 8 and denoted by $\{D_4, *\}$.

By rigid motion, we mean the rotation of the square about its centre through angles 90°, 180°, 270°, 360° in the anticlockwise direction and reflection of the square about 4 lines of symmetry is as given in Fig. 4.3.

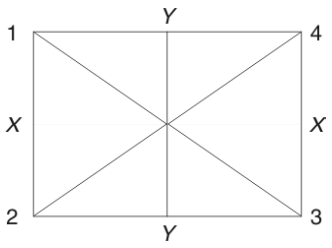


Fig. 4.3

$$r_1 = r(90°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}; \qquad r_2 = r(180°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$r_3 = r(270°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}; \qquad r_4 = r(360°) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$r_5 = r(XX) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \qquad r_6 = r(YY) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$r_7 = r(13) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}; \qquad r_8 = r(2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

The composition table is given in Table 4.8. For example, the composition $r_1 * r_2$ is obtained as usual as given below:

$$\begin{matrix} & 1 & 2 & 3 & 4 \\ r_1 & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 2 & 3 \\ r_1 & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 1 & 2 \end{matrix}$$

i.e., $$r_1 * r_1 = r_2$$

Table 4.8

*	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8
r_1	r_2	r_3	r_4	r_1	r_8	r_7	r_5	r_6
r_2	r_3	r_4	r_1	r_2	r_6	r_5	r_8	r_7
r_3	r_4	r_1	r_2	r_3	r_7	r_8	r_6	r_5
r_4	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8
r_5	r_7	r_6	r_8	r_5	r_4	r_2	r_1	r_3
r_6	r_8	r_5	r_7	r_6	r_2	r_4	r_3	r_1
r_7	r_6	r_8	r_5	r_7	r_3	r_1	r_4	r_2
r_8	r_5	r_7	r_6	r_8	r_1	r_3	r_2	r_4

From the Table 4.8, it is seen that

$$r_4 * r_i = r_i * r_4 = r_i;\ i = 1, 2, \ldots 8.$$

$\therefore$ r_4 is the identity element of $\{D_4, *\}$.

Also we see that the inverses of $r_1, r_2, \ldots, r_8$ are respectively $r_3, r_2, r_1, r_4, r_5, r_6, r_7$ and r_8.

Example 4.14 Show that, if $\{U_n\}$ is the set of n^{th} roots of unity, $\{U_n, \times\}$ is a cyclic group. Is it abelian?

$$1^{1/n} = (e^{i0 + 2r\pi i})^{1/n} = e^{2r\pi i/n};\ r = 0, 1, 2, \ldots (n - 1)$$

i.e., the n^{th} roots of 1 are

$$1, e^{2\pi i/n}, e^{4\pi i/n}, e^{6\pi i/n}, \ldots e^{2(n-1)\pi i/n}.$$

If we denote $e^{2\pi i/n}$ by ω, the n^{th} roots of 1 are $\{U_n\} = \{1, \omega, \omega^2, \omega^3, \ldots, \omega^{n-1}.\}$

Now $\{U_n\}$ is closed under multiplication. Obviously $1 \in U_n$ is the identity element,

as $1 \times \omega^r = \omega^r \times 1 = \omega^r$, for $r = 1, 2, \ldots (n - 1)$.

Also for every element $\omega^r \in U_n$, there exists an element $\omega^{n-r} \in U_n$, such that

$$\omega^r \times \omega^{n-r} = \omega^{n-r} \times \omega^r = \omega^n = e^{2\pi i} = 1$$

$\therefore$ ω^{n-r} is the inverse of ω^r $[(r = 0, 1, \ldots n - 1)]$

Hence $\{U_n, \times\}$ is a group

Also $\omega^r \times \omega^s = \omega^s \times \omega^r$, for $\omega^r, \omega^s \in U_n$

$\therefore$ $\{U_n, \times\}$ is an abelian group.

The generator of this group is obviously ω. Even 1 is generated by ω, as $\omega^n = 1$.

Hence $\{U_n, \times\}$ is a cyclic group of order n.

Example 4.15 Show that every group of order 3 is cyclic and every group of order 4 is abelian.

(i) Since G is of order 3, it must have two distinct elements a, b apart from the identity element e.

Since G is closed under the operation $*$,

$$a * b \in G$$

$\therefore$ $a * b = a$ or $a * b = b$ or $a * b = e$

If $a * b = a$, $a * b = a * e$

$\therefore$ $b = e$, by cancellation law

If $a * b = b$, $a * b = e * b$

$\therefore$ $a = e$, by cancellation law

But a and b are not equal to e.

$\therefore$ $a * b = e$ (1)

Again by closure law, $a^2 \in G$

$\therefore$ $a^2 = a$ or $a^2 = b$ or $a^2 = e$

If $a^2 = a$ or $a * a = a * e$, then $a = e$, which is not true

If $a^2 = e$, then $a^2 = a * b$, by (1)

$\therefore$ $a = b$, which is not true.

$\therefore$ $a^2 = b$ (2)

Also $a^3 = a * a^2 = a * b$, by (2)

$= e$, by (1)

Hence $G = \{a, a^2, a^3 (=e)\}$ is a cyclic group with generator a.

(ii) Let $G = \{e, a, b, c\}$, where e is the identity element.

By closure law, either $a^2 = b^2 = c^2 = e$ or at least one of (a^2, b^2 and c^2) $\neq e$.

Case 1 Let $a^2 = b^2 = c^2 = e$ (1)

Then in the composition table of (G) given in Table 4.9, the elements in the first row and first column are fixed by the property of e.

Table 4.9

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

By the assumption (1), the elements in the principle diagonal are also fixed as e.

Let us now consider the element $a * b$ in the second row and third column.

If $a * b = a$, then $a * b = a * e$ and so $b = e$, which is not true. Similarly $a * b \neq b$. Hence $a * b = c$. Similarly the element in the second row and fourth column is b. By similar reasoning, we find the other elements of Table 4.9.

From the table, it is obvious that $\{G, *\}$ is abelian.

Note The four-element group $\{G, *\}$ represented by Table 4.9 is called *Klein's four group*. This group is not cyclic, since no element can generate the other elements of G.

Case 2 At least one of a^2, b^2 and c^2 is not equal to e. Let $a^2 \neq e$. Also $a \neq e$.

Hence $a^2 = b$ or c, since the elements of G are to be distinct.

Let $a^2 = b$. Then $c \neq e$ or a or a^2.

$\therefore$ $c = a^3$, since, $a^3 = a^2 * a \in G$.

Similarly if $a^2 = c$, then $b = a^3$.

Thus, $G \equiv \{e, a, a^2, a^3\}$

Obviously, $\{G, *\}$ is abelian. Also it is cyclic with a as the generator.

EXERCISE 4(A)

Part A: (Short answer questions)

1. What is an algebraic system? Name some properties satisfied by algebraic systems.
2. Define identity, inverse and idempotent elements of an algebraic system.
3. Find the identity element of the algebraic system $\{S, *\}$, where S is the set of integers and $*$ is defined by $a * b = a + b + 2$, for all $a, b \in S$.
4. Find the inverse of the element $a \in S$ in the previous question.
5. What is homomorphism with respect to an algebraic system?
6. Define isomorphism with respect an algebraic system.
7. What is Cayley's composition table? Give an example for the same.
8. Define sub-algebraic system with an example.
9. Define direct product of two algebraic systems.
10. Define semigroup and monoid with an example for each.
11. If $\{S, *\}$ is a semigroup such that $a * c = c * a$ and $b * c = c * b$, where $a, b, c \in S$, prove that $(a * b) * c = c * (a * b)$.
12. If $\{(x, y), *\}$ is a semigroup such that $x * x = y$, show that (i) $x * y = y * x$ and (ii) $y * y = x$.
13. If $\{S, *\}$ is a commutative semigroup such that $x * x = x$ and $y * y = y$, show that $(x * y) * (x * y) = x * y$, where $x, y \in S$.
14. A binary operation $*$ is defined on Z by $a * b = a + b - ab$, where $a, b \in Z$. Show that $\{Z, *\}$ is a semigroup.
15. If $\{M, *\}$ is a monoid with identity e and b, b' are inverses of $a \in M$, show that $b = b'$. [*Hint:* $b * (a * b') = (b * a) * b'$]
16. Show that $\{Z^+, *\}$, where $*$ is defined by $a * b = a$, for all $a, b \in Z^+$, is a semigroup. Is it a monoid?
17. If $S = N \times N$ and the binary operation $*$ is defined by $(a, b) * (c, d) = (ac, bd)$, for all $a, b, c, d \in N$, show that $\{S, *\}$ is a semigroup. Is it a monoid?
18. Show that $\{Z^+, *\}$ where $*$ is defined by $a * b = \max(a, b)$ for all $a, b \in Z^+$, is a monoid. What is the identity element?
19. If $S = \{1, 2, 3, 6\}$ and $*$ is defined by $a * b = \text{lcm}(a, b)$, where $a, b \in S$, show that $\{S, *\}$ is a monoid. What is the identity element?
20. Define subsemigroup and submonoid with an example for each.
21. Define a group with an example.
22. State the basic properties of a group.
23. Define the order of a group and order of an element of a group.
24. Find the order of every element of the group $\{(1, -1, i, -i), \times\}$, for which the identity element is 1.
25. Find the order of every element of the multiplication group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$.
26. Show that the identity element of a group is the only element whose order is 1.

27. Prove that the inverse of the inverse of an element of a group is equal to the element itself.
28. Show that the set {1, 2, 3, 4} is not a group under addition modulo 5.
29. Show that the set {1, 2, 3} is not a group under multiplication modulo 4.
30. If a is an element of a group with identity e such that $a^2 = a$, prove that $a = e$.
31. If every element of a group $(G, *)$ is its own inverse, prove that G is abelian. [*Hint:* Use $(a * b) = (a * b)^{-1}$, where $a, b \in G$].
32. If a and b are any two elements of an abelian group, prove that $(ab)^2 = a^2b^2$.
33. If a and b are any two elements of a group G such that $(ab)^2 = a^2b^2$, show that G is abelian.
34. Define a permutation group.
35. Define a dihedral group.
36. How are $\{S_n, *\}$ and $\{D_n, *\}$ related? What are their orders?
37. Define a cyclic group with an example.
38. Show that the multiplication group $\{1, \omega, \omega^2\}$ where ω is a complex cube root of unity is a cyclic group. What are the generators?
39. Show that the group $\{G, +_5\}$ is a cyclic group where $G = \{0, 1, 2, 3, 4\}$. What are its generators?
40. How many generators are there for a cyclic groups of order 8? What are they? [*Hint:* Use property (4) of cyclic groups]

Part B

41. If N is the set positive integers and $*$ denotes the least common multiple on N, show that $\{N, *\}$ is a commutative semigroup. Find the identity element of $*$. Which elements in N have inverses and what are they?
42. If Q is the set of rational numbers and $*$ is the operation on Q defined by
$$a * b = a + b - ab,$$
show that $\{Q, *\}$ is a commutative semigroup. Find also the identity element of $*$. Find the inverse of any element of Q if it exists.
43. If Z_6 is the set of equivalence classes generated by the equivalence relation "congruence modulo 6", prove that $\{Z_6, +_6\}$ is a monoid, where the operation and $+_6$ on Z_6 is defined by $[i] +_6 [j] = [(i + j)(\text{mod } 6)]$, where $[i], [j] \in Z_6$. What are the inverses of the elements of Z_6?
44. If R is the set of real numbers and $*$ is the operation defined by $a * b = a + b + 3ab$, where $a, b \in R$, show that $\{R, *\}$ is a commutative monoid. Which elements have inverses and what are they?
45. Show that there exists a homomorphism from the algebraic system $\{N, +\}$ to the system $\{Z_4, +_4\}$, where N is the set of natural numbers and Z_4 is the set of integers modulo 4. Is it an isomorphism?
[*Hint:* Define $g: N \to Z_4$ by $g(i) = [i]$}
46. If $\{S, +\}$ and $\{T, \times\}$ are two algebraic systems, where S is the set of all real numbers and T is the set of non-zero real numbers, prove that the mapping $g: S \to T$ defined by $g(a) = 3^a$, for $a \in S$ is a homomorphism but not an isomorphism.

47. If $\{R^+, \times\}$ and $\{R, +\}$ are two semigroups in the usual notation, prove that the mapping $g(a)$: $R^+ \to R$ defined by $g(a) = \log_e a$ is a semigroup isomorphism.
48. If $\{Z, +\}$ and $\{E, +\}$, where Z is the set of all integers and E is the set of all even integers, show that the two semigroups $\{Z, +\}$ and $\{E, +\}$ are isomorphic. [*Hint:* $g(a) = 2a$, where $a \in Z$.]
49. If C is the semigroup of non-zero complex numbers under multiplication and R is the semigroup of non-zero real numbers under multiplication, show that g: $C \to R$, defined by $g(z) = |z|$ is a homomorphism.
50. If $S = N \times N$ is the set of ordered pairs of positive integers and $*$ is an operation on S defined by $(a, b) * (c, d) = (a + c, b + d)$, show that $\{S, *\}$ is a semigroup. If $f : (S, *) \to (Z, +)$ is defined by $f(a, b) = a - b$, show that f is a homomorphism.
51. If $S = N \times N$ is the set of ordered pairs of positive integers and $*$ is an operation on S defined by $(a, b) * (c, d) = (ac, bd)$, show that $\{S, *\}$ is a semigroup. If $f : (S,*) \to (Q, \times)$ is defined by $f(a, b) = a/b$, show that f is a homomorphism.
52. (i) Prove that the set $\{0, 1, 2, 3, 4\}$ is a finite abelian group of order 5 under addition modulo 5 as composition.
    (ii) Prove that the set $\{1, 3, 7, 9\}$ is an abelian group under multiplication modulo 10.
53. (i) If $*$ is defined on Q^+ such that $a * b = \frac{ab}{3}$, for $a, b \in Q^+$, show that $\{Q^+, *\}$ is an abelian group.
    (ii) If $*$ is defined on Z such that $a * b = a + b + 1$ for $a, b \in Z$, show that $\{Z, *\}$ is an abelian group.
    (iii) If $*$ is defined on R such that $a * b = a + b - ab$, for $a, b \in R$, show that $\{R, *\}$ is an abelian group.
54. Show that the set of all polynomials in x under the operation of addition is a group.
55. Show that the sets of 2×2 matrices in (i), (iii), (iv) form groups under matrix multiplication and the set in (ii) forms a group under matrix addition. Which of them are abelian groups?

    (i) $\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}\right\}$

    (ii) $\left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}; a, b, c, d \in R; ad - bc \neq 0\right\}$

    (iii) $\left\{\begin{bmatrix}a & b\\ -b & a\end{bmatrix}; a, b \in R; a^2 + b^2 \neq 0\right\}$

    (iv) $\left\{\begin{bmatrix}a & a\\ a & a\end{bmatrix}; a \neq 0 \text{ and} \in R\right\}$

56. If $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 4 & 6 & 2 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{pmatrix}$ are two elements of the symmetric group S_6, find $\alpha\beta$, $\beta\alpha$, α^2, β^2, α^{-1} and β^{-1}.
57. If α, β are elements of the symmetric group S_4, given by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

find $\alpha\beta$, $\beta\alpha$, α^2 and α^{-1}. Find also the orders of α, β and $\alpha\beta$.
58. In the symmetric group S_3, find all those elements a and b such that
(i) $(a * b)^2 \neq a^2 * b^2$; (ii) $a^2 = e$; $a^3 = e$.
59. Show that the group $\{(1, 2, 3, 4, 5, 6), \times_7\}$ is cyclic. How many generators are there for this group? What are they?
60. Show that the group $\{(1, 2, 4, 5, 7, 8), \times_9\}$ is cyclic. What are its generators?

SUBGROUPS

Definition

If $\{G, *\}$ is a group and $H \subseteq G$ is a non-empty subset, that satisfies the following conditions:

1. For $a, b \in H$, $a * b \in H$.
2. $e \in H$, where e is the identity of $\{G, *\}$.
3. For any $a \in H$, $a^{-1} \in H$, then $\{H, *\}$ is called a *subgroup* of $\{G, *\}$.

Note $\{H, *\}$ is itself a group with the same identity as that of $\{G, *\}$ and with the same binary operation $*$ defined on G.

Obviously $\{e, *\}$ and $\{G, *\}$ are *trivial subgroups* of $\{G, *\}$. All other subgroups are called *proper subgroups*.

For example, (1) the additive group of even integers is a subgroup of the additive group of all integers, and (2) the multiplicative group $(1, -1)$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

Theorem

The necessary and sufficient condition for a non empty subset H of a group $\{G, *\}$ to be a subgroup is $a, b \in H \Rightarrow a * b^{-1} \in H$.

Proof

(i) Let H be a subgroup.
Then if $a, b \in H$, $b^{-1} \in H$
$\therefore$ $a * b^{-1} \in H$, by closure property.
Thus, the condition is necessary.

(ii) Let $a * b^{-1} \in H$, where $a, b \in H$, where H is a nonempty subset of G.
If $b = a$, the given condition gives

$$a * a^{-1} \in H$$

i.e., $e \in H$ (1)

Using the given condition for the pair $e, a \in H$, we have $e * a^{-1} \in H$

i.e., $a^{-1} \in H$ (2)

Similarly, $b^{-1} \in H$

Using the given condition for the pair a and $b^{-1} \in H$, we have

$$a * (b^{-1})^{-1} \in H$$

i.e., $a * b \in H$ (3)

From (1), (2) and (3), it follows that $\{H, *\}$ is a group and hence a subgroup of G.

Thus the condition is sufficient.

GROUP HOMOMORPHISM

Definition

If $\{G, *\}$ and $\{G', \Delta\}$ are two groups, then a mapping $f : G \to G'$ is called a *group homomorphism*, if for any $a, b \in G$,

$$f(a * b) = f(a) \Delta f(b).$$

A group homomorphism f is called *group isomorphism*, if f is one-to-one onto.

Theorem

If $f : G \to G'$ is a group homomorphism from $\{G, *\}$ to $\{G', \Delta\}$, then

(i) $f(e) = e'$, where e and e' are the identity elements of G and G' respectively,

(ii) for any $a \in G$, $f(a^{-1}) = [f(a)]^{-1}$

(iii) if H is a subgroup of G, then $f(H) = \{f(h) | h \in H\}$ is a group of G'.

Proof

(i) $f(e * e) = f(e) \Delta f(e)$, by definition of homomorphism.

i.e., $f(e) = f(e) \Delta f(e)$.

i.e., $f(e)$ is an idempotent element of $\{G', \Delta\}$

But the only idempotent element of a group is its identity.

$\therefore$ $f(e) = e'$

(ii) For any $a \in G$, $a^{-1} \in G$

$\therefore$ $f(a * a^{-1}) = f(a) \Delta f(a^{-1})$

i.e., $f(e) = f(a) \Delta f(a^{-1})$

i.e., $e' = f(a) \Delta f(a^{-1})$ (1)

Similarly, $f(a^{-1} * a) = f(a^{-1}) \Delta f(a)$

i.e., $e' = f(e) = f(a^{-1}) \Delta f(a)$ (2)

From (1) and (2), we see that

$f(a^{-1})$ is the inverse of $f(a)$

i.e., $f(a^{-1}) = [f(a)]^{-1}$.

(iii) Let $h_1, h_2 \in H$.

Then $h_1' = f(h_1)$ and $h_2' = f(h_2) \in f(H)$

Now $h_1' \Delta (h_2')^{-1} = f(h_1) \Delta [f(h_2)]^{-1}$

$= f(h_1) \Delta f(h_2^{-1})$, by (ii)

$= f(h_1 * h_2^{-1})$, by homomorphism

$= f(h_3)$, where $h_3 = h_1 * h_2^{-1} \in H$, as H is a subgroup.

i.e. $h_1' \Delta (h_2')^{-1} \in f(H)$

Thus $h_1', h_2' \in f(H) \Rightarrow h_1' \Delta (h_2')^{-1} \in f(H)$.

$\therefore$ $f(H)$ is a subgroup of G'.

KERNEL OF A HOMOMORPHISM

Definition

If $f : G \to G'$ is a group homomorphism from $\{G, *\}$ to $\{G', \Delta\}$, then the set of elements of G, which are mapped into e', the identity element of G', is called the *kernel of the homomorphism* f and denoted by $\ker(f)$.

Theorem

The kernel of a homomorphism f from a group $(G, *\}$ to another group (G', Δ) is a subgroup of $(G, *\}$.

Proof

By the previous theorem,

$f(e) = e'$, where e and e' are the identities of G and G'

$\therefore$ $e \in \ker(f)$

i.e., $\ker(f)$ is a non empty subset of $(G, *)$

Let $a, b \in \ker(f)$

$\therefore$ $f(a) = e'$ and $f(b) = e'$, by definition

Now $f(a * b^{-1}) = f(a) \Delta f(b^{-1})$

$= f(a) \Delta \{f(b)\}^{-1}$, by the previous theorem

$= e' \Delta \{e'\}^{-1}$

$= e' \Delta e'$

$= e'$

$\therefore$ $a * b^{-1} \in \ker(f)$

Thus, when $a, b \in \ker(f)$, $a * b^{-1} \in \ker(f)$

$\therefore$ $\ker(f)$ is a subgroup of $\{G, *\}$.

COSETS

Definition

If $\{H, *\}$ is a subgroup of a group $\{G, *\}$, then the set aH, where $a \in G$, defined by

$$aH = \{a * h | h \in H\}$$

is called the *left coset* of H in G generated by the element $a \in G \cdot a$ is called the *representative* (element) of the left coset aH.

Similarly the set Ha defined by

$$Ha = \{h * a | h \in H\}$$

is called the *right coset* of H in G generated by $a \in G \cdot a$ is again called the representative (element) of Ha.

Lagrange's Theorem

The order of a subgroup of a finite group is a divisor of the order of the group.

Proof

Let aH and bH be two left cosets of the subgroup $\{H, *\}$ in the group $\{G, *\}$. Let the two cosets aH and bH be not disjoint.

Then let c be an element common to aH and bH i.e., $c \in aH \cap bH$.

Since, $c \in aH$, $c = a * h_1$, for some $h_1 \in H$ (1)

Since, $c \in bH$, $c = b * h_2$, for some $h_2 \in H$ (2)

From (1) and (2), we have

$$a * h_1 = b * h_2$$

$$\therefore \quad a = b * h_2 * h_1^{-1} \quad (3)$$

Let x be an element in aH

$$\therefore \quad x = a * h_3, \text{ for some } h_3 \in H$$

$$= b * h_2 * h_1^{-1} * h_3, \text{ using (3)}$$

Since H is a subgroup, $h_2 * h_1^{-1} * h_3 \in H$

Hence, (3) means $x \in b\,H$

Thus, any element in aH is also an element in bH. $\therefore$ $aH \subseteq bH$

Similarly, we can prove that $bH \subseteq aH$

Hence $aH = bH$

Thus, if aH and bH are not disjoint, they are identical.

$\therefore$ The two cosets aH and bH are disjoint or identical. (4)

Now every element $a \in G$ belongs to one and only one left coset of H in G, for,

$$a = ae \in aH, \text{ since } e \in H$$

i.e., $$a \in aH$$

$a \notin bH$, since, aH and bH are disjoint i.e., a belongs to one and only left coset of H in G i.e., aH. (5)

From (4) and (5), we see that the set of left cosets of H in G form a partition of G. Now let the order of H be m.

viz., let $H = \{h_1, h_2, \ldots, h_m\}$, where h_i's are distinct

Then $$aH = \{ah_1, ah_2, \ldots ah_m\}$$

The elements of aH are also distinct, for, $ah_i = ah_j \Rightarrow h_i = h_j$, which is not true.

Thus H and aH have the same number of elements, namely m.

In fact every coset of H in G has exactly m elements.

Now let the order of the group $(G, *)$ be n, i.e., there are n elements in G.

Let the number of distinct left cosets of H in G be p. [p is called the *index* of H in G.]

$\therefore$ the total number of elements of all the left cosets = pm = the total number of elements of G i.e. $n = p \cdot m$

i.e. m, the order of H is a divisor of n, the order of G.

Deductions

1. The order of any element of a finite group is a divisor of the order of the group.

   Proof

   Let $a \in G$ and let $O(a) = m$. Then $a^m = e$. Let H be the cyclic subgroup generated by a. Then $H = \{a, a^2, \ldots, a^m(= e)\}$. i.e., $O(H) = m$.

   By Lagrange's theorem,

   $O(H)$ is a divisor of $O(G)$

   $\therefore$ $O(a)$ is a divisor of $O(G)$

2. If G is a finite group of order n, then $a^n = e$ for any element $a \in G$.

   Proof

   If m is the order of a, then $a^m = e$. Then m is a divisor of n. i.e., $n = km$

   Now $a^n = a^{km} = (a^m)^k = e^k = e$.

3. Every group of prime order is cyclic.

   Proof

   Let $a(\neq e)$ be any element of G

   $\therefore$ $O(a)$ is a divisor of $O(G) = p$, a prime number

   $\therefore$ $O(a) = 1$ or p ($\because$ the divisors of p are 1 and p only)

   If $O(a) = 1$, then $a = e$, which is not true.

   Hence, $O(a) = p$. i.e., $a^p = e$

   $\therefore$ G can be generated by any element of G other than e and is of order p. i.e., the cyclic group generated by $a(\neq e)$ is the entire G.

   i.e., G is a cyclic group.

NORMAL SUBGROUP

Definition

A subgroup $\{H, *\}$ of the group $\{G, *\}$ is called a *normal subgroup*, if for any $a \in G$, $aH = Ha$ (i.e., the left and right cosets of H in G generated by a are the same)

Note $aH = Ha$ does not mean that $a * h = h * a$ for any $h \in H$, but it means that $a * h_1 = h_2 * a$, for some $h_1, h_2 \in H$.

Theorem

A subgroup $(H, *)$ of a group $(G, *)$ is a normal subgroup if and only if $a^{-1} * h * a \in H$ for every $a \in G$ and $h \in H$.

Proof

(i) Let $(H, *)$ be a normal subgroup of $(G, *)$.

Then $aH = Ha$ for any $a \in G$, by definition of normal subgroup.

Now $h * a \in Ha = aH$

$\therefore$ $h * a = a * h_1$, for some $h_1 \in H$

i.e., $a^{-1} * h * a = h_1 \in H$.

(ii) Let $a^{-1} * h * a \in H$, for every $a \in G$ and $h \in H$

Then $a * (a^{-1} * h * a) \in aH$

i.e., $(a * a^{-1}) * (h * a) \in aH$

i.e., $e * (h * a) \in aH$

i.e., $h * a \in aH$

$\therefore$ $Ha \subseteq aH$ (1)

Let $b = a^{-1} \in G$, since, $a^{-1} \in G$

$\therefore$ $b^{-1} * h * b \in H$

i.e., $(a^{-1})^{-1} * h * a^{-1} \in H$

i.e., $a * h * a^{-1} \in H$

$\therefore$ $(a * h * a^{-1}) * a \in Ha$

i.e., $(a * h) * (a^{-1} * a) \in Ha$

i.e., $(a * h) * e \in Ha$

i.e., $a * h \in Ha$

$\therefore$ $aH \subseteq Ha$ (2)

From (1) and (2), it follows that $aH = Ha$.

QUOTIENT GROUP (OR) FACTOR GROUP

Definition

If H is a normal subgroup of a group $(G, *)$ and G/H denotes the set of all (left or right) cosets of H in G and if the binary operation $\otimes$ is defined on G/H by $aH \otimes bH = (a * b)H$ [or $Ha \otimes Hb = H(a * b)$] for all $a, b \in G$, then $\{G/H, \otimes\}$ is a group called a *quotient group* or *factor group*.

Theorem

If H is a normal subgroup of a group $(G, *)$, then $\{G/H, \otimes\}$ is a group, where G/H and $\otimes$ are defined as above:

Proof

Let $G/H = \{aH/a \in G\}$

Then $eH = H$, where e is the identity of $(G, *)$

$\therefore$ $eH(=H) \in G/H$

i.e., G/H is not an empty set (1)

If $aH, bH \in G/H$, then $aH \otimes bH = (a * b)H \in G/H$

Hence, G/H is closed under $\otimes$ (2)

Let $aH, bH, cH \in G/H$

Now $aH \otimes \{bH \otimes cH\} = aH \otimes (b * c)H$

$= \{a * (b * c)\}H$

$= \{(a * b) * c\}H$, since, $a, b, c \in G$

$= (a * b)\, H \otimes cH$

$= \{aH \otimes bH\} \otimes cH$

$\therefore$ the operator $\otimes$ is associative (3)

Now $aH \otimes eH = (a * e)\ H$ {$\because\ eH \in G/H$ by (1)}
$= aH$

Also $eH \otimes aH = (e * a)H = aH$

$\therefore$ eH is the identity element of G/H (4)

Since, $aH \in g/H,\ a^{-1}H \in G/H.$

Now $aH \otimes a^{-1}H = (a * a^{-1})H = eH$

Also $a^{-1}H \otimes aH = (a^{-1} * a)H = eH$

$\therefore$ $a^{-1}H$ is the inverse of aH (5)

By (1), (2), (3), (4) and (5), $\{G/H, \otimes\}$ is a group

Note The operation $\otimes$ is called coset multiplication.

Theorem

If $f : (G, *) \to (G', \Delta)$ is a homomorphism with kernel K, then K is a normal subgroup of G and the quotient group G/K is isomorphic to $f(G)$.

Proof

(i) We have already proved that
$K = \ker(f) = \{a \in G | f(a) = e'\}$ is a subgroup of $(G, *)$, where e' is the identity of (G', Δ).
Now for any $a \in G$ and $k \in K$,

$$f(a^{-1} * k * a) = f(a^{-1})\ \Delta\ f(k)\ \Delta\ f(a)$$
$$= f(a^{-1})\ \Delta\ e'\ \Delta\ f(a)$$
$$= [f(a)^{-1}\ \Delta\ f(a) = e'$$

$\therefore$ $a^{-1} * h * a \in K$

$\therefore$ $\{K, *\}$ is a normal subgroup of $(G, *)$

(ii) Let ϕ: $G/K \to G'$ such that $\phi(aK) = f(a)$, for any $a \in G$.
Let $a, b \in G$ such that $aK = bK$

Then $(a^{-1} * a)K = (a^{-1} * b)K$

i.e., $eK = (a^{-1} * b)K$, where e is the identity of G and so of K.

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

i.e., $a^{-1} * \in K$

Thus, if $aK = bK,\ a^{-1} * b \in K$ (1)

$\therefore$ $f(a^{-1} * b) = e'$, where e' is the identity of G'

i.e., $f(a^{-1})\ \Delta\ f(b) = e'$

i.e., $[f(a)]^{-1}\ \Delta\ f(b) = e'$

i.e., $f(a)\ \Delta\ [f(a)]^{-1}\ \Delta\ f(b) = f(a)\ \Delta\ e'$

i.e., $f(b) = f(a)$

i.e., $\phi(aK) = \phi(bK)$

This means that the ϕ is well defined (2)

Now $\phi(aK \otimes bK) = \phi\{a * b)K\}$
$= f(a * b)$

$= f(a) \Delta f(b)$

$= \phi(aK) \Delta \phi(aK)$

$\therefore$ ϕ is a homomorphism. (3)

Now let $\phi(aK) = \phi(bK)$

Then $f(a) = f(b)$

$\therefore$ $[f(a)]^{-1} \Delta f(a) = [f(a)]^{-1} \Delta f(b)$

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

$\therefore$ $a^{-1} * b \in K$

$\therefore$ $aK = bK$, by (1)

This means that ϕ is one-to-one (4)

Let x be any element of G'

Since $f : G \to G'$ is a homomorphism from G to G', there is an element $a \in G$ such that

$f(a) = x$.

$\therefore$ $\phi(aK) = f(a) = x$

Since $aK \in G/K$, $\phi: G/K \to G'$ is an isomorphism, or $\phi: G/K \to f(G)$ is an isomorphism.

ALGEBRAIC SYSTEMS WITH TWO BINARY OPERATIONS

Introduction

So far we have studied algebraic systems with one binary operation, namely semigroup, monoid and group. As these are not adequate to describe the system of real numbers satisfactorily, we shall now consider an abstract algebraic system, called a ring, with two basic operations of addition and multiplication. By imposing more restrictions on rings, other algebraic systems with two binary operations will be obtained and discussed in this section.

RING

Definition

An algebraic system $(R, +, \bullet)$, where R is a nonempty set and $+$ and $\bullet$ are two closed binary operations (which may be different from ordinary addition and multiplication) is called a *ring*, if the following conditions are satisfied:

1. $(R, +)$ is an abelian group
2. $(R, \bullet)$ is a semigroup
3. The operation $\bullet$ is distributive over $+$, i.e., for any $a, b, c \in R$,

$a \bullet (b + c) = a \bullet b + a \bullet c$ and

$(b + c) \bullet a = b \bullet a + c \bullet a$

Note Conditions (1) and (2) given above include the following:

(i) $a + b = b + a$, for any $a, b \in R$

(ii) $(a + b) + c = a + (b + c)$, for any $a, b, c \in R$.

(iii) There exists an identity element, denoted by $0 \in R$, such that $a + 0 = 0 + a = a$, for every $a \in R$.

(iv) For every $a \in R$, there is an element $b(= -a)$ such that $a + b = b + a = 0$.

(v) $a \bullet (b \bullet c) = (a \bullet b) \bullet c$, for any a, b, c.

Example of rings are the set of integers (Z), real numbers (R), rational numbers (Q) and complex numbers (C).

Definitions

1. If $(R, \bullet)$ is commutative, then the ring $(R, +, \bullet)$ is called a *commutative ring*.
2. If $(R, \bullet)$ is a monoid, then the ring $(R, +, \bullet)$ is called a *ring with identity or unity*.
3. If a and b are two non-zero elements of a ring R such that $a \bullet b = 0$, then a and b are *divisors of 0* or *zero divisors*.
   (For example, if R is the set of integers modulo 6, under addition and multiplication modulo 6, the elements of R are [0], [1], [2], … [5].
   Now $[2] \times_6 [3] = [0]$, but $[2] \neq [0]$ and $[3] \neq 0$.
   The [2] and [3] are zero divisors in R, i.e., in a ring R, $a \bullet b = 0$ with neither $a = 0$ nor $b = 0$.)
4. A commutative ring with unity (containing at least 2 elements) and without zero divisors is called an *integral domain*.

Example

The ring of integers is an example of an integral domain, whereas $(Z_6, +_6, \times_6)$ is not an integral domain, since $[2]_6 \times_6 [3]_6 = [0]_6$.

5. A commutative ring R with multiplication identity, containing at least two elements is called a field, if every non-zero element of R has a multiplicative inverse in R.

Example

The ring of rational numbers $(Q, +, \bullet)$ is a field, since it is a commutative ring with identity and the multiplicative inverse of every non-zero element of Q is in Q.

Similarly the set R of real numbers and the set of complex numbers under ordinary addition and multiplication are fields.

6. A non-empty subset $S \subseteq R$, where $(R, +, \bullet)$ is a ring, is called a *subring* of R, if $(S, +, \bullet)$ is itself a ring with the operations + and $\bullet$ restricted to S.

Example

The ring of even integers is a subring of the ring of integers under ordinary addition and multiplication.

7. If $(R, +, \bullet)$ and $(S, \otimes, \odot)$ be rings and $f: R \to S$ is a mapping from R to S, then f is called a *ring homomorphism* from R to S, if for any $a, b \in R$, $f(a + b) = f(a) \otimes f(b)$ and $f(a \bullet b) = f(a) \odot f(b)$.

Some Elementary Properties of a Ring

1. (a) The additive identity or the zero element of a ring $(R, +, \bullet)$ is unique.
   (b) The additive inverse of every element of the ring is unique.
   (c) The multiplicative identity of a ring, if it exists, is unique.
   (d) If the ring has multiplicative identity, then the multiplicative inverse of any non-zero element of the ring is unique.

Proof

(a) If possible, let there be two elements of the ring, say 0 and 0′

Since $0' \in R$ and 0 is a zero element, $0' + 0 = 0 + 0' = 0'$ (1)

Since $0 \in R$ and 0′ is a zero element, $0 + 0' = 0' + 0 = 0$ (2)

From (1) and (2), we get $0' = 0$.

i.e., zero element of ring is unique.

(b) Let b and c be two additive inverses of $a \in R$, if possible.

Then $a + b = b + a = 0$ (1)

Similarly, $a + c = c + a = 0$ (2)

Now $b = b + 0 = b + (a + c)$, by (2)

$= (b + a) + c$, by associativity

$= 0 + c$, by (1)

$= c$

Thus the additive inverse of a is unique. In a similar manner, the proofs of (c) and (d) may be given.

2. *The cancellation laws of addition*
   For all $a, b, c \in R$,
   (a) If $a + b = a + c$, then $b = c$ (left cancellation)
   (b) If $b + a = c + a$, then $b = c$ (right cancellation)

Proof

(a) $a + b = a + c$

$\therefore$ $(-a) + a + b = (-a) + a + c$, where $-a$ is the additive inverse of a

i.e., $(-a + a) + b = (-a + a) + c$, by associativity

i.e., $0 + b = 0 + c$

i.e., $b = c$.

Similarly (b) part may be proved.

3. If $(R, +, \bullet)$ is a ring and $a \in R$, then $a \bullet 0 = 0 \bullet a = 0$, where 0 is the zero (additive identity) element of R.

Proof

$a \bullet 0 = a \bullet (0 + 0)$, since $0 + 0 = 0$

$= a \bullet 0 + a \bullet 0$, by distributivity (1)

$\therefore$ $0 + a \bullet 0 = a \bullet 0$

$= a \bullet 0 + a \bullet 0$, by (1)

$\therefore$ By the cancellation law,

$a \bullet 0 = 0$.

Similarly we can prove that $0 \bullet a = 0$.

Note The operation $\bullet$ need not represent ordinary multiplication.

4. If $(R, +, \bullet)$ is a ring, then for any $a, b, c \in R$,
   (a) $-(-a) = a$
   (b) $a \bullet (-b) = (-a) \bullet b = -(a \bullet b)$
   (c) $(-a) \bullet (-b) = a \bullet b$
   (d) $a \bullet (b - c) = a \bullet b - a \bullet c$
   (e) $(a - b) \bullet c = a \bullet c - b \bullet c$

Proof

(a) $(-a) + a = a + (-a) = 0$
$\therefore$ a is the additive inverse of $(-a)$
Also the additive inverse of $(-a)$ is unique
$\therefore$ $-(-a) = a$.

(b) We have $a \bullet (-b + b) = a \bullet (-b) + a \bullet b$, by distributivity
i.e., $a \bullet 0 = a \bullet (-b) + a \bullet b$
i.e., $0 = a \bullet (-b) + a \bullet b$, by property (3)
$\therefore$ the additive inverse of $a \bullet b$ is $a \bullet (-b)$
i.e., $-(a \bullet b) = a \bullet (-b)$ (1)
Similarly, we may prove that
$-(a \bullet b) = (-a) \bullet b$ (2)

(c) From (1) of (b), we have
$(-a) \bullet (-b) = -[(-a) \bullet b)]$, by replacing a by $-a$
$= -[-(a \bullet b)]$, from (2) of (b)
$= a \bullet b$, by property 4(a)

(d) $a \bullet (b - c) = a \bullet [b + (-c)]$
$= a \bullet b + a \bullet (-c)$, by distributivity
$= a \bullet b + [-(a \bullet c)$, by (b)(1)
$= a \bullet b - a \bullet c$

(e) $(a - b) \bullet c = [a + (-b)] \bullet c$
$= a \bullet c + (-b) \bullet c$, by distributivity
$= a \bullet c + [-(b \bullet c)]$
$= a \bullet c - b \bullet c$

5. A commutative ring with unity is an integral domain if and only if it satisfies cancellation law of multiplication.

Proof

(a) Let R be an integral domain and $a(\neq 0) \in R$ and let $a \bullet b = a \bullet c$ (1)
i.e., $a \bullet (b - c) = 0$
Since R is an integral domain, $a = 0$ or $b - c = 0$. But $a \neq 0$.
$\therefore$ $b - c = 0$ or $b = c$ (2)
From (1) and (2), we see that the left cancellation holds. Since the ring is commutative, the right cancellation also holds.

(b) *Converse*

Let the cancellation law hold good for R.

Then for $a, b \in R$ where $a \neq 0$,

if $a \bullet b = 0 = a \bullet 0$, then $b = 0$

Similarly, if $b \neq 0$, then $a = 0$.

Thus, if $a \bullet b = 0$, then $a = 0$ or $b = 0$

i.e., R has no zero divisors

i.e., R is an integral domain.

6. Every field is an integral domain.

Proof

Since a field F is a commutative ring with unity, it is enough we prove that F has no zero divisors to show that it is an integral domain.

Let $a, b \in F$ such that $a \neq 0$ and $a \bullet b = 0$ (1)

Since $a \neq 0$, a^{-1} exists.

Hence, from (1), we have

$$a^{-1} \bullet (a \bullet b) = a^{-1} \bullet 0 = 0$$

i.e., $(a^{-1} \bullet a) \bullet b = 0$

i.e., $1 \bullet b = 0$

i.e., $b = 0$

Similarly if $b \neq 0$, b^{-1} exists.

Hence, from (1), we have

$$(a \bullet b) \bullet b^{-1} = 0 \bullet b^{-1} = 0$$

i.e., $a \bullet (b \bullet b^{-1}) = 0$

i.e., $a \bullet 1 = 0$

i.e., $a = 0$

Thus, if $a \bullet b = 0$, where $a, b \in F$, then

$$a = 0 \text{ or } b = 0$$

i.e., the field F has no zero divisors

$\therefore$ F is an integral domain.

Note The converse of property (6) need not be true, viz., every integral domain is not a field.

For example, the ring of integers is an integral domain, but it is not a field, as the elements 1 and –1 only have inverses.

7. Every finite integral domain is a field.

Proof

Let $\{D, +, \bullet\}$ be a finite integral domain. Then D has a finite number of distinct elements, say, $\{a_1, a_2, \ldots, a_n\}$.

Let a $(\neq 0)$ be any element of D.

Then the elements $a \bullet a_1, a \bullet a_2, \ldots a \bullet a_n \in D$, since D is closed under multiplication. The elements $a \bullet a_1, a \bullet a_2, \ldots, a \bullet a_n$ are distinct, because if $a \bullet a_i = a \bullet a_j$, then $a \bullet (a_i - a_j) = 0$.

But $a \neq 0$. Hence $a_i - a_j = 0$, since D is an integral domain i.e., $a_i = a_j$, which is not true, since $a_1, a_2, \ldots, a_n$ are distinct elements of D.

Hence, the sets $\{a \bullet a_1, a \bullet a_2, \ldots, a \bullet a_n\}$ and $\{a_1, a_2, \ldots, a_n\}$ are the same.

Since $a \in D$ is in both sets, let $a \bullet a_k = a$, for some k (1)

Then a_k is the unity of D, detailed as follows:

Let $a_j (\in D) = a \bullet a_i$ (2)

Now
$$\begin{aligned} a_j \bullet a_k &= a_k \bullet a_j, \text{ by commutativity} \\ &= a_k \bullet (a \bullet a_i), \text{ by (2)} \\ &= (a_k \bullet a) \bullet a_i \\ &= (a \bullet a_k) \bullet a_i \text{ by commutativity} \\ &= a \bullet a_i, \text{ by (1)} \\ &= a_j, \text{ by (2)} \end{aligned}$$

Since, a_j is an arbitrary element of D

a_k is the unity of D

Let it be denoted by 1.

Since, $1 \in D$, there exist a ($\neq 0$) and $a_i \in D$ such that $a \bullet a_i = a_i \bullet a = 1$

$\therefore$ a has an inverse.

Hence, $(D, +, \bullet)$ is a field.

8. If $(R, +, \bullet)$ is a ring and S is non-empty subset of R, then $(S, +, \bullet)$ is subring of R, if and only if for all $a, b \in S$, $a - b \in S$ and $a \bullet b \in S$.

Proof

Since $(R, +, \bullet)$ is a ring, $(R, +)$ is an abelian group.

Since S is a non-empty set of R, it is a subgroup of R, if and only if, for all $a, b \in S$, $a * b^{-1} \in S$.

Here the binary operation is + and the additive inverse of b is $-b$

$\therefore$ S is a subring of the ring R, if and only if $a + (-b) \in S$

i.e., $a - b \in S$.

Now S is a ring by itself.

$\therefore$ When $a, b \in S$, $a \bullet b \in S$.

9. If $f : (R, +, \bullet) \to (S, \otimes, \odot)$ is a ring homomorphism, then
   (a) $f(0) = 0'$, where 0 and $0'$ are the additive identities (zeros) of R and S.
   (b) $f(-a) = -f(a)$, for every $a \in R$.
   (c) $f(na) = nf(a)$, for every $a \in R$, where n is an integer.
   (d) $f(a^n) = [f(a)]^n$, for every $a \in R$, where n is a positive integer.

Proof

(a) Since $f(0) \in S$, we have

$$\begin{aligned} 0' \oplus f(0) &= f(0) \\ &= f(0 + 0), \text{ since 0 is the identity of } R \\ &= f(0) \oplus f(0) \end{aligned}$$

$\therefore$ By cancellation law of addition in S, we have $f(0) = 0'$.

(b) $0' = f(0) = f\{a + (-a)\}$
$= f(a) \oplus f(-a)$

Since additive inverses in S are unique, $f(-a)$ is the additive inverse of $f(a)$

i.e., $f(-a) = -f(a)$.

(c) When $n = 0$, $f(na) = f(0) = 0' = n\,f(a)$

When $n = 1$, $f(a) = 1\,f(a)$

Hence, the result is true for $n = 0$ and 1.

Let the result be true for $n = k$ (≥ 1) (induction hypothesis)

Now $f\{(k + 1)\,a\} = f(ka + a)$
$= f(ka) \oplus f(a)$
$= k\,f(a) \oplus f(a)$, by inductions hypothesis
$= (k + 1)\,f(a)$

i.e., the result is true for $n = k + 1$

$\therefore$ By mathematical induction, the result $f(na) = nf(a)$ for all $a \in R$, $n \in Z^+$.

Now if $n \in Z^+$,

$f(-na) \oplus f(na) = f\{n(-a)\} \oplus f(na)$
$= n\,f(-a) \oplus n\,f(a)$, by the previous part
$= n[f(-a) \oplus f(a)]$
$= n[-f(a) \oplus f(a)]$, by part (b)
$= n(0')$
$= 0'$

$\therefore$ $f(-na)$ = the additive inverse of $f(na)$ in S
$= -f(na)$
$= -n\,f(a)$, by previous part.

$\therefore$ The result is true for all $n \in Z$.

(d) This result too can be proved by mathematical induction.

WORKED EXAMPLES 4(B)

Example 4.1 Every subgroup of a cyclic group is also cyclic.

Let G be the cyclic group generated by the element a and let H be a subgroup of G. If $H = G$ or $\{e\}$, evidently H is cyclic. If not, the elements of H are non-zero integral powers of a, since, if $a^r \in H$, its inverse $a^{-r} \in H$.

Let m be the least positive integer for which $a^m \in H$ (1)

Now let a^n be any arbitrary element of H. Let q be the quotient and r the remainder when n is divided by m.

Then $n = mq + r$, where $0 \leq r < m$ (2)

Since, $a^m \in H$, $(a^m)^q \in H$, by closure property

i.e., $a^{mq} \in H$

$\therefore$ $(a^{mq})^{-1} \in H$, by existence of inverse, as H is a subgroup

i.e., $a^{-mq} \in H$.

Now since, $a^n \in H$ and $a^{-mq} \in H$,

$a^{n-mq} \in H$

i.e., $a^r \in H$

By (1) and (2), we get $r = 0 \quad \therefore \quad n = mq$

$\therefore \quad a^n = a^{mq} = (a^m)^q$

Thus, every element $a^n \in H$ is of the form $(a^m)^q$.

Hence H is a cyclic subgroup generated by a^m.

Example 4.2 If G is an abelian group with identity e, prove that all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

$H = \{x | x^2 = e\}$

$e^2 = e \quad \therefore$ the identity element e of $G \in H$

Now $x^2 = e$

$\therefore \quad x^{-1} \cdot x^2 = x^{-1} \cdot e$

i.e., $x = x^{-1}$ (1)

Hence, if $x \in H$, $x^{-1} \in H$.

Let $x, y \in H$

Since, G is abelian, $xy = yx$

$= y^{-1}x^{-1}$, by (1)

$= (xy)^{-1}$

$\therefore \quad (xy)^2 = e$. i.e., $xy \in H$

Thus, if $x, y \in H$, we have $xy \in H$

Thus, all the 3 conditions in the definition of a subgroup are satisfied.

$\therefore \quad H$ is a subgroup of G.

Example 4.3 If G is the set of all ordered pairs (a, b), where $a(\neq 0)$ and b are real and the binary operation $*$ on G is defined by

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

show that $(G, *)$ is a non-abelian group. Show also that the subset H of all those elements of G which are of the form $(1, b)$ is a subgroup of G.

The reader can verify the closure and associative property of G.

If (e_1, e_2) is the identity of $(a, b) \in G$,

then $(e_1, e_2) * (a, b) = (a, b)$

i.e., $(e_1a, e_2a + b) = (a, b)$

$\therefore \quad e_1a = a$ and $e_2a + b = b$

$\therefore \quad e_1 = 1$ and $e_2 = 0$

i.e., $(1, 0)$ is the identity of G.

If (x, y) is the inverse of $(a, b) \in G$,

then $(x, y) * (a, b) = (1, 0)$

i.e., $(xa, ya + b) = (1, 0)$

$\therefore \quad xa = 1$ or $x = \dfrac{1}{a}$

and $ya + b = 0$ or $y = -\frac{b}{a}$

$\therefore$ Inverse of (a, b) is $\left(\frac{1}{a}, -\frac{b}{a}\right)$ (1)

Thus, $(G, *)$ is a group.

Obviously, H is not an empty set.

Now $(1, b) * (1, c)^{-1} = (1, b) * \left(\frac{1}{1}, -\frac{c}{1}\right)$ by (1)

$= (1, b) * (1, -c)$

$= (1 \cdot 1, b \cdot 1 - c)$, by definition of $*$

$= (1, b - c)$

$(1, b - c) \in H$.

Hence, the necessary and sufficient condition for a subgroup is satisfied.

$\therefore$ H is a subgroup of G.

Example 4.4 Prove that the intersection of two subgroups of a group G is also a subgroup of G. Give an example to show that the union of two subgroups of G need not be a subgroup of G.

Let H_1 and H_2 be any two subgroups of G. $H_1 \cap H_2$ is a non-empty set, since, at least the identity element e is common to both H_1 and H_2.

Let $a \in H_1 \cap H_2$. Then $a \in H_1$ and $a \in H_2$

Let $b \in H_1 \cap H_2$. Then $a \in H_1$ and $b \in H_2$

H_1 is a subgroup of G.

$\therefore$ $a * b^{-1} \in H_1$, since, a and $b \in H$.

H_2 is a subgroup of G.

$\therefore$ $a * b^{-1} \in H_2$, since a and $b \in H$.

Hence, $a * b^{-1} \in H_1 \cap H_2$

Thus, when $a, b \in H_1 \cap H_2$, $a * b^{-1} \in H_1 \cap H_2$

$\therefore$ $H_1 \cap H_2$ is a subgroup of G.

Let G be the additive group of integers.

Then $H_1 = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$ and

$H_2 = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$ are both subgroups of G.

Now $H_1 \cup H_2$ is not closed under addition.

For example, $2 \in H_1 \cup H_2$ and $3 \in H_1 \cup H_2$

But $2 + 3 = 5 \notin H_1 \cup H_2$

$\therefore$ $H_1 \cup H_2$ is not a subgroup of G.

Example 4.5 Show that the group $\{Z_n, +_n\}$ is isomorphism to every cyclic group of order n.

Let the cyclic group $(G, *)$ of order n be generated by an element $a \in G$. Then the elements of G are $\{a, a^2, a^3, \ldots, a^n(= e)\}$.

Let us consider the mapping $f : Z_n \to G$, defined by $f([i]) = a^i$, $i = 0, 1, 2, \ldots, n - 1$. Obviously [1] is the generator of $\{Z_n, +_n\}$, as $[1] +_n [1] = [2]$ etc., $[1] +_n [1] +_n \ldots n$ times $= [n] = [1]$

Now $f([i + j]) = a^{i+j}$
$= a^i \cdot a^j$
$= f([i]) \cdot f([j])$

$\therefore$ f is a homomorphism from Z_n to G. Also f is onto. Hence, f is an isomorphism.

Example 4.6 If G is the set of all ordered pairs (a, b) of real numbers and $*$ is the binary operation defined by $(a, b) * (c, d) = (a + c, b + d)$, prove that $(G, *)$ is a group. If G' is the additive group of all real numbers, prove that the mapping $f : G \to G'$ defined by $f(a, b) = a$, for all $a, b \in G$ is a homomorphism.

It is easily verified that $(G, *)$ is a group, with the identity element $(0, 0)$. The inverse of (a, b) is $(-a, -b)$.

Now $\{f(a, b) * (c, d)\} = f\{a + c, b + d\}$
$= a + c$, since $f(a, b) = a$
$= f(a, b) + f(c, d)$

Hence, f is a homomorphism from G to G'.

Example 4.7 If R and C are additive groups of real and complex numbers respectively and if the mapping $f: C \to R$ is defined by $f(x + iy) = x$, show that f is a homomorphism. Find also the kernal of f.

Let $a + ib$ and $c + id$ be any two elements of C.

Then $f\{a + ib) + (c + id) = f\{(a + c) + i(b + d)\}$
$= a + c$
$= f(a + ib) + f(c + id)$

Hence, f is a homomorphism from C to R.

The identity of R is the real number 0.

The images of all complex numbers with real part 0 are each equal to 0, the identity of R, under f.

Hence, the kernal of f is the set of all purely imaginary numbers.

Example 4.8 If G is the multiplicative group of all $(n \times n)$ non-singular matrices whose elements are real numbers and G' is the multiplicative group of all non-zero real numbers, show that the mapping $f: G \to G'$, where $f(A) = |A|$, for all $A \in G$ is a homomorphism. Find also the kernel of f.

Let $A, B \in G$.

Now $f(AB) = |AB|$
$= |A| \cdot |B|$
$= f(A) \cdot f(B)$

$\therefore$ f is a homomorphism from G to G'. The identity of $G' = 1$.

$\therefore$ The elements of G whose images under f is 1 form the kernel of f.

Thus, the set of all matrices whose determinant values are equal to 1 form the kernel of f.

Example 4.9 If G is the additive group of integers and H is the subgroup of G obtained by multiplying each element of G by 3, find the distinct right cosets of H in G.

$G = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$H = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Now $0 \in G$.
$H + 0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = H$
$1 \in G$.
$\therefore$ $H + 1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$
$2 \in G$.
$\therefore$ $H + 2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$
$3 \in G$.
$\therefore$ $H + 3 = \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}$

We see that $H + 3 = H$.

Similarly $H + 4 = H + 1$, $H + 5 = H + 2$, $H + 6 = H$ etc.

We can also see that $H + (-1) = H + 2$, $H + (-2) = H + 1$, $H + (-3) = H$ and so on.

Hence, the three distinct right cosets of H in G are H, $H + 1$ and $H + 2$, as they are disjoint. Also $H \cup (H + 1) \cup (H + 2) = G$.

Example 4.10 Show that $(H, *)$ is a subgroup of the symmetric group $(S_3, *)$ of degree 3, where $H = \{p_1, p_2\}$. Find also the left cosets of H in G.

Refer to Table 4.2, which is the Cayley's composition table of permutations on S_3. From the table, it is seen that $(H, *)$ is a group by itself with identity p_1 and with $p_1^{-1} = p_1$ and $p_2^{-1} = p_2$.

Hence, $(H, *)$ is a subgroup of $(S_3, *)$.

Now
$p_1H = (p_1 * p_1, p_1 * p_2) = (p_1, p_2) = H$
$p_2H = (p_2 * p_1, p_2 * p_2) = (p_2, p_1) = H$
$p_3H = (p_3 * p_1, p_3 * p_2) = (p_3, p_6)$
$p_4H = (p_4 * p_1, p_4 * p_2) = (p_4, p_5)$
$p_5H = (p_5 * p_1, p_5 * p_2) = (p_5, p_4)$
$p_6H = (p_6 * p_1, p_6 * p_2) = (p_6, p_3)$

$\therefore$ The three distinct left cosets of H in G are (p_1, p_2), (p_3, p_6) and (p_4, p_5).

Example 4.11 Show that the set of inverses of the elements of a right coset is a left coset, viz., show that $(Ha)^{-1} = a^{-1}H$.

Let Ha be a right coset of H in G, where $a \in G$. If $h \in H$, then $h * a \in H$

Now $(h * a)^{-1} = a^{-1} * h^{-1}$ (1)

Since H is a subgroup of G and $h \in H$, $h^{-1} \in H$. Hence, $a^{-1} * h^{-1} \in a^{-1} H$ or $(h * a)^{-1} \in a^{-1} H$, by (1)

i.e., the inverse of every element of Ha belongs to the left coset $a^{-1}H$

$\therefore$ $(Ha)^{-1} \subseteq a^{-1}H$ (2)

Now let $a^{-1} * h \in a^{-1} H$.

Then $a^{-1} * h = a^{-1} * (h^{-1})^{-1} = (h^{-1} * a)^{-1} \in (Ha)^{-1}$, since, $h^{-1} \in H$

i.e., every element of $a^{-1}H$ belongs to the set of inverses of the elements of Ha

$\therefore$ $a^{-1}H \subseteq (Ha)^{-1}$ (3)

From (2) and (3), it follows that

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

Example 4.12 If H is a normal subgroup of G and K is a subgroup of G such that $H \subseteq K \subseteq G$, show that H is a normal subgroup of K also.

H is a normal subgroup of G

$\therefore$ H is a subgroup of G.

Since $H \subseteq K \subseteq G$ and K is a subgroup of G, H is a subgroup of K also.

Let x be any element of K.

Then x is an element of G too.

Since H is a normal subgroup of G, we have $xH = Hx$, for every $x \in G$. Since H is a subgroup of K and $x \in K$,

$xH = Hx$, for every $x \in K$

$\therefore$ H is a normal subgroup of K also.

Example 4.13 Show that the intersection of two normal subgroups of a group G is also a normal subgroup of G.

Let H_1 and H_2 be two normal subgroups of G.

The H_1 and H_2 are subgroups of G and hence, $H_1 \cap H_2$ is also a subgroup of G. [Refer to the Example 4.4.]

Now let x be any element of G and h any element of $H_1 \cap H_2$.

Then $h \in H_1$ and $h \in H_2$

Since H_1 is a normal subgroup of G, we have $x^{-1} * h * x \in H_1$.

Similarly $x^{-1} * h * x \in H_2$. ($\because$ H_2 is a normal subgroup of G)

$\therefore$ $x^{-1} * h * x_2 \in H_1 \cap H_2$

Hence, $H_1 \cap H_2$ is a normal subgroup.

Example 4.14 If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$, prove that H is a normal subgroup of G.

For any $a \in G$ and $h \in H$, we have $a * h \in G$, by closure property.

$\therefore$ $(a * h)^2 \in H$, by the given condition (1)

Also, since, $a^{-1} \in G$, $(a^{-1})^2 = a^{-2} \in H$, by the given condition.

Since H is a subgroup (viz., a group by itself) and h^{-1}, $a^{-2} \in H$, we have

$h^{-1} * a^{-2} \in H$ (by closure property) (2)

From (1) and (2), we have

$(a * h)^2 * h^{-1} * a^{-2} \in H$

i.e., $a * h * a * h * h^{-1} * a^{-2} \in H$

i.e., $a * h * a * e * a^{-2} \in H$, where e is the identity

i.e., $a * h * a^{-1} \in H$

or $a^{-1} * h * a \in H$ (by replacing a by a^{-1})

$\therefore$ H is a normal subgroup.

Example 4.15 If G is the additive group of integers and H is a subgroup of G, defined by $H = \{4x | x \in G\}$, write down the elements of the quotient group G/H. Also give the composition table for G/H.

$$G = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$
$$H = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$$

Obviously G is an abelian group. Let $a \in G$ and $h \in H$.

Now $a^{-1} * h * a = a^{-1} * a * h \quad [\because G \text{ is abelian}]$
$= e * h$
$= h \in H$

Hence, H is a normal subgroup of G.

Note In this problem the binary operation $*$ is the ordinary addition.

The elements of G/H are the left (or right) cosets of H in G which are as follows:

$$0 + H = H = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$$
$$1 + H = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$$
$$2 + H = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$$
$$3 + H = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$$
$$4 + H = \{\ldots, -8, -4, -0, 4, 8, 12, 16, \ldots\} = H$$

Similarly $5 + H = 1 + H$, $6 + H = 2 + H$, $7 + H = 3 + H$ etc.

Thus, there are 4 distinct elements in the set G/H.

If we define the binary operation $\otimes$ as the ordinary addition, we see that

$$(1 + H) \otimes (3 + H) = (1 = H) + (3 + H) = 4 + H$$

In general, if $a, b \in G$, we see that

$$aH \otimes bH = (a + b)H$$

Hence, $\{G/H, +\}$ is a quotient group.

The composition table for this quotient group is given in Table 4.10.

Table 4.10

$+$	H	$1 + H$	$2 + H$	$3 + H$
H	H	$1 + H$	$2 + H$	$3 + H$
$1 + H$	$1 + H$	$2 + H$	$3 + H$	H
$2 + H$	$2 + H$	$3 + H$	H	$1 + H$
$3 + H$	$3 + H$	H	$1 + H$	$2 + H$

Example 4.16 Show that every quotient group of a cyclic group is cyclic.

Let G be a cyclic group and a be a generator of G.

Let H be a subgroup of G.

Since, every cyclic group is abelian and every subgroup of an abelian group is a normal subgroup, H is a normal subgroup of G.

Let a^r be any element of G when r is a positive integer. Then a^rH(or Ha^r) is any element of G/H.

Now $a^rH = a^rH^r = (aH)^r$

i.e., any element of G/H can be expressed as $(aH)^r$

$\therefore$ G/H is a cyclic group, generated by aH.

Example 4.17 Show that the set M of all $n \times n$ matrices with real elements is a non-commutative ring with unity with respect to matrix addition and matrix multiplication as binary operations.

The sum and product of two $n \times n$ real matrices are again $n \times n$ real matrices. Hence M is closed under matrix addition and matrix multiplication.

If $A, B \in M$, then $A + B = B + A$. Hence, the binary operation + (i.e., matrix addition) is commutative.

If $A, B, C \in M$, then $(A + B) + C = A + (B + C)$

Hence, matrix addition is associative.

If 0 is an $n \times n$ null matrix, then $A + 0 = 0 + A = A$, for every $A \in M$. Since $0 \in M$, 0 is the additive identity of $(M, +)$.

Corresponding to every $A \in M$, there exists a matrix $-A \in M$ such that

$$A + (-A) + (-A) + A = 0.$$

i.e., there exists an additive inverse for $(M, +)$.

If $A, B, C \in M$, then we can prove that

$$(AB)C = A(BC)$$

Hence, $(M, \times)$ is associative. Similarly we can prove that

$$A(B + C) = AB + AC \text{ and}$$
$$(B + C)A = BA + CA.$$

Thus, matrix multiplication is distributive over matrix addition

Hence, $(M, +, \times)$ is a ring.

In general, $AB \neq BA$. Hence $(M, +, \times)$ is a non-commutative ring.

If I is the $n \times n$ unit matrix, then $I \in M$ and $AI = IA = A$, for every $A \in M$.

Hence I is the multiplicative identity of $(M, +, \times)$ or $(M, +, \times)$ is a ring with unity.

Example 4.18 Prove that the set $Z_4 = (0, 1, 2, 3)$ is a commutative ring with respect to the binary operation $+_4$ and $\times_4$.

The composition tables for addition modulo 4 and multiplication modulo 4 are given in Tables 4.11(a) and 4.11(b).

Table 4.11(a)

$+_4$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

Table 4.11(b)

$\times_4$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

From the composition tables, we observe the following:

1. All the entries in both the tables belong to Z_4. Hence, Z_4 is closed under $+_4$ and $\times_4$.
2. The entries in the first row are the same as those of the first column in both the tables. Hence Z_4 is commutative with respect to both $+_4$ and $\times_4$.

3. If $a, b, c \in Z_4$, it is easily verified that
$$(a +_4 b) +_4 c = a +_4 (b +_4 c) \text{ and}$$
$$(a \times_4 b) \times_4 c = a \times_4 (b \times_4 c)$$
For example, $3 +_4 (1 +_4 2) = 3 +_4 3 = 2$
Also $(3 +_4 1) +_4 2 = 0 +_4 2 = 2$
and $3 \times_4 (1 \times_4 2) = 3 \times_4 2 = 2$
Also $(3 \times_4 1) \times_4 2 = 3 \times_4 2 = 2.$
Thus, associative law is satisfied for $+_4$ and $\times_4$ by Z_4.
4. $0 +_4 a = a +_4 0 = a$, for all $a \in Z_4$
and $1 \times_4 a = a \times_4 1 = a$, for all $a \in Z_4$
Hence 0 and 1 are the additive and multiplicative identities of Z_4.
5. It is easily verified that the additive inverses of 0, 1, 2, 3 are respectively 0, 3, 2, 1 and that the multiplicative inverses of the non-zero elements 1, 2, 3 are respectively 1, 2, 3.
6. If $a, b, c \in Z_4$, then it can be verified that
$$a \times_4 (b +_4 c) = a \times_4 b +_4 a \times_4 c$$
and $(b +_4 c) \times_4 a = b \times_4 a +_4 c \times_4 a$
For example,
$$2 \times_4 (3 +_4 1) = 2 \times_4 0 = 0$$
and $(2 \times_4 3) +_4 (2 \times_4 1) = 2 +_4 2 = 0$
i.e., $\times_4$ is distributive over $+_4$ in Z_4
Hence, $(Z_4, +_4, \times_4)$ is a commutative ring with unity.

Example 4.19 Show that $(Z, \oplus, \odot)$ is a commutative ring with identity, where the operations $\oplus$ and $\odot$ are defined, for any $a, b \in Z$ as $a \oplus b = a + b - 1$ and $a \odot b = a + b - ab$.

When $a, b \in Z$, $a + b - 1 \in Z$ and $a + b - ab \in Z$
Hence, Z is closed under the operations $\oplus$ and $\odot$.
$$b \oplus a = b + a - 1 = a + b - 1 = a \oplus b$$
$$b \odot a = b + a - ba = a + b - ab = a \odot b$$
Hence, Z is commutative with respect to the operations $\oplus$ and $\odot$.
If $a, b, c \in Z$, then
$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b + c - 2$$
and $a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 2$
Hence, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
Also
$$\begin{aligned}(a \odot b) \odot c &= (a + b - ab) \odot c \\ &= a + b - ab + c - (a + b - ab)\, c \\ &= a + b + c - ab - bc - ca + abc\end{aligned}$$
and
$$\begin{aligned}a \odot (b \odot c) &= a \odot (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - ab - bc - ca + abc\end{aligned}$$
Hence, $(a \odot b) \odot c = a \odot (b \odot c)$

Thus, associative law is satisfied by $\oplus$ and $\odot$ in Z.
If z is the additive identity of Z, then

$$a \oplus z = z \oplus a, \text{ for any } a \in Z$$

i.e., $a + z - 1 = a \quad \therefore z = 1$

If u is the multiplicative identity of Z then $a \odot u = u \odot a = a$
i.e., $a + u - au = a$
i.e., $u(1 - a) = 0$
$\therefore$ if $a \neq 1$, $u = 0$
Hence 1 and 0 are the additive and multiplicative identities of Z under $\oplus$ and $\odot$.
Now $a \oplus b = b \oplus a = 1$,
If $a + b - 1 = 1$
i.e., if $b = 2 - a$
$\therefore$ The additive inverse of $a \in Z$ is $(2 - a)$
Also $a \odot c = c \odot a = 0$,
If $a + c - ac = 0$
i.e., if $a + c(1 - a) = 0$
i.e., if $c = \dfrac{a}{a-1}$, $(a \neq 1)$

$\therefore$ The multiplicative inverse of a $(\neq 1) \in Z$ is $\dfrac{a}{a-1}$.

Finally, if $a, b, c \in Z$,

$$\begin{aligned} a \odot (b \oplus c) &= a \odot (b + c - 1) \\ &= a + b + c - 1 - a(b + c - 1) \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

and
$$\begin{aligned} (a \odot b) \oplus a \odot c &= (a + b - ab) \oplus (a + c - ac) \\ &= a + b - ab + a + c - ac - 1 \\ &= 2a + b + c - ab - ac - 1 \end{aligned}$$

Thus, $a \odot (b \oplus c) = a \odot b + a \odot c$.
Similarly, it can be verified that

$$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

Hence, $(Z, \oplus, \odot)$ is a commutative ring with identity.

Example 4.20 Prove that the set S of all ordered pairs (a, b) of real numbers is a commutative ring with zero divisors under the binary operations $\oplus$ and $\odot$ defined by

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

and $(a, b) \odot (c, d) = (ac, bd)$, where a, b, c, d are real.
Since, $a + c$, $b + d$, ac, bd are all real, S is closed under $\oplus$ and $\odot$.

$$\begin{aligned} (a, b) \oplus (c, d) &= (a + c, b + d) \\ &= (c + a, d + b) = (c, d) \oplus (a, b) \\ (a, b) \odot (c, d) &= (ac, bd) \\ &= (ca, db) = (c, d) \odot (a, b) \end{aligned}$$

Hence S is commutative under the operations $\oplus$ and $\odot$.

Let $(a, b), (c, d), (e, f) \in S$.

Now $[(a, b) \oplus (c, d)] \oplus (e, f)$
$= (a + c, b + d) \oplus (e, f)$
$= (a + c + e, b + d + f)$
$= [a + (c + e), b + (d + f)]$
$=(a, b) \oplus [c + e, d + f]$
$= (a, b) \oplus [(c, d) \oplus (e, f)]$

Thus, S is associative under $\oplus$.

Similarly it is associative under $\odot$. Now $(0, 0) \in S$.

$(a, b) \oplus (0, 0) = (0, 0) \oplus (a, b) = (a + 0, b + 0)$
$= (a, b)$

$\therefore$ $(0, 0)$ is the additive identity in S.

Also $(a, b) \odot (1, 1) = (1, 1) \odot (a, b) = (a, b)$

$\therefore$ $(1, 1)$ is the multiplicative identity in S.

If $(a, b) \in S$, $(-a, -b) \in S$, since a, b are real

Now $(a, b) \oplus (-a, -b) = (-a, -b) \oplus (a, b) = (0, 0)$

$\therefore$ $(-a, -b)$ is the additive inverse of (a, b)

Now $(a, b) \odot [(c, d) \oplus (e, f)]$
$= (a, b) \odot [c + e, d + f]$
$= a(c + e), b(d + f)$
$= (ac, bd) \oplus (ae, bf)$
$= (a, b) \odot (c, d) \oplus (a, b) \odot (e, f)$

Thus, the left distributivity holds.

Similarly the right distributivity also holds.

Now $(a, 0)$ and $(0, b) \in S$, where $a \neq 0, b \neq 0$

and $(a, 0) \odot (0, b) = (a \times 0, 0 \times b)$
$= (0, 0)$, which is the zero element of S.

But $(a, 0)$ and $(0, b)$ are not zero elements of S.

$\therefore$ $(a, 0)$ and $(0, b)$ are zero divisors of S.

Hence, $(S, \oplus, \odot)$ is a commutative ring with zero divisors.

Example 4.21 Prove that the set S of all real numbers of the form $a + b\sqrt{2}$, where a, b are integers is an integral domain with respect to usual addition and multiplication.

We can easily verify that S is closed with respect to addition and multiplication, S is commutative under $+$ and $\times$ and S is associative under $+$ and $\times$.

Let $c + d\sqrt{2}$ be the additive identity (zero) of $a + b\sqrt{2}$ in S.

Then $(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + b\sqrt{2}$

$\therefore$ $a + c = a$ and $b + d = b$

$\therefore$ $c = 0$ and $d = 0$

Hence, the zero element of S is $0 + 0\sqrt{2}$.

Let $e + f\sqrt{2}$ be the multiplicative identity (unity) of $a + b\sqrt{2}$ in S.

Then $(a + b\sqrt{2})\,(e + f\sqrt{2}) = a + b\sqrt{2}$

$\therefore$ $ae + 2bf = a$ and $af + be = b$

i.e., $2bf = a(1 - e)$ and $b(1 - e) = af$ (1)

Multiplying, we get $2b^2 f(1 - e) = a^2 f(1 - e)$

i.e., $(2b^2 - a^2) f(1 - e) = 0$

Since, a and b are arbitrary, $2b^2 - a^2 \neq 0$

$\therefore$ $f(1 - e) = 0$

$\therefore$ $f = 0$ or $1 - e = 0$

But, from (1), when $f = 0$, $e = 1$

$\therefore$ unity of S is $1 + 0\sqrt{2}$.

We can easily verify the distributive laws with respect to $\times$ and $+$ in S.

$\therefore$ $(S, +, \times)$ is a commutative ring with unity.

Let us now prove that this ring is without zero divisors.

Let $a + b\sqrt{2}$ and $c + d\sqrt{2} \in S$ such that

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 0 + 0\sqrt{2} \quad (2)$$

$\therefore$ $ac + 2bd = 0$ and $bc + ad = 0$

i.e., $(a - b)\,c + d(2b - a) = 0$ or

$(c - d)\,a + b(2d - c) = 0$

$\therefore$ Either $a = 0$ and $b = 0$ or $c = 0$ and $d = 0$

$\therefore$ $a + b\sqrt{2} = 0$ or $c + d\sqrt{2} = 0$, when (2) is true.

i.e., the ring has no zero divisors. Thus, $(S, +, \times)$ is an integral domain.

Example 4.22 If S is the set of ordered pairs (a, b) of real numbers and if the binary operations $\oplus$ and $\odot$ are defined by the equations

$$(a, b) \oplus (c, d) = (a + c, b + d)$$

and $$(a, b) \odot (c, d) = (ac - bd, bc + ad),$$

prove that $(S, \oplus, \odot)$ is a field.

As usual, the closure, associativity, commutativity and distributivity can be verified with respect to $\oplus$ and $\odot$ in S.

Also the additive and multiplicative identities can be seen to be $(0, 0)$ and $(1, 0)$ respectively.

Hence, $(S, \oplus, \odot)$ is a commutative ring with unity.

Let (a, b) be a non-zero element of S, i.e., a and b are not simultaneously zero.

Let (c, d) be the multiplicative inverse of (a, b).

Then $(a, b) \odot (c, d) = (1, 0)$

i.e., $(ac - bd, bc + ad) = (1, 0)$

$\therefore$ $ac - bd = 1$ and $bc + ad = 0$

Solving these equations for c and d, we get

$$c = \frac{a}{a^2+b^2} \text{ and } d = -\frac{b}{a^2+b^2}$$

$a^2 + b^2 \neq 0$, since a and b are not simultaneously zero.

$\therefore$ c or d or both are non-zero real numbers.

$\therefore$ $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ is the multiplicative inverse of (a, b)

Hence, $(S, \oplus \odot)$ is a field.

Example 4.23 If M is the set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$, where $a, b \in Z$ and Z is the set of integers, show that $(M, \oplus \odot)$ and $(Z, +, \times)$ are rings where $\oplus$ and $\odot$ represent matrix addition and matrix multiplication. Show that the mapping f: $M \to Z$ given by $f\left(\begin{bmatrix} a & b \\ b & a \end{bmatrix}\right) = a - b$ is a homomorphism.

The reader can verify that $(M, \oplus, \odot)$ and $(Z, +, \times)$ are rings.

Let $M_1 = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$ and $M_2 = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$

Now
$$f(M_1 \oplus M_2) = f\left(\begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix}\right)$$
$$= (a + c) - (b + d), \text{ by definition}$$
$$= (a - b) + (c - d)$$
$$= f(M_1) + f(M_2)$$

$$f(M_1 \odot M_2) = f\left(\begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix}\right)$$
$$= (ac + bd) - (ad + bc)$$
$$= (a - b) \times (c - d)$$
$$= f(M_1) \times f(M_2)$$

Hence, f is a ring homomorphism.

Example 4.24 Show that the set of matrices of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.

Let R be the ring of 2×2 matrices with integral elements and let R' be the subset of R consisting elements of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$.

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ be any two elements of R'.

Then $A - B = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix}$ belongs to R'

Also $AB = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{bmatrix}$ belongs to R'.

Hence, by property (8) of rings, R' is a subring of R under matrix addition and matrix multiplication.

EXERCISE 4(B)

Part A: (Short answer questions)

1. Define subgroup and proper subgroup.
2. State the condition for a subset of a group to be a subgroup.
3. Prove that the identity of a subgroup is the same as that of the group.
4. Prove that the inverse of any element of a subgroup is the same as the inverse of that element regarded as an element of the group.
5. Is the subset $\{1, 2, 2^2, 2^3, \ldots\}$ of the multiplicative group $\{\ldots, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, \ldots\}$ a subgroup?
6. Prove that $(E, +)$ is a subgroup of the group $(Z, +)$, where Z is the set of integers and E is the set of even integers.
7. Find all the subgroups of a group G of prime order.
8. Define group homomorphism and group isomorphism.
9. If G is a group with identity e, show that the mapping $f : G \to G$ defined by $f(a) = a$, for every $a \in G$ is a homomorphism.
10. Show that every homomorphic image of an abelian group under multiplication is also abelian.
11. If R^+ is the group of non-zero real numbers under multiplication and n is a positive integer, show that $f(x) = x^n$ is a homomorphism from R^+ to R^+.
12. If G is a group of real numbers under addition and G' is the group of positive real numbers under multiplication, show that the mapping defined by $f(x) = 2^x$ is a homomorphism.
13. If $(G, *)$ is a group, $a \in G$ and the mapping $f : G \to G$ is given by $f(x) = a * x * a^{-1}$ for every $x \in G$, prove that f is an isomorphism of G onto G.
14. Define the kernel of group homomorphism.
15. Define left and right cosets of a subgroup. When will they be the same?
16. State Lagrange's theroem in group theory.
17. If H is a finite subgroup of group G, show that H and any coset Ha have the same number of elements.
18. Find the left cosets of $\{[0], [3]\}$ in the group $(z_6, +_6]$.

19. Define normal subgroup and state a condition for a subgroup of a group to be normal.
20. Show that every subgroup of an abelian group is normal.
21. Define quotient group.
22. Define a ring and give an example of a ring.
23. Define a commutative ring and a ring with unity.
24. Define an integral domain and give an example.
25. Define a field with an example.
26. If $a, b, \in R$, where $(R +, \bullet)$ is a ring, show that
$$(a + b)^2 = a^2 + a \bullet b + b \bullet a + b^2.$$
27. If R is a Boolean ring such that $a^2 = a$ for every a, show that R is commutative.
28. If R is a Boolean ring, show that each element of R is its own additive inverse.
29. Define ring homomorphism.
30. Define subring and give an example.

Part B

31. If H is the subset of the additive group of integers $(G, +)$ whose elements are multiples of integers by a fixed integer m, show that H is a subgroup of G.
32. Prove that the set H of all elements a of a group $(G, *)$ such that $a * x = x * a$, where x is some (fixed) element of G is a subgroup of G.
[*Hint:* Verify that H is non-empty, satisfies closure and every element of H has an inverse in H]
33. Show that the set $\{a + bi \in C | a^2 + b^2 = 1\}$ is a subgroup of $(C, \bullet)$ where $\bullet$ is the multiplication operation of complex numbers.
[*Hint:* Verify that, if $a + bi$ and $c + di \in H$, then $(a + bi)(c + di)^{-1} \in H$]
34. If H is subgroup of a group G, prove that $aHa^{-1} = \{aha^{-1} | a \in G; h \in H\}$ is also a subgroup of G.
[*Hint:* Verify that $(ah_1a^{-1})\ (ah_2a^{-1})^{-1} \in aHa^{-1}$]
35. If $*$ is defined on $S = N \times N$ by
$$(a, b) * (a^1, b^1) = (a + a^1, b + b^1)$$
and if the mapping f: $(S, *) \to (Z, +)$ is defined by $f(a, b) = a - b$, show that f is a homomorphism.
36. If C^* is the multiplication group of non-zero complex numbers and if the mapping f: $C^* \to C^*$ is defined by $f(z) = z^4$, show that f is a homomorphism with kernel $= \{1, -1, i, -i\}$.
37. If R is the additive group of real numbers and C^* is the multiplication group of complex numbers whose modulus is unity, prove that the mapping $f : R \to C^*$ given by $f(x) = e^{ix}$ is a homomorphism. Find the kernel of f.
38. If C^* and R^* are multiplication groups of non-zero complex numbers and non-zero real numbers respectively and if the mapping $f : C^* \to R^*$ is

defined by $f(z) = |z|$. Show that f is a homomorphism. What is the kernel of f?

39. Show that $(H, *)$ is a subgroup of the symmetric group $(S_3, *)$ of degree 3, where $H = \{p_1, p_3, p_5\}$. Find also the right cosets of H in G.
40. If G is the additive group of integers and H is a subgroup of G, defined by $H = \{5x \mid x \in G\}$, find the distinct left cosets of H in G.
41. If H is a subgroup of a group G and K is a normal subgroup of G, show that $H \cap K$ is a normal subgroup of H.
42. Show that $\{p_1, p_2\}$, $\{p_1, p_4\}$, $\{p_1, p_6\}$ are subgroup of the symmetric group $(S_3, *)$ of degree 3. Are they normal subgroups?
43. Find whether the subgroup $H = \{p_1, p_3, p_5\}$ of $(S_3, *)$ is a normal subgroup of S_3.
44. If G is a finite group and H is a normal subgroup of G, show that $0(G/H) = 0(G) \div 0(H)$, where G/H is the quotient group.
45. Show that every quotient group of an abelian group is abelian.
46. Show that $(z_6, +_6, \times_6)$ is a commutative ring.
47. Find all the values of the integers m and n for which $(Z \oplus, \odot)$ is a ring under the binary operations $a \oplus b = a + b - m$ and $a \odot b = a + b - nab$, where $a, b \in Z$.
48. Show that $(Z, \oplus, \odot)$ is a commutative ring with identity, where the operations $\oplus$ and $\odot$ are defined, for any $a, b \in z$, as $a \oplus b = a + b + 1$ and $a \odot b = a + b + ab$.
49. Show that $(Q, \oplus, \odot)$ is a ring, where $\oplus$ and $\odot$ are defined, for any $a, b \in Q$, as $a \oplus b = a + b + 7$ and $a \odot b = a + b + (ab/7)$.
50. Prove that the set M of 2×2 real matrices is a ring with zero divisors.
51. Show that the set of complex numbers $a + ib$, where a and b are integers is an integral domain under ordinary addition and multiplication.
52. Show that the set of complex numbers of the form $a + b\sqrt{-5}$, where a, b, are integers is an integers is an integral domain.
53. Show that the set of numbers of the from $a + b\sqrt{2}$, where a and b are rational numbers is a field.
54. If R' is the set of all even integers and $*$ is defined by $a * b = \frac{ab}{2}$; $ab \in R'$. Show that $(R', +, *)$ is a commutative ring. If R is the ring of integers under ordinary addition and multiplication, prove that R is isomorphic to R'.
55. If M is the set of matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ where a, b are real numbers, show that M is a subring of the ring R of all 2×2 real matrices.
56. Show that $S = \{[0], [2], [4]\}$ and $T = \{[0], [3]\}$ are subrings of the ring $(Z_6, +_6, \times_6)$ and that every of Z_6 can be expressed as $s +_6 t$, where $s \in S$ and $t \in T$.

CODING THEORY

Introduction

The process of communication involves transmitting some information carrying signal (message} that is conveyed by a sender to a receiver. Even though the sender may like to have his message received by the receiver without any distortion, it is not possible due to a variety of disturbances (noise) to which the communication channel is subjected. Coding theory deals with minimizing the distortions of the conveyed message due to noise and to retrieve the original message to the optimal extent possible from the corrupted message.

ENCODERS AND DECODERS

An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable. A *decoder* is a device which transforms the encoded message into their original form that can be understood by the receiver. By using a suitable encoder and decoder, it may be possible to detect the distortions in the messages due to noise in the channel and to correct them. The model of a typical data communication system with noise is given in Fig. 4.4.

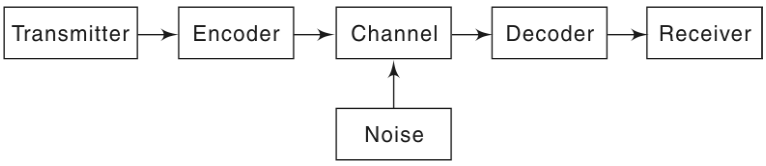


Fig. 4.4

The input message which consists of a sequence of letters, characters or symbols from a specified set (called alphabet) will be transformed by the encoder into a string of characters or symbols of another alphabet in a one-to-one fashion. In our discussion, we will deal with only a binary channel in which the encoder will transform an input message into a binary string consisting of the symbols 0 and 1. Decoding is only the inverse operation of encoding.

GROUP CODE

Definition

If $B = \{0, 1\}$, then $B^n = \{x_1, x_2, \ldots x_n | x_i \in B, i = 1, 2, 3, \ldots n\}$ is a group under the binary operation of addition modulo 2, denoted by $\oplus$. This group $(B^n, \oplus)$ is called a *group code*.

Let us now prove that $(B^n, \oplus)$ is a group.

If $x_1\ x_2 \ldots x_n \equiv (x_1, x_2 \ldots x_n)$ and $y_1y_2,\ldots,y_n \equiv (y_1, y_2 \ldots, y_n) \in B^n$, then

$x_1\ x_2 \ldots x_n \oplus y_1, y_2 \ldots y_n = (x_1 +_2 y_1, x_2 +_2 y_2 \ldots, x_n +_2 y_n) \in, B^n$

since $x_i +_2 y_i = 1$ or 0, as $0 +_2 0 = 0$, $0 +_2 1 = 1$, $1 +_2 0 = 1$ and $1 +_2 1 = 1$.

Note The operation $+_2$ is also called binary addition.

(0, 0, 0, …, 0) is the identity element of B^n. Also the inverse of $x_1x_2 \ldots x_n$ is itself.

Hence, $(B^n, \oplus)$ is a group—it is abelian.

In general, any code which is a group under the operation $\oplus$ is called a group code.

HAMMING CODES

The codes obtained by introducing additional digits called *parity digits* to the digits in the original message are called Hamming codes. If the original message is a binary string of length m, the Hamming encoded message is string of length n, $(n > m)$. Of the n digits, m digits are used to represent the information part of the message and the remaining $(n - m)$ digits are used for the detection and correction of errors in the message received.

In Hamming's single-error detecting code of length n, the first $(n - 1)$ digits contain the information part of the message and the last digit is made either 0 or 1. If the digit introduced in the last position gives an even number/odd number of 1's in the encoded word of length n, the extra digit is called an *even/odd parity check*.

For example, when a single even parity check is appended, the words 000, 001, 010, 011, 100, 101, 110 and 111 become 0000, 0011, 0101, 0110, 1001, 1010, 1100 and 1111. On the other hand, when an odd parity is appended to each of the above words, they will become 0001, 0010, 0100, 0111, 1000, 1011, 1101 and 1110.

We note that a single mistake in a word, say, 0000 produces another word 0001 or 0010 or 0100 or 1000. None of these words appear in the set of 8 words transmitted. Hence, it is an indication that an error has occurred in transmission. However, it is not possible to correct the error, as, for example, 0001 might have been got from any of the words 0000, 0011, 0101, 1001 due to a single error.

An error correcting method based on parity checks that helps the detection of positions of erroneous digits, as developed by Hamming will be discussed later.

Definitions

1. The number of 1's in the binary string $x \in B^2$ is called the weight of x and is denoted by $|x|$.
2. If x and y represent the binary strings $x_1\, x_2\, x_3 \ldots x_n$ and $y_1\, y_2\, y_3 \ldots y_n$, the number of positions in the strings for which $x_i \neq y_i$ is called the *Hamming distance* between x and y and denoted by $H(x, y)$.
   Obviously $H(x, y)$ = weight of $x \oplus y$

$$= \sum_{i=1}^{n} (x_i +_2 y_i).$$

For example, if $x = 11010$ and $y = 10101$, then

$$H(x, y) = |x \oplus y| = |01111| = 4$$

3. The minimum distance of a code (a set of encoded words) is the minimum of the Hamming distances between all pairs of encoded words in that code.

   For example, if $x = 10110$, $y = 11110$ and $z = 10011$, then

   $H(x, y) = 1$, $H(y, z) = 3$ and $H(z, x) = 2$ and so the minimum distance between these code words = 1.

Note The term 'code' used above is sometime called an (m, n) *encoding function*, which is a one-to-one function $e: B^m \to B^n$ (where $n > m$). If $b \in B^m$ is the original word, them $e(b)$ is the code word or encoded word representing b.

Theorem

A code [an(m, n) encoding function] can detect at the most k errors if and only if the minimum distance between any two code words is at least $(k + 1)$.

Proof

A set (combination) of errors in various digit positions cannot be detected if and only if the set transforms a code word x into another code word y.

Since, the minimum distance between any two code words is at least $(k + 1)$, a set of at least $(k + 1)$ errors would be required to change the code word x into the code word y.

Hence, if the code word x is transformed to the word y due to at least $(k + 1)$ errors, almost k errors can be detected.

Example

Let 000 and 111 be the encoded words, viz., two values of the encoding function.

These two code words differ in 3 digits, viz. the distance between them is 3.

If one error occurs during transmission, the word 000 would have become 100 or 010 or 001, whereas the word 111 would have been received as 011 or 101 or 110. The two sets of received words are disjoint.

Hence, if any of the above six words is received due to one error, it is easily found out which encoded word has get altered and in which digit position the error has occurred and hence, the error is corrected. On the other hand if two errors occur during transmission, the word 000 would have been received as 110 or 011 or 101, whereas the word 111 would have been received as 001 or 100 or 010. If an error in a single digit is corrected in any of the received words 110, 011 and 101, the corrected word would be 111, which is not the transmitted word.

Similarly if a single error correction is made in any of the received words 001, 100 and 010, the corrected word would be 000, which is not the transmitted word. Hence error correction is not possible.

Theorem

A code can correct a set of at the most k errors if and only if the minimum distance between any two code words is at least $(2k + 1)$.

Proof

Let the code correct at the most k errors.

Then we have to prove that the minimum distance between any two code words is at least $2k + 1$.

If possible, let there be at least one pair of code words, say x and y such that $H(x, y) < 2k + 1$.

By the previous theorem, $H(x, y) \geq k + 1$, as otherwise the k errors cannot even be detected.

$\therefore$ $$k + 1 \leq H(x, y) \leq 2k \quad (1)$$

Let x' be another word which differs from x in exactly k digits, which form a subset of the set of the digits in which x and y differ i.e.,

$$H(x, x') = k \quad (2)$$

Since, $H(x, x')$, $+ H(x', y) \geq H(x, y)$, we have from (1) and (2), $H(x', y) \leq k$.

$\therefore$ By the previous theorem, the code can detect at the most $(k - 1)$ errors.

Thus, we get a contradiction.

$\therefore$ $$H(x, y) \geq 2k + 1.$$

Converse: Let us assume that $H(x, y) \geq 2k + 1$.

Let x be a code word and x' be a received erroneous word with at most k errors. If a decoding rule correctly decodes x' as x, then x' is nearer to x than any other word y.

Since, $$H(x, x') + H(x', y) \geq H(x, y), \quad \text{we get}$$
$$H(x', y) \geq k + 1 \quad [\because H(x, y) \geq 2k + 1 \text{ and } H(x, x') \leq k]$$

This means that every code word y is farther away form x' than x.

Hence x' can be correctly decoded.

Example

Let us consider the encoded words 000 and 111. These words differ in 3 digits. So zero or one error can be corrected.

If zero or one error occurs during transmission, 000 would have become any one of 000, 100, 010 and 001 and 111 would have become any one of 111, 011, 101 and 110. These two sets of received words are disjoint. So whatever be the words received, the single or no error can be easily detected and corrected.

Basic Notions of Error Correction using Matrices

When $m, n \in Z^+$ and $m < n$, the encoding function e: $B^m \to B^n$, where $B \equiv (0, 1)$ is given by a $m \times n$ matrix G over B. This matrix G is called the *generator matrix* for the code and is of the form $[I_m|A]$, where I_m is the $m \times m$ unit matrix and A is an $m \times (n - m)$ matrix to be chosen suitably. If w is a message $\in B^m$, then $e(w) = wG$ and the code (the set of code words) $C = e(B^m) \subseteq B^n$, where w is a $(1 \times m)$ vector. For example, if the message $w \in B^2$, we may assume G

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Note Now row of A has only zeros or only 1.

The words that belong to B^2 are 00, 10, 01 and 11. Then the code words corresponding to the above message words are respectively

$$e(00) = [0\ 0]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [00\ 000]$$

$$e(10) = [1\ 0]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [10\ 110]$$

$$e(01) = [0\ 1]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [01\ 011]$$

$$e(11) = [1\ 1]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix} = [111\ 01]$$

Note While getting wG, the modulo 2 arithmetic is to be used.

Clearly $C = e(B^2) \subseteq B^5$.

We observe that we can get back the message word from the corresponding code word by dropping the last 3($= n - m$) digits.

For all $w = x_1\ x_2 \in B^2$

$$e(w) = x_1\ x_2\ x_3\ x_4\ x_5 \in B^5 \tag{1}$$

where $x_i \in B$.

Since, $$e(w) = wG = [x_1\ \ x_2]\begin{bmatrix}1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1\end{bmatrix}$$

$$= [x_1, x_2, x_1, x_1 + x_2, x_2] \tag{2}$$

From (1) and (2), we have $x_1 = x_3$, $x_1 + x_2 = x_4$ and $x_2 = x_5$ (3)

Since, $x_i \in B$, by modulo 2 arithmetic $-x_i \pmod 2 = (-x_i + 2x_i) \pmod 2$.

Hence, the equations (3) become

$$\left.\begin{aligned} x_1 \quad\quad + x_3 \quad\quad &= 0\\ x_1 + x_2 \quad\quad + x_4 \quad &= 0\\ x_2 \quad\quad\quad + x_5 &= 0\end{aligned}\right\} \tag{4}$$

i.e., $$\begin{bmatrix}1 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ x_3\\ x_4\\ x_5\end{bmatrix} = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix}$$

i.e., $$H \cdot [e(w)]^T = \begin{bmatrix}0\\ 0\\ 0\end{bmatrix} \tag{5}$$

The $(n - m)$ equations in (3) are called *the parity check equations*.
The matrix H in (5) is called *the parity check matrix*.
We note that H is an $(n - m) \times n$ matrix, whereas G is an $m \times n$ matrix.
Also $H = [A^T | I_{n-m}]$. In the present example

$$A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } I_{n-m} = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

We also note that H does not contain a column of only 0's and no two columns of H are the same. This is achieved by a careful choice of A. This unique parity check matrix H provides a decoding scheme that corrects a single error in transmission as explained below:

(i) If r is a received word considered as $a(1 \times n)$ matrix and if $H \cdot r^T = [0]$, then we conclude that there is no error in transmission and that r is the code word transmitted. The decoded (original) message then consists of the first m components of r.

In the present example, if $r = [1\ 1\ 1\ 0\ 1]$, then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Hence, r is itself the code word transmitted and the decoded message is 11 (got by taking the first $(m =)2$ components of r).

(ii) If $H \cdot r^T =$ the i^{th} column of H, then we conclude that a single error has occurred during transmission and it has occurred in the i^{th} component of r. Changing the i^{th} component of r, we get the code word c transmitted. As before the first m components of c give the original message.

In the present example if $r = [11\ 011]$, then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Since, $H\, r^T =$ the first column of H, a single error has occurred in the first component of r. Changing the first component of r, we get the code word transmitted as 01011. Taking the first 2 components of the code word, we get 01 as the original message.

(iii) If neither case (i) nor case (ii) occurs then we conclude that more than one transmission error have occurred. Though detection of errors is possible in this case, correction is not possible.

In the present example, if r = [11 010], then

$$H \cdot r^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Since, $H \cdot r^T \neq$ any column of H, more than one transmission error has occurred.

Since $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ = 1st column of H + 5th column of H,

2 errors have occurred in transmission, one in the first component and the other in the fifth component of r. Changing these components in r, the code word transmitted may be assumed as 01 011 and hence the original message may be taken as 01.

Also $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ = the 2nd column of H + the 3rd column of H.

Hence, 2 errors might have occurred, one in the 2nd component and the other in the 3rd component of r. Changing these components in r, the code word transmitted may be assumed as 10110 and hence, the original message may be taken as 10. Thus, there is an ambiguity as to which message has been encoded and transmitted. In other words, the correction of errors is not possible, even though errors have been detected.

We note that the minimum distance between any pair of code words is 3 in the present example. Hence, according to the two previous theorems, atmost 2 errors can be detected and atmost 1 error can be corrected. We have verified the same in the examples considered above.

ERROR CORRECTION IN GROUP CODES

We have already introduced a group code, that is any code which is a group under the binary operation of addition modulo 2, denoted by $\oplus$. In general when the code words form a group, it is easier to find the minimum distance between code words, using the following theorem.

Theorem

In a group code, the minimum distance between distinct code words is the minimum weight of the non zero code words in it.

Proof

Let a, b, c be 3 members of a group code C, such that $a \neq b$, $H(a, b)$ is minimum and c is a non zero element with minimum weight.

Now $a \oplus b \in C$, by closure property in the group C.

As already seen, $H(a, b) = \text{Wt}(a \oplus b)$

Since the weight of c is minimum, we have

$$H(a, b) \geq \text{Wt}(c) \tag{1}$$

Also $\text{Wt}(c) = H(c, 0)$, where 0 is the identity element of c.

Now $H(c, 0) \geq H(a, b)$, since, $H(a, b)$ is the minimum

i.e., $$\text{Wt}(c) \geq H(a, b) \tag{2}$$

From (1) and (2), it follows that $H(a, b) = \text{Wt}(c)$.

The parity check matrix H defined in the previous section satisfies

$$H \cdot [e(w)]^T = [0],$$

where $e(w)$ is a code word and [0] is a column matrix consisting of 0's. Conversely, if $x = [x_1, x_2 \ldots x_n]$ satisfies

$H \cdot [x]^T = [0]$, where H is an $(n - m) \times n$ matrix, $[x]$ is a $1 \times n$ row matrix and [0] is an $(n - m) \times 1$ column matrix, then x is a code word.

The following two theorems will show that H always defines a group code and the minimum weight of the code can be obtained from H.

Theorem

If H is a parity check matrix with $n - m$ rows and n columns, then the set C of code words $x = (x_1\ x_2 \ldots x_n)$ such that $C = \{x | H \cdot [x]^T = [0], \text{ modulo } 2\}$ is a group code under the operation $\oplus$.

Proof

Since, $$[H]_{n-m \times n} \cdot [0]^T_{n \times 1} = [0]_{m-n \times 1},\ [0]_{1 \times n} \in C.$$

If $x, y, \in C$, then $H \cdot [x]^T = [0]$ and $H \cdot [y]^T = [0]$

$\therefore$ $$H \cdot [x^T \oplus y^T] = [0]$$

i.e., $$H[x \oplus y]^T = [0]$$

$\therefore$ $x \oplus y \in C$ satisfies the closure property.

Similarly the associativitly is satisfied by $\oplus$.

Since $(x \oplus x)^T = [0]$ or $x \oplus x = [0]^T$, every element x in C is its own inverse. Hence, $[C, \oplus]$ is a group code.

Theorem

The parity check matrix H generates a code word of weight q if and only if there exists a set of q columns of H such that their k-tuple sum (mod 2) is a zero column, where $k = n - m$.

Proof

In the code word x generated by H let the components $x_{i1}, x_{i2}, \ldots x_{iq}$ be 1 each and the remaining components be 0 each.

Note The components $x_{i1}, x_{i2}, \ldots, x_{in}$ of x are the same as the components $x_1, x_2, \ldots, x_n$ written in a different order.

Now the weight of the code word x is q.

Since $H \cdot [x]^T = [0]$, we get

$$h_{i1} \oplus h_{i2} \oplus \ldots \oplus h_{iq} = 0, \text{ where}$$

$h_{i1}, h_{i2}, \ldots, h_{iq}$ are the elements of any row of H corresponding to the positions of $x_{i1}\ x_{i2}, \ldots, x_{iq}$ in x.

As the above result is true for all the $k = n - m$ rows for H, the result follows:

Conversely, let us assume that there is a set of q distinct columns of H such that $h_{i1} \oplus h_{i2} \oplus \cdots \oplus h_{iq} = 0$ for all the rows (where $h_{i1}, h_{i2}, \ldots, h_{iq}$ are the elements of any row in the q columns). Then we can chosen $x = [x_{i1}, x_{i2}, \ldots, x_{in}]$ such that $x_{i1}, x_{i2}, \ldots, x_{iq}$ are 1 each and the remaining components are 0 each.

Then x will satisfy the equation

$$H[x]^T = [0]$$

This means that x is a code word of weight q generated by H.

Example

Let us consider the example considered in the previous section on "error correction using parity check matrix".

In that example, we established that

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now it is obvious that the sum of the 1st, 2nd, 3rd and 5th columns of H (mod 2) is the zero column.

The weight of the corresponding code word [1 1 1 0 1] is 4, that verifies the above theorem.

STEP BY STEP PROCEDURE FOR DECODING GROUP CODES

Step 1

We list in a row all the code words in C, starting with the identity.

Thus, we have $c_1(=0)\ c_2\ c_3\ \ldots\ c_{2^m}$

For clarity, we shall write the corresponding step with respect to the problem discussed in the previous section, in which $m = 2$

i.e., 0 0 0 0 0 1 0 1 1 0 0 1 0 1 1 1 1 1 0 1

Step 2

We select some word $y_j \in B^n$ but not in C having minimum weight and construct a new row or coset $y_j \oplus c_i$ for all i such that $1 \le i \le 2^m$.

Thus, we have

$$y_j \oplus c_1 \; y_j \oplus c_2 \; y_j \oplus c_3 \; \ldots \; y_j \oplus c_{2^m}$$

i.e., $$y_2 \quad y_2 \oplus c_2 \; y_2 \oplus c_3 \; \ldots \; y_2 \oplus c_{2^m}$$

In the example, if $y_2 = 10000$, then the second row would be

1 0 0 0 0 0 0 1 1 0 1 1 0 1 1 0 1

Step 3

We now form the third row by selecting some $y_k \in B^n$ which is not in the preceding two rows and which has the minimum weight and proceeding as in step 2.

Thus we have

$$y_3 \quad y_3 \oplus c_2 \; y_3 \oplus c_3 \; \ldots \; y_3 \oplus c_{2^m}$$

In the example, if $y_3 = 0\ 1\ 0\ 0\ 0$, then the third row would be

0 1 0 0 0 1 1 1 1 0 0 0 0 1 1 1 0 1 0 1

Step 4

This process is continued until all the elements in B^n are entered in the table. The complete decoding Table 4.12 will be of the form.

Table 4.12

c_1 (= 0)	c_2	c_3	…	c_{2^m}
y_2	$y_2 \oplus c_2$	$y_2 \oplus c_3$	…	$y_2 \oplus c_{2^m}$
y_3	$y_3 \oplus c_2$	$y_3 \oplus c_3$	…	$y_3 \oplus c_{2^m}$
…	…	…	…	…
$y_{2^{n-m}}$	$y_{2^{n-m}} \oplus c_2$	$y_{2^{n-m}} \oplus c_3$	…	$y_{2^{n-m}} \oplus c_{2^m}$

For the example in consideration, the complete decoding table is given in Table 4.13.

Table 4.13

0 0 0 0 0	1 0 1 1 0	0 1 0 1 1	1 1 1 0 1
1 0 0 0 0	0 0 1 1 0	1 1 0 1 1	0 1 1 0 1
0 1 0 0 0	1 1 1 1 0	0 0 0 1 1	1 0 1 0 1
0 0 1 0 0	1 0 0 1 0	0 1 1 1 1	1 1 0 0 1
0 0 0 1 0	1 0 1 0 0	0 1 0 0 1	1 1 1 1 1
0 0 0 0 1	1 0 1 1 1	0 1 0 1 0	1 1 1 0 0
1 1 0 0 0	0 1 1 1 0	1 0 0 1 1	0 0 1 0 1
1 0 0 0 1	0 0 1 1 1	1 1 0 1 0	0 1 1 0 0

Note The elements in the first row of the decoding table are the code words, whereas the elements in the first column are the *coset leaders*, which represent the errors that occur during transmission.

Step 5

Once the decoding table is constructed, the decoding of any received word r is done as follows. First we identify the column of the decoding table in which r occurs. If the weight of the coset leader corresponding to r is 1, then the decoded word (viz. the coded word transmitted) is the element at the top of the column in which r occurs.

In the current example, if the received word is 11011, we note that it lies in the 3rd column and 2nd row of the table. Since, the weight of the coset leader in the 2nd row is 1, the decoded word is 01011 that lies at the top of the 3rd column. The corresponding message transmitted is 01.

Note If, by chance the received word happens to lie at the top of any column (or in the first row) of the decoding table, no error has occurred during transmission and the received word itself is the coded word transmitted.

Step 6

If the weight of the coset leader corresponding to the received word r is 2, the decoding cannot be done, viz., the coded word transmitted cannot be determined uniquely, as two coded words might have been received as the same word r due to 2 errors during transmission, as explained below with respect to the current example.

If the received word is 1 1 0 1 0, the weight of the corresponding coset leader is 2 and hence, the top element in the 3rd column, namely, 0 1 0 1 1 cannot be taken as the code word transmitted for the following reason.

After filling up the first 7 rows of the decoding table, the words belonging to B^5 with weight 2 and not included in the table are 10001 and 01100. We have constructed the 8th row by taking coset leader as 10001. Instead had we taken 0 1 1 0 0 as the coset leader of the 8th row, it would have become

0 1 1 0 0 1 1 0 1 0 0 0 1 1 1 1 0 0 0 1

Now as per the alternative 8th row of the decoding table, the received word 1 1 0 1 0 occurs in the record column. The top element in that column is 1 0 1 1 0 and this too can be taken as the code word transmitted. Thus if 2 errors occur during transmission, they can be detected but not corrected.

WORKED EXAMPLES 4(C)

Example 4.1 A binary symmetric channel has probability $p = 0.05$ of incorrect transmission. If the code word c = 011 011 101 is transmitted, what is the probability that (a) we receive r = 011 111 101? (b) we receive r = 111 011 100? (c) a single error occurs? (d) a double error occurs? (e) a triple error occurs?

(a) The received word r = 011 111 101 differs from the transmitted word c = 011 011 101 only in the fourth position.

The probability of occurrence of this specific error

$$= P(1 \text{ error and } 8 \text{ non-errors})$$
$$= 0.05 \times (0.95)^8 = 0.0332.$$

(b) The received word $r = 111\ 011\ 100$ differs from the transmitted word $c = 011\ 011\ 101$ only in the first and ninth positions.

The probability of occurrence of these specific error

$$= P(2 \text{ errors and } 7 \text{ non-errors})$$
$$= (0.05)^2 \times (0.95)^7 = 0.0017.$$

(c) P(1 error in any one position and 8 non-errors in the remaining positions)

$= "nC_1 \cdot p' \cdot q^{n-1}"$, by Bernoulli's theorem in Probability theory

$$9C_1 \times (0.05)^1 \times (0.95)^8 = 0.2985$$

(d) P(2 errors in any two positions and 7 non-errors in the remaining positions)

$$= 9C_2 \times (0.05)^2 \times (0.95)^7 = 0.0629.$$

(e) P(3 errors in any three positions and 6 non-errors in the remaining positions)

$$= 9C_3 \times (0.05)^3 \times (0.95)^6 = 0.0077$$

Example 4.2 The (9, 3) three times repetition code has the encoding function $e = B^3 \to B^9$, where $B = (0, 1)$.

(a) If d: $B^9 \to B^3$ is the corresponding decoding function, apply 'd' to decode the received words (i) 111 101 100, (ii) 000 100 011; (iii) 010 011 111 by using the majority rule.

(b) Find three different received words r for which $d(r) = 000$

(a) *Triple repetition code* means that when we encode a word $w = B^m$, all the m elements of w are repeated three times so as to produce $e(w) \in B^{3m}$.

To decode any received word by the *majority rule* we examine the 1st, 4th and 7th positions and note down the element (0 or 1) which appear more times. This process is continued with 2nd, 5th and 8th positions, 3rd, 6th and 9th positions and so on and finally with m^{th}, $(2m)^{th}$ and $(3m)^{th}$ positions. The m elements thus noted down are written in the order to give the original word.

(i) The received word is 111 101 100.

Among the elements in the 1st, 4th and 7th positions, 1 appears all the three times. Hence 1 is taken as the first element of the original word.

Among the elements in the 2nd, 5th and 8th positions, 0 appears twice. Hence 0 is taken as the second element of the original word. Among the elements in the 3rd, 6th and 9th positions, 1 appears twice. Hence 1 is taken as the third element of the original word.

$\therefore \quad d(111\ 101\ 100) = 101$

(ii) Similarly $d(000\ 100\ 011) = 000$

(iii) $d(010\ 011\ 111) = 011$

(b) Since $d(r) = 000$, 0 must appear more times in the 1st, 4th and 7th positions and similarly in the 2nd, 5th and 8th positions and in the 3rd, 6th and 9th positions.

One set of such three words is:

100 000 000, 000 010 000, 000 000 001.

Example 4.3 Find the code words generated by the encoding function e: $B^2 \to B^5$ with respect to the parity check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Note In our discussion, if the encoding function is e: $B^m \to B^n$, the generator matrix was assumed as an $m \times n$ matrix $G = [I_m|A]$ and the parity check matrix was assumed as an $(n - m) \times m$ matrix $H = [A^T|I_{n-m}]$ and as such there was less number of rows and more number of columns in H. We shall stick to our notation. As per our notation, what is given in this problem is not H, but H^T. However some authors use this notation to denote the parity check matrix.

Rewriting the given matrix as per our notation, we have

$$H = \left[\begin{array}{cc|ccc} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T|I_{n-m}]$$

Here $n = 5$ and $m = 2$.

Hence, the generator matrix G is given by

$$G = [I_m|A] = \left[\begin{array}{cc|ccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Now $B^2 \equiv \{0\ 0, 0\ 1, 1\ 0, 1\ 1\}$ and $e(w) = w\ G$

$$\therefore \quad e(0\ 0) = [0\ 0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 0\ 0\ 0\ 0]$$

$$\therefore \quad e(0\ 1) = [0\ 1]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 1\ 0\ 1\ 1]$$

$$\therefore \quad e(1\ 0) = [1\ 0]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 0\ 0\ 1\ 1]$$

$$\therefore \quad e(1\ 1) = [1\ 1]\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [1\ 1\ 0\ 0\ 0]$$

Hence, the code words generated by H are 0 0 0 0 0, 0 1 0 1 1, 1 0 0 1 1 and 1 1 0 0 0.

Example 4.4 Find the code words generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

when the encoding function is e: $B^3 \to B^6$.

Taking $$H = \left[\begin{array}{ccc|ccc} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right] = [A^T | I_{n-m}]$$

as per our notation, the generator matrix

G is given by $$G = [I_m | A] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

Now $B^3 = \{0\ 0\ 0,\ 0\ 0\ 1,\ 0\ 1\ 0,\ 1\ 0\ 0,\ 0\ 1\ 1,\ 1\ 0\ 1,\ 1\ 1\ 0,\ 1\ 1\ 1\}$

$\therefore$
$e(0\ 0\ 0) = [0\ 0\ 0] \cdot G = [0\ 0\ 0\ 0\ 0\ 0]$
$e(0\ 0\ 1) = [0\ 0\ 1] \cdot G = [0\ 0\ 1\ 0\ 1\ 1]$
$e(0\ 1\ 0) = [0\ 1\ 0] \cdot G = [0\ 1\ 0\ 1\ 0\ 1]$
$e(1\ 0\ 0) = [1\ 0\ 0] \cdot G = [1\ 0\ 0\ 1\ 1\ 1]$
$e(0\ 1\ 1) = [0\ 1\ 1] \cdot G = [0\ 1\ 1\ 1\ 1\ 0]$
$e(1\ 0\ 1) = [1\ 0\ 1] \cdot G = [1\ 0\ 1\ 1\ 0\ 0]$
$e(1\ 1\ 0) = [1\ 1\ 0] \cdot G = [1\ 1\ 0\ 0\ 1\ 0]$
$e(1\ 1\ 1) = [1\ 1\ 1] \cdot G = [1\ 1\ 1\ 0\ 0\ 1]$

Thus, the code words generated are

0 0 0 0 0 0, 0 0 1 0 1 1, 0 1 0 1 0 1, 1 0 0 1 1 1, 0 1 1 1 1 0,
1 0 1 1 0 0, 1 1 0 0 1 0 and 1 1 1 0 0 1.

Example 4.5 Decode each of the following received words corresponding to the encoding function e: $B^3 \to B^6$ given by $e(000) = 000\ 000$, $e(001) = 001\ 011$, $e(010) = 010\ 101$, $e(100) = 100\ 111$, $e(011) = 011\ 110$, $e(101) = 101\ 100$, $e(110) = 110\ 010$ and $e(111) = 111001$, assuming that no error or signal error has occurred:

0 1 1 1 1 0, 1 1 0 1 1 1, 1 1 0 0 0 0, 1 1 1 0 0 0, 0 1 1 1 1 1.

We note that the minimum distance between the code words (viz., the minimum weight of the non-zero code words) is 3 and hence, atmost 1 error can be corrected that might have occurred in the received words.

(i) The word 0 1 1 1 1 0 is identical with $e(0\ 1\ 1)$. Hence, no error has occurred in this word and the original message is 0 1 1.

(ii) The word 1 1 0 1 1 1 differs from $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 1\ 1$ in the second position only. Correcting this single error, the transmitted word is 1 0 0 1 1 1 and the original message is 1 0 0.

(iii) The word 1 1 0 0 0 0 differs from $e(1\ 1\ 0) = 1\ 1\ 0\ 0\ 1\ 0$ in the fifth position only. Correcting this error, the transmitted word is 1 1 0 0 1 0 and the original message is 1 1 0.

(iv) The word 1 1 1 0 0 0 differs from $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 1$ in the sixth position only. Correcting this error, the transmitted word is 1 1 1 0 0 1 and the original message is 1 1 1.

(v) The word 0 1 1 1 1 1 differs from $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 1\ 0$ in the sixth position only. Correcting this error, the transmitted word is 0 1 1 1 1 0 and the original message is 0 1 1.

Example 4.6 If x is a specific encoded word that belongs to B^{10} and $S(x, k)$ is the set of all received words corresponding to x with at most k errors, determine $|S(x, 1)|$, $|S(x, 2)|$, $|S(x, 3)|$. If $x \in B^n$, what is $|S(x, k)|$, where $1 \le k \le n$.

$S(x, 1)$ is the set of all received words $\in B^{10}$. Since the position for the single error can be chosen from the 10 positions of x in $10C_1 = 10$ ways. As $S(x, 1)$ includes the word with no error, $S(x, 1)$ contains $1 + 10 = 11$ words.

i.e., $|S(x, 1)| = 11$

Similarly $|S(x, 2)|$ = No. of words with no error, 1 error and 2 errors
$= 1 + 10C_1 + 10C_2$
$= 56.$

$|S(x, 3)|$ = No. of words with no error, 1 error, 2 errors and 3 errors
$= 1 + 10C_1 + 10C_2 + 10C_3$
$= 176.$

In general,

$$|S(x, k)| = 1 + nC_1 + nC_2 + \cdots nC_k = \sum_{i=o}^{k} nC_i$$

Example 4.7 Given the generator matrix $G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, corresponding to the encoding function e: $B^3 \to B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all the words decoded uniquely?

(i) 1 1 0 1 0 1, (ii) 0 0 1 1 1 1, (iii) 1 1 0 0 0 1, (iv) 1 1 1 1 1 1

If we assume that $G = [I_3 | A]$, then

$$H = [A^T | I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We compute the *syndrome* of each of the received word by using $H \cdot [r]^T$.

(i) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$

Since, $H \cdot [e(w)]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, the received word in this case is the transmitted (encoded) word itself. Hence, the original message is 1 1 0.

(ii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

Since, the syndrome $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is the same as the fifth column of H, the element in the fifth position of r is changed.

$\therefore$ The decoded word is 0 0 1 1 0 1 and the original message is 0 0 1.

(iii) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

Since, the syndrome $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ is the same as the fourth column of H, the fourth component of r is changed to get the decoded word. It is 1 1 0 1 0 1 and the original message is 1 1 0.

(iv) $H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

Since, the syndrome is not identical with any column of H, the received word cannot be decoded uniquely.

Example 4.8 Construct the decoding table for the group code given by the generator matrix.

$$G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Decode the following received words using the decoding table obtained. Which of the words could not be decoded uniquely?

1 0 1 1 1 1, 0 1 1 0 1 0, 1 0 1 1 1 0, 1 1 1 1 1 1.

Since G is a 3×6 matrix, it corresponds to the encoding function e: $B^3 \to B^6$.

Now, $B^3 = \{0\ 0\ 0, 0\ 0\ 1, 0\ 1\ 0, 1\ 0\ 0, 0\ 1\ 1, 1\ 0\ 1, 1\ 1\ 0, 1\ 1\ 1\}$

$e(0\ 0\ 0) = [0\ 0\ 0]G = [0\ 0\ 0\ 0\ 0\ 0]$;

Similarly $e(0\ 0\ 1) = [0\ 0\ 1\ 0\ 1\ 1]$; $e(0\ 1\ 0) = [0\ 1\ 0\ 1\ 0\ 1]$

$e(1\ 0\ 0) = [1\ 0\ 0\ 1\ 1\ 1]$; $e(0\ 1\ 1) = [0\ 1\ 1\ 1\ 1\ 0]$;

$e(1\ 0\ 1) = [1\ 0\ 1\ 1\ 0\ 0]$; $e(1\ 1\ 0) = [1\ 1\ 0\ 0\ 1\ 0]$

and $e(1\ 1\ 1) = [1\ 1\ 1\ 0\ 0\ 1]$.

We form the decoding table by making these encoded words as the elements of the first row and the coset leaders as the elements of the first column. The coset leaders with only one 1 have been taken in a certain order and then those with two 1's have been taken. The decoding table is given in Table 4.14.

Table 4.14

Code words→							
000000	001011	010101	100111	011110	101100	110010	111001
100000	101011	110101	000111	111110	001100	010010	011001
010000	011011	000101	110111	001110	111100	100010	101001
001000	000011	011101	101111	010110	100100	111010	110001
000100	001111	010001	100011	011010	101000	110110	111101
000010	001001	010111	100101	011100	101110	110000	111011
000001	001010	010100	100110	011111	101101	110011	111000
011000	010011	001101	111111	000110	110100	101010	100001

↑
Coset leaders

Note The decoding table is not unique as the coset leader of the last row could have been taken as 1 0 0 0 0 1 or 0 0 0 1 1 0.

Decoding of the received words

(i) 101 111 appears in the 4^{th} row and 4^{th} column. The coset leader of the 4^{th} row is 001 000, which contains only one 1,

Since the minimum weight of the code words is 3, atmost one error can be corrected in the received word.

The corrected (received) word, viz., the code word transmitted is the top element of the 4^{th} column. It is 100 111 and hence the original message is 100.

(ii) 0 1 1 0 1 0 appears in the 5^{th} row and 5^{th} column. Hence the corresponding code word transmitted is 0 1 1 1 1 0 and hence the original message is 0 1 1.

(iii) 1 0 1 1 1 0 appears in the 6^{th} row and 6^{th} column. Hence the corresponding code word transmitted is 1 0 1 1 0 0 and hence the original message is 1 0 1.

(iv) 1 1 1 1 1 1 appears in the 8^{th} row, the coset leader of which contains two 1's viz., the received word contains 2 errors. Hence, they cannot be corrected and the code word transmitted cannot be uniquely determined.

EXERCISE 4(C)

Part A: (Short answer questions)

1. What is the main objective of coding theory?
2. What do you mean by encoder and decoder?
3. What is group code?
4. Define Hamming code.
5. Define even and odd parity checks.
6. What is meant by (i) the weight of a code word (ii) the Hamming distance between two code words?
7. If the minimum distance between two code words is (i) 3, (ii) 4 and (iii) 5, how many errors can be detected and how many can be corrected in each case?
8. Define generator matrix corresponding to the encoding function e: $B^m \to B^n$.
9. What are the restrictions on A occurring in the generator matrix $G = [I_m | A]$?
10. How will you use the generator matrix to get the code words corresponding to the given message words?
11. Define the parity check matrix. How is it related to the generator matrix?
12. How will you use the parity check matrix to retrieve the code word from a received word?
13. How will you find the minimum distance between any two code words in a group code?

14. What are the possible weight of the code word x, if

$$H \cdot [x]^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} [x]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} ?$$

15. Explain briefly the step by step procedure for constructing the decoding table for group code.
16. How will you make use of the decoding table to get back the code word corresponding to a received word, if it contains a single error?
17. If $x, y, z \in B^n$, prove that (i) $H(x, y) \geq 0$ (ii) $H(x, y) = 0 \Rightarrow x = y$ (iii) $H(x, y) = H(y, x)$.
18. If $x, y, z \in B^n$, prove the triangle inequality $H(x, z) \leq H(x, y) + H(y, z)$ [*Hint:* $H(x, z) = \text{Wt}(x \oplus z) = \text{Wt}\{x \oplus (y \oplus y) \oplus z\} = \text{Wt}\{(x \oplus (y \oplus y) \oplus z)\}$, since $y \oplus y = 0$]
19. If $C \subseteq B^7$, where C is a set of code words and $r = c + e$, where $c \in C$, e is the error pattern and r is the received word, find r, e and c respectively from the following:
    (i) $c = 1\ 0\ 1\ 0\ 1\ 1\ 0$ and $e = 0\ 1\ 0\ 1\ 1\ 0\ 1$
    (ii) $c = 1\ 0\ 1\ 0\ 1\ 1\ 0$ and $r = 1\ 0\ 1\ 1\ 1\ 1\ 1$
    (iii) $e = 0\ 1\ 0\ 1\ 1\ 1\ 1$ and $r = 0\ 0\ 0\ 0\ 1\ 1\ 1$
20. If e: $B^2 \rightarrow B^6$ is given by $e(0\ 0) = 0\ 0\ 0\ 0\ 0\ 0$, $e(1\ 0) = 1\ 0\ 1\ 0\ 1\ 0$, $e(0\ 1) = 0\ 1\ 0\ 1\ 0\ 1$ amd $e(1\ 1) = 1\ 1\ 1\ 1\ 1\ 1$, list the elements in $S(1\ 0\ 1\ 0\ 1\ 0, 1)$ and $S(1\ 1\ 1\ 1\ 1\ 1, 1)$, where $S(x, k)$ is the set of all received words corresponding to x with at most k errors.
21. For each of the following encoding fucntions, find the minimum distance between the code words. State also the error-detecting and error-correcting capabilities of each code:
    (i) $e(0\ 0) = 0\ 0\ 0\ 0$, $e(1\ 0) = 0\ 1\ 1\ 0$, $e(0\ 1) = 1\ 0\ 1\ 1$, $e(1\ 1) = 1\ 1\ 0\ 0$
    (ii) $e(0\ 0) = 0\ 0\ 0\ 0\ 1$, $e(1\ 0) = 1\ 0\ 1\ 0\ 0$, $e(0\ 1) = 0\ 1\ 0\ 1\ 0$, $e(1\ 1) = 1\ 1\ 1\ 1\ 1$
    (iii) $e(0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$; $e(1\ 0) = 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0$, $e(0\ 1) = 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1$; $e(1\ 1) = 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1$.
    (iv) $e(0\ 0\ 0) = 0\ 0\ 0\ 1\ 1\ 1$; $e(0\ 0\ 1) = 0\ 0\ 1\ 0\ 0\ 1$; $e(0\ 1\ 0) = 0\ 1\ 0\ 0\ 1\ 0$; $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 0\ 0$; $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 0\ 0$; $e(1\ 0\ 1) = 1\ 0\ 1\ 0\ 1\ 0$; $e(1\ 1\ 0) = 1\ 1\ 0\ 0\ 0\ 1$, $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 0$.
    (v) $e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$; $e(0\ 0\ 1) = 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0$; $e(0\ 1\ 0) = 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1$; $e(1\ 0\ 0) = 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0$; $e(0\ 1\ 1) = 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1$; $e(1\ 0\ 1) = 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1$, $e(1\ 1\ 0) = 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0$; $e(1\ 1\ 1) = 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1$.

Part B

22. A binary symmetric channel has probability $p = 0.001$ of incorrect transmission. If the code word 110 101 101 is transmitted, what is the probability (i) of correct transmission (ii) of making atmost one error in transmission (iii) of making atmost 2 errors in transmission?

23. The (24, 8) triple repetition code has the encoding function e: $B^8 \to B^{24}$, where $B \equiv (0, 1)$. If d: $B^{24} \to B^8$ is the corresponding decoding function, apply d to decode the received word 1 0 1 0 0 1 1 1 0 0 1 1 0 1 1 1 1 0 1 1 0 1 1 0, by using the majority rule.
24. Find the code words generated by the parity check matrix $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$, when the encoding function is e: $B^2 \to B^5$.
25. Find the code words generated by the parity check matrix $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$, when the encoding function is e: $B^3 \to B^6$.
26. Prove that the code words generated by the parity check matrix $H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ with respect to the encoding function e: $B^4 \to B^7$ form a group code.
27. If the encoding function e: $B^3 \to B^8$ is given by
$e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$, $e(0\ 0\ 1) = 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0$,
$e(0\ 1\ 0) = 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0$, $e(1\ 0\ 0) = 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1$;
$e(0\ 1\ 1) = 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0$, $e(1\ 0\ 1) = 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1$,
$e(1\ 1\ 0) = 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1$, and $e(111) = 11101011$,
find the corresponding parity check matrix.
28. Decide each of the following received words corresponding to the encoding function e: $B^3 \to B^6$ given by $e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0$, $e(0\ 0\ 1) = 0\ 0\ 1\ 1\ 0\ 1$, $e(0\ 1\ 0) = 0\ 1\ 0\ 0\ 1\ 1$, $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 1\ 0$, $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 1\ 0$, $e(1\ 0\ 1) = 1\ 0\ 1\ 0\ 1\ 1$, $e(1\ 1\ 0) = 1\ 1\ 0\ 1\ 0\ 1$ and $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 0\ 0$, assuming that no error or single error has occurred:
1 0 0 1 0 1, 1 0 1 1 0 1, 0 1 1 0 1 0, 1 1 1 0 1 0, 1 0 0 0 1 0.
29. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$, corresponding to the encoding function e: $B^4 \to B^7$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message:
1 1 0 0 0 0 1, 1 1 1 0 1 1 1, 0 0 1 0 0 0 1, 0 0 1 1 1 0 0.

30. Given the generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ corresponding to the encoding function e: $B^3 \to B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence to find the original message:

    1 1 1 1 0 1, 1 0 0 1 0 0, 1 1 1 1 0 0, 0 1 0 1 0 0

31. Repeat problem (30) with $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$, e: $B^2 \to B^6$ and received words 0 0 0 1 0 0, 0 1 1 1 0 1, 1 1 1 0 1 0 and 1 0 1 0 1 1.

32. Repeat problem (30) with $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, e: $B^3 \to B^8$ and received words 1 0 1 1 0 1 0 1, 1 0 0 1 1 0 0 1, 0 0 0 1 0 1 0 0, 0 0 1 1 0 0 1 1.

33. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

    Use the decoding table to decode the following received words:
    1 1 1 1 0, 1 1 1 0 1, 1 1 0 1 1, 1 0 1 0 1, 1 0 0 1 1, 1 1 1 1 1 and 0 1 1 0 0.

34. Construct the decoding table for the group code given by the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

    Use the decoding table to decode the following received words:
    0 0 0 1 1 0, 0 0 0 0 1 1, 0 0 0 1 0 1, 1 1 0 0 0 1, 1 0 1 0 0 1 and 0 1 1 1 1 1.

35. Construct the decoding table for the group code generated by the parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

    Use the decoding table to decode the following received words:
    1 1 1 0 0 0, 1 1 0 0 0 0, 1 0 1 0 0 0, 1 0 1 1 1 1, 0 0 1 1 1 0 and 1 1 0 1 0 1.

36. Construct the decoding table for the group code generated by the parity check matrix.

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Use the decoding table to decode the following received words:
0 1 1 1 0 1, 1 1 1 0 1 0, 1 0 1 0 1 1, 1 0 1 1 1 1, 1 1 0 1 0 1 and 1 1 1 0 1 1

ANSWERS

Exercise 4(A)

3. $e = -2$ 4. $a^{-1} = -(a + 4)$ 16. No 17. Yes
18. 1 19. 6 24. $O(1) = 1$, $O(-1) = 2$, $O(\pm i) = 4$
25. $O(a) = 6$, $O(a^2) = 3$, $O(a^3) = 2$, $O(a^4) = 3$, $O(a^5) = 6$, $O(a^6) = 1$
36. $O(S_n) = n!$, $O(D_n) = 2n$; (38) w, w^2 39. [1], [2], [3] and [4];
40. 4; a, a^3, a^5, a^7 41. 1, only 1 42. 0, $a^{-1} = a/(a - 1)$ $(a \neq 1)$;
43. Inverses of 1, 2, 3, 4, 5 are 5, 4, 3, 2, 1 respectively
44. 0, $-\dfrac{a}{3a+1}$ 45. No

56. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 1 & 4 \end{pmatrix}$, $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 4 & 3 \end{pmatrix}$,

$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 4 & 2 & 1 \end{pmatrix}$, $\beta^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 3 & 6 \end{pmatrix}$,

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 3 & 5 \end{pmatrix}$, $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix}$;

57. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$, $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, $\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$,

$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, $O(\alpha) = 4$, $O(\beta) = 3$, $O(\alpha\beta) = 4$;

58. $a \neq p_1$, $b \neq p_1$ and $a \neq b$; $a = p_1, p_2, p_4, p_6$; $a = p_1, p_3, p_5$;
59. 2; 3 and 5; 60. 2 and 5

Exercise 4(B)

5. No 7. $\{e\}$ and G
18. The distinct left cosets are {[0], [3]}, {[1], [4]} and {[2], [5]}

37. ker $(f) = 2n\pi$, $n \in Z$ 38. ker $(f) = e^{i2n\pi}$, $n \in Z$;
39. $\{p_1\ p_3\ p_5\}$ and $\{p_2, p_4, p_6\}$ 40. H, $1 + H$, $2 + H$, $3 + H$, $4 + H$
42. All the three are not normal subgroups;
43. Yes 47. $m = n = 1$ or $m = n = -1$.

Exercise 4(C)

7. (i) 2, 1 (ii) 2, 1 (iii) 4, 2
14. 3 or 4
19. (i) 1111011 (ii) 0001001 (iii) 0101000
20. (i) {101010, 001010, 111010, 100010, 101110, 10100, 101011}
    (ii) {111111, 011111, 101111, 110111, 111011, 111101, 111110}
21. (i) 2; can detect atmost 1 error; cannot correct any error.
    (ii) 3; can detect atmost 2 errors; can correct atmost 1 error;
    (iii)5; can detect atmost 4 errors and can correct atmost 2 erros;
    (iv) 2; can detect atmost 1 error and cannot correct any error.
    (v) 3; can detect 2 errors and can correct 1 error;
22. (i) 0.991036 (ii) 0.999964 (iii) 0.999999
23. 10110111
24. $e(00) = 00000$, $e(01) = 01011$, $e(10) = 10110$, $e(11) = 11101$;
25. $e(000) = 000000$, $e(001) = 001011$, $e(010) = 010101$, $e(100) = 100110$; $e(011) = 011110$, $e(101) = 101101$, $e(110) = 110011$, $e(111) = 111000$.

27. $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

28. 110101, 001101, 011110, 111000, 100110;
29. 1100, 1110, 0010, 0011
30. 101, 010, 100, could not be decoded.
31. 00, 01, 10, 10;
32. 011, 101, 110, 111.

33. **Table 4.15**

0 0 0 0 0	0 1 1 1 0	1 0 0 1 1	1 1 1 0 1
0 0 0 0 1	0 1 1 1 1	1 0 0 1 0	1 1 1 0 0
0 0 0 1 0	0 1 1 0 0	1 0 0 0 1	1 1 1 1 1
0 0 1 0 0	0 1 0 1 0	1 0 1 1 1	1 1 0 0 1
0 1 0 0 0	0 0 1 1 0	1 1 0 1 1	1 0 1 0 1
1 0 0 0 0	1 1 1 1 0	0 0 0 1 1	0 1 1 0 1
1 1 0 0 0	1 0 1 1 0	0 1 0 1 1	0 0 1 0 1
1 0 1 0 0	1 1 0 1 0	0 0 1 1 1	0 1 0 0 1

01110, 11101, 10011, 10011, 10011, 11101, 11101 and 01110
Massages are: 01, 11, 10, 10, 10, 11, 11, and 01,

34. **Table 4.16**

000000	100110	010011	001101	110101	101011	011110	111000
100000	000110	110011	101101	010101	001011	111110	011000
010000	110110	000011	011101	100101	111011	001110	101000
001000	101110	011011	000101	111101	100011	010110	110000
000100	100010	010111	001001	110001	101111	011010	111100
000010	100100	010001	001111	110111	101001	011100	111010
000001	100111	010010	001100	110100	101010	011111	111001
010100	110010	000111	011001	100001	111111	001010	101100

100110, 010011, 001101, 110101, 101011 and 011110.
Messages: 100, 010, 001, 110, 101 and 011.

35. **Table 4.17**

000000	001011	010101	011110	100111	101100	110010	111001
100000	101011	110101	111110	000111	001100	010010	011001
010000	011011	000101	001110	110111	111100	100010	101001
001000	000011	011101	010110	101111	100100	111010	110001
000100	001111	010001	011010	100011	101000	110110	111101
000010	001001	010111	011100	100101	101110	110000	111011
000001	001010	010100	011111	100110	101101	110011	111000
000110	001101	010011	011000	100001	101010	110100	111111

111001, 110010, 101100, 100111, 011110 and 010101.
Messages: 111, 110, 101, 100, 011 and 010.

36. **Table 4.18**

000000	010101	101010	111111
000001	010100	101011	111110
000010	010111	101000	111101
000100	010001	101110	111011
001000	011101	100010	110111
010000	000101	111010	101111
100000	110101	001010	011111
110000	100101	011010	011111
100100	110001	001110	011011
100001	110110	001011	011110
011000	001101	110010	100111
010010	000111	111000	101101
001100	011001	100110	110011
001001	011100	100011	110110
000110	010011	101100	111001
000011	010110	101001	111100

010101, 101010, 101010, 111111, 010101 and 111111.
Messages: 01, 10, 10, 11, 01 and 11.