12 CHAPTER Group Theor

12.1. Introduction

Group theory is one of the most important fundamental concepts of modern algebra. Groups arise naturally in various mathematical situations. They have found wide applications in physical sciences and biological sciences particularly in the study of crystal structure, configuration molecules and structure of human genes.

The structure of a group is one of the simplest mathematical structures. Hence, groups may be considered as the starting point of the study of various algebraic structures. In this chapter, we shall define groups and study some of their basic properties.

12.2. Binary Operations

Let G be a nonempty set. Then $G \times G = \{(a, b) : a \in G, b \in G\}$.

If $f : G \times G \to G$, then f is said to be binary operation on G. Thus a binary operation on G is a function that assign each ordered pairs of elements of G a unique element of G.

The symbols +, ·, 0, * etc. are used to denote binary operations on a set. Thus + will be a binary operation on G if and only if

$a + b \in G$ for all $a, b \in G$ and $a + b$ is unique.

Similarly * will be a binary operation on G if and only if

$a * b \in G$ for all $a, b \in G$ and $a * b$ is unique.

This is said to be the **closure property** of the binary operation and the set G is said to be closed with respect to the binary operation. For example, addition (+) and multiplication (×) are binary operations on the set N of natural numbers, for, the sum and product of two natural numbers are also natural numbers. Therefore, N is closed with respect to addition and multiplication *i.e.*,

$$a + b \in N \text{ for all } a, b \in N.$$

$$a \times b \in N \text{ for all } a, b \in N.$$

Note that subtraction is not a binary operation on N, for $5 - 9 = -4 \notin N$ whereas $5 \in N$, $9 \in N$. But subtraction is a binary operation on Z, the set of integers, positive and negative.

A binary operation on a set G is sometimes called a composition in G. For finite set, a binary operation on the set can be defined by means of a table, called the **composite table.** Let S be a set with n distinct elements. To construct a table, the elements of S are arranged horizontally in a row called the initial row or 0-row ; these are again arranged vertically in a column, called the initial column or 0-column. The (i, j) th position in the table is determined by the intersection of the ith row and the jth column. For example, let $S = \{a, b, c\}$. Define * on S by the following table.

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

Table 12.1

To determine the elements of S assigned to $a * b$, we look at the intersection of the row labelled by a and the element headed by b. We see that $a * b = b$. Note that $b * a = a$.

Algebraic Structure

A non-empty set together with one or more than one binary operations is called algebraic structure. For example,

(N, +), (Z, +), (R, +, .) are all algebraic structures. Obviously addition and multiplication are both binary operations on the set R of real numbers. Therefore, (R, +, .) is an algebraic structure equipped with two operations.

Laws of Binary Operations

***Associative law*:** A binary operation * on a set S is said to be associative or to satisfy associate property, if and only if, for any elements $a, b, c \in S$

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

***Commutative law*:** A binary operation * on the elements of the set is commutative or to satisfy commutative property, if and only if, for any two elements a and $b \in S$,

$$a * b = b * a.$$

Example 1. The algebraic structure (Z, +), (Z, .), where the binary operations of addition and multiplication on Z are both associative and commutative since addition and multiplication of integers is both associative and commutative.

Example 2. Let M_2 (R) be the set of all 2 × 2 matrices over R *i.e.*,

$$M_2(R) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d, \in R \right\}$$

Since addition and multiplication of 2 × 2 matrices over R is a 2 × 2 matrix over R, it follows that both + and . is a binary operation on M_2 (R). Hence (M_2 (R), +, .) is a algebraic structure. Note that + is both associative and commutative and . is associative, but not commutative.

Example 3. The algebraic structure (Z, –) where – denotes the binary operation of subtraction on Z is neither associative nor commutative since

$$3 - (4 - 5) = 4 \neq -6 = (3 - 4) - 5$$

and also $3 - 4 \neq 4 - 3$

Identity Element

An element e in a set S is called an identity element with respect to the binary operation * if, for any element a in S

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

If $a * e = a$, then e is called the **right identity** element for the operation * and if $e * a = a$, then e is called the **left identity** element for the operation *.

Consider any element x of the set Q of rational numbers with respect to the binary operation addition. Obviously, 0 is the identity element, since $0 + x = x + 0 = x$, for every $x \in Q$.

1 is the identity element of Q for the binary operation multiplication, since $1.x = x.1 = x$, for every $x \in Q$.

It is easily seen that for the set N of natural numbers there is no identity element for addit but 1 is an identity element with respect to multiplication.

Theorem 12.1. The identity element (if it exists) of any algebraic structure is unique.

Proof. Let, if possible, e and e' be two identity elements of the algebraic structure (S, *). Hence $e' \in S$.

Now e is an identity element $\Rightarrow e * e' = e'$.

Again e' is an identity element $\Rightarrow e * e' = e$.

But $e * e' = e'$ and $e * e' = e$ $\Rightarrow e = e'$.

Thus the identity element is unique.

Inverse Element

Consider a set S having the identity element e with respects to the binary operation *. If corresponding to each element $a \in S$ there exists an element $b \in S$ such that $a * b = b * a = e$.

Then b is said to be the inverse of a and is usually denoted by a^{-1}. We say a is invertible.

Consider the set R of real numbers which has 0 as the identity element with respect to the binary operation addition. Then, for any $a \in R$, we see that

$$(-a) + a = a + (-a) = 0.$$

Thus, for any a of the real number set, $(-a)$ is its inverse. This is called the **additive inverse**.

Similarly, for the set Q of rational numbers, 1 is the identity element for the binary operation of multiplication. Then, for any $a \in Q$ we see that

$$a \,.\, (1/a) = (1/a) \,.\, a = 1.$$

Thus, for any a (non-zero) of the rational number set, its reciprocal is its inverse. This is called the **multiplicative inverse**.

Note that the inverse of the identity element is the identity element itself.

Theorem 12.2. For an associative algebraic structure, the inverse of every invertible element is unique.

Proof. Let (S, *) be an associative structure with identity element e. Let x be an invertible element of S. If possible, let y, z be two inverses of x. We then have

$$x * y = e = y * x \quad \ldots (1)$$

and $$x * z = e = z * x. \quad \ldots (2)$$

Now $$(y * x) * z = e * z \text{ from (1)}$$
$$= z \quad (e \text{ is the identity})$$

so that $$(y * x) * z = z \quad \ldots (3)$$

and $$y * (x * z) = y * e \text{ from (2)}$$
$$= y \quad (e \text{ is the identity})$$

Thus $$y * (x * z) = y \quad \ldots (4)$$

Since the composition * is associative, we have

$$(y * x) * z = y * (x * z).$$

Then from (3) and (4), we have $y = z$, showing that the inverse of every invertible element is unique.

Note. It may be noted that while an identity element is the same for all element x in S, the inverse of an element x is determined by the given element x.

From the composite table, one can conclude

(*i*) **Closure property :** If all the entries in the table are elements of S, then S is closed for *.

(*ii*) **Commutative law :** If every row of the table coincides with the corresponding column, then * is commutative on S.

(*iii*) **Identity element :** If the row headed by an element a_1 of S coincides with the top row, then a_1 is the identity element.

(*iv*) **Inverses :** If the identity element e is placed in the table at the intersection of the row headed by a and the column headed by b, then $a^{-1} = b$ and $b^{-1} = a$.

Example 4. Show that the binary operation * defined on $(R, *)$ where $x * y = \max(x, y)$ is associative.

Solution. $(x * y) * z = \max(x, y) * z$

$= \max(\max(x, y), z) = \max(x, y, z)$

Again $x * (y * z) = x * \max(y, z)$

$= \max(x, \max(y, z))$

$= \max(x, y, z)$

Hence $(x * y) * z = x * (y * z)$

Thus, * is associative.

Example 5. Show that the binary operation * defined on $(R, *)$ where $x * y = x^y$ is not associative.

Solution. $(x * y) * z = x^y * z$

$= (x^y)^z = x^{yz}$

Again $x * (y * z) = x * y^z$

$= x^{y^z}$

Since $x^{yz} \neq x^{y^z}$, $(x * y) * z \neq x * (y * z)$

Thus, * is not associative.

Example 6. Prepare the composition table for multiplication on the element in the set $A = \{1, w, w^2\}$, where w is the cube root of unity. Show that multiplication satisfies the closure property, associative law, commutative law and 1 is the inverse element. Write down the multiplicative inverse of each element.

Solution. Since w is a cube root of unity, $w^3 = 1$. We can operate on various elements and prepare the table as below.

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

From the table we can conclude that

(*i*) **Closure property :** Since all the entries in the table are in A so closure property is satisfied.

(*ii*) **Associative law :** Since multiplication is associative on complex numbers and A is a set of complex numbers, so multiplication is associative on A.

(*iii*) **Commutative law :** Since 1st, 2nd and 3rd rows coincide with 1st, 2nd and 3rd columns respectively, so multiplication is commutative on S.

(*iv*) **Identity element :** Since row headed by 1 is same as the initial row, 1 is the identity element.

(*v*) **Inverses :** Clearly $1^{-1} = 1$; $w^{-1} = w^2$; $(w^2)^{-1} = w$

Example 7. Let the binary operation * be defined on $S = \{a, b, c, d\}$ by means of composite Table 11.2.

(*a*) Compute $c * d$, $b * b$, $(a * b) * c$ and $[(a * c) * e)] * a$ from the table.

(*b*) is * commutative ? why ?

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

Table 11.2

Solution. (*a*) $c * d = b, b * b = c$

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

and $[(a * c) * e] * a = (c * e) * a = a * a = a$

(*b*) No, since $b * e = c$ and $e * b = b$ and hence $b * e \neq e * b$.

Example 8. Let Z be the set of integers, show that the operation * on Z, defined by $a * b = a + b + 1$ for all $a, b \in Z$ satisfies the closure property, associative law and the commutative law. Find the identity element. What is the inverse of an integer a ?

Solution. Since Z is closed for addition, as we have

$$a + b \in \mathrm{Z} \text{ for all } a, b \in \mathrm{Z}$$
$$\Rightarrow a + b + 1 \in \mathrm{Z}$$
$$\Rightarrow a * b \in \mathrm{Z}$$

So * is a binary operation on Z.

Again, $a * b = a + b + 1$

$= b + a + 1$ (by commutative law of addition on Z)

$= b * a$ for all $a, b \in \mathrm{Z}$

Hence * is commutative.

Again, $(a * b) * c = (a + b + 1) * c$

$= (a + b + 1) + c + 1 = (a + b + c) + 2$

and $a * (b * c) = a * (b + c + 1)$

$= a + (b + c + 1) + 1 = (a + b + c) + 2$

Thus $(a * b) * c = a * (b * c)$ for all $a, b, c \in \mathrm{Z}$

Hence, * is associative.

Now, if e is the identity element in Z for *, then for all $a \in \mathrm{Z}$

$$a * e = a \Rightarrow a + e + 1 = a$$
$$\Rightarrow e = -1 \in \mathrm{Z}$$

So, –1 is the identity element for * in Z.

Let the integer a have its inverse b. Then,

$$a * b = -1 \Rightarrow a + b + 1 = -1$$
$$\Rightarrow b = -(2 + a)$$
$$\Rightarrow \text{So, the inverse of } a \text{ is } -(2 + a).$$

12.3. Group

Let (G, *) be an algebraic structure, where * is a binary operation, then (G, *) is called a group under this operation if the following conditions are satisfied.

1. Closure law: The binary * is a closed operation *i.e.*, $a * b \in \mathrm{G}$ for all $a, b \in \mathrm{G}$.

2. Associative law: The binary operation * is an associative operation *i.e.*, $a * (b * c) = (a * b) * c$ for all $a, b, c \in \mathrm{G}$.

3. Identity element: There exists an identity element *i.e.*, for some $e \in G$, $e * a = a * e = a$, $a \in G$.

4. Inverse element: For each a in G, there exists an element a' (the inverse of a) in G such that $a * a' = a' * a = e$.

Many books do not mention the first property as this is a consequence of the definition of binary operation.

A group G is said to be **Abelian** if the commutative law holds *i.e.*, $a * b = b * a$ for all $a, b \in G$.

A group with addition binary operation is known as **additive group** and that with multiplication binary operation is known as **multiplicative group.**

Example 9.

(*i*) The set R of real numbers, for the binary operation of addition, is a group, with 0 as identity element and $(-a)$ as the inverse of a. The same is true of the set Z of integers or the set Q of all rational numbers or the set C of complex numbers.

(*ii*) The set R* of non-zero real numbers, for the binary operation of multiplication, is group with 1 as identity element, and $1/a$ as the inverse of a. The same is true of the set Q* of non-zero rational numbers or the set C* of non-zero complex numbers.

(*iii*) The set Z^+ of positive integers with operation + is not a group. There is no identity element for + in Z^+. The set Z^+ with operation multiplication is not a group. There is an identity element 1, but no inverse of 3.

Example 10. *Prove that the fourth roots of unity 1, −1, i, −i form an abelian multiplicative group.*

Solution. Let $G = \{1, -1, i, -i\}$. We form the composite table as

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

Table 1.3

Closure Property : Since all the entries in the table are the elements of G and hence G is closed with respect to multiplication.

Associative Law : $a\,(bc) = (ab)\,c$ for all values of a, b, c in G.

For example $1\,[(-1)\,i] = -i = [1\,(-1)]\,i$

Commutative Law : $ab = ba$ for all a, b in G.

From the composition table it is clear that elements in each row are the same as elements in the corresponding column so that $ab = ba$.

Identity element : $1 \in G$ is identity element as $1.a = a.1 = a$. It can be seen from the first row and first column of the table.

Inverses : As $1.1 = i\,.\,(-i) = (-1)\,.\,(-1) = 1$, the inverses of $1, -1, i, -i$ are $1, -1 - i, i$ respectively and all those belong to G. Hence it follows that G is an abelian multiplicative group.

Example 11. *Show that the set of all positive rational numbers forms an abelian group under the composition defined by* $a * b = (ab)/2$

Solution. Let Q^+ denote the set of all positive rational numbers. We have to show that $(Q^+, *)$ is a group under the composition $a * b = (ab)/2$.

Closure Property : Since for every element $a, b \in Q^+$, $(ab)/2$ is also in Q^+, therefore Q^+ is closed with respect to operation *.

Associative Law : For $a, b \in Q^+$, we have

$$(a * b) * c = (ab/2) * c \Rightarrow (ab/2)\, c/2 = a/2\, (bc/2) = a * (bc/2) = a * (b * c)$$

Commutative Law : For $a, b \in Q^+$, we have

$$a * b = (ab)/2 = (ba)/2 = b * a$$

Identity Element : Let e be the identity element in Q^+, such that $e * a = a = a * e$.

Now $e * a = a \Rightarrow (ea)/2 = a \Rightarrow (a/2)\,(e - 2) = 0$

$\Rightarrow e = 2$, since $a \in Q^+ \Rightarrow a > 0$

But $2 \in Q^+$ and we have $2 * a = (2a)/2 = a = a * 2$ for all $a \in Q^+$

Inverses : Let a be any element of Q^+. If the number b is to be the inverse of a, then we must have

$$b * a = e = 2 \Rightarrow (ba)/2 = 2 \Rightarrow b = 4/a \in Q^+$$

We have $(4/a) * a = 4a/2a = 2 = a * (4/a)$

Therefore, $4/a$ is the inverse of a. Thus each element of Q^+ is invertible.

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

Example 12. Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition and multiplication modulo 6.

Solution. Let $G = \{1, 2, 3, 4, 5\}$. The operation addition modulo 6 is denoted by $+_6$. We can operate $+_6$ on the elements in G and prepare the composition table as

In the system $(G, +_6)$

$2 +_6 5 = 1$. For $2 + 5 = 7 = 1 \times 6 + 1$

$1 +_6 4 = 5$. For $1 + 4 = 5$

$3 +_6 5 = 2$. For $3 + 5 = 8 = 1 \times 6 + 2$ etc.

Hence the composition table is

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Since all the entries in the composition table do not belong to G, in particular $0 \notin G$.

Hence G is not closed w.r.t. $+_6$. Consequently $(G, +_6)$ is not a group.

(*ii*) The operation multiplication modulo 6 is denoted by $\times_6$.

In the system $(G, \times_6)$.

$2 \times_6 5 = 4$. For $2 \times 5 = 10 = 1 \times 6 + 4$

$3 \times_6 4 = 0$. For $3 \times 4 = 12 = 2 \times 6 + 0$.

Hence the composition table is:

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

From the composition table, it is clear that all the entries in the composition table do not belong to G, in particular $0 \notin G$. Hence G is not closed w.r.t. $\times_6$.

Consequently $(G, \times_6)$ is not a group.

Example 13. Show that the matrices

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$$

form a multiplicative abelian group.

Solution. Let $A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, B = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}, C = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, D = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}$, $G = \{A, B, C, D\}$.

$$A.A = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \cdot \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}0+1 & 0+0\\ 0+0 & 0+1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} = A,$$

$$AB = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \cdot \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}-1+0 & 0+0\\ 0+0 & 0+1\end{bmatrix} = \begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix} = B.$$

Similarly AC = C, AD = D, BB = A etc.

Hence we find the composition table as

×	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

(*i*) **Closure property :** We can see that all entries in the composition table are the elements of G and hence G is closed w.r.t. matrix multiplication.

(*ii*) **Associative law :** Multiplication is associative in G. Since associative law holds in case of matrix multiplication, *i.e.*,

$$(AB)\,C = A\,(BC).$$

(*iii*) **Commutative law :** The entries in the first, second, third and fourth columns of the composition table coincide with the corresponding entries in the first, second, third and fourth row. This shows that G is commutative.

(*iv*) **Existence of Identity :** From the composition table it follows that

$$AA = A,\ AB = B,\ AC = C,\ AD = D$$

Thus there exists an identity element A in G.

(*v*) **Existence of Inverse :** From the composition table it can be seen that

$$AA = A,\ BB = A,\ CC = A,\ DD = A$$

Thus every element is its own inverse.

Hence the set of four matrices form a multiplicative group which is commutative as well *i.e.*, (G, .) is an abelian group.

Example 14. Let $G = \{(a, b) \mid a, b \in R, a \neq 0\}$. Define a binary operation * on G by

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

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

Solution.

Closure Property : Let (a, b) and (c, d) be any two members of G. Then $a \neq 0$ and $c \neq 0$. Therefore, $ac \neq 0$. Consequently $(a, b) * (c, d) = (ac, bc + d)$ is also a member of G. Hence G is closed with respect to the given composition.

Associative law : Let (a, b), (c, d) and (e, f) be any three members of S. Then

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

$$\begin{aligned}\text{Also } (a, b) * [(c, d) * (e, f)] &= (a, b) \times (ce, de + f) \\ &= (a\,[ce], b\,[ce] + de + f) \\ &= (ace, bce + de + f).\end{aligned}$$

Hence the given composition * is associative.

Identity element : Suppose (x, y) is an element of G such that $(x, y) * (a, b) = (a, b)\ \forall$ $(a, b) \in G$

Then $(xa, ya + b) = (a, b)$. Hence $xa = a$ and $ya + b = b$.

These give $x = 1$ and $y = 0$. Now $(1, 0) \in G$

Therefore, $(1, 0)$ is the identity element

Inverse element : Let (a, b) be any member of G. Let (x, y) be a member of G such that $(x, y) \times (a, b) = (1, 0)$, then (x, y) be the inverse of (a, b).

Then $(xa, ya + b) = (1, 0)$. Hence $xa = 1$, $ya + b = 0$.

These give $x = 1/a$, $y = -b/a$.

Since $a \neq 0$, therefore, x and y are real numbers.

Also $x = \dfrac{1}{a} \neq 0$. Thus $\left(\dfrac{1}{a}, -\dfrac{b}{a}\right)$ is the inverse of (a, b).

Hence G is a group.

Note. In the above group, we have

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

and $$(c, d) * (a, b) = (ca, da + b).$$

Thus, in general, $(a, b) * (c, d) \neq (c, d) * (a, b)$ *i.e.*, the composition is not commutative and hence the group is not abelian.

Example 15. Let Q be the set of positive rational numbers which can be expressed in the form 2^a3^b, where a and b are integers. Prove that the algebraic structure $(Q, .)$ is a group where . is multiplication operator.

Solution.

Closure property: Let $q_1 = 2^a3^b$, $q_2 = 2^c3^d \in Q$ where $a, b, c, d, \in Z$, the set integers.

Here $q_1 \cdot q_2 = (2^a3^b)\cdot(2^c3^d) = 2^{a+c}.3^{b+d} \in Q$

Since $a + c, b + d \in Z$. Therefore Q is closed with respect multiplication operator.

Associative law: Let $q_1 = 2^a3^b$, $q_2 = 2^c3^d$, $q_3 = 2^e3^f \in Q$

We have

$$\begin{aligned}q_1\cdot(q_2 \cdot q_3) &= 2^a3^b\cdot(2^c3^d \cdot 2^e3^f) \\ &= 2^a\, 3^b . (2^{c+e}\, 3^{d+f}) \\ &= 2^{a+(c+e)} . 3^{b+(d+f)} \\ &= 2^{(a+c)+e} . 3^{b+(d+f)}\end{aligned}$$

$$= 2^{a+(c+e)}.3^{(b+d)+f} \quad \text{(Since addition is associative in Z)}$$
$$= (2^{a+c} \cdot 3^{b+d}) \cdot 2^e 3^f$$
$$= (2^a 3^b \cdot 2^c 3^d) \cdot 2^e 3^f$$
$$= (q_1 \cdot q_2) \cdot q_3$$

Identity element: Let $q = 2^a 3^b \in Q$, there exists an identity element e such that $q \cdot e = q$.

Now $2^a 3^b \cdot e = 2^a 3^b \Rightarrow e = 2^0 3^0$ where $0 \in Z$.

since $2^a 3^b \cdot 2^0 3^0 = 2^{a+0} 3^{b+0} = 2^a 3^b$

Inverse Element: Let $q = 2^a 3^b \in Q$. If p is the inverse of q, then we must have

$$q \cdot p = e$$
$$\Rightarrow \quad 2^a 3^b \cdot p = 2^0 3^0 \quad \therefore \quad p = 2^{-a} 3^{-b} \text{ since}$$
$$q \cdot p = 2^a 3^b \cdot 2^{-a} 3^{-b} = 2^{a-a} 3^{b-b} = 2^0 3^0 \text{ and } -a, -b \in Z$$

There $(Q_1, \cdot)$ is a group.

Example 16. Prove that the set

$$\{0, 1, 2, 3, 4\}$$

is a finite abelian group of order 5 under addition modulo 5 as composition.

Solution. To test the nature of the system $(G, +_5)$ where $G = \{0, 1, 2, 3, 4\}$

$2 +_5 4 = 1$ for $2 + 4 = 6 = 1 \times 5 + 1$

$3 +_5 4 = 2$ for $3 + 4 = 7 = 1 \times 5 + 2$

$4 +_5 4 = 3$ for $4 + 4 = 8 = 1 \times 5 + 3$ etc.

We have the following composition table :

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

From the table, we see that (*i*) the given composition is binary (*ii*) 0 is the identity element (*iii*) every element has an inverse. Thus the inverses of 0, 1, 2, 3, 4 are 0, 4, 3, 2, 1 respectively. The composition is associative and commutative.

Hence the given set is a finite abelian group of order 5 under addition modulo 5.

Elementary Properties of Groups

We now prove some elementary properties of groups.

Theorem 12.3. (Cancellation Law). If (G, *) is a group and a, b, c are in G, then

(*i*) $a * b = a * c \Rightarrow b = c$ (left cancellation law)

(*ii*) $b * a = c * a \Rightarrow b = c$ (right cancellation law)

Proof. (*i*) Since $a^{-1} \in G$, operating on the left with a^{-1}, we have

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

(*ii*) We have $b * a = c * a$

Operating on the right by a^{-1}, we get

or $b * e = c * e$

or $b = c$

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

Theorem 12.4. The left identity is also the right identity, *i.e.*,

$$e * a = a = a * e \text{ for all } a \in G.$$

Proof. If a^{-1} be the left inverse of a, then

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

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

$$= e$$

$$= a^{-1} * a.$$

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

$$a * e = a.$$ by Theorem 1

Hence e is also the right identity element of a group.

Theorem 12.5. The left inverse of an element is also its right inverse *i.e.*,

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

Proof. Now $a^{-1} * (a * a^{-1}) = (a^{-1} * a) * a^{-1}$ (associativity)

$$= e * a^{-1}$$

$$= a^{-1} * e$$ by Theorem 1

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

Therefore, $a * a^{-1} = e$ by Theorem 1

Thus the left inverse of an element in a group is also its right inverse.

Theorem 12.6. In a group (G, *)

(*i*) the equation $a * x = b$ has a unique solution $x = a^{-1} * b$

(*ii*) the equation $y * a = b$ has a unique solution $y = b * a^{-1}$, where $a, b \in G$.

Proof. If possible, let the equation $a * x = b$ have two solutions x and x' in G. Then

$$a * x = b \text{ and } a * x' = b.$$

Therefore, $a * x = a * x'$, where $a, x, x' \in G$.

By left cancellation law, we have $x = x'$, $\therefore$ $a * x = b$ has unique solution in G.

Again, assuming $x = a^{-1} * b$, we have

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

$$= (a * a^{-1}) * b \text{ (associativity)}$$

$$= e * b \text{ (e being the identity element)}$$

$$= b.$$

This shows that $x = a^{-1} * b$ satisfies the equation $a * x = b$.

The second part can similarly be proved.

Theorem 12.7. In a group (G, *)

(*i*) $(a^{-1})^{-1} = a$ *i.e.*, the inverse of the inverse of an element is equal to the element;

(*ii*) $(ab)^{-1} = b^{-1} a^{-1}$ *i.e.*, the inverse of the product of two elements is the product of the inverse in the reverse order.

Proof. (*i*) Let e be the identity element for * in G.

Then we have $a * a^{-1} = e$, where $a^{-1} \in G$.

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

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

Thus, by right cancellation law, we have $(a^{-1})^{-1} = a$.

(*ii*) Let a and $b \in G$ and G is a group for *, then

$a * b \in G$ (closure).

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

Let a^{-1} and b^{-1} be the inverses of a and b respectively, then $a^{-1}, b^{-1} \in G$. ... (1)

Therefore, $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b$ (associativity)

$= b^{-1} * e * b = b^{-1} * b = e$

From (1) and (2) we have $(a * b)^{-1} * (a * b) = (b^{-1} * a^{-1}) * (a * b)$ ... (2)

$(a * b)^{-1} = b^{-1} * a^{-1}$. by right concellation law.

Example 17. Prove that if $a^2 = a$, then $a = e$, a being an element of a group.

Solution. Let a be an element of a group G such that $a^2 = a$.

To prove that $a = e$.

$$a^2 = a \Rightarrow a.a = a \Rightarrow (aa)\, a^{-1} = aa^{-1}$$

$$\Rightarrow a\,(aa^{-1}) = e. \qquad (\because aa^{-1} = e)$$

$$\Rightarrow ae = e \Rightarrow a = e. \qquad (\text{since } ae = a.)$$

Example 18. Show that if every element of a group (G, o) be its own inverse, then it is an abelian group.

Is the converse true ?

Solution. Let $a, b \in G$, then $a \circ b \in G$ (closure).

Hence, by the given condition, we have

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

$$= b^{-1} \circ a^{-1}$$

$$= b \circ a, \text{ since } a^{-1} = a \text{ and } b^{-1} = b.$$

Thus $a \circ b = b \circ a$, for every $a, b \in G$.

Therefore, it is an abelian group.

The converse is not true. For example, (R, +), where R is the set of all real numbers, is an abelian group, but no element except 0 is its own inverse.

Example 19. Show that if a, b are arbitrary elements of a group G, then $(ab)^2 = a^2b^2$ if and only if G is abelian.

Solution. Let a and b be arbitrary elements of a group G. Suppose $(ab)^2 = a^2\, b^2$. ... (1)

To prove G is abelian, we have to show that

$$ab = ba$$

$$(ab)^2 = a^2b^2 \Rightarrow (ab)\,(ab) = (aa)\,(bb)$$

$\Rightarrow a\,(ba)\,b = a\,(ab)\,b$, by associative law

$\Rightarrow (ba)\,b = (ab)\,b$, by left cancellation law

$\Rightarrow ba = ab$, by right cancellation law.

$$ab = ba \quad \forall\, a, b \in G \qquad \ldots (2)$$

To prove that $(ab)^2 = a^2b^2$

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b, \quad \text{by (2)}$$
$$= (aa)(bb) = a^2b^2.$$

Hence proved.

Example 20. G is a group and there exist two relatively prime positive integers m and n such that $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a, b, \in G$. Prove that G is Abelian.

Solution. Since m and n are relatively prime, gcd $(m, n) = 1$, we get $mx + ny = 1$ for some x, $y \in Z$.

Now
$$(a^m b^n)^{mx} = a^m (b^n a^m)^{mx-1} b^n$$
$$= a^m (b^n a^m)^{mx} (b^n a^m)^{-1} b^n$$
$$= (b^n a^m)^{mx} a^m a^{-m} b^{-n} b^n$$
$$= (b^n a^m)^{mx}. \qquad \ldots (1)$$

Similarly it can be proved that
$$(a^m b^n)^{ny} = (b^n a^m)^{ny} \qquad \ldots (2)$$

From (1) and (2) we get
$$a^m b^n = (a^m b^n)^{mx + ny}$$
$$= (b^n a^m)^{mx + ny} = b^n a^m. \qquad \ldots (3)$$

Finally
$$ab = a^{mx + ny} b^{mx + ny}$$
$$= a^{mx} (a^{ny} b^{mx}) b^{ny}$$
$$= a^{mx} b^{mx} a^{ny} b^{ny} \quad \text{by (3)}$$
$$= b^{mx} a^{mx} b^{ny} a^{ny} \quad \text{by hypothesis}$$
$$= b^{mx + ny} a^{mx + ny} \quad \text{by (3)}$$
$$= ba.$$

Hence G is Abelian.

Order of an Element

The order of an element g in a group G is the smallest positive integers n such that $g^n = e$.

If no such integer exists, we say g has infinite order. The order of an element g is denoted by $o(g)$.

So, to find the order of a group element g, one need only compute the sequence of products g, g^2, g^3, ..., until one reach the identity for the first time. The exponent of this product is the order of g. If the identity never appears in the sequence, then g has infinite order.

Example 21. Let $G = \{1, -1, i, -i\}$ be a multiplicative group. Find the order of every element.

Solution. 1 is the identity element in G.

(*i*) $1^1 = 1 \Rightarrow o(1) = 1$.

(*ii*) $(-1)^2 = 1$, $(-1)^n \neq 1$ for any positive integer $n < 2$

Hence $o(-1) = 2$.

(*iii*) $(i)^4 = 1$ and $(i)^n \neq 1$ for any positive integer $n < 4$.

Hence $o(i) = 4$.

(*iv*) $(-i)^4 = 1$ and $(-i)^n \neq 1$ for any positive integer $n < 4$.

Hence $o(-i) = 4$.

Example 22. Find the order of every element in the multiplicative group $G = \{a, a^2, a^3, a^4, a^5, a^6 = e\}$

Solution. The identity element of the given group is $a^6 = e$.

$a^6 = e \Rightarrow o(a) = 6$

$(a^2)^3 = a^6 = e \Rightarrow o(a^2) = 3$

$(a^3)^2 = a^6 = c \Rightarrow o(a^3) = 2$

$(a^4)^3 = a^{12} = (a^6)^2 = e^2 = e \Rightarrow o(a^4) = 3$

$(a^5)^6 = (a^6)^5 = e^5 = e \Rightarrow o(a^5) = 6.$

and $(a^5)^n \neq e$ for any $n < 6$

$(a^5)^1 = a^6 = e \Rightarrow o(a^6) = 1.$

Thus the orders of elements $a, a^2, a^3, a^4, a^5, a^6$ are 6, 3, 2, 3, 6, 1 respectively.

Example 23(*i*). In a group (G, o), a is an element of order 30. Find the order of a^5.

Solution. Given $o(a) = 30$ so $a^{30} = e$, the identity element. Let $o(a^5) = n$. So, $(a^5)^n = e$ i.e., $a^{5n} = e$ where n is the least positive integer. Hence 30 is a divisor of $5n$. $\therefore n = 6$. Hence $o(a^5) = 6$.

Example 23(*ii*). *In a group G for a, b ∈ G, o(a) = 5, b ≠ e and $aba^{-1} = b^2$. Show that o(b) is 31.*

Solution.

$$(ab\,a^{-1})^2 = (ab\,a^{-1})(ab\,a^{-1}) = ab(a^{-1}a)ba^{-1} = abeba^{-1}$$
$$= abba^{-1} = ab^2a^{-1} = a(ab\,a^{-1})a^{-1} \quad (\because aba^{-1} = b^2)$$
$$= a^2\,ba^{-2}$$
$$(ab\,a^{-1})^4 = (ab\,a^{-1})^2\,(ab\,a^{-1})^2 = (a^2\,ba^{-2})\,(a^2\,ba^{-2})$$
$$= a^2b\,(a^{-2}a^2)\,ba^{-2} = a^2\,be\,ba^{-2} = a^2\,b^2\,a^{-2} \quad (\because a^0 = e)$$
$$= a^2(ab\,a^{-1})\,a^{-2} = a^3\,ba^{-3}$$

Similarly, $(ab\,a^{-1})^8 = a^4\,b\,a^{-4}$ and $(ab\,a^{-1})^{16} = a^5b\,a^{-5}$

$$(ab\,a^{-1})^{16} = ebe^{-1} \quad (\because o(a) = 5 \text{ i.e., } a^5 = e)$$
$$= be \quad (\because e^{-1} = e)$$
$$= b$$

Thus $(b^2)^{16} = b \Rightarrow b^{32} = b$ or $b^{31}\,b.b^{-1} = bb^{-1}$

$\therefore$ $b^{31}.e = e \Rightarrow b^{31} = e$

so, $o(b) = 31$

12.4. Groupoid, Semigroup and Monoid

Let (S, *) be an algebraic structure in which S is a non-empty set and * is a binary operation on S. Thus S is closed with the operation *. Such a structure consisting of a non-empty set S and a binary operation defined in S is called a **groupoid.**

An algebraic structure (S, *) is called a **semigroup** if the following conditions are satisfied:

1. The binary operation * is a closed operation *i.e.*, $a * b \in S$ for all $a, b \in S$. (closure law).
2. The binary operation * is an associative operation *i.e.*, $a * (b * c) = (a * b) * c$ for all $a, b, c \in S$. (associative law).

An algebraic structure (S, *) is called a **monoid** if the following conditions are satisfied:

1. The binary operation * is a closed operation. (closure law).
2. The binary operation * is an associative operation (associative law).
3. There exists an identity element, *i.e.*, for some $e \in S$, $e * a = a * e = a$ for all $a \in S$.

Thus a monoid is a semigroup (S, *) that has an identity element.

For example,

(*i*) If N be a set of natural numbers, then (N, +) is groupoid because the set N is closed under addition. But the set of odd integers is not a groupoid under addition operation since 3 + 3 = 6 do not belong to the set of odd integers and hence is not closed.

(*ii*) If Z be a set of all integers, then (Z, +) and (Z, .) are semi group as these two operations are closed and associative in Z.

(*iii*) N, the set of positive integers, and * is the operation of least common multiple (l.c.m) on N, (N, *) is a semigroup, it is also commutative.

Solution. For $a, b \in N$, define $a * b$ = l.c.m (a, b). Clearly $a * b \in N$ and for $a, b, c, \in N$.

$$\begin{aligned}(a * b) * c &= (\text{l.c.m. } (a, b)) * c \\ &= \text{l.c.m. } [\text{l.c.m. } (a, b), c] \\ &= \text{l.c.m. } [a, b, c] \\ &= \text{l.c.m. } [a, \text{l.c.m. } (b, c)] \\ &= a * (b * c).\end{aligned}$$

Hence * is associative. Hence $(N, *)$ is a semigroup. Clearly, $a * b$ = l.c.m (a, b) = l.c.m (b, a) $= b * a$ for all $a, b \in N$. Hence * is commutative.

The structure (Z, +) is a monoid with identity element 0 and (Z, .) is a monoid with 1 as the identity element. (P(S), U) is a monoid with φ as identity element.

We note that every group (G, *) is a semigroup. A semigroup (S, *) is commutative if * is commutative *i.e.*, $a * b = b * a$ for all $a, b \in$ S. A semi group (S, *) which is not commutative is called non-commutative. The set of integers (Z, +) and (Z, .) are commutative semigroups, where the binary operation on Z are usual addition and multiplication of integers.

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

Theorem 12.8. A semigroup (S, *) is a group if and only if

(*i*) there exists $e \in$ S such that $e * a = a$ for all $a \in$ S and

(*ii*) for all $a \in$ S there exists $b \in$ S such that $b * a = e$.

Proof: Suppose (S, *) is a semigroup that satisfies (*i*) and (*ii*). Then for $b \in$ S, there exists $c \in$ S such that $c * b = e$ by (*ii*).

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

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

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

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

The converse can be proved from the definition of a group.

Theorem 12.9. A semi group {S, *} is a group if and only if for $a, b \in$ S each of the equations $a * x = b$ and $y * a = b$ has a solution in S for x and y.

Proof: If S is a group, then by theorem 12.6, the equation $a * x = b$ and $y * a = b$ have solutions in S.

Conversely, suppose the given equations have solutions in S. Let the equation $y * a = a$ have a solution $e \in$ S. Then $e * a = a$. For any $b \in$ S, if t (depending on a and b) be the solution of the equations $a * x = b$, then $a * t = b$.

Now, $e * b = e * (a * t) = (e * a) * t = a * t = b$.

Consequently, $e * b = b$, for all $b \in$ S $\Rightarrow e$ is a left identity in S.

Next, a left inverse of an element $a \in$ S is given by the solution $y * a = e$ and the solution belongs to S.

Hence, for each $a \in$ S, there exist a left inverse in S. Thus S is a group.

Theorem 12.10. A finite semi-group (S, *) is a group if and only if (S, *) satisfies the cancellation laws (*i.e.*, $a * c = b * c$ implies $a = b$ and $c * a = c * b$ implies $a = b$ for all $a, b, c \in$ S).

Proof: Let (S, *) be a finite semi-group satisfying cancellation law *i.e.*,

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

and

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

Let S = $\{a_1, a_2 \ldots\ldots, a_n\}$ where a_i are all distinct element of S.

Consider now the elements $a_1 * a_1, a_1 * a_2, \ldots\ldots, a_1 * a_n$.

These elements belong to S and are distinct. If they are not distinct, let, $a_1 * a_i = a_1 * a_j$.

Then, by cancellation law, $a_i = a_j$, which contradicts the fact $a_i \neq a_j$.

Then composite elements $a_1 * a_1, a_1 * a_2 \ldots\ldots, a_1 * a_n$, being all distinct, they are the n given elements of S in some order. This shows that the equation $a * x = b$ for $a, b \in$ S has a solution in S.

Similarly, by forming the products $a_1 * a_1, a_2 * a_1, \ldots\ldots, a_n * a_1$, it can be shown that the equation $y * a = b$ for $a, b \in$ S has a solution in S.

Thus {S, *} is a semi-group in which each of the equations $a * x = b$ and $y * a = b$ has a solution in S for all $a, b \in$ S.

Hence by Theorem 12.9, {S, *} is a group.

Free Semi-group

Let A = $\{a_1, a_2 \ldots\ldots, a_n\}$ be a non empty set. A word ω on A is a finite sequence of its elements. For example.

$u = aab\ aabb = a^2ba^2b^2$ and $v = aaccbccab = a^2c^2b\ c^2ab$ are words on A = $\{a, b, c\}$

The length of a word w denoted by L (w) is the number of elements in w.

Thus L (u) = 7 and L (v) = 9.

Let A* consists of all words that can be formed from the alphabet A. Let α and β be elements of A*. If $\alpha = a_1\ a_2 \ldots\ldots\ a_m$ and $\beta = b_1 b_2 \ldots\ldots\ b_n$, then

$$\alpha\beta = a_1\ a_2 \ldots\ldots a_m\ b_1 \ldots\ldots b_n$$

Thus if α, β and γ are any elements of A*, then it is easy to see $\alpha\ (\beta.\ \gamma) = (\alpha \cdot \beta) \cdot \gamma$.

So * is an associative binary operation, and (A *) is a semi-group. The semi-group (A *) is called the free semi-group generated by A.

Let (S, *) be a group and B be a non-empty subset of S. If B is closed under operation *, then B is called a **sub semi-group** of (S, *). Since the elements of B are also elements of S, the associative law automatically holds for the elements of B.

Examples

(*i*) Let A and B denote, respectively, the set of even and odd positive integers. Then (A, ×) and (B, ×) are sub semi groups of (N, ×) since A and B are closed under multiplication. On the other hand, (A, +) is a sub semi group of (N +) since A is closed under addition, but (B, +) is not a sub semi group of (N, +) since B is not closed under addition.

(*ii*) Consider the free semi group K on the set A = $\{a, b\}$. Let L consist of all even words, that is, words with even length. The concatenation of two such words is also even. Thus L is a sub semi group of K.

12.5. Subgroup

Let (G, *) be a group and H is a subset of G. (H, *) is said to be subgroup of G if (H, *) is also group by itself.

Now every set is a subset of itself. Therefore, if G is a group, then G itself is a subgroup of G. Also if e is the identity element of G. Then the subset of G containing only identity element is also a subgroup of G. These two subgroups (G, *) and ($\{e\}$, *) of the group (G, *) are called **improper** or **trivial** subgroups, others are called proper or nontrivial subgroups.

Example 24

(*i*) The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$

(*ii*) The additive group of even integers is a subgroup of the additive group of all integers.

(*iii*) The set Q^+ of all non-zero positive rational numbers is a subgroup of the multiplicative group Q^* of all non-zero rational numbers.

Important Theorems

Theorem 12.11. The identity element of a sub group is the same as that of the group.

Proof: Let H be the subgroup of the group G and e and e' be the identity elements of G and H respectively.

Now, if $a \in H$, then $a \in G$ and $ae = a$, since e is the identity element of G.

Again $a \in H$, then $ae' = a$, since e' is the identity element of H.

Thus $ae = ae'$ which gives $e = e'$

Theorem 12.12. The inverse of any element of a subgroup is the same as the inverse of the same regarded as an element of the group.

Proof: Let H be the subgroup of the group G, and let e be the common identity element.

Let $a \in H$. Suppose b is the inverse of a in H and c is the inverse in G. Then we have $ba = e$ and $ca = e$.

Hence, in G we have $ba = ca \Rightarrow b = c$

Note. Since the identity of H is the same as that of G, it is easy to see that the order of an element of H is the same as the order of that element regarded as a member of G.

The next two theorems provide simple tests that suffice to show that a subset of a group is a subgroup.

Theorem 12.13. (two step subgroup test) A non-empty subset H of a group G is a subgroup of G if and only if

(*i*) $a \in H, b \in H \Rightarrow a * b \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

Proof: The condition is necessary. Suppose H is a subgroup of G. Then H must be closed with respect to operation * *i.e*, $a \in H, b \in H \Rightarrow a * b \in H$.

Let $a \in H$ and let a^{-1} be the inverse of a in G. Then the inverse of a in H is also a^{-1}. Since H itself is a group, therefore, each element of H must possess inverse. Therefore, $a \in H \Rightarrow a^{-1} \in H$

Thus the condition is necessary.

The Condition is Sufficient

We observe that the binary operation * in G is also a binary operation in H. Hence H is closed under the operation.

As the elements of H is also the elements of G and the elements of G satisfy the associative law for the binary operation, therefore, the elements of H will also satisfy the associative law.

Now $a \in H \Rightarrow a^{-1} \in H$

From the condition (*i*), we have $a \in H, a^{-1} \in H \Rightarrow aa^{-1} \in H = e \in H$ which shows the existence of identity element in H.

Thus all the conditions are satisfied, H is a subgroup of G.

Theorem 12.14. The necessary and sufficient condition for a non-empty sub-set H of a group (G, *) to be a subgroup is

$$a \in H, b \in H \Rightarrow a * b^{-1} \in H,$$

where b^{-1} is the inverse of b in G.

Proof: Let H be a sub-group and $a \in H$, $b \in H$. Since H is a sub-group and $b \in H$, b^{-1} must exist and will belong to H.

Now $a \in H$, $b^{-1} \in H \Rightarrow a * b^{-1} \in H$, by closure property.

Thus the condition is necessary.

To prove that this condition is also sufficient, we assume that

$$a \in H, b \in H \Rightarrow a * b^{-1} \in H.$$

We are to show that H is a sub-group of G.

By the given condition, we have

$$a \in H, a^{-1} \in H \Rightarrow a * a^{-1} \in H$$
$$\Rightarrow e \in H,$$

where e is the identity element. Hence H contains the identity elemente.

Again, we have $e \in H$, $a \in H \Rightarrow e * a^{-1} \in H$

$$\Rightarrow a^{-1} \in H,$$

where a^{-1} is the inverse of a. Therefore, the inverse of each element in H exists in H.

Now, if $b \in H$, then $b^{-1} \in H$.

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

$$\Rightarrow a * b \in H \text{ (closure property).}$$

Now, $H \subset G$ and the associative law holds good for G, as G is a group. Hence it is true for the elements of H. Thus all postulates for a group are satisfied for H. Hence H is a subgroup of G.

Example 25. Let G be the additive group of all integers and H be the subset of G consisting of all positive integers. Then H is closed with respect to addition *i.e.*, the composition in G. But H is not a subgroup of G since the identity $0 \notin H$.

Example 26. Let $G = \{.....3^{-2}, 3^{-1}, 1, 3, 3^2, ...\}$ be the multiplicative group consisting of all integral powers of 3. Let $H = \{1, 3, 3^2, ...\}$. Then $H \subset G$ and H is closed with respect to multiplication, But H is not a subgroup of G since the inverse of 3 *i.e.*, 3^{-1} does not belong to H.

Theorem 12.15. The intersection of any two sub-groups of a group (G, *) is again a sub-group of (G, *).

Proof: Let H_1 and H_2 form any two sub-groups of (G, *).

We have $H_1 \cap H_2 \neq \phi$, since at least the identity element is common to both H_1 and H_2

Let $a \in H_1 \cap H_2$ and $b \in H_1 \cap H_2$.

Now $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1$ and $b \in H_2$

Since H_1 and H_2 from sub-groups under the group (G, *), we have

$$a \in H_1, b \in H_1 \Rightarrow a * b^{-1} \in H_1,$$
$$a \in H_2, b \in H_2 \Rightarrow a * b^{-1} \in H_2$$

Finally, $a * b^{-1} \in H_1$, $a * b^{-1} \in H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

Thus we see,

$a \in H_1 \cap H_2$, $b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

Therefore, $H_1 \cap H_2$ forms a sub-group under (G, *)

Note: The union of two subgroups is not necessarily a subgroup.

For example, let G be the additive group of integers.

Then $H_1 = \{....., -6, -4, -2, 0, 2, 4, 6, ...\}$ and

$H_2 = \{....., -12, -9, -6, -3, 0, 3, 6, 9, 12.....\}$

are both subgroups of G.

Now $H_1 \cup H_2 = \{....., -4, -3, -2, 0, 2, 3, 4, 6, ...\}$

Obviously $H_1 \cup H_2$ is not closed with respect to addition as $2 \in H_1 \cup H_2$,

$3 \in H_1 \cup H_2$ but $2 + 3 = 5 \notin H_1 \cup H_2$. Therefore, $H_1 \cup H_2$ is not a subgroup of G.

Cosets

Let H be a subgroup of a group G and let $a \in G$. Then the set $\{a * h : h \in H\}$ is called the left coset generated by a and H and is denoted by aH.

Similarly the set $Ha = \{h * a : h \in H\}$ is called the right coset and is denoted by Ha. The element a is called a representative of aH and Ha.

It is evident that both aH and Ha are subsets of G.

If e be the identity element of G, then $e \in H$ and $He = H = eH$. Therefore, H itself is a right as well as a left coset.

In general $aH = Ha$, but in the abelian group, each left coset coincides with the corresponding right coset.

If the group operation be addition, then the right coset of H in G generated by a is defined as

$$H + a = \{h + a : h \in H\}.$$

Similarly, the left coset $a + H = \{a + h : h \in H\}$.

Index of a subgroup in a group. If H is a subgroup of a group G, the number of distinct right (left) oosets of H in G is called the index of H in G and is denoted by [G : H] or by i_G (H).

Example 27. Let G be te additive group of integers *i.e.*,

$G = \{... -3, -2. - 1, 0, 1, 2, 3, ...\}$.

Let H be the subgroup of G obtained on multiplying each element of G by 3. Then

$H = \{....., -9, -6, -3, 0, 3, 6, 9,....\}$.

Since the group G is abelian any right coset will be equal to the corresponding left coset. Let us form the right cosets of H in G.

We have $0 \in G$ and

$$H = H + 0 = \{...., -9, -6, -3, 0, 3, 6, 9,....\}$$

Again $1 \in H$ and $H + 1 = \{...., -8, -5, -2, 1, 4, 7, 10, ...\}$.

Then $2 \in G$ and $H + 2 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$.

We see that the right cosets H, H + 1 and H + 2 are all distinct and moreover these are disjoint *i.e.*, have no element common.

Now $3 \in G$ and $H + 3 = \{...., -6, -3, 0, 3, 6, 9, 12, ...\}$.

We see that H + 3 = H. Also we observe that $3 \in H$.

Again $4 \in G$ and $H + 4 = \{...., -5, -2, 1, 4, 7, 10, 13,....\} = H + 1$

Thus there exists three disjoint right cosets namely H, H + 1, H + 2.

The union of all right cosets of H in G will be equal to G. i.e.

$$G = H \cup (H + 1) \cup (H + 2)$$

The index of H in G is 3.

Properties of Cosets

Let H be a subgroup of G, and a and b belong to G, Then,

1. $a \in aH$
2. $aH = H$ if and only if $a \in H$
3. $aH = bH$ or $aH \cap bH = \phi$
4. $aH = bH$ if and only if $a^{-1} b \in H$,

Analogous results hold for right cosets.

Proof 1. $a = ae \in aH$, e is the identity element of G.

2. If e be the identity in G and so is in H, then

$$aH = H \Rightarrow ae \in H$$

i.e., $$aH = H \Rightarrow a \in H$$

Again, if $a \in H$ and $h \in H$ then ... (1)

$$a \in H \Rightarrow ah \in H \; \forall \; h \in H$$

$\therefore$ $$aH \subset H$$

Also $a \in H \Rightarrow a^{-1} H$, H being a sub-group of the group G, satisfies group axioms.

$\Rightarrow a^{-1} h \in H \; \forall \; h \in H$ by closure law in H

$\Rightarrow a(a^{-1} h) \in H \; \forall \; h \in H$ by closure law in H

$\Rightarrow h \in aH \; \forall \; h \in H$

$\therefore$ $H \subset aH$

So $aH \subseteq H$ and $H \subset aH \Rightarrow aH = H$

Next $$a \in H \Rightarrow aH = H$$

Hence $aH = H \Leftrightarrow a \in H$ by (1) and (2). ... (2)

3. Let H be a sub-group of a group G and let aH and bH be two of its left cosets. Assume that $aH \cap bH \neq \phi$ and let c be the common element of the two cosets.

Then we may write $c = ah$ and $c = bh'$, for $h, h' \in H$.

Therefore $ah = bh'$, giving $a = bh' h^{-1}$.

Since H is a sub-group, we have $h' h^{-1} \in H$.

Let $$h' h^{-1} = h'' \text{ so that } a = bh''.$$

Hence $aH = (bh'')H = b(h'' H) = bH$, since $h'' H = H$.

Hence the two left cosets aH and bH are identical if $aH \cap bH \neq \phi$.

Thus either $aH \cap bH = \phi$ or $aH = bH$.

4. We have,

$$aH = bH \Rightarrow a^{-1} aH = a^{-1} bH$$

$$\Rightarrow (a^{-1} a) H = (a^{-1} b) H$$

$$\Rightarrow eH = (a^{-1} b)H, \; e \text{ being the identity in G and so in H.}$$

$$\Rightarrow H = (a^{-1} b)H$$

$\therefore$ $$aH = bH \Rightarrow a^{-1} b \in H$$

Also, if $a^{-1} b \in H$, then ... (1)

$bH = e(bH) = (aa^{-1})(bH) = a(a^{-1} b)H = aH$

(1) and (2) follow that $aH = bH \Leftrightarrow a^{-1} b \in H$. ... (2)

Normal Subgroup

A subgroup H of a group G is said to be a normal subgroup of G if $Ha = aH$ for all $a \in G$.

Clearly every subgroup of an Abelian group is a normal subgroup. To verify that a subgroup is normal one can use the following theorem.

Theorem 12.16. A subgroup H of a group G is normal if and only if $g^{-1} hg \in H$ for every $h \in H, g \in G$.

Proof: Let H be a normal subgroup of G. Let $h \in H, g \in G$

Then $$Hg = gH \text{ (Definition of normal subgroup)}$$

Now $$hg \in Hg = gH$$

so $$hg = gh_1 \text{ for some } h_1 \in H.$$

i.e., $$g^{-1} hg = h_1 \in H.$$

Conversely let H be such that

$$g^{-1} hg \in H \ \forall \ h \in H, g \in G.$$

Consider $a \in G$ For any $h \in H$, $a^{-1}h\,a \in H$

Therefore, $ha = a(a^{-1}ha) \in aH.$

Consequently $Ha \subseteq aH.$

Let $b = a^{-1}$

then $b^{-1} hb \in H$

But $b^{-1} hb = (a^{-1})^{-1} ha^{-1} = aha^{-1}$

This gives $aha^{-1} \in H$

so that $ah = (aha^{-1})\, a \in Ha$

which proves that $aH \subseteq Ha.$

Hence $aH = Ha.$

This theorem shows that, equivalently a subgroup H of a group G can be defined to be a normal subgroup if

$$g^{-1}hg \in H \ \forall \ h \in H, g \in G.$$

Example 28. Consider the group $(Z, +)$. Let $H = \{3n : n \in Z\}$ show that H is a subgroup of Z

Solution. It is a subgroup of Z since

(*i*) H is non-empty.

(*ii*) Let $x, y \in H$. Then there exist $p, q \in Z$ such that $x = 3p, y = 3q.$

Now $xy^{-1} = 3p - 3q = 3(p - q)$ where $p - q \in Z.$

Thus $xy^{-1} \in H$

Hence H is a subgroup of Z.

Example 29. Let G be a group. For a fixed element of G, let $G_x = \{a \in G : ax = xa\}$. Show that G_x is a subgroup of G for all $x \in G$.

Solution. Since (*i*) $ex = xe$, $e \in G_x$. Therefore, $G_x \neq \phi$.

(*ii*) $a, b \in G_x \Rightarrow ax = xa$ and $bx = xb$.

Now
$$\begin{aligned} (ab)\, x &= abx, \\ &= axb, && (\because bx = xb) \\ &= xab, && (\because ax = xa) \\ &= x\,(ab). \end{aligned}$$

This shows $ab \in G_x$. Hence G_x satisfies the closure axiom.

(*iii*)
$$\begin{aligned} a \in G_x &\Rightarrow ax = xa. \\ &\Rightarrow a^{-1}(ax)\, a^{-1} = a^{-1}(xa)\, a^{-1}. \\ &\Rightarrow a^{-1} axa^{-1} = a^{-1} xaa^{-1}, \\ &\Rightarrow exa^{-1} = a^{-1} xe, \\ &\Rightarrow xa^{-1} = a^{-1} x, \\ &\Rightarrow a^{-1} \in G_x. \end{aligned}$$

Thus the inverse of each element of G_x is in G_x.

Order of a group. The number of elements in a group is called the *order* of the group.

The order of a group G is denoted by $o(G)$. A group of finite order is called a *finite group*. In using the concept of cosets we prove a theorem due to Langrange which expresses a relation between the order of a finite group and the order of its subgroup.

Lagrange's Theorem

Theorem 12.18. The order of each sub-group of a finite group G is a divisor of the order of the group G.

Proof. Let H be any sub-group of order m of a finite group G of order n. We consider the left coset decomposition of G relative to H.

We first show that each coset a H consists of m different elements.

Let $\quad H = \{h_1, h_2, ..., h_m\}$.

Then $a\,h_1, a\,h_2, ..., a\,h_m$ are the m members of a H, all distinct.

For, we have

$$a\,h_i = a\,h_j \Rightarrow h_i = h_j, \text{ by cancellation law in } G.$$

Since G is a finite group, the number of distinct left cosets will also be finite, say k. Hence the total number of elements of all cosets is $k\,m$ which is equal to the total number of elements of G. Hence:

$$n = mk. \qquad \ldots (1)$$

This shows that m, the order of H, is a divisor of n, the order of the group G.

Note. The converse of Lagrange's theorem is not true.

Cor. 1. If G be a finite group of order n and $n \in G$, then

$$a^n = e.$$

Let o $(a) = m$ which implies $a^m = e$.

Now, the sub-set H of G consisting of all the integral powers of a is a sub-group of G and the order of H is m.

Then, by the above theorem, m is a divisor of n.

Let $n = mk$, then

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

SOLVED EXAMPLES

Example 30. If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$, then prove that H is a normal subgroup of G.

Solution. For any $g \in G$, $h \in H$; $(gh)^2 \in H$ and $g^{-2} \in H$.

Since H is a subgroup; $h^{-1} g^{-2} \in H$ and so $(gh)^2 h^{-1} g^{-2} \in H$. This gives that $gh\,gh\,h^{-1} g^{-2} \in H$, i.e., $ghg^{-1} \in H$. Hence H is a normal subgroup of G.

Example 31. If G be an abelian group with identity e, then prove that all elements x of G satisfying the equation $x^2 = e$ form a sub-group H of G.

Solution. Let $H = \{x : x^2 = e\}$.

Now $x^2 = e \Rightarrow x = x^{-1}$.

Therefore, if $x \in H$, then x^{-1} also belongs to H.

Furthermore $e^2 = e$.

Hence the identity element of G also belongs to H.

Let $x, y \in H$.

Then, since G is abelian, we have

$$\begin{aligned} xy &= yx \\ &= y^{-1} x^{-1}, \text{ as } x^{-1} = x \text{ and } y^{-1} = y \\ &= (xy)^{-1}. \end{aligned}$$

Therefore, $\quad (xy)^2 = e$.

Hence $xy \in H$ and H is a sub-group of G.

Example 32. For any two subgroups H and K of a group G following hold:

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

(2) If H is normal in G then $H \cap K$ is normal in K.

(3) If H and K are both normal in G, then $H \cap K$ is normal in G.

Solution. (1) Since $e \in H \cap K$, $H \cap K$ is non-void.

Now $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow ab^{-1} \in H$ and $ab^{-1} \in K$

$\Rightarrow ab^{-1} \in H \cap K$.

Hence $H \cap K$ is a subgroup of G.

(2) Let H be normal in G. Let $x \in K$, $a \in H \cap K$.

Then $x^{-1} ax \in K$ since $x, a \in K$.

Further $x^{-1} ax \in H$ since H is normal and $a \in H$. Consequently $x^{-1} ax \in H \cap K \ \forall\ x \in K$, $a \in H \cap K$.

Hence $H \cap K$ is a normal subgroup of K.

Example 33. If H is a subgroup of index 2 in a group G, then H is a normal subgroup of G.

Solution. Suppose H is a subgroup of index 2 in a group G so that number of distinct right (or left) cosets of H in G is 2.

To prove that H is normal in G, it suffices to show that

$Hx = xH \ \forall\ x \in G$.

Let $x \in G$ be arbitrary. Then $x \in H$ or $x \notin H$.

If $x \in H$, then $Hx = xH = H$ and so $Hx = xH$

If $x \notin H$, then index of H is 2 says that right coset (left coset) decomposition contains only two cosets

$\therefore\ G = He \cup Hx$, $G = eH \cup xH$

Hence $H \cup Hx = G = H \cup xH \Rightarrow xH = G - H = Hx$

$\Rightarrow xH = Hx$

$\therefore$ In either case $Hx = xH$, meaning thereby H is normal in G.

12.6. Cyclic Group

A Group G is called a cyclic group if, for some $a \in G$, every element of G is of the form a^n, where n is some integer i.e., $G = \{a^n : n \in Z\}$. The element a is then called a generator of G.

If G is a cyclic group generated by a, it is denoted by $G = \langle a \rangle$. The elements of G are in the form

$\ldots\ldots a^{-2}, a^{-1}, a^0, 0, a, a^2, a^3 \ldots\ldots$

There may be more than one generator of a cyclic group. Every cyclic group has at least two generators, generator and inverse of it.

Example 34. The set of integers with respect to + *i.e.*, $(Z, +)$ is a cyclic group, a generator being 1.

Solution. We have $1^0 = 1$, $1^1 = 1$, $1^2 = 1 + 1 = 2$, $1^3 = 1 + 1 + 1 = 3$ and so on.

Similarly 1^{-1} = inverse of $1 = -1$

$1^{-2} = (1^2)^{-1} = -2$, $1^{-3} = (1^3)^{-1} = (3)^{-1} = -3$ and so on.

Thus each element of G can be expressed as some integral power of 1.

Similarly we can show that -1 is also a generator.

Example 35. *The multiplicative group $\{1, w, w^2\}$ is a cyclic group.*

Solution. We have $w^0 = 1$, $w^1 = w$, $w^2 = w^2$, $w^3 = 1$

and $(w^2)^0 = 1$, $(w^2)^1 = w^2$, $(w^2)^2 = w^4 = w$

Thus each element of the group can be expressed as some integral powers of w and w^2. Hence the group is a cyclic group with generators w and w^2.

Example 36. The group $(G, +_6)$ is a cyclic group where $G = \{0, 1, 2, 3, 4, 5\}$.

Solution. We see that

$$1^1 = 1,\ 1^2 = 1 +_6 1 = 2,\ 1^3 = 1 +_6 1^2 = 3,\ 1^4 = 1 +_6 1^3 = 1 +_6 3 = 4,\ 1^5 = 1 +_6 1^4 = 1 +_6 4 = 5,\ 1^6 = 0$$

Thus $G = \{1^1, 1^2, 1^3, 1^4, 1^5, 1^6 = 0\}$

Hence G is a cyclic group and 1 is a generator.

Similarly, it can be shown that 5 is another generator.

Some Important Properties of Cyclic Grous

Theorem 12.18. Every cyclic group is an abelian group.

Solution. Let G be a cyclic group and let a be a generator of G so that

$$G = \langle a \rangle = \{a^n : n \in Z\}$$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 g_1$$

So, G is abelian.

Note: 1. The symmetric group S_3 is not cyclic, since it is not abelian.

The dihedral group D_4 is not cyclic, since it is not abelian.

2. An abelian group is not necessarily a cyclic group. For example, Klein's 4-group V is abelian but it is not cyclic.

Theorem 12.19. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

Proof. Let $G = \langle a \rangle$ be a cyclic group generated by a. Let a^r be any element of G, where r is some integer. We can write $a^r = (a^{-1})^{-r}$. Since $-r$ is also some integer, therefore each element of G, is generated by a^{-1}. Thus a^{-1} is also a generator of G.

Theorem 12.20. If a cyclic group G is generated by an element a of order n, then a^m is a generator of G if and only if the greatest common divisor of m and n is 1 *i.e.*, if and only if m and n are relative primes.

Proof. Suppose m is relatively prime to n. Consider the cyclic subgroup $H = \{a^m\}$ of G generated by a^m. Obviously $H \subseteq G$ since each integral power of a^m will also be an integral power of a.

Since m is relatively prime to n, therefore, there exist two integers r and s such that $rm + sn = 1$.

So $a^{rm+sn} = a^1$

$\Rightarrow a^{rm} \cdot a^{sn} = a$

$\Rightarrow (a^m)^r = a$; since $a^{sn} = (a^n)^s = e^s = e$

So, each integral power of a will also be some integral power of a^m. Therefore, $G \subseteq H$. Hence $H = G$ and a^m is a generator of G.

Conversely, suppose a^m is a generator of G. Let the greatest common divisor of m and n be d and $d \neq 1$ *i.e.*, $d > 1$. Then m/d and n/d must be integers.

Now $(a^m)^{n/d} = (a^n)^{m/d} = e^{m/d} = e$, Obviously n/d is a positive integer less than n itself. Thus $o(a^m) < n$. Therefore a^m can not be a generator of G because the order of a^m is not equal to the order of G. Hence d must be equal to 1. Thus m is prime to n.

Example 37. How many generators are there of the cyclic group G of order 8?

Solution. Let a be generator of G. Then o $(a) = 8$. We can write G $= \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

7 is prime to 8, therefore, a^7 is also a generator of G.

5 is prime to 8, therefore, a^5 is also a generator of G.

3 is prime to 8, therefore, a^3 is also a generator of G.

Thus there are only four generators of G *i.e.*, a, a^3, a^5, a^7

Example 38. Show that the group $(\{1, 2, 3, 4, 5, 6\}, \times_7)$ is cyclic. How many generators.

Solution. G be a given group. If there exists an element $a \in G$ such that $o(a) = 6$ *i.e.*, equal to the order of the group G then the group G will be a cyclic group and a will be a generator of G.

Note that $o(3) = 6$ because $3^1 = 3$, $3^2 = 3 \times_7 3 = 2$, $3^3 = 3^2 \times_7 3 = 6$, $3^4 = 6 \times_7 3 = 4$, $3^5 = 4 \times_7 3 = 5$, $3^6 \times_7 3 = 5 \times_7 3 = 1$ *i.e.*, the identity element.

So, G is cyclic and 3 is a generator of G. We can write

$$G = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}.$$

Now 5 is prime to 6. There 3^5 *i.e.*, 5 is also generator of G.

Infinite Cyclic Group

If H is a cyclic group generated by a subject to all the powers of a are distinct, then $H = \langle a \rangle$ is an infinite cyclic group.

Example 39. Let G be an infinite cyclic group generated by a. Show that

(*i*) $a^r = a^t$ if and only if $r = t$, where $r, t \in Z$,

(*ii*) G has exactly two generators.

Solution. (*i*) Suppose $a^r = a^t$ and $r = t$. Let $r > t$. Then $a^{r-t} = e$. Then $o(a)$ is finite, say, $o(a) = n$. Then $G = \{e, a, \ldots\ldots, a^{n-1}\}$, which is a contradiction since G is an infinite group. The converse is straightforward.

(*ii*) Let $G = \langle b \rangle$ for some $b \in G$. Since $a \in G = \langle b \rangle$ and $b \in G = \langle a \rangle$, $a = b^r$ and $b = a^t$ for some $r, t \in Z$. Thus, $a = b^r = (a^t)^r = a^{rt}$. Hence, by (*i*). $rt = 1$. This implies that either $r = 1 = t$ or $r = -1 = t$. Thus, either $b = a$ or $b = a^{-1}$. Now from (*i*), $a = a^{-1}$. Therefore, G has exactly two generators.

12.7 Permutation Group

Let A be a finite set. Then a function $f : A \to A$ is said to be a **permutation** of A if

(*i*) f is one – one

(*ii*) f is onto

i.e. A bijection from A to itself is called a permutation of A.

The number of distinct elements in the finite set A is called the **degree** of permutation.

Consider a set $A = \{a_1, a_2, \ldots\ldots, a_n\}$ and let $f : A \to A$ be a bijection function. Then every element of A has a unique image in A, no two distinct elements of A have the same image, and every element of A has a unique pre-image, under f. Thus, the range of f is of the form

$$\text{Ran}(f) = \{f(a_1), f(a_2) \ldots\ldots f(a_n)\}$$

In the notation of relations the function f is given by

$$f = \{(a_1, f(a_1)), (a_2, f(a_2)), \ldots\ldots, (a_n, f(a_n))\}$$

This is written in two line notation as

$$f = \begin{pmatrix} a_1 & a_2 \ldots\ldots\ldots a_n \\ f(a_1) & f(a_2) \ldots\ldots\ldots f(a_n) \end{pmatrix}$$

Since A is a finite set, its elements can be ordered as the first, the second, ..., the nth. Therefore, it is convenient to take A to be a set of the form $\{1, 2, 3, \ldots, n\}$ for some positive integer n instead of $\{a_1, a_2, a_3, \ldots\ldots a_n\}$.

In general, a permutation f on the set $\{1, 2, 3, \ldots\ldots, n\}$ can be written as

$$f = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots n \\ f(1) & f(2) & f(3)\ldots\ldots f(n) \end{pmatrix}$$

Obviously, the order of the column in the symbol is immaterial so long as the corresponding elements above and below in that column remain unchanged.

Equality of Two Permutations

Let f and g be two permutations on a set X. Then $f = g$ if and only if $f(x) = g(x)$ for all x in X.

Example 40. Let f and g be given by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \qquad g = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Evidently $f(1) = 2 = g(1)$, $f(2) = 3 = g(2)$

$f(3) = 4 = g(3)$, $f(4) = 1 = g(4)$

Thus $f(x) = g(x)$ for all $x \in \{1, 2, 3, 4\}$ which implies $f = g$.

Identity Permutation

If each element of a permutation be replaced by itself. Then it is called the identity permutation and is denoted by the symbol I. For example,

$$I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$ is an identity permutation.

Product of Permutations (or Composition of Permutation)

The product of two permutations f and g of same degree is denoted by $f\,o\,g$ or fg, meaning first perform f and then perform g.

$$f = \begin{pmatrix} a_1 & a_2 & a_3 \ldots . a_n \\ b_1 & b_2 & b_3 \ldots . b_n \end{pmatrix}.$$

$$g = \begin{pmatrix} b_1 & b_2 & b_3 \ldots . b_n \\ c_1 & c_2 & c_3 \ldots . c_n \end{pmatrix}.$$

Then $$f\,o\,g = \begin{pmatrix} a_1 & a_2 & a_3 \ldots . a_n \\ c_1 & c_2 & c_3 \ldots . c_n \end{pmatrix}.$$

For, f replaces a_1 by b_1 and then g replaces b_1 by c_1 so that $f\,o\,g$ replaces a_1 by c_1. Similarly $f\,o\,g$ replaces a_2 by c_2, a_3 by c_3,.... a_n by c_n.

Clearly $f\,o\,g$ is also a permutation on S.

It should be observed that the permutation g has been written in such a manner that the second row of f coincides with the first row of g. This is most essential in order to find $f\,o\,g$.

If we want to write gf, then f should be written in such a manner that the second row of g must coincide with the first row of f.

Example 41. Find the product of two permutations and show that it is not commutative.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \text{and} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Solution.

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}2&1&4&3\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$$

$$gf = \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\begin{pmatrix}3&2&1&4\\4&1&2&3\end{pmatrix}$$

$$= \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}.$$

We observe that $fg \neq gf$.

This shows that the product of two permutations is not commutative.

But it can be shown that permutation multiplication is associative.

Let $$P_1 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\ P_2 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\ P_3 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$\therefore$ $$P_1 (P_2 P_3) = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\left[\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right]$$

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

and $$(P_1 P_2) P_3 = \left[\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right]\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

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

$\therefore$ $$P_1 (P_2 P_3) = (P_1 P_2) P_3$$

Inverse Permutation

Since a permutation is one-one onto map and hence it is inversible, *i.e.*, every permutation f on a set

$$P = \{a_1, a_2 \ldots\ldots, a_n\}.$$

has a unique inverse permutation denoted by f^{-1}.

Thus if $$f = \begin{pmatrix}a_1 & a_2 \ldots\ldots a_n\\ b_1 & b_2 \ldots\ldots b_n\end{pmatrix}$$

then $$f^{-1} = \begin{pmatrix}b_1 & b_2 \ldots\ldots b_n\\ a_1 & a_2 \ldots\ldots a_n\end{pmatrix}.$$

Total Number of Permutations

Let X be a set consisting of n distinct elements. Then the elements of X can be permuted in $n!$ distinct ways. If S_n be the set consisting of all permutations of degree n, then the set S_n will have $n!$ distinct permutations of degree n. This set S_n is called the symmetric set of permutations of degree n.

For example, if $A = \{1, 2, 3\}$, then $S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ where

$$p_0 = I_A = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad p_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad p_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\quad p_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

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

The multiplication table for the composition of permutations in S_3 is as given below:

Multiplication Table for S_3

$\circ$	p_0	p_1	p_2	p_3	p_4	p_5
p_0	p_0	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	p_0	p_5	p_3	p_4
p_2	p_2	p_0	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	p_0	p_1	p_2
p_4	p_4	p_5	p_3	p_2	p_0	p_1
p_5	p_5	p_3	p_4	p_1	p_2	p_0

The table shows that

(*i*) The multiplication of any two permutations of S_3 gives a permutation of S_3. So, S_3 is closed with respect to multiplication.

(*ii*) Associativity law holds for $(p_1\, p_3)\, p_4 = p_5\, p_4 = p_0$ and $p_1\, (p_3\, p_4) = p_1 p_1 = p_0$

(*iii*) Identity element exists, p_0 when composed with any permutation gives that permutation.

(*iv*) Every permutation has its own inverse.

Hence S_3 is a group. It is a non-commutative group since $p_1 p_2 \neq p_2 p_1$, $p_3 p_2 \neq p_2 p_3$

Let A be a set of degree n. Let P_n be the set of all permutations of degree n on A. Then $(P_n, *)$ is a group, called a **permutation group** and the operation $*$ is the composition (multiplication) of permutations. This is proved in the following theorem.

Theorem 12.21. The set P_n of all permutation on n symbols is finite group of order $n!$ with respect to the binary composition of permutations. For $n \leq 2$, P_n is abelian and for $n > 2$ it is always non-abelian.

Proof Let $X = \{a_1, a_2, a_3, \ldots, a_n\}$ is a finite set. Since the different arrangements of the elements of X are $n!$, then the number of distinct permutations of degree n will be $n!$. If P_n is the set of all such permutations, then P_n has $n!$ distinct elements.

Closure Property : Let f and g be any two permutations in P_n where

$$f = \begin{pmatrix} b_1 & b_2 & b_3 & \ldots & b_n \\ c_1 & c_2 & c_3 & \ldots & c_n \end{pmatrix} \text{and } g = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ b_1 & b_2 & b_3 & \ldots & b_n \end{pmatrix}$$

be any two permutations of degree n. Then,

$$fg = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix}$$

Since, $c_1, c_2, \ldots, c_n$ are also of arrangement of n elements $a_1, a_2, \ldots a_n$ of X, then fg is a permutation of degree n.

Thus $fg \in P_n$ for all $f, g \in P_n$

Hence, P_n is closed for the composition known as product of two permutations.

Associativity

Let $f = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ d_1 & d_2 & \ldots & d_n \end{pmatrix}$, $g = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ c_1 & c_2 & \ldots & c_n \end{pmatrix}$ and $h = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$

be any three permutations of degree n, then

$$fg = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

$$(fg)\,h = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

Also $$gh = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

$$f(gh) = \begin{pmatrix} c_1 & c_2 & \dots & c_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ d_1 & d_2 & \dots & d_n \end{pmatrix}$$

Now from (1) and (2), we get $(fg)\,h = f(gh)$

Hence, the composition is associative in P_n

Existence of Identity

The identity permutation of degree n is the identity element of P_n.

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ and $I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$

Then $$f\,I = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = f$$

Also $$I\,f = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = f$$

Thus $$f\,I = I\,f = f$$

Existence of Inverse

Let $f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ be a permutation of degree n then the permutatio

$f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ is also a permutation of degree n.

Now, $$f\,f^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = I$$

Also, $$f^{-1}\,f = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = I$$

Therefore, f^{-1} is the inverse of f.

Therefore $(P_n, *)$ is a group of order $n!$ with respect to composition of permutations. For $n=1$ the set P_n has only one element and for $n = 2$, the number of elements in P_n is 2.

We know that every group of order one or of order two is abelian. Thus $(P_n, *)$ is a abelian group for $n \le 2$.

For $n > 2$, $(P_n, *)$ is not an abelian group as composition of permutation is not a commutative operation *i.e.* $fg \neq gf$.

The group $(P_n, *)$ is also called **symmetric group** of degree n and denoted by S_n.

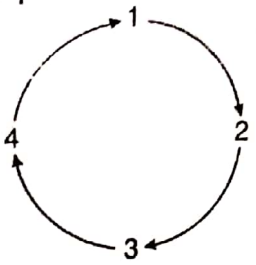
Cyclic Permutations

A permutation which replaces n objects cyclically is called a cyclic permutation of degree n.

Let us consider the permutation.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

This assignment of values could be presented schematically as follows.



Such diagrams are cumbersome, we leave out the arrows and simply write S = (1 2 3 4). We read the new symbol in cyclical order from left to right as follows : 1 is replaced by 2, 2 is replaced by 3, 3 is replaced by 4, and 4 is replaced by 1.

Thus the meaning of the symbol is to replace each number which follows and the last number by the first.

Note that (1 2 3 4) = (2 3 4 1) = (3 4 1 2) = (4 1 2 3). Thus a circular permutation may be denoted by more than one rowed symbols.

The number of elements permuted by a cycle is said to be its **length** and the **disjoint cycles** are those which have no common elements. A cycle of length one means that the image of an element is the element itself and represents identity permutation. Cycles of length one are generally omitted.

Every permutation of a finite set can be expressed as a cycle or as a product of disjoint cycles e.g.,

$$t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{pmatrix}$$

is written as $t = (1, 2)\ (3, 4, 6)\ (5)$

The cycle (1, 2) has length 2. The cycle (3, 4, 6) has length 3 and the cycle (5) has length 1 and none of them have a symbol common and hence they are disjoint cycles.

Transpositions

A cyclic permutation such as (a, b) which interchanges the symbols leaving all other unchanged is called a transposition. In other words, transposition is cycle of length two of the form (a, b) *i.e.*, it is a mapping which maps each object onto itself excepting two, each of which is mapped on the other *e.g.*, (1, 2) is a transposition.

Every permutation can be resolved as a product of finite number of transpositions but the decomposition is not unique. However, for a given permutation the number of transpositions is always even or always odd.

The process consists of two steps:

(*i*) Express the permutation as a product of disjoint cycles.

(*ii*) Express each cycle as a product of transpositions.

Even and Odd Permutations

A permutation is said to be even or odd according as it can be expressed as a product of even or odd number of transpositions.

SOLVED EXAMPLES

Example 42. If $A = (1\ 2\ 3\ 4\ 5)$ and $B = (2\ 3)\ (4\ 5)$, find AB

Solution. We have $AB = (1\ 2\ 3\ 4\ 5)\ (2\ 3)\ (4\ 5)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1\ 3\ 5).$$

Example 43. Express the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ as a product of transpositions.

Solution. First we express the given permutation as a product of disjoint cycles. Here 1 is moved to 6 and then 6 to 1, giving the cycle (1, 6). Then 2 is moved to 5, which is moved to 3, which is moved to 2, giving (2, 5, 3). This takes care of all the elements except 4 which is left fixed. Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 6)\ (2\ 5\ 3)$$

Multiplication of disjoint cycles is clearly commutative, so the order of the factors (1, 6) (2, 5, 3) is not important.

Example 44. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ is odd, while the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is even.

Solution. We have $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 5)\ (2\ 6\ 3)$

$$= (1\ 5)\ (2\ 6)\ (2\ 3)$$

Thus the given permutation can be expressed as the product of an odd number of transpositions and hence the permutation is an odd permutation.

Again $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix} = (1\ 6)\ (2\ 3\ 4\ 5)$

$$= (1\ 6)\ (2\ 3)\ (2\ 4)\ (2\ 5)$$

Since it is a product of an even number of transpositions, the permutation is an even permutation.

Example 45. Find the inverse of the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

Solution. Let the inverse of the given permutation be

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix}$$

Then $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ x & y & z & u & v \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

i.e., $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ y & z & x & v & u \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

$\therefore\ x = 3, y = 1, z = 2, u = 4, v = 5$

Hence the required inverse is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$.

Alternating Group

The set A_n of all even permutations of degree n forms a finite group of order $n!/2$ with respect to the composition of permutation and is called alternative group and is denoted by A_n.

Theorem 12.22 Out of $n!$ permutations of n symbols, $n!/2$ are even permutations and $n!/2$ are odd permutations.

Proof. Let P_n be the set of all permutations on n symbols. Let the number of even and odd permutations in P_n be s and t. Then $n! = s + t$.

Let $e_1, e_2, ..., e_s$ be s distinct even permutations and $o_1, o_2, ... o_t$ be t number of distinct odd permutations, then

$$P_n = \{e_1, e_2, ..., e_s, o_1, o_2, ... o_t\}$$

Let I be any proposition in P_n then by closure property $Ie_1, Ie_2, ..., Ie_s, Io_1, Io_2, ... Io_t$ are all distinct elements of P_n. For if $Io_1 = Io_2$, then $o_1 = o_2$ which contradicts that o_1 and o_2 are distinct.

Now $Ie_1, Ie_2, ..., Ie_s$ are odd permutations. Since there are t number of odd permutations, then $s \le t$. Similarly, we can show that the even permutations $Io_1, Io_2, ..., Io_t$ are distinct elements of P_n. Therefore $t \le s$.

Thus $t = s = n!/2$.

Theorem 12.23 If A_n is the set of all even permutations of degree n, then A_n is a finite group of order $n!/2$ with respect to the composition of permutation.

Proof Let f and g be any two even permutations on n symbols.

Closure property : It is known that the product of two even permutations is an even permutation. Therefore the set A_n is closed with respect to the composition of permutation.

Associativity : It is known that the multiplication of permutations is an associative composition.

Existence of Identity : An identity permutation is an even permutation. If I is an identity permutation then $I \in A_n$. Then $If = f = fI \in A_n$.

I is an identity element.

Existence of Inverse : Let $f \in A_n$. be any even permutation. Then $f \in P_n$. Thus there exists an inverse f^{-1} in P_n such that $ff^{-1} = f^{-1}f = I$. Since f is an even permutation so f^{-1} is also an even permutation and hence $f^{-1} \in A_n$. Hence every element of A_n has multiplicative inverse in A_n.

Hence A_n is a group of all even permutations of order $n!/2$.

Note that the set O_n of all odd permutations does not form a group with respect to the composition of permutation. As the product of two odd permutations is an even permutation, the set O_n is not closed.

Dihedral Group D_n

Symmetry : A symmetry of a body is a transformation (mapping) which brings the body into coincidence with itself. The transformation can be thought of as a rigid motion (*i.e.*, a motion which keeps the distance between any points of the body unchanged) or as a mapping of the set of points comprising the body (or space) to itself.

Group of Symmetries: The set of all symmetries of a figure forms an another permutation group called the group of symmetries or symmetry group.

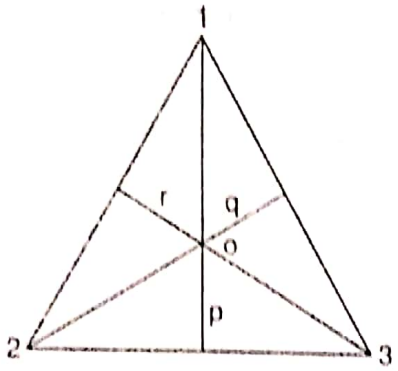
Dihedral group: The symmetry group of the regular polygon of n sides is called the dihedral group of degree n and is denoted by D_n. For example, D_3 is the dihedral group of an equilateral

triangle, D_4 is the dihedral group of a square, D_5 is the dihedral group of a regular pentagon. It is easy to find that D_3 has 6 elements, D_4 has 8 elements and D_5 has 10 elements.

The group D_4 is also known as the **Octic group.**

Example 46. Find the group of symmetries of an equilateral triangle.

Solution. Consider an equilateral whose vertices are marked 1, 2, 3 as shown in Fig. and O be its centre.



Let G be the set consisting of six elements:

(*i*) The elements ρ_0, ρ_1, ρ_2 which represent, respectively, the anticlockwise rotations about its centre O by 0°, 120° and 240°. Evidently the identity mapping is a symmetry. The rotation by an angle 120° and 240° are symmetry.

(*ii*) The reflections about perpendicular bisector of the sides of the triangle represented by μ_1, μ_2 and μ_3 are three other symmetries of the set G. In the line p, the image of the vertex 2 is 3, and the image of the vertex 3 is 2, and the image of 1 is itself. Thus 1, 3, 2 are the images of 1, 2, 3 in the line p. Then μ_1 represents this arrangement of images. Similarly μ_2 and μ_3 represent the arrangements images of 1, 2, 3 in the line q and r respectively.

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

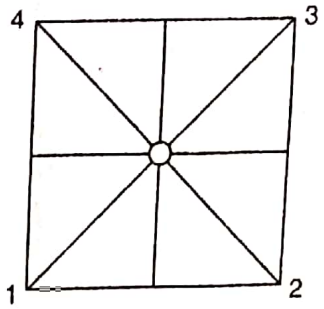
The composition table is given below and it follows from the table that $(G, *)$ is a non-abelian group of order six and known as the **dihedral group of degree 3 (D_3).**

Note that the composition of the symmetries of the triangle is equivalent to the multiplication of the corresponding permutation. This group is same as S_3. This is also called a **symmetric group of degree 3.**

o	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Example 47. Find the group of symmetries of a square.

Solution. Consider a square whose vertices are marked 1, 2, 3, 4 as shown in Fig. and O be its centre.



Let G be the set consisting of eight elements:

(*i*) The elements $\rho_0, \rho_1, \rho_2, \rho_3$ which represent, respectively, the anticlockwise rotation about its centre O by 0°, 90°, 180° and 270°.

(*ii*) The two reflections denoted by μ_1, μ_2 about the lines passing through the centre of the square and parallel to the sides.

(*iii*) The two reflections denoted by σ_1, σ_2 about the diagonals of the square.

Thus $G = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \sigma_1, \sigma_2\}$

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

The composition table is given below. To prepare the table, it is sufficient to know for each $x, y \in G$, first the effect of x and then the effect of y on the vertices to obtain $y \circ x$, and it follows from the table that $(G, *)$ is a non-abelian group of order eight and known as the **dihedral group of degree 4 (D_4).**

$\circ$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	σ_1	σ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	σ_1	σ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	σ_2	σ_1	μ_1	μ_2
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	σ_2	σ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	σ_1	σ_2	μ_2	μ_1
μ_1	μ_1	σ_1	μ_2	σ_2	ρ_0	ρ_2	ρ_1	ρ_3
μ_2	μ_2	ρ_2	μ_1	σ_1	ρ_2	ρ_0	ρ_3	ρ_1
σ_1	σ_1	μ_2	σ_2	μ_1	ρ_3	ρ_1	ρ_0	ρ_2
σ_2	σ_2	μ_1	σ_1	μ_2	ρ_1	ρ_3	ρ_2	ρ_0

12.8. Homomorphism and Isomorphism of Groups

Structure preserving maps between groups are called morphisms. So, to relate two groups requires notions about such maps, which is defined below.

Definition. Let (G, o) and $(G', *)$ be two groups. A mapping $f : G \to G'$ is said to be a **homomorphism** if

$$f(a \circ b) = f(a) * f(b), \forall\ a, b \in G.$$

A homomorphism is said to be a **monomorphism** if it is one-to-one, *i.e.*, $f(x) = f(x') \Rightarrow x = x'$ where $x, x' \in G$.

A homomorphism is said to be an **epimorphism** if it is onto, *i.e.*, every element of G' is an image of some element $x \in G$.

A homomorphism of a group (G, o) into itself is called an **endomorphism,** *i.e.*, $f : G \to G$ is said to be an **endomorphism** if $f(a \circ b) = f(a) \circ f(b), \forall\ a\ b, \in G$.

The image of f is called the **homomorphic image** of f and is denoted by $f(G)$.

For example,

Let $G = (R, +)$ and $G' = (R^+.)$. The mapping $f : G \to G'$ is defined by $f(x) = 2^x$. Then for $a, b \in G$, $a + b \in G$ we have $f(a) = 2^a$, $f(b) = 2^b$ and $f(a + b) = 2^{a+b}$.

Now, $f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b)$

So, f is a homomorphism.

Basic Properties on Homomorphisms

Theorem 12.24. Let (G, o) and $(G', *)$ be two groups and $f : G - G'$ be a homomorphism. Then

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

(*ii*) $f(a^{-1}) = \{f(a)\}^{-1}, \forall\ a \in G$.

(*iii*) if $a \in G$ then $f(a^n) = \{f(a)\}^n$, n being an integer

(*iv*) if $a \in G$ and $o(a)$ is finite then $o(f(a))$ is a divisor of $o(a)$.

Proof:

(*i*) Here $a \in G \Rightarrow f(a) \in G'$

$\Rightarrow$ $f(a) * e' = f(a)$, as e' is the identity element of G'.

$= f(a \circ e)$, as e is the identity element of G.

$= f(a) * f(e)$, as f is a homomorphism

$\therefore$ $f(a) * e' = f(a) * f(e)$, in G'

$\Rightarrow$ $e' = f(e)$, by left cancellation law in G'.

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

(*ii*) $a \in G \Rightarrow a^{-1} \in G$. Then $f(a) \in G'$ and $f(a^{-1}) \in G'$.

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

Also, $e' = f(e) = f(a^{-1} \circ a) = f(a^{-1}) * f(a)$ ...(2)

From (1) and (2), we get

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

Hence $f(a^{-1})$ is the inverse of $f(a)$ in G'.

$\therefore$ $f(a^{-1}) = \{f(a)\}^{-1}, \forall\ a \in G$.

(*iii*) **Case 1 : $n = 0$**

In this case the given statement reduces to (*i*) and hence it holds.

Case 2 : n is a positive integer

The given statement is true for $n = 1$. Let us assume that it is true for $n = m$, m being a positive integer.

Then $f(a^m) = \{f(a)\}^m$,

$\therefore$ $f(a^{m+1}) = f(a^m \circ a)$

$= f(a^m) * f(a)$, since f is a homomorphism

$= \{f(a)\}^m * f(a)$, by (1)

$= \{f(a)\}^{m+1}$.

This show that if the given statement is true for m then it is also true for $m + 1$. But we have already seen that it is true for $n = 1$, so by the principle of mathematical induction the given statement is true for any positive integer n.

Case 3 : n is a negative integer

Let $n = -m$ where m is a positive integer.

$\therefore \quad f(a^n) = f(a^{-m}) = f\{(a^{-1})^m\}$

$= \{f(a^{-1})\}^m$, by Case 2

$= [\{f(a)\}^{-1}]^m$, by (*ii*)

$= [f(a)\}^{-m} = \{f(a)\}^n$.

$\therefore \quad f(a^n) = [f(a)\}^n$, for any integer n.

(*iv*) Let $a \in G$ and $o(a) = m$, a finite number.

$\therefore \quad a^m = e \Rightarrow f(a^m) = f(e) = e'$, by (*i*)

$\Rightarrow \quad \{f(a)\}^m = e'$, by (*iii*)

$\Rightarrow o(f(a))$ is a divisor of $m = o(a)$.

Example 48. Show that the group $\{Z_9, +\}$ is a homomorphic image of the group $\{Z, +\}$.

Solution. Here Z = the set of all integers and $Z_9 = \{[0], [1], [2], \ldots [8]\}$ where $[0], [1], \ldots, [8]$ are residue classes modulo 9.

Let us consider the mapping

$$f : Z \to Z_9 \text{ defined by } f(m) = [m] \pmod 9.$$

f is a homomorphism, since

$$f(m + n) = [m + n] = [m] + [n] = f(m) + f(n), \forall\ m, n \in Z.$$

Note that $[m + n] = [r] \in Z_9$, where r is the least non-negative remainder when $m + n$ is divided by 9. Also for any $[r] \in Z9$, there exists $9q + r \in Z$ s.t. $f(9q + r) = [r]$. So, f is onto $\{Z_9, +\}$.

Hence the group $\{Z_9, +\}$ is a homomorphic image of the group $\{Z, +\}$.

Theorem 12.25. Let (G, o) and $(G', *)$ be two groups and the mapping $f : G \to G'$ is a homomorphism. Then the homomorphic image $f(G)$ is a subgroup of the group G'.

Proof. Let e and e' be the identity elements of the groups G and G' respectively. Since e' $(= f(e)) \in f(G)$, therefore, $f(G)$ is non-empty. Let us take two arbitrary elements $a', b' \in f(G)$. Then there exist elements $a, b \in G$ such that $a' = f(a)$ and $b' = f(b)$. Also $a \circ b^{-1} \in G$.

Now, $a' * (b')^{-1} = f(a) * (f(b))^{-1} = f(a) * f(b^{-1}) = f(a \circ b^{-1}) \in f(G)$.

Thus $a', b' \in f(G) = a' * (b')^{-1} \in f(G) \Rightarrow f(G)$ is a subgroup of the group G'.

Kernel of Homomorphism

Let (G, o) and $(G', *)$ be two groups and $f : G \to G'$ is a homomorphism. Then the ***kernel*** of f, denoted by $ker\ f$, is a subset of G defined by

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

Thus $ker\ f$ is the set of those elements of G that are mapped to the identity element of G' under the homomorphism f.

Theorem 12.26. Let (G, o) and $(G', *)$ be two groups and $f : G \to G'$ is a homomorphism. Then ker f is a normal subgroup of G.

Proof. By definition $ker\ f$ is a subset of G. Let e and e' be the identity elements of G and G' respectively. Then $f(e) = e'$ implying that $ker\ f$ is a non-empty subset of G.

Let us take two arbitrary elements $a, b \in ker\ f$. Then $f(a) = e'$ and $f(b) = e'$.

Now, $f(a \circ b^{-1}) = f(a) * f(b^{-1}) = f(a) * (f(b))^{-1}$ [by Theorem 12.24 (*ii*)]

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

$\therefore a \circ b^{-1} \in ker\ f$. Thus, $a, b \in ker\ f \Rightarrow a \circ b^{-1} \in ker\ f$. Hence $ker\ f$ is a subgroup of G.

To prove that $ker\ f$ is normal in G, let $g \in G$ and $h \in ker\ f$. Then

$f(g \circ h \circ g^{-1}) = f(g) * f(h) * f(g^{-1}) = f(g) * e' * (f(g))^{-1} f(g) * (f(g))^{-1} = e'$.

$\therefore g \circ h \circ g^{-1} \in ker\ f$. Hence $ker\ f$ is normal in G.

Theorem 12.27. Let $(G, \circ)$ and $(G', *)$ be two groups and $f: G \to G'$ is a homomorphism. Then f is one-to-one if and only if $ker\ f = \{e\}$, e being the identity element of G.

Proof. Let f be one-to-one. We take an arbitrary element $a \in ker\ f$. If e' is the identity element of G', then

$f(a) = e' = f(e)$ $[\because f(e) = e']$ $\Rightarrow$ $a = e$ $[\because f$ is one-one$]$

Since a is an arbitrary element of $ker\ f$ and $a \in ker\ f \in a = e$, it follows that $ker\ f = \{e\}$.

Conversely, let $ker\ f = \{e\}$. We take two arbitrary elements $a, b \in G$.

Since f is homomorphism, therefore,

$$f(a) = f(b) \Rightarrow f(a) * (f(b))^{-1} = f(b) * (f(b))^{-1} \Rightarrow f(a) * f(b^{-1}) = e'$$
$$\Rightarrow f(a \circ b^{-1}) = e' \Rightarrow a \circ b^{-1} \in ker\ f \Rightarrow a \circ b^{-1} = e \Rightarrow a = b.$$

Hence f is one-to-one.

Isomorphism of Groups

Let $(G, \circ)$ and $(G', *)$ be two groups and $f: G \to G'$ is a homomorphism. f is said to be an ***isomorphism*** if f is one-to-one and onto, *i.e.*, f is monomorphism as well as an epimorphism.

Two groups $(G, \circ)$ and $(G', *)$ are said to be ***isomorphic groups*** if there exists an isomorphism $f: G \to G'$. If G and G' are isomorphic groups, then we write, $G \simeq G'$.

An isomorphism of a group onto itself is called an ***automorphism.***

Example 49. If R be the group of real numbers under addition and let R^+ be the group of positive real numbers under multiplication. Let $f: R \to R^+$ be defined by $f(x) = e^x$ then show that f is an isomorphism.

Solution. If $f(a) = f(b)$, so that $e^a = e^b$, then $a = b$. Thus f is one to one.

If $c \in R^+$, then $\ln c \in R$ and $f(\ln c) = e^{\ln c} = c$,

Thus each element of R^+ is the f image of some element of R and hence f is onto.

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

Hence f is an isomorphism.

Example 50. If R^+ be the multiplicative group of all positive real numbers.

Define $f: R^+ \to R^+$ by $f(x) = x^2$ for all $x \in R^+$. Show that f is automorphism of R^+.

Solution. Now for any $x, y \in R^+$, $f(xy) = (xy)^2 = x^2y^2 = f(x) f(y)$.

Thus f is an endomorphism of R^+.

Further $f(x) = f(y) \Rightarrow x^2 = y^2 \Rightarrow x = y$, since $x > 0, y > 0$.

Hence f is a one-one mapping.

Given $x \in R^+$, $\sqrt{x} \in R^+$ such that $f(\sqrt{x}) = (\sqrt{x})^2 = x$.

This proves that f is also onto.

Consequently f is an automorphism.

Theorem 12.28. Let G and G_1 be two groups and $f : G \to G_1$ be a group homomorphism. Then Ker f is a normal subgroup of G.

Proof. Let e_1 be the identity element of the group G_1. Then $Ker\ f = \{x \in G | f(x) = e_1\}$. Since $f(e) = e_1$ it follows that $e \in Ker\ f$. Hence $Ker\ f \neq \phi$. Let $a, b \in Ker\ f$. Then $f(a) = e_1$, $f(b) = e_1$ and hence $f(ab^{-1}) = f(a)f(b^{-1}) = e_1e_1^{-1} = e_1e_1 = e_1$. This implies that $ab^{-1} \in Ker\ f$, whence $Ker\ f$ is a subgroup of G. To show that $Ker\ f$ is a normal subgroup, let $a \in Ker\ f$ and $g \in G$; then $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)e_1f(g^{-1}) = f(g)f(g)^{-1} = e_1$ and hence $gag^{-1} \in Ker\ f$. Consequently, $Ker\ f$ is a normal subgroup of G.

Factor or Quotient Group

If H is a normal subgroup of a group G, then the set of all left cosets of G forms a group with respect to the multiplication of left coset and defined as

$$(aH)\,(bH) = (ab)\,H$$

called the factor group or quotient group of G by N and is denoted by G/N *i.e.* $G/H = \{gH : g \in G\}$.

One can similarly define multiplication of right cosets as $(H/a)(H/b) = H(ab)$ which makes the set of right cosets of H in G a group, also called the *factor group* of G by H. It is easy to observe that the factor groups obtained by left cosets and also by right cosets are isomorphic.

Theorem 12.29. Every homomorphism image of group G is isomorphic to some quotient group of G.

Proof. Let G′ be the homomorphic image of the group G, and f be the corresponding homomorphism.

Let K be the kernel of this homomorphism. Then K is a normal subgroup of G. We shall prove that

$G/k \cong G'$.

If $a \in G$, then $Ka \in G/K$ and $f(a) \in G'$. Consider the mapping

$\varphi : G/K \to G'$ such that $\varphi(Ka) = f(a)$, $\forall\ a \in G$.

First we shall show the mapping φ is well defined, *i.e.*, if $a, b \in G$ and $Ka = Kb$. Then $\varphi(Ka) = \varphi(Kb)$.

We have
$$Ka = Kb \Rightarrow ab^{-1} \in K$$
$$\Rightarrow f(ab') = e' \qquad \text{(the identity of G')}$$
$$\Rightarrow f(a)\,f(b^{-1}) = e'$$
$$\Rightarrow f(a)\,(f(b))^{-1} = e'$$
$$\Rightarrow f(a)\,(f(b))^{-1}\,f(b) = e'\,f(b)$$
$$\Rightarrow f(a)\,e' = f(b)$$
$$\Rightarrow f(a) = f(b)$$
$$\Rightarrow \varphi(Ka) = \varphi(Kb)$$
$$\Rightarrow \varphi \text{ is well defined}$$

Now we show φ is one-one G′. We have
$$\varphi(Ka) = \varphi(Kb) \Rightarrow f(a) = f(b)$$
$$\Rightarrow f(a)\,(f(b))^{-1} = f(b)\,(f(b))^{-1}$$
$$\Rightarrow f(a)\,f(b^{-1}) = e^{-1}$$
$$\Rightarrow f(ab^{-1}) = e'$$

$\Rightarrow ab^{-1} \in K$ [$\because$ K is Kernel]

$Ka = Kb$

i.e. φ is one-one.

Now we show φ is onto G'.

Let $y \in G'$. Then $y = f(a)$ for some $a \in G$ because f is onto G'. Now $Ka \in G/K$, and we have

$$\varphi(Ka) = f(a) = y$$

φ is onto G'

Finally we have $\varphi\{(Ka)(Kb)\} = \varphi(Kab) = f(ab)$

$= f(a) f(b)$

$= \varphi(Ka)\, \varphi(Kb)$

$\therefore$ φ is an isomorphism of G/K into G'.

Hence $G/K \cong G'$.

Homomorphism of Semigroups

Let $(S, *)$ and $(T, 0)$ be any two semigroups. A mapping $f : S \to T$ such that for any two elements $a, b \in S$.

$$f(a * b) = f(a)\, 0\, f(b)$$

is called a **semigroup homomorphism** of S into T.

A homomorphism of a semigroup into itself is called a semigroup **endomorphism.**

A homomorphism $f : S \to T$ is called a semigroup **isomorphism** if f is a one-to-one onto.

An isomorphism of a semigroup onto itself is called a semigroup **automorphism.**

Theorem 12.30 Let $(S, *)$, (V, Δ) be semigroups $f : S \to T$, and $T \to V$ be semigroup homomorphism. Then $gof : S \to V$ is a semigroup homomorphism from $(S, *)$ to (V, Δ).

Proof. Let $a, b \in S$ then

$$\begin{aligned}(gof)(a * b) &= g[f(a * b)] \\ &= g[f(a)\, 0\, f(b)] \\ &= g[\{f(a)\} \Delta g[f(b)] \\ &= (gof)(a) \Delta (gof)(b)\end{aligned}$$

which shows that $gof : S \to V$ is a semigroup homomorphism from $(S, *)$ to (V, Δ).

Example 51. Show that there exists a semigroup homomorphism from the semigroup $(N, +)$ of natural numbers under addition to the semigroup $(\{0, 1, 2, 3\}, +_4)$, where $+_4$ denotes the operation of addition modulo 4 on the set $(0, 1, 2, 3\}$.

Solution. Let us define a mapping $f : N \to (0, 1, 2, 3\}$ as follows:

$$\begin{aligned}f(a) &= a(\text{mod } 4) \text{ for all } a \in N \\ &= \text{the remainder } r,\ 0 \le r < 4, \text{ when } a \text{ is divided by 4.}\end{aligned}$$

For any $a, b \in N$, let $f(a) = i$ and $f(b) = j$. Then

$$\begin{aligned}f(a + b) &= (a + b)\ (\text{mod } 4) \\ &= (i + j)\ (\text{mod } 4) \\ &= i +_4 j \\ &= f(a) +_4 f(b)\end{aligned}$$

Thus, f is a homomorphism.

Solved Examples

Example 52. Define a binary operation o on the set of non-negative integers as follows:

$$a \circ b = a^2 + b^2$$

Does the operation has (*i*) an identity element? (*ii*) an inverse element?

Solution. (*i*) If possible let there exists an identity element e which is a non-negative integer such that

$$e \circ a = a \text{ for all non-negative integers } a$$

$$\Rightarrow \quad e^2 + a^2 = a \quad \Rightarrow \quad e^2 = a - a^2$$

which is negative for all integers greater than one and also for different values of a we get different values of e^2. So an identity element does not exist.

(*ii*) Since an identity element does not exist, so an inverse element also does not exist.

Example 53. In a group G, prove that $(ab)^2 = a^2 b^2$ if $(ab)^{-1} = a^{-1} b^{-1}$ where $a, b \in G$.

Solution. Let $(ab)^2 = a^2 b^2$

Now, $(ab)^2 = a^2 b^2 \Rightarrow (ab)(ab) = (aa)(bb)$

$\Rightarrow$ $a(ba)b = a(ab)b$ (by associative law)

$\Rightarrow$ $ba = ab$ (by left and right cancellation laws)

$\Rightarrow$ $(ba)^{-1} = (ab)^{-1}$

$\Rightarrow$ $a^{-1} b^{-1} = (ab)^{-1}$

Let $\mathbf{(ab)^{-1} = a^{-1}b^{-1}}$

Now, $(ab)^{-1} = a^{-1}b^{-1} \Rightarrow (ab)^{-1} = (ba)^{-1}$

$\Rightarrow$ $\{(ab)^{-1}\}^{-1} = \{(ba)^{-1}\}^{-1}$

$\Rightarrow$ $ab = ba$ ...(1)

$\therefore$ $(ab)^2 = (ab)(ab)$

$= a(ba)b$ (by associative law)

$= a(ab)b$ (by (1))

$= (aa)(bb)$ (by associative law)

$= a^2 b^2$.

Example 54. Let G be a group. If $a, b \in G$ such that $a^4 = e$, the identity element of G and $ab = ba^2$, prove that $a = e$.

Solution. Given: $ab^2 = ba^2$ ...(1)

$\therefore$ $b^{-1}(ab) = b^{-1}(ba^2)$

$\Rightarrow$ $b^{-1}ab = (b^{-1}b)a^2$ (by associative law)

$\Rightarrow$ $b^{-1}ab = ea^2 = a^2$

$\Rightarrow$ $(b^{-1}ab)(b^{-1}ab) = a^2 a^2 = a^4 = e$ ($\because$ Given, $a^4 = e$)

$\Rightarrow$ $b^{-1}a(bb^{-1})ab = e$ (by associative law)

$\Rightarrow$ $b^{-1}(ae)ab = e$ *i.e.* $b^{-1}a^2b = e$

$\Rightarrow$ $(bb^{-1})a^2b = be$ *i.e.* $(ea^2)b = b$

$\Rightarrow$ $ba^2 b = bb$ *i.e.* $(ab)b = b$ using (1)

$\Rightarrow$ $ab = b$ *i.e.* $ab = eb$

$\Rightarrow$ $a = e$ (by right cancellation law)

Example 55. Let G be a group having elements a and b such that o $(a) = 4$, o $(b) = 2$ and $a^3b = ba$. Find the order of ab.

Solution. Given G be a group, $a, b \in G$,

$$o(a) = 4, o(b) = 2 \text{ and } a^3b = ba$$

$\therefore$ $a^4 = e$, $b^2 = e$, where e is the identity element of G

Now, $a^3b = ba \Rightarrow a(a^3b) = a(ba)$

$\Rightarrow$ $(aa^3)b = (ab)a$ (by associative law)

$\Rightarrow$ $a^4b = (ab)a$

$\Rightarrow$ $eb = (ab)\,a$ ($\because a^4 = e$)

$\Rightarrow$ $b = (ab)\,a$ (e being the identity element)

$\Rightarrow$ $bb = (ab)\,ab$

$\Rightarrow$ $b^2 = (ab)^2$

$\Rightarrow$ $e = (ab)^2$ ($\because b^2 = e$)

So, the order of ab is either 1 or 2. If possible, let o $(ab) = 1$, *i.e.*, $ab = e$ —(1)

Then $a^3b = ba \Rightarrow a^2(ab) = ba$

$\Rightarrow$ $a^2e = ba$ (by assumption (1))

$\Rightarrow$ $aa = ba$

$\Rightarrow$ $a = b$ (by right cancellation law)

$\Rightarrow$ o(a) = o(b), which is a contradiction since given o $(a) = 4$ and o $(b) = 2$.

So our assumption o$(ab) = 1$ is not possible. Hence o$(ab) = 2$.

Example 56. Let G be an Abelian group. Prove that the subset $S = \{p \in G : p = p^{-1}\}$ forms a subgroup of G.

Solution. (i) Since $e = e^{-1}$, so $e \in S$. Hence S is a non-empty subset of G.

(ii) $x \in S \Rightarrow x = x^{-1} \Rightarrow x^{-1} \in S$. —(2)

(iii) Let $x, y \in S \quad \therefore x = x^{-1}, y = y^{-1}$

Here $S \subseteq G$ and G is Abelian.

$\therefore$ $x, y \in S \Rightarrow x, y \in G$

$\Rightarrow$ $xy = yx$ (by (1))

$\Rightarrow$ $xy = y^{-1}x^{-1}$

$\Rightarrow$ $xy = (xy)^{-1}$

$\Rightarrow$ $xy \in S$.

From (i)–(iii) it follows that S is a subgroup of G.

Example 57. Show that the set $G = \{1, 2, 3, 4, 5, 6\}$ forms an Abelian group with respect to multiplication modulo 7. Is it a cyclic group?

Solution. Let us form the following composition table under multiplication modulo 7 on G.

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Example 58. Let $W = \{0, 1, 2, ...\}$ then $(W, +)$ is a monoid with identity element 0. Let $S = \{e, 0, 1\}$ and * be a binary operation defined on S as given in the following composition table:

*	e	0	1
e	e	0	1
0	0	0	0
1	1	0	1

Then $(S, *)$ is a monoid with identity element e. Let $f : W \to S$ be defined as $f(0) = 1$ and $f(i) = 0$ for $i \neq 0$. Show that f is a semi-group homomorphism but not a monoid homomorphism.

Solution. Using the given composition table we see that

$$f(a + b) = f(a) * f(b), \forall\, a, b \in W$$

Hence f is a semigroup homomorphism. But $f(0) \neq e$ where 0 is the identity element of $(W, +)$ and e is the identity element of $(S, *)$

Therefore f is not a monoid homomorphism.

Example 59. Prove that a group G is Abelian if and only if $(ab)^{-1} = a^{-1} b^{-1}, \forall\, a, b \in G$.

Solution. Let $(ab)^{-1} = a^{-1} b^{-1}, \forall\, a, b \in G$

Now, $(ab)^{-1} = a^{-1} b^{-1} \Rightarrow (ab)^{-1} = (ba)^{-1}$

$\Rightarrow$ $\{(ab)^{-1}\}^{-1} = \{(ba)^{-1}\}^{-1}$

$\Rightarrow$ $ab = ba$ $\quad (\because (x^{-1})^{-1} = x, \forall\, x \in G)$

$\therefore$ $ab = ba, \forall\, a, b \in G$

Hence G is an Abelian group

Let G be an Abelian group

$\therefore$ $ab = ba, \forall\, a, b \in G$

$\Rightarrow$ $(ab)^{-1} = (ba)^{-1}$

$\Rightarrow$ $(ab)^{-1} = a^{-1} b^{-1}$

$\therefore$ $(ab)^{-1} = a^{-1} b^{-1}, \forall\, a, b \in G.$

Example 60. If a group G has four elements, show that it is Abelian.

Solution. Let $G = \{e, a, b, c\}$ be a multiplicative group of order four where e is the identity element. Since $e^{-1} = e$, there must be at least one more element in G which is its own inverse.

Let $a^{-1} = a$. If $b^{-1} = b$ and $c^{-1} = c$ then G is Abelian

If $b^{-1} = c$, then $c^{-1} = b$ and we have $bc = cb = e$. Now $a^{-1} = a \Rightarrow aa = e$.

Observe that $ab = a \Rightarrow b = e$ and $ab = b \Rightarrow a = e$ which are not possible. So, $ab = c$. Similarly, $ba = c$, $ac = ca = b$, $bb = a$ and $cc = b$.

The composition table for G is a follows:

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

From this composition table it is clear that G is commutative, *i.e.*, G is an Abelian group.

Problem Set 12.1

1. Given an example of a set which is closed under certain binary operation but a sub-set of it may not be closed under the same operation.
2. S is a given set and $x, y \in S$. Show that the operation x on S as given with S confirm the statement along with it.
   (*i*) $S = \{2, 4, 6, 8, \ldots\ldots\ldots\}$: $x * y = x + y$ is a binary operation
   (*ii*) $S = \{1,3,5,7, \ldots\ldots\ldots\}$: $x * y = xy$ is a binary operation
   (*iii*) S = the set of integers : $x * y = x - y$ is a binary operation
   (*iv*) S = the set of integers : $x * y = x \div y$ is not a binary operation
   (*v*) S = the set of positive integers : $x * y = x + \log_x y$ is not a binary operation.
3. On the set N of all natural numbers, define the operation * on N by $x * y = gcd\ (x, y)$ for all $x, y \in N$. Show that * is commutative and associative.
4. Show that the operation * on the set $Q - \{1\}$ of all rational numbers except 1, defined by $a * b = a + b - ab$ satisfies (*i*) the closure property (*ii*) the commutative law and (*iii*) the associative law. What is the identity element? Find the inverse $\in Q - \{1\}$.
5. An operation * is defined on the set of positive rational number Q^+ by $a * b = ab/2$ for all $a, b \in Q^+$. Show that (*i*) * is a binary operation on Q^+ (*ii*) * is commutative (*iii*) * is associative.
6. Show that each element of $\{-2, -1, 0, 1, 2,\}$ has a unique inverse element for the operation arithmetic addition, as defined on Z.
7. Which of the following are associative binary operations ?
   (*i*) (Z, *), where $x * y = (x + y) - (x \cdot y)$ for all $x, y \in Z$.
   (*ii*) (R, *), where $x * y = |x + y|$ for all $x, y \in Z$.
8. Show that the binary operation * defined by $a * b = a.b^2$, $a, b \in R$ is not associative.
9. An operation * defined on the set Z of integers as $(a, b) * (c, d) = (a + c, b + d)$. Show that * is commutative as well as associative $(-a, -b)$ is an inverse of (a, b).
10. For each operation * defined below, determine whether it is commutative and whether it is associative
    (*i*) on Z, $a * b = b - a$
    (*ii*) on Q, $a * b = ab + 2$
    (*iii*) on R, $a * b = a + b + ab$
    (*iv*) on N, $a * b = a^2 + b^2$.
    (*v*) on $R^0 = R - \{0\}$, where $x * y = |x|\, y$
    (*vi*) on $R^0 = R - \{0\}$, where $x * y = \min\{x, y\}$
    (*vii*) on R, where $a * b = ab/3$
11. Give examples of binary operations on a finite set which is (*i*) associative but not commutative (*ii*) Commutative but not associative.
12. If a set A has n elements, then (*i*) what is the number of binary composition on A? (*ii*) What is the number of commutative composition in A?
13. Let $A = \{a, b\}$
    (*i*) Prepare a composition table for each of the binary operations that can be defined on A.
    (*ii*) Using part (*i*), identify the binary operations on A that are commutative.
14. Let $X = \{0, 1, 2, 3\}$. Given $a, b \in X$ define $a * b = a$. Prepare a composition table.
15. Let $X = \{0, 1, 2\}$. Given $a, b \in X$ define $a * b = c$ where c is the remainder after $a + b$ is divided by 3. Prepare a composition table and show that 0 is the identity element.

16. Let S = {a, b, c} and * is an operation on s, defined by the table given below:

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

(*i*) Is * a binary operation on S?
(*ii*) Is * commutative.

17. Let S = {a, b, c, d}. Compute the missing entries in the table so that the composition may be associative.

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

18. Show that for the binary operation $a * b = a.b$ on G = {1, −1, *i*, − *i*} all the following properties are satisfied (*i*) associativity (*ii*) the existence of unit element (*iii*) existence of inverse for each element.

Problem Set 12.2

1. State the axioms which a set must obey so that it may form a group.
2. Define a group, giving at least two examples. If G is a group, then show that the identity element of G is unique and every $a \in G$ has a unique inverse in G.
3. Show that the set of even integers (including Zero) form an additive group. Show further that the group is abelian. If the set be of odd integers, then prove that it does not form a group with respect to addition.
4. If * is a binary operation in Q^+ defined by (*i*) $a \times b = ab/3$ and (*ii*) $a \times b = ab/2$, $a, b \in Q^+$ (the set of all positive rational numbers). Show that (Q^+, *) are abelian groups.
[**Hints.** (*i*) $e = 3, a^{-1} = 9/a$ (*ii*) $e = 2, a^{-1} = 4/a$].
5. Prove that (G, X) is a abelian group in each of the following cases where *x* denotes multiplication of numbers.
   (*i*) $G = \{2n : n \in Z\}$
   (*ii*) $G = \{a + ib : a, b \in R\}$
   (*iii*) $G = \{-1, 1\}$.
6. Examine which of the following are groups. For those which fail to be groups mention which group axioms do not hold.
   (*a*) The set R with respect to * where $a * b = a$, for all $a \in R$.
   (*b*) The set Z with respect to *, where $a * b = a + b + 1$ for $a, b \in Z$.
   (*c*) The set R with respect to, where $a * b = a + b - ab$ for all $a, b \in Z$
   (*d*) The set Z with respect to, where $a * b = |ab|$ for all $a, b \in Z$.
7. Show that {1, 2, 3} under multiplication modulo 4 is not a group but that {1, 2, 3, 4} under multiplication modulo 5 is a group.
8. Show that {1, 5, 7, 11} is a group under multiplication modulo 12.
9. Show that {0, 1, 2, 3} forms a group with respect to addition modulo 4.
10. Is the set {1, 2, 3, 4, 5} a group under addition modulo 6?
11. Which of the following sets are groups under multiplication modulo 11?
    (*i*) {1, 3, 5, 7, 8} (*ii*) {1, 8} (*iii*) {1, 10}.
12. Let, *a* be any real number and let $S = \{na : n \in Z\}$. Prove that (S, +) is a group what happens when $a = 0$?

(i) The set of matrices of the form $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, $ad \neq 0$, $a, b, d \in R$. Is the group abelian?

(ii) The set of matrices of the form $\begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix}$, $c \in R$.

(iii) The set of matrices of the form $\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$, $a \neq 0$, $a \in R$. Is the group abelian?

(iv) The set of matrices of the form $\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$ $\alpha \in R$.

14. (a) If in a group G, the elements a and b commutate, then prove that.

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

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

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

(b) Suppose that $x, y \in G$ and that $(xy)^2 = y^2 x^2$. Show that x and y commute.

15. Let $(G, *)$ be a group and $a, b \in G$. Suppose that $a * b = b * a^2$ and $b * a = a * b^2$. Show that $a^3 = b^3 = e$.

16. Let $G = \{(a, b) : a, b \in R, b \neq 0\}$. Define a binary operation $*$ on G by

(i) $(a, b) * (c, d) = (ac, bd)$ and (ii) $(a, b) * (c, d) = (ac + c, bd + d)$ for all $(a, b), (c, d) \in G$. Show that (i) is a non-commutative group and (ii) is a commutative group.

17. If $G = \{1, w, w^2\}$, then find order of every element of G. 1, w, w^2 are cube roots of unity.

18. In any group, show that identity is the only element whose order is one.

19. Determine whether the set together with the binary operation is a semi group, a monoid or neither. If it is a monoid, specify the identity element.

(a) $\mathbb{N}$, where $*$ is defined as ordinary addition.

(b) Z^+, where $a * b = \max(a, b)$ for all $a, b \in Z^+$.

(c) Z^+, where $a * b = a$ for all $a, b \in Z^+$.

(d) $S = \{1, 2, 3, 6\}$, where $a * b = gcd(a, b)$.

(e) $S = \mathbb{N} \times \mathbb{N}$, where $(a, b) * (a', b') = (aa', bb')$.

20. Let S be a semi group with identity e, and b and b' be inverse of a. Show that $b = b'$ i.e., that inverse are unique if they exist.

21. A binary operation $*$ is defined on Z by $x * y = x + y - xy$, $x, y \in Z$. Show that $(Z, *)$ is a semi group.

22. Let $A = \{x : x \in I, x \leq 1\}$. Show that $\{A, *\}$ is a sub-semi group of $(Z, *)$.

23. Let $(S, *)$ be a commutative semi group. Show that if $x * x = x$ and $y * y = y$, then

$$(x * y)(x * y) = x * y$$

24. Let $(S, *)$ be a semi group where $x . x = y$ show that (i) $x . y = y . x$ (ii) $y . y = y$

25. Let $(A, *)$ be a semi group. Show that for a, b, c in A, if $a * c = c * a$ and $b * c = c * b$, then $(a * b)^n = a^n * b^n$.

Problem Set 12.3

1. Define a subgroup. Give examples.
2. Show by means of examples that the union of two subgroups may or may not be subgroup.
3. If a is any element of a group G, then $\{a^n : n \in Z\}$ is a subgroup of G.
4. If G is a group, then show that $C = \{c \in g : cx = xc \text{ for all } x \in G\}$ is a subgroup of G.
5. What is the order of a non-abelian group ? Show that all proper subgroups of a group of order 6 are abelian.

6. If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$, these prove that H is a normal subgroup of G.
7. Sow that the set $H = \{a + bi \in C : a^2 + b^2 = 1\}$ is a subgroup (C, .) where, is the multiplication operation of complex numbers.
8. Let $G = \{(a, b) : a, b \in R, b \neq 0\}$. Prove that (G, *) is a non-commutative group under the binary operation, $(a, b) * (c, d) = \{a + c, bd\}$ for all $(a, b), (c, d) \in G$.
   (*i*) Let $H = \{(a, b) \in G : a = 0\}$. Show that H is a subgroup of G.
   (*ii*) Let $K = \{(a, b) \in G : b > 0\}$. Show that K is a subgroup of G.
   [Hints (*i*) (0, 1) identity element, inverse of (a, b) is $(-a/b, 1/b)$ (*ii*) Since $(0, 1) \in K$, $K \neq \phi$. Let $(a, b), (c, d) \in K$. Thus $b > 0$ and $d > 0 \Rightarrow bd, 0$. Hence $(a, b)(c, d)^{-1} = (a, b)(c, d, 1/d) = (a - c/d, b/d) \in K$. Thus K is a subgroup.
9. Show that each of the following sets is a subgroup of the multiplicative group of 2×2 non-singular matrices over R.

   (*i*) $S = \left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \neq 0\right\}$ (*ii*) $S = \left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}, a \neq 0\right\}$

   (*iii*) $S = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad \neq 0\right\}$ (*iv*) $S = \left\{\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right\}$.

10. Let *a* be a fixed element of group G.
    Let $H = \{x \in G : xa^2 = a^2x\}$
    and $K = \{x \in g : xa = ax\}$.
    Show that H is a subgroup of G and that K is a subgroup of H.
11. Let H be a subgroup of group G and *a* be an element of G. Let $aH = \{ah : h \in H\}$. Prove that (*i*) aH is a subgroup of G, (*ii*) for $b \in G$, if $b \in aH$, then $aH \cap bH = \phi$.
12. Let a binary operation * on G be defined by $(a, b) * (c, d) = (ac, bc + d)$ for all ordered pairs (a, b) of real numbers, $a \neq 0$. Show that (G, *) is a non-abelian group. Does that sub set H of all those elements of G which are of the form $(1, b)$ from a subgroup of G?
13. Let G be a multiplication group of all positive real numbers and R the additive group of all real numbers. Is G a subgroup of R? Given reasons.
14. Answers the followings: (*i*) Can abelian group have a non abelian subgroup? Can a non-abelian group have an abelian subgroup? Can a non-abelian group have a non-abelian subgroup?
15. Show that the set of inverses of the elements of a right coset is a left coset ϕ *i.e.*, $(Ha)^{-1} = a^{-1}H$.
16. Let $H = \{0, \pm 3, \pm 6, \pm 9, ...\}$. Find all the left cosets of H in Z.
17. If G be a group of prime order *p*, then show that G has no proper subgroup.
18. Let G be a group of integers under addition and let N be the set of all integral multiples of 5. Prove that *n* is a subgroup of G and determine all the cosets of N in G.
19. Let (Z, *) be an algebraic structure, where Z is the set of integers and * is defined by $n * m = \max(n, m)$, (n, m). Determine whether (Z, *) is a monoid or a group or an abelian group.

Problem Set 12.4

1. Define a cyclic group. Show that the set $\{1, \omega, \omega^2\}$ is a cyclic group of order 3 with respect to ω^2 with respect to multiplication, ω being the cube root of unity.
2. Prove that the group $[\{1, -1, i, -i\}, .]$ is cyclic with generators *i* and $-i$.
3. Show that the group (*a*) $\{(1, 2, 3, 4), \times_5\}$ and (*b*) $\{(1, 2, 3, 4, 5, 6), \times_7\}$, is cyclic
4. How many generators are there of cyclic group of (*i*) order 6 and (*ii*) order 10.
5. Show that the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ is even, while the permutation $\begin{pmatrix} 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 \end{pmatrix}$ is odd.

6. Show that (6 5 4 3 1 2) is an even permutation while (6 7 5 4 1 2) is an odd permutation.

7. Determine which of the following permutations is even or odd :

(*i*) (1 3 5)

(*ii*) (1 3 5 6)

(*iii*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

(*iv*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$

(*v*) (1 2) (1 3 4) (1 5 2).

8. Find the inverse of each of the following permutations :

(*i*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$

(*ii*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

(*iii*) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

(*iv*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$.

9. Express each of the following as a product of transpositions and hence determine whether it is odd or even.

(*i*) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

(*ii*) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

(*iii*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

10. Show that the inverse of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ is an identity permutation.

11. If $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ show that $fg \neq gf$.

12. Express the following permutations as the product of disjoint cycles:

(*i*) a = (1 2 3) (4 5) (1 6 7 8 9) (1 5),

(*ii*) b = (1 2) (1 2 3) (1 2),

(*iii*) c = (1 3 2 5) (1 4 3) (2 5 1).

13. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, show that $fg \neq gf$

14. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, find gfg^{-1}.

15. Show that the mapping f from the group of real numbers under addition to itself given by $f(x) = [x]$, the greatest integer less than or equal to x, is not a homomorphism.

16. Let R^+ be the group of nonzero real numbers under multiplication, and ler r be a positive integer. Show that $f(x) = x^r$ is a homomorphism from R^+ to R^+.

17. Let G be a group of real numbers under addition and G′ be the group of positive real numbers under multiplication. Show that the mapping defined by $f(x) = 2^x$ is a homomorphism.

18. Let S = N × N. Let * be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$

(*a*) Show that * is associtive.

(*b*) Define $f: (S, *) \to (Q, x)$ by $f(a, b) = a/b$. Show that f is a homomorphism.

19. Let S = N × N. Let * be the operation on S defined by

$$(a, b) * (a', b') = (a + a', b + b')$$

(*a*) Show that * is associative.

(*b*) Define $f: (S, *) \to (Z, +)$ by $f(a, b) = a - b$. Show that f is a homomorphism.

20. Let G be a group. Define a function $g : G \to G$ by $g(x) = gxg^{-1}$. Show that g is an isomorphism of G onto G, *i.e.*,

(*a*) g is a homomorphism, (*b*) g is one-to-one, (*c*) g is onto.

21. Determine which of the following maps is homomorphism. If the map is a homomorphism, describe the image and the kernel.

(*a*) $f : Z \Rightarrow R$ under additive given by $f(n) = n$

(*b*) $f : R \Rightarrow Z$ under addition given by $f(x) = [x]$

22. Let G be a group. Prove that the map $f : G \to G$ given by $f(a) = a^{-1}$ for all $a \in G$ is an isomorphic if and only if G is commutative.

23. Let e be the identity element of a group G. Then the map $f : G \to G$ defined by $f(x) = x$ for all $x \in G$ is an endomorphism.

24. Consider the mapping $f : C^* \to C^*$ defined by $f(x) = x^4$, where C^* is the multiplicative group of non zero complex numbers. Show that the mapping is homomorphism with kernel $f = \{1, -1, i, -i\}$.

25. Show that the mapping defined by $f : R^* \to R^*$, defined by $f(x) = |x|$ is a homomorphism with kernel $f = \{1, -1\}$.

26. Prove that if for a group G, $f : G \to G$ given by $f(x) = x^3$, $x \in G$ is an isomorphism then G is abelian.

27. Let f be a homomorphism mapping of a group G into a group G'. Let f(G) be the homomorphic image of G in G', then f(G) is a subgroup of G'.

28. Show that the mapping $f : C \to R$ defined by $f(x + iy) = x$ is a homomorphism of the additive group of complex numbers on the additive group of real numbers and find the kernel of f.

29. Show that the mapping $f : C^* \Rightarrow R^*$ defined by $f(z) = |z|$ for all $z \in C^*$ is homomorphism of C^* into R^*. What is the kernel of f.

30. Show that if $f : G \to G'$ is an isomorphism, then $f^{-1} : G' \to G$ is also an isomorphism.

31. Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups, and let $f : S_1 \to S_2$ and $g : S_2 \to S_3$ be isomorphisms. Show that $g \circ f : S_1 \to S_3$ is an isomorphism.

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

ANSWERS 12.1

1. The set Z of all integers is closed under the binary operation multiplication but the set of negative integers which is a proper subset Z is not closed w.r.t. this operation as the product of two negative numbers is not a negative integer.

4. Identity element 0, $a^{-1} = a/(a - 1)$.

7. (*i*) associative, (*ii*) Non associative.

11. (i) Neither commutative nor associative,

(ii) Only commutative,

(iii) Commutative,

(iv) Only commutative,

(v) Associative not commutative,

(vi) Associative and commutative,

(vii) Associative and commutative.

12. (i) n^{n^2} (ii) $(n^2 + n)/2$.

13. (1)

	a	b
a	a	a
b	a	a

(2)

	a	b
a	b	a
b	a	a

(3)

	a	b
a	a	b
b	a	a

(4)

	a	b
a	a	a
b	b	a

(5)

	a	b
a	a	a
b	a	b

(6)

	a	b
a	b	b
b	a	a

(7)

	a	b
a	b	a
b	b	a

(8)

	a	b
a	b	a
b	a	b

(9)

	a	b
a	a	b
b	b	a

(10)

	a	b
a	a	b
b	a	b

(11)

	a	b
a	a	a
b	b	b

(12)

	a	b
a	b	b
b	b	a

(13)

	a	b
a	b	b
b	a	b

(14)

	a	b
a	b	a
b	b	b

(15)

	a	b
a	a	b
b	b	b

(16)

	a	b
a	b	b
b	b	b

16. (*i*) Yes, (*ii*) Yes.

17. First row $\to d$, Second row $\to a$, fourth row $\to c, b$.

ANSWERS 12.2

6. (*a*) does not have identity element
   (*d*) does not have identity element
   (*e*) does not have identity element.

20. Only {1, 10}

21. S is a trivial group ({0}, +)

17. $0(1) = 1, 0(w) = 0, 0(w^2) = 3$.

19. (*a*) Semi group,
    (*b*) Monoid, identity 1,
    (*c*) Semi group,
    (*d*) Monoid, identity 6
    (*e*) Semi group.

ANSWERS 12.3

14. No, Yes, Yes

19. Monoid

ANSWERS 12.4

4. Two, a and a^5 Four, a, a^3, a^7, a^9

7. (*i*) even, (*ii*) odd, (*iii*) even, (*iv*) even, (*v*) odd

8. (*i*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ (*ii*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ (*iii*) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ (*iv*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

9. (*i*) (1, 2) odd, (*ii*) (1, 3) odd, (*iii*) (1 4) (2 3) even

12. (*i*) $a = (1\ 2\ 3\ 6\ 7\ 8\ 9\ 5\ 4)$, (*ii*) $b = (1\ 3\ 2)$ (*iii*) $c = (1\ 2)(3\ 5\ 4)$

14. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & \end{pmatrix}$

21. (*a*) yes, image of $f = Z$, kernel of $f = \{0\}$ (*b*) no.

28. Ker f = all complex numbers where real part is zero

29. Ker f = *multiplicative subgroup of all complex numbers whose modulus is 1*

SHORT/MULTIPLE CHOICE QUESTIONS

1. Mark each of the following True or False.
   (*a*) If * is any binary operation on any set S, then $a * a = a$ For all $a \in S$.
   (*b*) If * is any binary operation on any set S, then $a*(b * c) = (b * c)*$ a for all $a, b, c \in S$.
   (*c*) Every binary operation defined on S set having exactly one element is both commutative and associative.
   (*d*) A binary operation on a set S assigns at least one element S to each ordered pair of elements of S.
   (*e*) A binary operation on a set S assigns at most one element S to each ordered pair of elements of S.
   (*f*) A binary operation on a set S assigns at exactly one element S to each ordered pair of elements of S.
2. Let S be a set having exactly one element. How many different binary operations can be defined on S? If S has exactly 2 elements; exactly 3 elements; exactly n elements.
3. Which of the following are associative binary operations?
   (*a*) $(N, *)$, where $x * y = \gcd(x, y)$ for all $x, y \in N$.
   (*b*) $(N, *)$, where $x * y = \text{lcm}(x, y)$ for all $x, y \in N$.
   (*c*) $(R, *)$, where $x * y = \min(x, y)$ for all $x, y \in N$.
   (*d*) $(N, *)$, where $x * y = x^y$ for all $x, y \in N$.
   (*e*) $(R, *)$, where $x * y = |x| + |y|$ for all $x, y \in R$.
4. Mark each of the following true or false.
   (*a*) The associative law holds for every group.
   (*b*) There may be a group in which cancellation law fails.
   (*c*) Every group is a subgroup of itself.
   (*d*) Every group has exactly two improper subgroups.
   (*e*) In every cyclic group, every element is a generator.
5. Consider the mathematical system represented by the table

×	*a*	*b*	*c*
a	*a*	*a*	*a*
b	*a*	*b*	*c*
c	*a*	*c*	*b*

   (*a*) Is the system closed under multiplication?
   (*b*) Is multiplication commutative?
   (*c*) Identify the multiplicative identity.
   (*d*) Identify the multiplicative inverse of each element that has a multiplicative inverse.
   (*e*) Does the system form a group under multiplication?
6. Consider the mathematical system represented by the table.

+	*x*	*y*	*z*
x	*x*	*y*	*z*
y	*y*	*z*	*z*
z	*z*	*x*	*y*

   (*a*) Is the system closed under addition?
   (*b*) Is addition commutative?
   (*c*) Identify the additive identity.
   (*d*) Identify the additive inverse of each element that has an additive inverse.
   (*e*) Does the system appear to form a commutative group under addition?

7. Determine whether the indicated set and binary operation form a group. If so,is it commutaive?

*	−1	1
−1	1	−1
1	−1	1

8. Which of the following is closed under multiplication?
   (*a*) {1, − 1, 0, 2} (*b*) {1, *i*} (*c*) {1, *w*, w^2} (*d*) {*w*, 1}
9. A binary on a set *A* is a mapping from *A* × *A* into
   (*a*) *A* × *A* (*b*) *A* (*c*) set of integers (*d*) set of real numbers
10. A binary operation on a set *A* is a mapping whose domain is
    (*a*) *A* × *A* (*b*) *A* (*c*) set of integers (*d*) set of real numbers
11. Which of the algebraic structures is a semi-group but not a group
    (*a*) (*N*, +) (*b*) (*Z*, +) (*c*) (*R*, +) (*d*) (*C*, +)
12. The number of binary relations or a set with *n* element is
    (*a*) n^2 (*b*) 2^n (*c*) 2^{n^2} (*d*) none of these
13. Let *G* be a group and $a \in G$. If o(*a*) = 17 then o(a^8) is
    (*a*) 17 (*b*) 16 (*c*) 8 (*d*) 5
14. Let *G* be a group having elements *a* and *b* such that o(*a*) = 4, o(*b*) = 2 and $a^3 b = ba$. Then o(*ab*) is
    (*a*) 2 (*b*) 1 (*c*) 3 (*d*) 4
15. The generators of the cyclic group (Z, +) are
    (*a*) 1, −1 (*b*) 0, 1 (*c*) 0, −1 (*d*) 2, −2
16. If the cyclic group *G* contain 11 distinct elements, then it has
    (*a*) 2 generators (*b*) 7 generators (*c*) 9 generators (*d*) 10 generators
17. The number of generators of an infinite cyclic group is
    (*a*) 1 (*b*) 2 (*c*) 0 (*d*) infinite
18. The inverse of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ is
    (*a*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ (*b*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ (*c*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ (*d*) none of these
19. In a group (*G*, o) if $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$ then
    (*a*) *G* is finite (*b*) *G* is infinite (*c*) *G* is Abelian (*d*) None of these
20. A group *G* is commutative iff
    (*a*) *ab* = *ba* (*b*) $(ab)^{-1} = b^{-1} a^{-1}$ (*c*) $(ab)^{-1} = a^{-1} b^{-1}$ (*d*) $(ab)^2 = ab$
21. If a binary operation * is defined by
    $$a * b = a^2 - b^2 + ab + 4$$
    then (2 * 3) * 4 is
    (*a*) 223 (*b*) 33 (*c*) 55 (*d*) − 55
22. The algebraic system (*N*, *) where * is defined by
    $a * b = 13$ for all $a, b \in N$ is *a*
    (*a*) Semigroup (*b*) Monoid
    (*c*) Commutative semigroup (*d*) None of these
23. The set of all even integers under multiplication is not a group, since the following is not true
    (*a*) Associative law (*b*) Closure (*c*) Existence of identity (*d*) Commutative law

24. A groupoid $(G, *)$ is a semi-group if for all $a, b, c \in G$
(a) $a * b = b \times a$ (b) $a * a = a$
(c) $(a * b) * c = (b * c) * a$ (d) $(a * b) * c = a * (b * c)$

25. A semi group $(G, *)$ will lee monoid if
(a) $*$ is associative (b) $*$ is commutative
(c) G contains inverse of every element (d) G contains identity element.

26. In the group $\{1, -1, i, -i\}$ under multiplication, order of $-i$ is
(a) 0 (b) 2 (c) 4 (d) – 4

27. The set P of all prime numbers is a group under
(a) + (b) . (c) – (d) none of these

28. Find the length of each of the following cyclic group
(a) (1, 4) (b) (1, 4, 6) (c) (1, 4, 6, 7, 2)

29. Mark True of false.
(a) A group has only idempotent element.
(b) Every group of four elements is commutative.
(c) A semigroup with only one idempotent is a group.
(d) If a semigroup S satisfies the cancellation laws, then S is a group.

30. Which of the following statements is false?
(a) The set of rational numbers is an abelian group under addition
(b) The set of integers is an abelian group under addition.
(c) The set of rational number form an abelian group under multiplication.
(d) The set of real numbers excluding zero is an abelian group under multiplication.

31. Let* be the operations on Q (The set of rational numbers) defined by $a*b = a + b - ab$, find
(a) $2 * 3$ (b) $3 * 4$

32. State whether or not the given set constitutes a group with respect to the given operation. If it does not, state why not.
(a) {The natural number:} +. (b) {The rational number}: +.
(c) {the integers}; (d) $\{-1, 0, 1\}$; x.
(e) $\{0, 1\}$, + (f) $\{-1, 0, 01\}$; +. (g) $\{0, 1\}$; (h) $\{-1, 1\}$;

33. If S and T are two subgroups of a group G, then which of the following is a subgroup?
(a) $S \cup T$ (b) $S \cap T$ (c) $S - T$ (d) $G - S$

34. The order of the permutation $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is
(a) 2 (b) 3 (c) 1 (d) none of these

35. The order of the alternating group An is
(a) $n!$ (b) n (c) $\frac{n}{2}$ (d) $\frac{n!}{2}$

36. If G be a group of order n and H be a subgroup of order m then
(a) $m = n$ (b) $m = nq$, q is the index of H is G
(c) $n = mq$ (d) none of these

37. If G is a group then the quotient group G/H is defined if
(a) H is a subgroup of G (b) H is a finite subgroup of G
(c) H is a normal subgroup is G (d) none of these

38. Index of a subgroup is 5 and its order is 3. The order of the group is
(a) 8 (b) 10 (c) 15 (d) none of these

39. The right and left cosets of a subgroup H are identical if
(a) H is finite (b) G is abelian (c) G is finite (d) none of these

40. If $c \in a H \cap b H$, then
(a) $aH = bH$ (b) $aH = cH$ (c) $bH = cH$ (d) $aH = bH = cH$

41. The inverse of (1, 3, 2) is S_3 is
(a) (1, 3, 2) (b) (1, 2, 3) (c) (3, 1) (3, 2) (d) (2, 3) (2, 1)

ANSWERS

1. (a) False, (b) False, (c) True, (d) True, (e) True (f) True
2. 1, 16, 19628, n^2 3. (a) Yes, (b) Yes, (c) Yes, (d) No, (e) Yes
4. (a) True, (b) False, (c) True, (d) False, (e) False
5. (a) Yes
(b) Yes
(c) b
(d) the multiplicative inverse of b is b and c is c (a does not have a multiplicative inverse)
(e) no
6. (a) Yes, (b) Yes, (c) x, (d) the additive inverse of x is x, of y is z, of z is y. (e) Yes
7. Yes, commutative

8. (c)	9. (b)	10. (a)	11. (a)	12. (c)	13. (a)
14. (a)	15. (a)	16. (d)	17. (b)	18. (c)	19. (c)
20. (c)	21. (b)	22. (c)	23. (c)	24. (d)	25. (d)
26. (c)	27. (d)	28. (a) Two, (b) Three, (c) Five			
29. (a) True, (b) True, (c) False, (d) False			30. (c)	31. –1, 11	

32. (a) not a group; no identity element and no inverse
(b) group
(c) not a group; only –1 and 1 have inverses
(d) not a group; 0 has no inverse.
(e) not a group; the set is not closed since $1 + 1 = 2$ and $-1 + (-1) = -2$
(f) not a group; the set is not closed since $1 + 1 = 2$.
(g) not a group; 0 has no inverse.
(h) not a group; the set in not closed as $-1 + (-1) = -2$
(i) a group

33. (b)	34. (b)	35. (d)	36. (c)	37. (c) 38. (c)
39. (c)	40. (d)	41. (b)		

13 CHAPTER Rings and Fields

13.1. Introduction

In the previous chapter, we studied group which is an algebraic structure with one binary operations. But even the set of integers have two binary operations-addition and multiplication and satisfy properties involving both addition and multiplication. In this chapter we shall study ring which is an algebraic structure equipped with two binary operations.

13.2. Ring

An algebraic structure $(R, +, \cdot)$ where R is a non-empty set with two binary operations + (addition) and. (multiplication) defined on R is called a ring if the following conditions are satisfied.

(*i*) (R, +) is an abelian group.

(*ii*) (R, ·) is semigroup

(*iii*) The operation is distributive over the operation +.

The above three conditions in details are

(*i*) (R, +) is an abelian group

(R_1) $a + b \in R$ for all $a, b \in R$.

(R_2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(R_3) $a + b = b + a$ for all $a, b \in R$.

(R_4) There exists an element 0 in R such that $a + 0 = a$ for all $a \in R$.

(R_5) For all $a \in R$, there exists an element $-a \in R$ such that

$$a + (-a) = 0.$$

(*ii*) (R, ·) is semigroup.

(R_6) $a \,.\, b \in R$, for all $a, b \in R$.

(R_7) $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$ for all $a, b, c \in R$.

(*iii*) Distributive over the operation +.

(R_8) Left distribution law: $a \,.\, (b + c) = a \,.\, b + a \,.\, c$ for all $a, b, c \in R$

and Right distribution law: $(b + c) \,.\, a = b \,.\, a + c \,.\, a$ for all $a, b, c \in R$

Note. 1. The identity element w.r.t. the binary operation + in R is called additive identity element or the zero element of the ring and is denoted by 0.

2. $-a$ is called additive inverse of a.

3. For convenience, we write ab in place of $a \,.\, b$.

Commutative Ring

A ring R is said to be commutative if $a \,.\, b = b \,.\, a$ for all a, b in R.

Ring with Unity

A ring R is said to be a ring with unity if in addition to $R_1 - R_8$, it satisfies the following axiom:

$$e \,.\, a = a \,.\, e = a \;\forall\; a \in R$$

Obviously e is the multicative identity of R.

The following are some examples of rings.

1. The set Z of integers under ordinary addition and multiplication is a commutative ring with unity 1. Since the sum and product of any two integers is an integer.

Further, $\{Z, +\}$ is an abelian group and $\{Z, \cdot\}$ is a semi-group. Also multiplication is both left and right distributive with respect to addition. Hence $(Z, +, \cdot)$ is a ring. Again, multiplication is commutative and 1 is the unit element for multiplication. So, $(Z, +, \cdot)$ is a commutative ring with unity element.

2. The set 2Z of even integers under ordinary addition and multiplication is a commutative ring without unity since there is no even integer e such that $e \times y = y \times e = y$ for all even integers y.

3. The set $Z_n = \{0, 1, 2, \ldots\ldots, n-1\}$ under addition and multiplication modulo n is a commutative ring with unity 1.

4. The set $M_2(Z)$ of 2×2 matrices with integer elements under addition and multiplication is a non commutative ring with unity. The unit element is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

5. $R = \{a + b\sqrt{-5} : a, b \in Z\}$ is a ring for the usual addition and multiplication of complex numbers. It is a commutative ring with unit element $1 = 1 + 0\sqrt{-5}$.

Some Elementary Properties of a Ring

Let a, b and c belong to a ring R. Then

1. $a.0 = 0.a = 0$
2. $a.(-b) = (-a).b = -(a.b)$
3. $(-a).(-b) = a.b$
4. $a.(b - c) = a.b - a.c$ and $(b - c).a = b.a - c.a$

Proof. 1. We have $a.0 + a.a = a \,.\, (0 + a)$, left distributive law

$= a \,.\, a$, since $0 + a = a$

$= 0 + a \,.\, a$

Hence, by the right cancellation law, $a \,.\, 0 = 0$

Similarly, by using the right distributive law, we can show that

$$0 \,.\, a = 0$$

2. We have $a \,.\, (-b + b) = a \,.\, (-b) + a \,.\, b$, left distributive law

i.e. $a \,.\, 0 = a \,.\, (-b) + a \,.\, b$, $(-b)$ is the additive inverse of b

$0 = a \,.\, (-b) + a \,.\, b$ from (1) above.

Therefore $a \,.\, (-b)$ is an additive inverse of $a \,.\, b$.

Hence $a \,.\, (-b) = -(a \,.\, b)$.

Similarly, by using the right distributive law *i.e.*, $(-a + a) \,.\, b = (-a) \,.\, b + a \,.\, b$ we can easily show

That $(-a) \,.\, b = -(a \,.\, b)$.

3. From the two results of 2 we have

$$(-a) \,.\, (-b) = -[(-a) \,.\, (b)] = -[-(a \,.\, b)] = a \,.\, b,$$

since the inverse of the inverse of an element is the element itself in any group *i.e.* $-(-x) = x$

4. We have $a \,.\, (b - c) = a \,.\, [b + (-c)]$

$= a \,.\, b + a \,.\, (-c)$, left distributive law

$= a \,.\, b + [-(a \,.\, c)]$

$= a \,.\, b - a \,.\, c$

Similarly, using the right distributive law, we can show that,

$$(b - c) \,.\, a = b \,.\, a - c \,.\, a.$$

Example 1. Prove that if $a, b \in R$ then $(a + b)^2 = a^2 + ab + ba + b^2$.

Solution. We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b) + b(a+b) \quad \text{(by right distributive law)}\\ &= (aa + ab) + (ba + bb) \quad \text{(by left distributive law)}\\ &= a^2 + ab + ba + b^2.\end{aligned}$$

Example 2. If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

Solution. Since 1 is an element of R, we have

$$(a+b)(1+1) = a(1+1) + b(1+1) \quad \text{(by right distributive law)}$$
$$= (a1 + a1) + (b1 + b1) = (a + a) + (b + b) \quad \ldots\ldots(i)$$

Also
$$(a+b)(1+1) = (a+b)1 + (a+b)1. \quad \text{(by left distributive law)}$$
$$= (a+b) + (a+b) \quad \ldots (ii)$$
$(\because$ 1 is the unit element)

From (i) and (ii), we get

$$(a + a) + (b + b) = (a + b) + (a + b)$$
$$\Rightarrow \quad [(a + a) + b] + b = [(a + b) + a] + b \quad \text{(by associativity of addition)}$$
$$\Rightarrow \quad (a + a) + b = (a + b) + a \quad \text{(by right cancellation law for addition in R)}$$
$$\Rightarrow \quad a + (a + b) = a + (b + a) \quad \text{(by associativity of addition in R)}$$
$$\Rightarrow \quad a + b = b + a \quad \text{(by left cancellation law for addition in R)}$$

Thus addition is commutative in R. Hence R is a ring.

Example 3. If in a ring R with unity, $(xy)^2 = x^2 y^2$ for all $x, y \in R$, then R is commutative.

Solution. Since 1 is an element of R, for all $x, y \in R$, then $x + 1, y + 1 \in R$

$\therefore$ Given $(xy)^2 = x^2 y^2$

$$[x(y+1)]^2 = x^2 (y+1)^2$$
$$\Rightarrow \quad [x(y+1)][x(y+1)] = x^2 (y+1)(y+1)$$
$$\Rightarrow \quad (xy + x)(xy + x) = x^2 [y(y+1) + 1(y+1)] \quad \text{(by distributive law)}$$
$$\Rightarrow \quad [xy(xy + x) + x(xy + x)] = x^2 (y^2 + y + y + 1)$$
$$\Rightarrow \quad (xy)^2 + xyx + x^2 y + x^2 = x^2 y^2 + 2x^2 y + x^2$$
$$\Rightarrow \quad x^2 y^2 + xyx + x^2 y + x^2 = x^2 y^2 + 2x^2 y + x^2$$
$$\Rightarrow \quad xyx = x^2 y \quad \ldots(1)$$

Replacing x by $x + 1$ in (1), we get

$$(x+1)y(x+1) = (x+1)^2 y$$
$$= (x+1)(x+1)y$$
$$\Rightarrow \quad (xy + y)(x + 1) = (x(x+1) + 1(x+1))y$$
$$\Rightarrow \quad (xy + y)x + (xy + y)1 = (x^2 + x + x + 1)y$$
$$\Rightarrow \quad xyx + yx + xy + y = x^2 y + xy + xy + y$$
$$\Rightarrow \quad yx = xy \quad \text{since } xyx = x^2 y \text{ by (1)}$$

Hence R is a commutative ring.

Example 1. Prove that if $a, b \in R$ then $(a + b)^2 = a^2 + ab + ba + b^2$.

Solution. We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b) + b(a+b) \quad \text{(by right distributive law)}\\ &= (aa + ab) + (ba + bb) \quad \text{(by left distributive law)}\\ &= a^2 + ab + ba + b^2.\end{aligned}$$

Example 2. If R is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in R and that R is thus a ring.

Solution. Since 1 is an element of R, we have

$$(a+b)(1+1) = a(1+1) + b(1+1) \quad \text{(by right distributive law)}$$
$$= (a1 + a1) + (b1 + b1) = (a + a) + (b + b) \quad \ldots\ldots(i)$$

Also
$$(a+b)(1+1) = (a+b)1 + (a+b)1. \quad \text{(by left distributive law)}$$
$$= (a+b) + (a+b) \quad \ldots (ii)$$

($\because$ 1 is the unit element)

From (i) and (ii), we get

$$(a+a) + (b+b) = (a+b) + (a+b)$$
$$\Rightarrow \quad [(a+a) + b] + b = [(a+b) + a] + b \quad \text{(by associativity of addition)}$$
$$\Rightarrow \quad (a+a) + b = (a+b) + a \quad \text{(by right cancellation law for addition in R)}$$
$$\Rightarrow \quad a + (a+b) = a + (b+a) \quad \text{(by associativity of addition in R)}$$
$$\Rightarrow \quad a + b = b + a \quad \text{(by left cancellation law for addition in R)}$$

Thus addition is commutative in R. Hence R is a ring.

Example 3. If in a ring R with unity, $(xy)^2 = x^2y^2$ for all $x, y \in R$, then R is commutative.

Solution. Since 1 is an element of R, for all $x, y \in R$, then $x + 1, y + 1 \in R$

$\therefore$ Given
$$(xy)^2 = x^2y^2$$
$$[x(y+1)]^2 = x^2(y+1)^2$$
$$\Rightarrow \quad [x(y+1)][x(y+1)] = x^2(y+1)(y+1)$$
$$\Rightarrow \quad (xy + x)(xy + x) = x^2[y(y+1) + 1(y+1)] \quad \text{(by distributive law)}$$
$$\Rightarrow \quad [xy(xy + x) + x(xy + x)] = x^2(y^2 + y + y + 1)$$
$$\Rightarrow \quad (xy)^2 + xyx + x^2y + x^2 = x^2y^2 + 2x^2y + x^2$$
$$\Rightarrow \quad x^2y^2 + xyx + x^2y + x^2 = x^2y^2 + 2x^2y + x^2$$
$$\Rightarrow \quad xyx = x^2y \quad \ldots(1)$$

Replacing x by $x + 1$ in (1), we get

$$(x+1)y(x+1) = (x+1)^2y$$
$$= (x+1)(x+1)y$$
$$\Rightarrow \quad (xy + y)(x+1) = (x(x+1) + 1(x+1))y$$
$$\Rightarrow \quad (xy + y)x + (xy + y)1 = (x^2 + x + x + 1)y$$
$$\Rightarrow \quad xyx + yx + xy + y = x^2y + xy + xy + y$$
$$\Rightarrow \quad yx = xy \quad \text{since } xyx = x^2y \text{ by (1)}$$

Hence R is a commutative ring.