CHAPTER 11

Group Theory

11.1. 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.

11.2. 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 an element of G.

The symbols $+, \cdot, 0, *$ 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.*,

$a + b \in N$ for all $a, b \in N$.

$a \times b \in N$ 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.

The most important of describing a particular binary operation $*$ on a given set is to characterize the element $a * b$ assigned to each pair (a, b) by some property defined in terms of a and b.

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 11.1

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 addition; but 1 is an identity element with respect to multiplication.

Theorem 11.1. 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, $e' \in S$.

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 11.2. 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 $(y * x) * z = e * z$ from (1)

$= z$ (e is the identity)

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

and $y * (x * z) = y * e$ from (2)

$= y$ (e 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, an 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 $x * (y * z) = x * y^z$

$= x^{yz}$

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

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~~ identity 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.

SemiGroup → closure, associative

monoid → closure, associative & identity

Group → closure, associative, identity & inverse

(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	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

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

(b) is * commutative ? why ?

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

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

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 $a, b \in Z$

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 $a, b, c \in Z$

Hence, * is associative.

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

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

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

Let the integer a have its inverse b. Then,

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

11.3. 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.*, $a * b \in G$ for all $a, b \in G$.

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

Qu:- Show that $\mathbb{Z}$ is a group w.r. to addition.

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

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

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

u:- let $G = \{0, 1, 2\}$ and define $*$ on G by $a * b = |a - b|$ is group or not ?

$*$ a is said to be congruent to b under modulo n addition if $(a-b)$ is divisible by n

i.e $a \equiv b \pmod n$

$\Rightarrow (a-b)$ is divisible by n

or $n \mid (a-b)$

basically b is remainder when a is divided by n

if $a < n$ then $a \equiv a \pmod n$

table of $\mathbb{Z}_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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 $(xa, ya + b) = (1, 0)$. 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 $2^a 3^b$, where a and b are integers prove that the algebraic structure $(Q, .)$ is a group where . is multiplication operator.

Solution.

Closure property: Let $q_1 = 2^a 3^b$, $q_2 = 2^c 3^d \in Q$ where $a, b, c, d, \in Z$, the set integers.

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

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

Associative law: Let $q_1 = 2^a 3^b$, $q_2 = 2^c 3^d$, $q_3 = 2^e 3^f \in Q$

We have

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

$= 2^{a+(c+e)} \cdot 3^{(b+d)+f}$ (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 11.3. (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 $$b = c.$$

* The order of the group is the no. of elements in the group and denoted by $o(G)$ or $|G|$

Eg: forth root of unity has order 4.

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

$$a * e = a. \qquad \text{by Theorem 11.3}$$

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

Theorem 11.5. 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)

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

$$= a^{-1} * e \qquad \text{by Theorem 11.4}$$

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

Therefore, $a * a^{-1} = e \qquad \text{by Theorem 11.3}$

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

Theorem 11.6. 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 11.7. 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 inverses 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, $(a * b)^{-1} * (a * b) = e$. ... (1)

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

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

$= b^{-1} * e * b = b^{-1} * b = e$ ... (2)

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

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

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

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

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

Again, suppose G is abelian so that

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

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

$$(ab)^2 = (ab)(ab) = a(ba)b = a(ab)b,$$
$$= (aa)(bb) = a^2b^2.$$

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

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

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

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 $g^n = e$. — formul.

If no such integer exists, we say g has infinite order. The order of an element g is denoted by $o(g)$. — for addition $na = 0$ (identity)

So, to find the order of a group element g, one need only compute the sequence of products g, $g^2, g^3, \ldots\ldots$, 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 and a^{12}.

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.

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

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

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

$= be$ ($\because$ $e^{-1} = e$)

$= b$

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, $o(b) = 31$

11.4 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.

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

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 11.9 {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.

11.5 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.

$H \leq G \rightarrow$ improper

$H < G \rightarrow$ proper

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 11.11. 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 11.12. 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 11.13. (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. Suppsoe 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 11.14. 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.

is not subgroup of $(\mathbb{Z}, +_8)$ → Operation change

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

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

where e is the identity element.

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.

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

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

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) cosets 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.*,

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

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

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

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

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

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

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

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 $H + 3 = \{\ldots., -6, -3, 0, 3, 6, 9, 12, \ldots\}$.

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

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

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

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

$$aH = H \Rightarrow a \in H \quad \ldots (1)$$

i.e., if $a \in H$ and $h \in H$ then

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

$$aH \subset H$$

$\therefore$ 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 $aH \subset H$ and $H \subset aH \Rightarrow aH = H$

Next $$a \in H \Rightarrow aH = H \quad \ldots (2)$$

Hence $aH = H \Leftrightarrow a \in H$ by (1) and (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 $$aH = (bh'') H = b (h'' H) = bH, \text{ since } h'' H = H.$$

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,

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

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

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

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

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

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

$$bH = e (bH) = (aa^{-1}) (bH) = a (a^{-1}b)H = aH \quad \ldots (2)$$

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

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 11.16. 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

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

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

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

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 $(ab)\,x = abx,$

$= axb,$ $(\because bx = xb)$

$= xab,$ $(\because ax = xa)$

$= x\,(ab).$

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

(*iii*) $a \in G_x \Rightarrow ax = xa.$

$\Rightarrow a^{-1}\,(ax)\,a^{-1} = a^{-1}\,(xa)\,a^{-1}.$

$\Rightarrow a^{-1}\,axa^{-1} = a^{-1}\,xaa^{-1},$

$\Rightarrow exa^{-1} = a^{-1}\,xe,$

$\Rightarrow xa^{-1} = a^{-1}\,x,$

$\Rightarrow a^{-1} \in G_x.$

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*. By using the concept of cosets we prove a theorem due to Langrange which expresses a relationship between the order of a finite group and the order of its subgroup.

Lagrange's Theorem

Theorem 11.18. 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 $$H = \{h_1, h_2, ..., h_m\}.$$

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: $$n = mk. \quad \ldots (1)$$

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, $$(xy)^2 = e.$$

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

(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

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

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.

11.6. 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 $(w^2)^0 = 1$, $(w^2)^1 = w^2$, $(w^2)^2 = w^4 = w$

The group $Z_n = \{0, 1, 2 \ldots n-1\}$, addition modulo $(n \geq 1)$ is a cyclic group

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

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 Groups

Theorem 11.18. Every cyclic group is an abelian group.

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

$$G = <a> = \{a^n : n \in Z\}$$

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

Proof. Let $G = <a>$ 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 11.20. 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*). $r^t = 1$. 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.

11.7 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

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

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

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

Clearly $f \circ g$ 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 $f \circ g$.

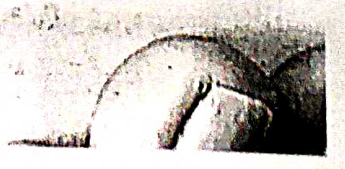
If we want to write gf, then f should be written in such a manner that the second row of g must coincide with the first row of f.

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

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

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

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

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

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

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

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

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 $(P_n, *)$ s a group, called a **permutation group** and the operation * is the composition (multiplication) of ermutations. This is proved in the following theorem.

Theorem 11.21. The set P_n of all permutation on n symbols is finite group of order $n!$ with espect to the binary composition of permutations. For $n \leq 2$, P_n is abelian and for $n > 2$ it is always on-abelian.

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

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

e 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 rmutation 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

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

$$(fg)h=\begin{pmatrix}b_1 & b_2 & \dots & b_n\\ d_1 & d_2 & \dots & d_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ b_1 & b_2 & \dots & b_n\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ d_1 & d_2 & \dots & d_n\end{pmatrix} \quad \dots (1)$$

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

$$f(gh)=\begin{pmatrix}c_1 & c_2 & \dots & c_n\\ d_1 & d_2 & \dots & d_n\end{pmatrix}\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ c_1 & c_2 & \dots & c_n\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ d_1 & d_2 & \dots & d_n\end{pmatrix} \quad \dots (2)$$

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

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

Thus $fI = If = f$

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 permutation

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

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

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.

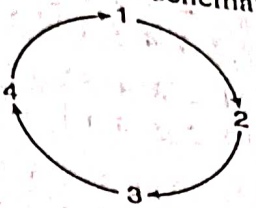
Cyclic Permutations

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

Let $(G, *)$ and $(G_1, *_1)$ be two groups and f is a function from G into G_1. Then f is called a homomorphism of G into G_1 if for all $a, b \in G$

$$f(a * b) = f(a) *_1 f(b)$$

A homomorphism is called an **epimorphism** if f is onto G_1 and f is called a monomorphism if f is one-one. If there is an epimorphism f from G onto G_1, then G_1 is called a **homomorphic Image**.

A homomorphism f of a group G into a group G_1 is called **a isomorphism of G onto G_1** if f is one-one onto G_1. G and G_1 are said to be isomorphic and denoted by $G \cong G_1$. An isomorphism of a group G onto G is called an **automorphism.**

The kernel of a homomorphism f of a group G into a group G_1 is the set of all elements of G mapped onto the identity element of G_1 by f. That is, the kernel of f, written as ker f, is defined to the set

$$\text{Ker } f = \{a \in G : f(a) = e_1, \text{ the identity of } G_1\}$$

Example 48. (*i*) Let $G = Z$ and $G' = \{1, -1\}$ the multiplicative group. The mapping $f: G \to G'$ defined by $f(n) = 1$ if n is even and $f(n) = -1$ if n is odd is a group homomorphism, as $f(m + n) = f(m) f(n)$ for all $m, n \in Z$.

(*ii*) Let $G = R$ be the group of real numbers under addition and $G' = R^+$, the group of positive real numbers for multiplication. The mapping $f: G \to G'$ given by $f(a) = 2^a$ is a group homomorphism, because $f(a + b) = 2^{a+b} = 2^a 2^b = f(a) . f(b)$.

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. → (i) one-one (ii) onto (iii) Homomorphism

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 $x, y \in R^+$, $f(xy) = (xy)^2 = x^2y^2 = f(x) f(y)$. (i) one-one

Thus f is an endomorphism of R^+. (ii) onto (iii) Homo.

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.

$f: R \to R$ Same then automorphism

Basic Properties on Homomorphisms

Theorem 11.24. Let $(G, *)$ and $(G_1, *_1)$ be two groups and let $f: G \to G_1$ be a homomorphism from G to G_1. Then

(*a*) $f(e) = e_1$ where e is the identity in G and e_1 is the identity in G_1.

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

(*c*) If H is a sub group of G, then $f(H) = \{f(h) : h \in H\}$ is a subgroup of G_1

Proof. (*a*) Since f is a homomorphism, $f(e) *_1 f(e) = f(e * e) = f(e)$

Now $f(e) \in G_1$ gives $f(e) = e_1 *_1 f(e)$

$f(e) *_1 f(e) = e_1 *_1 f(e)$

Thus $f(e) = e_1$ by the right cancellation law.

(*b*) For $a \in G$, $f(a) *_1 f(a^{-1}) = f(a * a^{-1}) = f(e) = e_1$ by part (*a*).

Similarly, $f(a^{-1}) *_1 f(a) = e_1$

Since, $f(a)$ has a unique inverse $f(a^{-1}) = (f(a))^{-1}$ for all $\in G$.

(*c*) Let H be a sub-group of G.

Then $e \in H$ by (*a*) $f(e) = e_1$.

Thus $e_1 = f(e) \in f(H)$ and so $f(H) \neq \phi$.

Let $f(a), f(b) \in f(H)$, where $a, b \in H$.

Since H is a sub-group, $ab^{-1} \in H$.

Thus $f(a) *_1 (f(b))^{-1} = f(a) *_1 f(b^{-1}) = f(a * b^{-1}) \in f(H)$.

Hence, $f(H)$ is subgroup of G_1.

Theorem 11.25. 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 11.26. 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

$$\begin{aligned} Ka = Kb &\Rightarrow ab^{-1} \in K \\ &\Rightarrow f(ab') = e' \qquad \text{(the identity of G')} \\ &\Rightarrow f(a)\, f(b^{-1}) = e' \\ &\Rightarrow f(a)\, (f(b))^{-1} = e' \\ &\Rightarrow f(a)\, (f(b))^{-1}\ f(b) = e'\, f(b) \end{aligned}$$

We have $f(g\,k\,g^{-1}) = f(g)f(k)f(g^{-1})$ ($\because f$ preserves compositions)

$= f(g)e'[f(g)]^{-1}$

$= f(g)[f(g)]^{-1} = e' \quad \Rightarrow g\,k\,g^{-1} \in K$

Therefore, K is normal subgroup of G.

Theorem 10. Prove that a homomorphism f of a group G into a group G' with Kernel K will be an isomorphism of G into G' iff $K = \{e\}$.

PF. Let G and G' be two groups with identities e and e' respectively and $f: G \to G'$ be an homomorphism with Kernel K. Suppose $f: G \to G'$ is an isomorphism, then if $a \in K$, we have

$$f(a) = e' \Rightarrow f(a) = f(e)$$

$$\Rightarrow a = e \qquad [\because f \text{ is one-to-one}]$$

This shows that if $a \in K \Rightarrow a = e$, so that $K = \{e\}$.

Conversely, Let $K = \{e\}$. Then in order to prove that f is an isomorphism we have only to prove that f is one-to-one. If $a, b \in G$, then

- Note:- Quaternion groups

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k$$

$$jk = -kj = i$$

$$ki = -ik = j$$

8.13. Rings

Now we shall study an important type of mathematical structure with two binary operations '+' and '·' known as ring.

Definition Let R is a non-empty set equipped with two binary operations, called addition (+) and multiplication (·). Then the mathematical structure $(R, +, \cdot)$ is called a ring if the following postulates are satisfied:

(a) $(R,+)$ is an abelian group

(i) Closure law $a+b \in R$ for all $a,b \in R$.

(ii) Associative law $a+(b+c)=(a+b)+c$, for all $a,b,c \in R$.

(iii) Additive identity. There exists an elements $0 \in R$ such that $0+a=a+0=a$ for all $a \in R$.

The elements $0 \in R$ is called the zero element of the ring.

(iv) Addiative inverse. To every element $a \in R$, there exists an element $b \in R$ such that $a+b=0=b+a$. Then b is called the inverse of a and is denoted by $(-a)$.

(v) Addition is commutative $a+b=b+a$, for all $a,b \in R$.

(b) Closure and associative law for multiplication

(i) Closure law $a \cdot b \in R$, for all $a,b \in R$.

(ii) Associative law $a \cdot (b \cdot c)=(a \cdot b) \cdot c$, for all $a,b,c \in R$.

(c) Distributive law

Multiplication is distributive with respect to addition, i.e. for all $a,b,c \in R$..

$$a \cdot (b+c)=a \cdot b+a \cdot c \qquad \text{[Left distributive law]}$$

and

$$(b+c) \cdot a=b \cdot a+c \cdot a \qquad \text{[Right distributive law]}$$

In other words, a group is said to be a ring provided following conditions are satisfied.

(i) $(R, +)$ is an abelian group

(ii) $(R, \cdot)$ is a semi group, i.e. multiplication is associative on R, and

(iii) Multiplication operation is distributive over addition operation,

Illustration

The set of integers I, the set of rational numbers Q, the set R of real numbers and the set of complex numbers C are examples of ring under ordinary addition and multiplication.

8.14 Properties of a Ring

If the algebraic structure $(R, +, \cdot)$ is a ring, then for all $a,b,c \in R.$, the following properties are satisfied:

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$
3. $(-a)(-b) = a \cdot b$
4. $a \cdot (b - c) = a \cdot b - a \cdot c$
5. $(b - c) \cdot a = b \cdot a - c \cdot a$

PF. 1. We have $a \cdot 0 = a \cdot (0 + 0)$ [since $0 + 0 = 0$]

$= a \cdot 0 + a \cdot 0$ [by distributive law]

Adding $-(a \cdot 0)$ to both sides we obtained

$$-(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + [a \cdot 0 + a \cdot 0]$$

$$0 = [-(a \cdot 0) + a \cdot 0] + a \cdot 0$$

$$0 = 0 + a \cdot 0 \text{ or } 0 = a \cdot 0$$

Similarly, $0 \cdot a = 0$

2. We have, $a[(-b) + b] = a \cdot 0$

$a \cdot (-b) + a \cdot b = 0$ [Distributive law]

so that $a \cdot (-b) = -(a \cdot b)$ [since $a + b = 0 \Rightarrow a = -b$]

Similarly, we have

$$(-a) \cdot b = -(a \cdot b)$$

Hence $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

3. $(-a) \cdot (-b) = -[(-a) \cdot b)] = -[-a \cdot b] = a \cdot b$, because $a \cdot (-b) = -(a \cdot b)$

4. $a \cdot (b - c) = a \cdot [b + (-c)] = a \cdot b + a \cdot (-c)$

$$= a \cdot b + [-(a \cdot c)] = a \cdot b - a \cdot c$$

5. $(b - c) \cdot a = [b + (-c)] \cdot a = b \cdot a + (-c) \cdot a$

$$= b \cdot a + [(-c \cdot a)] = b \cdot a - c \cdot a$$

Ex. 17 Show that the set, $S = \{0, 1, 2, 3, 4\}$ is a ring under the operation of addition and multiplication modulo 5.

Sol. Construct the composition tables for the two operations $+_5$ and $\times_5$ as follows:

$+5$	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

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

It is simple to prove from the first composition table that the structure $(S, +_5)$ is an abelian group.

From the second composition table we observe that S is closed with respect to the operation '$\times_5$'. Since S being a set of numbers, we have

(i) $(a \times_5 b) \times_5 c = a \times_5 \{(b \times_5 c)\}$ for all $a, b, c \in S$

(ii) $a \times_5 \{(b +_5 c)\} = (a \times_5 b) +_5 (a \times_5 c)$

and $(b +_5 c) \times_5 a = (b \times_5 a) +_5 (c \times_5 a)$, for all $a, b, c \in S$

Therefore S is a ring with respect to the given operations.

8.15 Type of Rings

Subring

A subset S of a ring $(R, +, \cdot)$ is said to be a subring of R, if and only if S is closed under the operations defined in R and form a ring under these operations.

For example, the set of even integers forms a subrings of the ring of the set of integers because for any even integer a and b, $a + b$ and $a \cdot b$ are both even.

Criteria for Subring

A non-empty subset S of a ring $(R, +, \cdot)$ will be a subring of R, if and only if the following conditions are satisfied:

(i) If $a, b \in S$, then $a - b \in S$

(ii) If $a, b \in S$, then $a \cdot b \in S$

Commutative ring

A ring $(R, +, \cdot)$ is said to be a commutative ring if it is commutative under the multiplicative operation, i.e., $a \cdot b = b \cdot a$, for all $a, b \in R$

Ring with unity

A ring $(R, +, \cdot)$ is said to be a ring with unity if it has a multiplicative identity, that is, if there exists an element in R denoted by 1 such that $1 \cdot a = a = a \cdot 1$, for all $a \in R$.

For example, the ring of all integers is a ring with unity, 1 being the unity of the ring.

Ring with or without zero divisors

A ring, R is to be a ring with-out zero divisors if the product of no two non-zero elements of R is zero, i.e. if $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$ or both $a = 0, b = 0$.

On the other hand if in a ring R there exist non-zero elements a and b s.t. $ab = 0$, then R is said to be a ring with zero divisors.

Illustrations

(i) The ring of integers is a ring without zero divisor because the product of the two non-zero integers cannot be equal to the zero.

(ii) The ring of integers with addition and multiplication modulo 6 is a ring with zero divisors.

For example. We have $2 \times_6 3 = 0$ so that the product of two non-zero elements 2 and 3 is zero.

Boolean ring

A ring R is said to be a Boolean ring if all its elements are idempotent, i.e.

$$a \cdot a = a, \text{ for all } a \in R.$$

Cancellation Law in a Ring

If R is a ring, then it is an abelian group under the operation of addition. For this operation, the cancellation law holds in all integers. Now we say that cancellation law holds in a ring R if

$ab = ac \Rightarrow b = c (a \neq 0)$ (Left cancellation law)

and $ba = ca \Rightarrow b = c (a \neq 0)$, (Right cancellation law)

for all $a, b, c \in R$

Hence, in a ring with zero divisors, it is impossible to define a cancellation law, i.e. from the equation $ab = 0$ we can not conclude that either a or b (or both) is zero.

Ex. 18 Show that a ring, R is without zero divisors if the cancellation law holds good in R.

Sol. Let a ring R is without zero divisors. Then we have to show that the cancellation law holds in R.

For this let, $a \cdot b = a \cdot c (a \neq 0)$, for all $a, b, c \in R$. Then

$$a \cdot b = a \cdot c \Rightarrow a \cdot b - a \cdot c = 0 \text{ or } a \cdot (b - c) = 0$$

Since R is without zero divisors and $a \neq 0$, therefore we must have $b - c = 0$, i.e $b = c$. Thus the left cancellation law holds in R. Similarly, we can show that the right cancellation law also holds in R.

Conversely, let the cancellation law holds in R. Then to show that R is without zero divisors, let $a \cdot b = 0 (a \neq 0, b \neq 0)$ or $a \cdot b = a \cdot 0$ (because $a \cdot 0 = 0$). So using left cancellation law, we have $b = 0$, which is a contradiction. Therefore R is without zero divisors.

8.16 Integral domain

A commutative ring with unity having no zero divisors is called an integral domain.

It is generally denoted by $(D, +, *)$. In other words we say that a ring will be an integral domain, if it

(i) is commutative,

(ii) has unit element,

(iii) is without zero divisors.

Illustrations

1. The set of integer, I is an integral domain, since I is a commutative ring with unity. Also, I does not contain zero divisors. We know that if $a, b \in I$ such that $a \cdot b = 0$, then either a or b (or both) is zero.

2. The ring R of numbers: $a+\sqrt{2}b; a,b \in I$ is an integral domain, R is a commutative ring with unity because $1+\sqrt{2}.0=1$. It is also without zero divisors. For example, we have

$$(a+\sqrt{2}b)(c+\sqrt{2}d)=(ac+2bd)+\sqrt{2}(bc+ad)=0$$

only if $ac+2bd=0$ and $bc+ad=0$ and this may be possible only when either $a=0$ or $b=0$ or $c=0$ and $d=0$. Hence, $(a+\sqrt{2}b)(c+\sqrt{2}d)=0$

$\Rightarrow$ either $a+\sqrt{2}b=0$ or $c+\sqrt{2}b=0$.

8. 17 Fields

A ring, R with atleast two elements is said to be the field if the nonzero elements of R form an abelian group under multiplication, i.e. a ring R is a field if it has two atleast two elements and

(i) is commutative, (ii) has a unit element,

(iii) is such that each nonzero element has a multiplicative inverse.

Illustrations

(a) Consider the set $\{0, 1\}$ under the addition and multiplication modulo 2. It can be easily seen that $[\{0, 1\}, +_2, \times_2]$ is a commutative ring with unit element. The only nonzero element is 1 which is inverse of itself. Hence, it is a field.

(b) The ring $(Q, +, \cdot)$ of rational numbers is a field because it is a commutative ring with unity and each nonzero element has a multiplicative inverse.

(c) The ring $(R, +, \cdot)$ of real numbers and $(C, +, \cdot)$ of complex numbers are also example of fields.

Remarks (a) For a field, 1 and 0 are distinct elements i.e. $1 \neq 0$. If a is any nonzero element, then a^{-1} exists and is nonzero. Now a field has no zero divisors. Therefore, $1 \neq a^{-1}.a \neq 0$.

(b) Every field is an integral domain but the converse is not true, i.e., every integral domain is not a field. For example, the ring of integers is an integral domain which is not a field since no element except 1 and -1 has a multiplicative inverse.

Ex. 19 Show that the set of all real numbers of the form $a+b\sqrt{2}$, where a and b are real numbers, forms a field under the operation of addition and multiplication.

Sol. (i) *Closure property* Let $R=\{a+b\sqrt{2}\,;a,b\in Q\}$. If $a_1+b_1\sqrt{2}\in R$ and $a_2+b_2\sqrt{2}\in R$, then

(a) $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})=[(a_1+b_2)+(b_1+b_2)\sqrt{2}]\in R$

(b) $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=[(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}]\in R$

Thus, R is closed under the operations of addition and multiplication.

(ii) *Associativity* Since all the elements of R are real numbers, therefore associative laws hold for addition and multiplication.

(iii) *Identity* Since $0\in Q$, it is easy to verify that $0+0\sqrt{2}$ is the additive identity.

(iv) *Inverse* The addiative inverse of $a+b\sqrt{2}$ is $(-a)+(-b)\sqrt{2}$.

(v) *Multiplicative identity* Since $(1+0\sqrt{2})(a+b\sqrt{2})=a+b\sqrt{2}$, Therefore $1+0\sqrt{2}$ is the multiplicative identity.

(vi) *Multiplicative inverse* Let $a+b\sqrt{2}$ be an element of the ring where $a\neq 0, b\neq 0$.

Now $\dfrac{1}{a+b\sqrt{2}}=\dfrac{1}{a+b\sqrt{2}}\times\dfrac{a-b\sqrt{2}}{a-b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}=\dfrac{a}{a^2-2b^2}-\left(\dfrac{b}{a^2-2b^2}\right)\sqrt{2}$

which is of the form $c+d\sqrt{2}$ where c, d are rational numbers. Therefore, the multiplicative inverse of $a+b\sqrt{2}$ is

$$\frac{a}{a^2-2b^2}+\sqrt{2}\left[-\frac{b}{a^2-2b^2}\right]$$

(vii) *Commutativity* Since all the elements if R are real numbers which are commutative for addition and multiplication.

Hence the given structure will be a field.