4 → 0110, 1000, 1001, 1010, 1011, 1100, 1101

(a) $a_0 = 1, a_1 = 2, a_2 = 4, a_3 = 7$ and $a_4 = 13$

(b) $a_n = a_{n-1} + a_{n-2} + a_{n-3}, n \geq 3$ (c) 24

16. (a) $a_n = a_{n-1} + (n-1)$ (b) $a_n = a_{n-1} + C(n-1, 2)$

17. $S_n = 3(-2)^n$

19. (a) $1 + 2n$ (b) $2^{n+2} - 1$ (c) $3 + n(n+1)/2$ (d) $5n!$

20. (a) $a_n = 3^n$ (b) $n(n-1)/2$ (c) $a_n = 2^n + 3.5^n$ (d) $a_n = (2+n)\,4^{n-1}$

(e) $a_n = 3.2^n + (-1)^n$

23. (a) $a_n = c_1 3^n + c_2 2^n + \frac{1}{2}$ (b) $a_n = c_1 2^n + c_2 4^n + 1$

(c) $a_n = c_1 + c_2 n + \frac{1}{2} n^3 + n^2$ (d) $a_n = c_1 2^n + c_2 3^n + \frac{1}{2} n^2 + \frac{3n}{2} + 5/2$

(e) $a_n = c_1 + c_2 n + \frac{1}{2} n^3 + n^2$ (f) $a_n = \frac{c_1}{2^n} + c_2 3^n - \left(\frac{4}{3}\right) 2^n$

(g) $a_n = (c_1 + c_2 n)\,2^n + n^2 \cdot 2^n\,(n/6 + 1)$

24. (a) $a_n = n(n+1)/2 + 2$ (b) $a_n = 10 \cdot 2^n - 6n - 12$

(c) $a_n = (n+1)^2$ (d) $a_n = 3^{n+1} - \frac{1}{2}$

(e) $a_n = (5/6)(-2)^n + 1 + 1/6 \cdot 4^n$ (f) $a_n = 5/8\,(-5)^n + (11/8)3^n - \frac{1}{2}n - 1$

(g) $a_n = 3^{n+1} - 2^{n+1}$

25. $a_n = n \cdot 2^{n-1}$.

ANSWERS 10.4

1. (a) $\frac{x^3}{1-x}$ (b) $\frac{x^2}{(1-x)^2}$ (c) $\frac{3}{1+x}$ (d) $\frac{3}{1-3x}$ (e) $\frac{1}{(1-x)^2}$

2. (a) $\frac{5}{1-x}$ (b) $\frac{x}{(1-x)^2} + \frac{3}{1-x}$ (c) $\frac{1}{1-3x}$

(d) $\frac{3x}{(1-x)^2} + \frac{5x(1+x)}{(1-x)^3}$ (e) $\frac{2x^2}{(1-x)^3}$

3. (a) $x^3\,G(x)$ (b) $G(x) - a_0 - a_1 x$ (c) $G(x^2)$ (d) $G(3x)$

4. (a) $a_0 = 0, a_n = 2^{n-1}, n > 0$ (b) $a_0 = a_1 = 0, a_n = 1, n > 1$ (c) $a_n = n$

(d) $a_n = n - 1$ for $n \geq 0$ (e) $a_n = 5^n$

$a_0 = a_1 = 0$

5. (a) $a_n = (c_0 + c_1 n)(-1)^n + \frac{1}{6}(2n-1)$ (b) $a_n = c_3 + c_4 n + 2^n$

(c) $a_n = (c_0 + c_1 n + \frac{1}{2} n^2)\,2^n$ (d) $a_n = c\,3^n + 2n + 3(1 - 2^{n+1})$

(e) $a_n = (c_0 + c_1 n + c_2 n^2)\,2^n + 27 \cdot 3^n$

6. (a) $a_n = n!$ (b) $a_n = 0$ if n is even $= 2^{n-1}$ if n is odd (c) $a_n = 1 + 2^n$

(d) $a_n = 1 - 2^n + 3^n$ (e) $a_n = 2^n(1-n)$ (f) $a_n = 13\,(5)^n - 10\,(2)^n$.

7. (a) C(15, 10) (b) 3^{10} (c) C(15, 10) (d) 3 (e) 4

8. $1 + x + x^2 + x^3 + 5x^4 + 5x^5 + 5x^6 + 5x^7$

9. 10 10. 6.

11. $(1 + x + x^2)(x + x^2 + x^3)(x^4 - x^6)$.

Shikhar

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 ($\times$) are binary operations on the set N of natural numbers, for, the sum and product of two natural numbers are also natural numbers. Therefore, N is closed with respect to addition and multiplication, i.e

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

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

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

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 headed 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 an 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 the 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 * 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 $e * a = a$, 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 $1 . x = x . 1 = x$ 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.

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

$= x^{y^z}$

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

Thus, * is not associative.

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

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

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

From the table we can conclude that

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

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

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

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

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

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

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

Table 11.2

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. Identity element. What is the inverse of an integer a ?*

Solution. Since I is closed for addition, we have

$a + b \in Z$ for all $a, b \in Z$

$\Rightarrow a + b + 1 \in Z$

$\Rightarrow a * b \in Z$

* is a binary operation on I.

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 I 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,

$a * b = -1 \Rightarrow a + b + 1 = -1$

$\Rightarrow b = -(2 + a)$

$\Rightarrow$ So, the inverse of a is $-(2 + a)$.

Group

Let, (G, *) be an algebraic structure, where * is a binary operation, then (G, *) is called a group with 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 $a, b, c \in G$.
3. (identity element) There exists an identity element *i.e.*, for some $e \in S$, $e * a = a * e$, $a \in G$.
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 * operation.

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

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 multiplic... with 1 as identity element, and $1/a$ as the inverse of a. The same is true ... 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... element for + in Z^+. The set Z^+ with operation multiplication is not a grou... identity element 1, but no inverse of 3.

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

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

×	1	−1	i	−i
1	1	−i	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 ... 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 el... 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 ... row and first column of the table.

Inverses : Inverses of $1, -1, i, -i$ are $1, -1, i, -i$ respectively and all those belong ... Hence it follows that G is an abelian multiplicative group.

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

Solution. Let Q^+ denote the set of all positive rational numbers. We have to sho... $(Q^+, *)$ 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^+, therefo... 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 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*

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

In the system $(G, +_6)$

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

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

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

Hence the composition table is

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

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

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

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

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

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

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

Hence the composition table is:

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

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

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

Example 13. *Show that the matrices*

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

form a multiplicative abelian group.

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

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

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

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 elem... G and hence G is closed w.r.t. matrix multiplication.

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

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

(*iii*) **Commutative law :** The entries in the first, second, third and fourth columns ... composition table coincide with the corresponding entries in the first, second, third and fourth ...

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 ... $(G, .)$ 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 $c \neq$ ... Therefore, $ac \neq 0$. Consequently $(a, b) * (c, d) = (ac, bc + d)$ is also a member of G. Hence G is clo... with respect to the given composition.

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

$$[(a, b) * (c, d)] * (e, f) = (ac, bc + d) * (e, f)$$
$$= ([ac]\, e, [bc + d]\, e + f)$$
$$= (ace, bce + de + f).$$

Also $(a, b) * [(c, d) * (e, f)] = (a, b) \times (ce, de + f)$
$$= (a\,[ce], b\,[ce] + de + f)$$

$$= (ace, bce + de + f).$$

...e the given composition * is associative.

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

...

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

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

...herefore, $(1, 0)$ is the identity element

...verse element : Let (a, b) be any member of G Let (x, y) be a member of G Let $(x, ...$ ... $(1, 0)$.

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

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

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

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

...ence G is a group.

...ote. In the above group, we have

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

...d,

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

...xample 15. *Let M_2 be the set of 2×2 matrices over R i.e.,*

$$M_2 = \left\{\begin{bmatrix}a & b\\ c & d\end{bmatrix} \mid a, b, c, d \in R, ad - bc \neq 0\right\}$$

Show that $(M_2, +)$ is both associative and commutative and $(M_2, .)$ is associative but not ...mutative.

Solution. For any two matrices

$$A = \begin{bmatrix}a_1 & b_1\\ c_1 & d_1\end{bmatrix}, B = \begin{bmatrix}a_2 & b_2\\ c_2 & d_2\end{bmatrix} \text{ where } \det(A) \neq 0, \det(B) \neq 0$$

...the usual sum and product

$$A + B = \begin{bmatrix}a_1 + a_2 & b_1 + b_2\\ c_1 + c_2 & d_1 + d_2\end{bmatrix} \quad AB = \begin{bmatrix}a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2\\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2\end{bmatrix}$$

The sum and product of two non zero determinant is also a non-zero determint follows from ...act

$\det(A + B) = \det A + \det B$ and $\det(AB) = \det(A) \det(B)$.

Thus $A + B$ and $A \cdot B$ also in G.

From the well-known properties of matrices, we know the addition in M_2 is commutative and ...ociative.

The matrix

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

is the identity under addition and

$$-A = \begin{bmatrix} -a_1 & -b_1 \\ -c_1 & -d_1 \end{bmatrix}$$

is the inverse of A under addition.

Again M_1 is associative under matrix multiplication

The matrix

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

is the identity element and the inverse of $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ is

$$\begin{bmatrix} \frac{d_1}{a_1d_1 - b_1c_1} & \frac{-b_1}{a_1d_1 - b_1c_1} \\ \frac{-c_1}{a_1d_1 - b_1c_1} & \frac{a_1}{a_1d_1 - b_1c_1} \end{bmatrix}$$

Matrix multiplication is not commutative *i.e.*, $AB \neq BA$ in general.

For $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $AB \neq BA$.

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. (Left Cancellation Law). If a, b, c are in G, then $a * b = a * c \Rightarrow b = c$.

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

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

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

$$e * b = e * c$$

$$b = c.$$

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

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

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

$$= e$$

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

Thus, $a^{-1} * (a * e) = a^{-1} * a$ by Theorem 11.3

$$a * e = a.$$

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)

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

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

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

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

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

Theorem 11.6. (Right Cancellation Law) If a, b, c are in G then

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

Proof. We have $b * a = c * a$

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

$$b * e = c * e$$

or $$b = c$$

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

Theorem 11.7. In a group (G, *) the equations

$$a * x = b \text{ and } y * a = b,$$

have unique solutions for the unknown x and y ; the solutions are $x = a^{-1} * b$ and $y = b * a^{-1}$, 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 11.8. 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 in the product 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, $(a * b)^{-1} * (a * b) = e$.

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)

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

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 cancellation

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 $a^2 = a$.

(*i*) To prove that $a = e$.

$$a^2 = a \Rightarrow a.a = a \Rightarrow (aa)\, a^{-1} = a a^{-1}$$
$$\Rightarrow a\,(aa^{-1}) = e. \quad (\because aa^{-1} = e)$$
$$\Rightarrow ae = e \Rightarrow a = e. \quad (\text{since } ae = a)$$

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

Is the converse true ?

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

Hence, by the given condition, we have

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

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

Therefore, it is an abelian group.

The converse is not true. For example, (R, +), where R is the set of all real numbers, is 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 $(ab)^2 = a^2 b^2$.

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,

Suppose G is abelian so that

$$ab = ba \quad \forall\, a, b \in G \qquad \ldots (3)$$

Prove that $(ab)^2 = a^2b^2$

$$(ab)^2 = (ab)\,(ab) = a\,(ba)\,b = a\,(ab)\,b, \qquad (\text{by } (3))$$
$$= (aa)\,(bb) = a^2b^2.$$

Hence proved.

Example 20. *G is a group and there exist two relatively prime positive integers m and n such that $(ab)^m = b^m a^m$ 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

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

Similarly it can be proved that

$$(a^m b^n)^{ny} = (b^n a^m)^{ny} \qquad \ldots (2)$$

From (1) and (2) we get

$$a^m b^n = (a^m b^n)^{mx + ny}$$
$$= (b^n a^m)^{mx + ny} = b^n a^m. \qquad \ldots (3)$$

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

Hence G is Abelian.

Order of an Element

The order of an element g in a group G is the smallest positive integers n such that $g^n = e$. If no such integer exists, we say g has infinite order. The order of an element g is denoted by

So, to find the order of a group element g, one need only compute the sequence of products $g, g^2, \ldots$ 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 $a^6 = e$.

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

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

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

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

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

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

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

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

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 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.

Example 23.

(*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 does not belong to the set of odd integers and hence is not closed.

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

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

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

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

Theorem 11.9. A semigroup (S, *) is a group if and only if

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

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

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

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

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

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

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

Converse can be proved from the definition of a group.

Theorem 11.10. A semi group (S, *) is a group if and only if for $a, b \in S$ each of the equations $a * x = b$ and $y * a = b$ has a solution in S for x and y.

Proof: If S is a group, then by theorem 11.7, the equation $a * x = b$ and $y * a = b$ have solutions in S.

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

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

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

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

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

Theorem 11.11: A finite semi-group (S, *) is a group if and only if (S, *) satisfies the cancellation laws (*i.e.*, $a * c = b * c$ implies $a = b$ and $c * a = c * b$ implies $a = b$ for all $a, b, c \in S$).

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

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

and

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

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

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

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

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

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

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

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

Hence by Theorem 11.10 {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 $A = \{a, b, c\}$

It consists of replacing an occurrence of $a_i = a_i^{m+n}$. 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 oper
B is called a **sub semi-group** of $(S, *)$. Since the elements of B are also elemen
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. T
and $(B, \times)$ are sub semi groups of $(N, \times)$ since A and B are closed under multiplicatio
other hand, $(A, +)$ is a sub semi group of $(N +)$ since A is closed under addition, but $(B$
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
is words with even length. The concatenation of two such words is also even. Thus L is
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
also group by itself.

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

Example 24

(*i*) The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1$
(*ii*) The additive group of even integers is a subgroup of the additive group of all integ
(*iii*) The set Q^+ of all non-zero positive rational numbers is a subgroup of the multipli
group Q^* of all non – zero rational numbers.

Important Theorems

Theorem 11.12. 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
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 11.13. The inverse of any element of a subgroup is the same as the inverse of it
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
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
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
subgroup.

Theorem 11.14. (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.* $a \in H, b \in H \Rightarrow a * b \in H$.

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

ndition is Sufficient

bserve that the binary operation * in G is also a binary operation in H. Hence H is closed
operation

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

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

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

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

Theorem 11.15. The necessary and sufficient condition for a non-empty sub-set H of a group
G be a subgroup is

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

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

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

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

hus the condition is necessary.

o 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 $G = \{\ldots\ldots 3^{-2}, 3^{-1}, 1, 3, 3^2, \ldots\ldots\}$ be the multiplicative group consisting of all
integral powers of 3. Let $H = \{1; 3, 3^2, \ldots\ldots\}$. 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 11.16. 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, $ab^{-1} \in H_1$, $ab^{-1} \in H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_1$

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

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

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 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. 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 H well as a left coset.

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

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

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

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 (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

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

Since the group G is abelian any right coset will be equal to the corresponding left coset 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 disj i.e., have no element common.

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

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

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

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

ion of all right cosets of H in G will be equal to G, i.e.

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

ndex of H in G is 3.

of Cosets

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

$a \in aH$

$aH = H$ if and only if $a \in H$

$aH = bH$ or $aH \cap bH = \phi$

$aH = bH$ if and only if $a^{-1} b \in H$,

nalogus results hold for right cosets.

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

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

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

$$\Rightarrow a \in H$$

$aH = H$ if and only if $a \in H$ and $h \in H$ then

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

$aH \subset H$

lso $a \in H \Rightarrow a^{-1} H$. 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

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

$H \subset aH$

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

ext $a \in H \Rightarrow aH = H$ ... (2)

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

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

hen 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 $h' h^{-1} = h''$ so that $a = bh''$.

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

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

Thus either $aH \cap bH = 0$ or $aH = bH$.

4. We have.

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

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

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

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

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

Also, if $a^{-1} b \in H$, then ... (2)

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

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

Normal Subgroup

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

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

Theorem 11.17. A subgroup H of a group G is normal if and only if $g^{-1}hg \in H$, $g \in G$.

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

Then $Hg = gH$ (Definition of normal subgroup)

Now $hg \in Hg = gH$

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

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

Conversely let H be such that

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

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

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 normal subgroup if

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

Example 28. *Consider the group $(Z, +)$. Let $H = \{3n : n \in Z\}$ show that H is a sub 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 $G_x = \{a \in G : ax = xa\}$. Sho 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*) $a \in G_x \Rightarrow ax = xa$.

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

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

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

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

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

inverse of each element of G_x is in G_x.

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

et of a group G is denoted by $o(G)$. A group of finite order is called a *finite group*. By ncept of cosets we prove a theorem due to Langrange which expresses a relationship rder of a finite group and the order of its subgroup.

Theorem

m 11.18. The order of each sub-group of a finite group G is a divisor of the order of

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

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

$$H = \{h_1, h_2, \ldots, h_m\}.$$

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

we have

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

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

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

his 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.

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

$$a^n = e.$$

$o(a) = m$ 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 of H is m.

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

et $n = mk$, then

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

olved 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 ormal 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 $ghgh\,h^{-1}g^{-2} \in H$, $ghg^{-1} \in H$. 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 tisfying 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

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

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 a subgroup of G.

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

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

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

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

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

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

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

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

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

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

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 (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 of 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. 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.

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

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 $1 = -1$

Thus $1^{-2} = (1^2)^{-1} = -2, 1^{-3} = (1^3)^{-1} = (3)^{-1} = -3$ 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 $w^0 = 1, w^1 = w, w^2 = w^2, w^3 = 1$

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

Thus each element of the group can be expressed as some integral powers of w and w^2. Hence it 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

$1^1 = 1, 1^2 = 1 +_6 1 = 2, 1^3 = 1 +_6 1^2 = 3, 1^4 = 1 +_6 1^3 = 1 +_6 3 = 4, 1^5 = 1 +_6 1^4 = 1$

$1^6 = 0$

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.

Important Properties of Cyclic Groups

Theorem 11.19. Every cyclic group is an abelian group.

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

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

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

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

So G is abelian.

Theorem 11.20. If a is a generator of a cyclic group G, then a^{-1} is also a generator of G.

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

Theorem 11.21. 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 $(a^m) < n$. Therefore a^m can not be a generator of G because the order of a^m is not equa 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 = $\{a, a^2, a^3, a^4, a$

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* $(\{1, 2, 3, 4, 5, 6\}, x_7)$ *is cyclic. How many ge*

Solution. G be a given group. If there exists an element $a \in G$ such that $o(a)$ to the order of the group G then the group G will be a cyclic group and a will be a gene

Note that $o(3) = 6$ because $3^1 = 3$, $3^2 = 3x_7 3 = 2$, $3^3 = 3^2 x_7 3 = 6$, $3^4 = 6x_7 3 = 4$, $3^6 x_7 3 = 5x_7 3 = 1$ *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 $= \langle a \rangle$ 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, $= n$. Then G = $\{e, a, \ldots\ldots, a^{n-1}\}$, which is a contradiction since G is an infinite group. The 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 some $r, t \in Z$. Thus, $a = b^r = (a^t)^r = a^{rt}$. Hence, by *(i)*, $rt = 1$. This implies that either $r = 1 = t$ $-1 = t$. Thus, either $b = a$ or $b = a^{-1}$. Now from *(i)*, $a = a^{-1}$. Therefore, G has exactly two gene

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 element of A has a unique image in A, no two distinct elements of A have the same image, and e element of A has a unique pre-image, under f. Thus, the range of f is of the form

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

In the notation of relations the function f is given by

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

This is written in two line notation as

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

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

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

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

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

of Two Permutations

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.

mple 40. Let f and g be given by

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

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

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

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

ity Permutation

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

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

uct 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 perform f and then perform g.

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

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

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

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 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.*

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

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. 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.

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

Multiplication of disjoint cycles is clearly commutative, so the order of the factors (1, 6) and (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

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

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

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

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

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

Alternating Group

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

Theorem 11.23 Out of $n!$ permutations of n symbols, $n!/2$ are even permutations and $n!/2$ are odd permutations.

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

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

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

Let l be any proposition in P_n then by closure property $le_1, le_2, \ldots, le_s, lo_1, lo_2, \ldots lo_t$ are all distinct elements of P_n. For if $lo_1 = lo_2$, then $o_1 = o_2$ which contradicts that o_1 and o_2 are distinct.

Now $le_1, le_2, \ldots, le_s$ are odd permutations. Since there are t number of odd permutations, $s \le t$. Similarly, we can show that the even permutations $lo_1, lo_2, \ldots, lo_t$ are distinct elements

Therefore $t \le s$.

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

Theorem 11.24 If A_n is the set of all even permutations of degree n, then A_n is a finite group of order $n!/2$ with respect to the composition of permutation.

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

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

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

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

I is an identity element.

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

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

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

Dihedral Group D_n

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

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

Dihedral group: The symmetry group of the regular polygon of n sides is called the dihedral group of degree n and is denoted by D_n. For example, D_3 is the dihedral group of an equilateral triangle, D_4 is the dihedral group of a square, D_5 is the dihedral group of a regular pentagon. It is easy to find that D_3 has 6 elements, D_4 has 8 elements and D_5 has 10 elements.

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

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

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

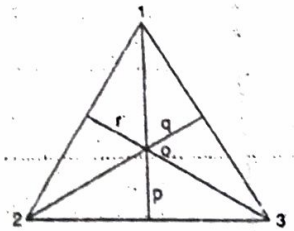


Fig.

Let G be the set consisting of six elements:

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

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

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

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

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

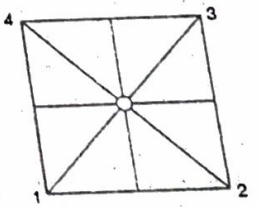
composition table is given below and it follows from the table that $(G, *)$ is a non-abelian der six and known as the **dihedral group of degree 3 (D_3).**

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

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

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

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



et G be the set consisting of eight elements:

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

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

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

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

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

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

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

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

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

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

11.8. Homomorphism and Isomorphism of Groups

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

Let $(G, *)$ and $(G_1, *_1)$ be two groups and f is a function from G into G_1. Then f is c 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 monomorp f is one-one. If there is an epimorphism f from G onto G_1, then G_1 is called a homomorphic

A homomorphism f of a group G into a group G_1 is called a **isomorphism** of G onto G_1 one-one onto G_1. G and G_1 are said to be isomorphic and denoted by $G \cong G_1$. An isomorphi 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 element mapped onto the identity element of G_1 by f. That is, the kernel of f, written as ker f, is defined to t

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

Example 46. (*i*) Let G = Z and G' = {1, – 1} the multiplicative group. The mapping $f: G \to$ 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 pos real numbers for multiplication. The mapping $f: G \to G'$ given by $f(a) = 2^a$ is a group homomorphi because $f(a + b) = 2^{a+b} = 2^a 2^b = f(a) . f(b)$.

Example 47. *If R be the group of real numbers under addition and let R^+ be the grou positive real numbers under multiplication. Let $f: R \to R^+$ be defined by $f(x) = e^x$ then show f is an isomorphism.*

Solution. If $f(a) = f(b)$, so that $e^a = e^b$, then $a = b$. Thus f is one to one.

If $c \in R^+$, then $\ln c \in R$ and $f(\ln c) = e^{\ln c} = c$,

Thus each element of R^+ is the f image of some element of R and hence f is onto.

Again $f(a + b) = e^{a+b} = e^a e^b = f(a) f(b)$

Hence f is an isomorphism.

Example 48. *If R^+ be the multiplicative group of all positive real numbers.*

Let $f: R^+ \to R^+$ by $f(x) = x^2$ for all $x \in R^+$. Show that f is automorphism of R^+.

Solution. Now for any $x, y \in R^+, f(xy) = (xy)^2 = x^2y^2 = f(x) f(y)$.

Thus f is an endomorphism of R^+.

Also $f(x) = f(y) \Rightarrow x^2 = y^2 \Rightarrow x = y$, since $x > 0, y > 0$.

Thus f is a one-one mapping.

Now $x \in R^+$, $\sqrt{x} \in R^+$ such taht $f(\sqrt{x}) = (\sqrt{x})^2 = x$,

which proves that f is also onto.

Consequently f is an automorphism.

Properties on Homomorphisms.

Theorem 11.22. Let $(G, *)$ and $(G_1, *_1)$ be two groups and let $f: G \to G_1$ be a homomorphism of G. 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 homomorpism, $f(e) *_1 f(e) = f(e * e) = f(e)$

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

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

$f(e) = e_1$ 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 11.23. 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 $Ker f \neq \emptyset$. Let $a, b \in Ker f$. Then $f(a) = e_1$, $f(b) = e_1$ and hence $f(ab^{-1}) = f(a) f(b^{-1}) = e_1 e_1^{-1} = e_1 e_1 = e_1$. 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 $f(gag^{-1}) = f(g) f(a) f(g^{-1}) = f(g) e_1 f(g^{-1}) = f(g) f(g)^{-1} = e_1$ 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

$$(aH)(bH) = (ab)H$$

and is called the factor group or quotient group of G by N and is denoted by G/N *i.e.* G/H = {gH : g ∈ G}.

Problem Set 11.3

1. Define a subgroup. Give examples.
2. Show by means of examples that the union of two subgroups may or may not be subg
3. If a is any element of a group G, then $\{a^n : n \in Z\}$ is a subgroup of G.
4. If G is a group, then show that $C = \{c \in g : cx = xc \text{ for all } x \in G\}$ is a subgroup of G.
5. What is least order of a non-abelian group ? Show that all proper subgroups of a group be abelian.
6. If H is a subgroup of G such that $x^2 \in H$ for every $x \in G$, these prove that H is a normal
7. Sow that the set $H = \{a + bi \in C : a^2 + b^2 = 1\}$ is a subgroup (C,) where, is the operation of complex numbers.
8. Let $G = \{(a, b) : a, b \in R, b \neq 0\}$. Prove that (G, *) is a non commutative group operation, $(a, b) * (c, d) = (a + c, bd)$ for all $(a, b), (c, d) \in G$.
   (*i*) Let $H = \{(a, b) \in G : a = 0\}$. Show that H is a subgroup of G
   (*ii*) Let $K = \{(a, b) \in G : b > 0\}$. Show that K is a subgroup of G
   [Hints (*i*) (0, 1) identity element, inverse of (a, b) is $(-a/b, 1/b)$ (*i*) Since $(0, 1) \in K$, $K \neq \phi$ $(c, d) \notin K$. Thus $b > 0$ and $d > 0 \Rightarrow bd$. 0. Hence $(a, b)(c, d)^{-1} = (a, b)(-c/d, 1/d) =$ $bd \notin K$. thus K is a subgroup.
9. Show that each of the following sets is a subgroup of the multiplicative group of 2×2 matrices over R.

   (*i*) $S = \left\{\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \neq 0\right\}$

   (*ii*) $S = \left\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \neq 0\right\}$

   (*iii*) $S = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : ad \neq 0\right\}$

   (*iv*) $S = \left\{\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right\}$.

10. Let a be a fixed element of group G.
    Let $H = \{x \in G : xa^2 = a^2x\}$
    and $K = \{x \in g : xa = ax\}$.
    Show that H is a subgroup of G and that K is a subgroup of H.
11. Let H be a subgroup of group G and a be an element of G. Let $aH = \{ah : h \in H\}$. Prove that (*i*) aH, (*ii*) for $b \in G$, if $b \in aH$, then $aH \cap bH = \phi$.
12. Let a binary operation * on G be defined by $(a, b) * (c, d) = (ac, bc + d)$ for all ordered pairs (a, b) real numbers, $a \neq 0$. Show that (G, *) is a non-abelian group. Does that sub set H of all those elements of G which are of the form $(1, b)$ from a subgroup of G?
13. Let G be a multiplication group of all positive real numbers and R the additive group of all numbers. Is G a subgroup of R? Given reasons.
14. Answers the followings: (*i*) Can abelian group have a non abelian subgroup? Can a non-abelian group have an abelian subgroup? Can a non-abelian group have a non-abelian subgroup?
15. Show that the set of inverses of the elements of a right coset is a left coset ϕ *i.e.*, $(Ha)^{-1} = a^{-1}H$.
16. Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\ldots\}$. Find all the left cosets of H in Z.
17. If G be a group of prime order p, then show that G has no proper subgroup.
18. Let G be a group of integers under addition and let N be the set of all integral multiples of 3. Prove that n is a subgroup of G and determine all the cosets of N in G.

...the algebraic structure, where Z is the set of integers and * is defined by $a * b = a + b - 1$. Determine whether (Z, *) is a monoid or a group or an abelian group.

...11.4

...a cyclic group. Show that the set $\{1, \omega, \omega^2\}$ is a cyclic group of order 3 with respect to ...ication, ω being the cube root of unity.

...that the group $\{1, -1, i, -i\}$, . } is cyclic with generators i and $-i$.

...that the group $\{(1, 2, 3, 4), \times_5\}$ is cyclic

...many generators are there of cyclic group of (*i*) order 6 and (*ii*) order 10.

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

...that (6 5 4 3 1 2) is an even permutation while (6 7 5 4 1 2) is an odd permutation.

...mine which of the following permutations is even or odd :

(1 3 5)

(ii) (1 3 5 6)

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

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

...(1 2) (1 3 4) (1 5 2).

...the inverse of each of the following permutations :

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

(ii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

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

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

...press each of the following as a product of transpositions and hence determine whether it is odd or ...ven.

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

(ii) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

(iii) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

...how that the inverse of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ is an identity permutation.

...If $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ show that $fg \neq gf$.

...Express the following permutations as the product of disjoint cycles

(*i*) $a = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$,

(*ii*) $b = (1\ 2)(1\ 2\ 3)(1\ 2)$,

(*iii*) $c = (1\ 3\ 2\ 5)(1\ 4\ 3)(2\ 5\ 1)$.

...If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$, show that $fg \neq gf$

...If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, find $g f g^{-1}$.

...Show that the mapping f from the group of real numbers under addition to itself given by $f(x) = [x]$, the greatest integer less than or equal to x, is not a homomorphism.

...Let R^+ be the group of nonzero real numbers under multiplication, and ler r be a positive integer. Show that $f(x) = x^r$ is a homomorphism from R^+ to R^+.

17. Let G be a group of real numbers under addition and G′ be the group of positive real numbers under multiplication. Show that the mapping defined by $f(x) = 2^x$ is a homomorphism.
18. Let S = N × N. Let * be the operation on S defined by $(a, b) * (a', b') = (aa', bb')$
    (*a*) Show that * is associative.
    (*b*) Define $f: (s, *) \to (Q, x)$ by $f(a, b) = a/b$. Show that f is a homomorphism.
19. Let S = N × N. Let * be the operation on S defined by
    $$(a, b) * (a', b') = (a + a', b + b')$$
    (*a*) Show that * is associative.
    (*b*) Define $f: (s, *) \to (Z, +)$ by $f(a, b) = a - b$. Show that f is a homomorphism.
20. Let G be a group. Define a function $g: G \to G$ by $g(x) = gxg^{-1}$. Show that g is an isomorphism of G onto g, *i.e.*,
    (*a*) g is a homomorphism, (*b*) g is one-to-one, (*c*) g is onto.
21. Determine which of the following maps is homomorphism. If the map is a homomorphism, describe the image and the kernel.
    (*a*) $f: Z \Rightarrow R$ under additive given by $f(n) = n$
    (*b*) $f: R \Rightarrow Z$ under addition given by $f(x) = [x]$
22. Let G be a group. Prove that the map $f: G \to G$ given by $f(a) = a^{-1}$ for all $a \in G$ is an isomorphism if and only if G is commutative.
23. Let e be the identity element of a group G. Then the map $f: G \to G$ defined by $f(x) = x$ for all $x \in G$ is an endomorphism.
24. Consider the mapping $f: C^* \to C^*$ defined by $f(x) = x^4$, where C^* is the multiplicative group of non-zero complex numbers. Show that the mapping is homomorphism with kernel $f = \{1, -1, i, -i\}$.
25. Show that the mapping defined by f: $R^+ \to R^+$, defined by $f(x) = |x|$ is a homomorphism with kernel $= \{1, -1\}$.
26. Prove that if for a group G, $f: G \to G$ given by $f(x) = x^3$, $x \in G$ is an isomorphism then G is abelian.
27. Let f be a homomorphism mapping of a group G into a group G′. Let $f(G)$ be the homomorphic image of G in G′, then $f(G)$ is a subgroup of G′.
28. Show that the mapping $f: C \to R$ defined by $f(x + iy) = x$ is a homomorphism of the additive group of complex numbers on the additive group of real numbers and find the kernel of f.
29. Show that the mapping $f: C^* \Rightarrow R^+$ defined by $f(z) = |z|$ for all $z \in C^*$ is homomorphism of C^* into R^+. What is the kernel of f.
30. Show that if $f: G \to G'$ is an isomorphism, then $f^{-1}: G' \to G$ is also an isomorphism.
31. Let $(S_1, *_1)$, $(S_2, *_2)$ and $(S_3, *_3)$ be semigroups, and let $f: S_1 \to S_2$ and $g: S_2 \to S_3$ be isomorphisms. Show that $g \circ f: s_1 \to s_3$ is an isomorphism.
32. Let T be the set of even integers. Show that the semigroups (Z, +) and (T, +) are isomorphic.

ANSWERS 11.1

1. The set Z of all integers is closed under the binary operation multiplication but the set of negative integers which is a proper subset Z is not closed w.r.t. this operation as the product of two negative numbers is not a negative integer.
4. Identity element 0, $a^{-1} = a/(a - 1)$.
7. (*i*) associative, (*ii*) Non associative.
10. (*i*) Neither commutative nor associative,
    (*ii*) Only commutative,
    (*iii*) Commutative,
    (*iv*) Only commutative,
    (*v*) Associative not commutative,
    (*vi*) Associative and commutative,
    (*vii*) Associative and commutative.

(*ii*) $(n^2 + n)/2$.

(1)

	a	*b*
a	*a*	*a*
b	*a*	*a*

(2)

	a	*b*
a	*b*	*a*
b	*a*	*a*

(3)

	a	*b*
a	*a*	*b*
b	*a*	*a*

(4)

	a	*b*
a	*a*	*a*
b	*b*	*a*

	a	*b*
a	*a*	*a*
b	*a*	*b*

(6)

	a	*b*
a	*b*	*b*
b	*a*	*a*

(7)

	a	*b*
a	*b*	*a*
b	*b*	*a*

(8)

	a	*b*
a	*b*	*a*
b	*a*	*b*

	a	*b*
a	*a*	*b*
b	*b*	*a*

(10)

	a	*b*
a	*a*	*b*
b	*a*	*b*

(11)

	a	*b*
a	*a*	*a*
b	*b*	*b*

(12)

	a	*b*
a	*b*	*b*
b	*b*	*a*

	a	*b*
a	*b*	*b*
b	*a*	*b*

(14)

	a	*b*
a	*b*	*a*
b	*b*	*b*

(15)

	a	*b*
a	*a*	*b*
b	*b*	*b*

(16)

	a	*b*
a	*b*	*b*
b	*b*	*b*

(*i*) Yes, (*ii*) Yes.
First row → *d*, Second row → *a*, fourth row → *c*, *b*.

ANSWERS 11.2

(*a*) does not have identity element
(*d*) does not have identity element
(*c*) does not have identity element.
Only {1, 10}
S is a trivial group ({0}, +)
0 (1) = 1, 0 (*w*) = 0, 0 (w^2) = 3.
(*a*) Semi group,
(*b*) Monoid, identity 1,
(*c*) Semi group,
(*d*) Monoid, identity 6
(*e*) Semi group.

ANSWERS 11.3

No, Yes, Yes

19. Monoid

ANSWERS 11.4

Two, a and a^3 Four, a, a^3, a^7, a^9.

7. (*i*) even, (*ii*) odd, (*iii*) even, (*iv*) even, (*v*) odd.

(*i*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ (*ii*) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ (*iii*) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ (*iv*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$

(*i*) (1, 2) odd, (*ii*) (1, 3) odd, (*iii*) (1 4) (2 3) even.
(*i*) a = (1 2 3 6 7 8 9 5 4). (*ii*) b = (1 3 2) (*iii*) c = (1 2) (3 5 4).

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

21. (*a*) yes, image of f = Z, kernel of f = {0} (*b*) no.

Ker f = all complex numbers where real part is zero.
Ker f = multiplicative subgroup of all complex numbers whose modulus is 1.