8

Groups

OBJECTIVES

- Introduction
- Binary Operation
- Algebraic Structures
- Semigroup & Monoid
- Composition Table
- Addition and multiplication modulo
- Group
- Abelian or Commutative Group
- Elementary Theorems Based on Groups
- Composition Table for Groups
- Subgroup
- Group Homomorphism and Isomorphism
- Permutation Group
- Cyclic Group
- Cosets
- Normal Subgroup
- Quotient Group (Factor Group)

8.1 Introduction

Here, we shall first explain what is meant by an algebraic structure and then discuss some of them such as semigroups, monoids, and groups. These structures have their applications in the field of computer science. For example, semigroups and monoids have useful applications in the areas of computer arithmetic, formal languages and study of finite–state machines, while group theory has its application in coding theory, which we will discussed later.

8.2 Binary Operation

An operation which combines two elements of a set to give another element of the same set is called the binary operation.

Mathematically, let A be a non–empty set then $A \times A = \{(a, b) : a \in A, b \in A\}$. If f is any mapping from $A \times A \to A$, i.e., $f : A \times A \to A$ then f is called a binary operation on A.

In general, $f : A^n \to A$ is called an n–ary operation. For $n = 1$, $f : A \to A$ is called a unary operation.

For $n = 2$, $f : A \times A \to A$ is called a binary operation.

It is customary to use symbols such as +, ., o, *, etc. to denote binary operations on a set.

Thus, * will be a binary operation on a set A if $a \in A, b \in A \Rightarrow a * b \in A$ and $(a * b)$ is unique.

The binary operation is also known as binary composition on the set A.

It is also to be noted that if * is a binary operation on A then A is said to be closed with respect to the composition *.

Example 1.

(i) Addition is a binary operation on the set N of natural numbers. Since $a \in N, b \in N \Rightarrow (a + b) \in N$, $\forall\ a, b \in N$.

In other words, N is closed under the operation addition.

(ii) Subtraction is not a binary operation on the set N of natural numbers.

Since $3 \in N, 4 \in N$ but $3 - 4 = -1 \notin N$.

(iii) Subtraction is a binary operation on the set Z of integers as

$a \in Z, b \in Z \Rightarrow (a - b) \in Z, \forall\ a, b \in Z$.

(iv) In the set of real numbers R, the operation $a * b = a/b$ is not a binary operation, since it is not defined for every ordered pair of elements of R. For example, $3 * 0 = 3/0$ is not defined.

8.2.1 Properties of Binary Operations

Commutative : A binary operation '*' on a set A is called commutative if $a * b = b * a, \forall\ a, b \in A$.

Example 2.

(i) The binary operation of addition on the set of integers Z is commutative as $a + b = b + a, \forall\ a, b \in Z$.

(ii) The binary operation of subtraction on Z is not commutative, since $3 - 2 \neq 2 - 3$.

Associative : A binary operation * on a set A is associative if $(a * b) * c = a * (b * c), \forall\ a, b, c \in A$.

Example 3.

(i) The binary operation of multiplication on Z is associative as $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall$ a, b, c $\in$ Z.

(ii) The binary operation of subtraction on Z is not associative,

since $(2 - 3) - 4 \neq 2 - (3 - 4)$.

8.3 Algebraic Structures

A structure consisting of a set and one or more binary operations on the set is called an algebraic structure. We shall denote an algebraic structure by $(A, f_1, f_2, ...)$, where A is a non–empty set and $f_1, f_2, ...$ are binary operations on A.

Example 4.

(i) Since + is a binary operation on the set of natural numbers N so (N, +) is an algebraic structure.

(ii) The operations + and · are binary operations on the set of real numbers R so (R, +, ·) is an algebraic structure.

8.4 Semigroup

Definition : An algebraic structure (S, *) is called a **semigroup** if the binary operation * is associative in S.

In other words, let S be a non–empty set and * be a binary operation defined on S. Then an algebraic structure (S, *) is said to be a **semigroup** if it satisfies the following properties

(i) Closure : S is closed w.r.t. the operation * i.e.,

$a \in S, b \in S \Rightarrow a * b \in S, \forall$ a, b, $\in$ S.

(ii) Associativity : The binary operation * is associative in S i.e.,

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

Example 5.

(i) (N, +) is a semigroup. Since $a \in N, b \in N \Rightarrow (a + b) \in N, \forall$ a, b $\in$ N

and $a + (b + c) = (a + b) + c, \forall$ a, b, c $\in$ N.

(ii) (Z, –) is not a semigroup. Since '–' is not associative in Z.

For eg. 2, 3, 4 $\in$ Z but $2 - (3 - 4) \neq (2 - 3) - 4$.

Remark 1.

Throughout the book we denote the composition multiplication by the symbol '·' i.e. dot.

Proof. Let $(S_1, *)$ and $(S_2, *)$ are two subsemigroups of a semigroup (S, *).

We have to show that $(S_1 \cap S_2, *)$ is a subsemigroup of (S, *).

To prove this, it is sufficient to show that $S_1 \cap S_2$ is a subset of S and $S_1 \cap S_2$ is closed w.r.t. the composition *.

Now, let $a \in S_1 \cap S_2 \Rightarrow a \in S_1$ and $a \in S_2$

$\Rightarrow a \in S$ ($\because S_1 \subseteq S$ and $S_2 \subseteq S$)

$\Rightarrow S_1 \cap S_2 \subseteq S$. .....(i)

Further, let $a \in S_1 \cap S_2$, $b \in S_1 \cap S_2$

$\Rightarrow a \in S_1, b \in S_1$ and $a \in S_2, b \in S_2$

$\Rightarrow (a * b) \in S_1$ and $(a * b) \in S_2$ ($\because S_1$ and S_2 are closed)

$\Rightarrow (a * b) \in S_1 \cap S_2$ .....(ii)

$\Rightarrow S_1 \cap S_2$ is closed w.r.t. operation *.

$\therefore$ From (i) and (ii) it is clear that $(S_1 \cap S_2, *)$ is a subsemigroup of $(S, *)$. **Hence proved.**

8.5 Monoid

Identity Element : An element 'e' in an algebraic structure $(S, *)$ is called an identity element if $e * a = a = a * e, \forall a \in S$.

Example 6.

(i) 0 is an identity element in $(Z, +)$ as $0 + a = a = a + 0, \forall a \in Z$.

(ii) 1 is an identity element in $(N, \cdot)$ as $1 \cdot a = a = a \cdot 1, \forall a \in N$.

Definition : An algebraic structure $(S, *)$ is said to be a **monoid** if it satisfies the following properties :

(i) Closure : S is closed w.r.t. the operation *, i.e.

$a \in S, b \in S \Rightarrow (a * b) \in S, \forall a, b \in S$.

(ii) Associativity : The binary operation * is associative in S i.e.,

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

(iii) Existence of identity element : There exists an element $e \in S$ such that

$a * e = a = e * a, \forall a \in S$.

The element 'e' is called identity of S and it is unique.

In other words, a semigroup $(S, *)$ with an identity element 'e' w.r.t. operation * is called a monoid.

Example 7.

(i) $(N, \cdot)$ is a monoid with identity element 1.

(ii) $(Z, +)$ is a monoid with identity element 0.

(iii) $(N, +)$ is not a monoid because for addition 0 is the identity element but $0 \notin N$.

ILLUSTRATIVE EXAMPLES

Example 8. Let $(S, *)$ be a semigroup. If $a * c = c * a$ and $b * c = c * b$, then prove that $(a * b) * c = c * (a * b), \forall a, b, c \in S$.

Solution : Given, $a * c = c * a$ .....(1)

and $b * c = c * b$ .....(2)

Now, LHS $= (a * b) * c$

$= a * (b * c)$[Since * is associative]

$= a * (c * b)$ [using (2)]

$= (a * c) * b$[by associativity]

$= (c * a) * b$ [using (1)]

$= c * (a * b)$[by associativity]

$=$ RHS.

Example 9. Let N be the set of natural numbers and $*$ be an operation on $S = N \times N$, defined by

(i) $(a, b) * (c, d) = (ac, bd)$

(ii) $(a, b) * (c, d) = (a + c, b + d)$.

Show that S is a semigroup.

Solution. Let $x = (a, b)$, $y = (c, d)$ and $z = (e, f)$, where a, b, c, d, e, f, are the elements of N.

(i) Given $(a, b) * (c, d) = (ac, bd)$ .....(1)

Closure property : Let $x, y \in S$ then

$x * y = (a, b) * (c, d)$

$= (ac, bd) \in S$ [Since $ac \in N$, $bd \in N \Rightarrow (ac, bd) \in N \times N = S$]

$\therefore$ S is closed.

Associativity : Let $x, y, z \in S$.

Now, $x * (y * z) = (a, b) * [(c, d) * (e, f)]$

$= (a, b) * (ce, df)$ [using (1)]

$= [a(ce), b(df)]$

$= [(ac)e, (bd)f]$(Since a, b, c, d, e, $f \in N$ and multiplication is associative in N)

$= (ac, bd) * (e, f)$

$= [(a, b) * (c, d)] * (e, f)$

$= (x * y) * z$

$\therefore$ $*$ is associative in S.

Hence, S is a semigroup w.r.t. operation $*$.

(ii) Given $(a, b) * (c, d) = (a + c, b + d)$ .....(2)

Closure : Let $x, y \in S$ then

$x * y = (a, b) * (c, d) = (a + c, b + d)$ [using (2)]

since $a, c \in N \Rightarrow (a + c) \in N$ and $b, d \in N \Rightarrow (b + d) \in N$

$\Rightarrow (a + c, b + d) \in N \times N = S$

$\Rightarrow x * y = (a + c, b + d) \in S$

$\therefore$ S is closed.

Associativity : Let $x, y, z \in S$

Now, $x * (y * z) = (a, b) * [(c, d) * (e, f)] = (a, b) * [c + e, d + f]$

$= [a + (c + e), b + (d + f)]$

$= [(a + c) + e, (b + d) + f]$ [since addition is associative in N]

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

$= [(a, b) * (c, d)] * (e, f)$

$= (x * y) * z$

$\therefore$ $*$ is associative in S.

Hence, S is a semigroup w.r.t. operation $*$.

Example 10. Show that the set N of natural numbers is a semigroup under the operation $x * y = \max \{x, y\}$. Is it a monoid ? **[Raj. 2000]**

Solution. Given $x * y = \max \{x, y\}$ .....(1),

$x, y \in N$

Closure : Let $x, y \in N$ then,

$x * y = \max \{x, y\} = x$ or $y \in N$

so N is closed w.r.t. operation $*$.

Associativity : Let $x, y, z \in N$ then,

$x * (y * z) = x * (\max \{y, z\}) = \max \{x, \max \{y, z\}\}$

$= \max \{x, y, z\}$

Also, $(x * y) * z = (\max \{x, y\}) * z = \max \{\max \{x, y\}, z\}$ .....(2)

$= \max \{x, y, z\}$

(2) and (3) $\Rightarrow x * (y * z) = (x * y) * z$ .....(3)

$\therefore$ $*$ is associative in N.

Hence, N is a semigroup w.r.t. operation $*$.

Further,

Existence of Identity Element

Since 1 is the least element in the set N so for all $x \in N$,

$1 * x = \max \{1, x\} = x$

and $x * 1 = \max \{x, 1\} = x$

Thus, 1 is the identity element in N.

Hence, N is a monoid w.r.t. operation $*$.

Example 11. Let S be any non-empty set with the operation $a * b = a$. Show that S is a semigroup but not a monoid.

Solution. Given $a * b = a$ (i.e., element appearing before the operation $*$)

Closure : Let $a, b \in S$ then $a * b = a \in S$ .....(1)

$\therefore$ S is closed.

Associativity : Let $a, b, c \in S$ then,

$a * (b * c) = a * (b)$ [using (1)] $= a$

and $(a * b) * c = (a) * c = a$.....(3)

(2) and (3) $\Rightarrow a * (b * c) = (a * b) * c$ .....(2)

$\therefore$ $*$ is associative in S.

Hence, S is a semigroup w.r.t. operation $*$.

Further suppose 'e' be the identity element in S. Then, by the property of identity element

$a * e = a = e * a, \forall a \in S$

Since $a * e = a$ but $e * a = e \neq a, \forall a \in S$ [using (1)]

So no such element 'e' exists in the set S which satisfies the property of identity element.

Hence, S is not a monoid.

Note : $a * b = a$ and $b * a = b \Rightarrow a * b \neq b * a$ so the operation $*$ is not commutative in S.

Example 12. An element $a \in S$, where (S, $*$) is a semigroup, is called a left cancellable element if for all x, $y \in S$, $a * x = a * y \Rightarrow x = y$. Show that if a and b are left cancellable then $a * b$ is also left cancellable.

Solution. Given that a and b are left cancellable

$\Rightarrow a * x = a * y \Rightarrow x = y$.....(1)

and $b * x = b * y \Rightarrow x = y$.....(2)

Now, $a, b \in S \Rightarrow (a * b) \in S$ [$\because$ S is closed]

We have to prove that $(a * b) * x = (a * b) * y \Rightarrow x = y$.

Let $(a * b) * x = (a * b) * y$

$\Rightarrow a * (b * x) = a * (b * y)$[Since $*$ is associative in S and $a, b, x, y \in S$]

$\Rightarrow b * x = b * y$ [Since a is left cancellable]

$\Rightarrow x = y$ [using (2)]

Hence $(a * b)$ is also left cancellable.

Example 13. Show that the set $S = \{1, 2, 3, 6, 12\}$ is a monoid for the operation defined by $a * b$ = G.C.D. (a, b), where G.C.D. is a greatest common divisor.

Solution. Here $S = \{1, 2, 3, 6, 12\}$ and $a * b$ = G.C.D. (a, b).

Closure : Since for each $a, b \in S$, $a * b$ = G.C.D. (a, b) $\in$ S, so S is closed.

For eg. $1 * 3$ = G.C.D. (1, 3) $= 1 \in S$; $2 * 3$ = G.C.D. (2, 3) $= 1 \in S$;

$3 * 12$ = G.C.D. (3, 12) $= 3 \in S$ and so on.

Associativity : Let a, b, c be any three elements of the set S.

Then, $a * (b * c) = a *$ [G.C.D. (b, c)] = G.C.D. [a, G.C.D.(b, c)]

$=$ G.C.D. [a, b, c] .....(1)

and $(a * b) * c$ = [G.C.D. (a, b)] $* c$ = G.C.D. [G.C.D. (a, b), c]

$=$ G.C.D. (a, b, c) .....(2)

(1) and (2) $\Rightarrow a * (b * c) = (a * b) * c, \forall a, b, c \in S$.

So $*$ is associative in S.

Identity Element : Since, $12 * a$ = G.C.D. (12, a) $= a, \forall a \in S$ .....(3)

and $a * 12$ = G.C.D. (a, 12) $= a, \forall a \in S$ .....(4)

$\therefore$ (3) and (4) $\Rightarrow 12 * a = a = a * 12, \forall a \in S$

Thus, 12 is the identity element of S.

Hence, S is a monoid for the operation *.

Example 14. Show that the set E of even integers is a monoid for the operation defined by $a * b = \frac{ab}{2}$.

Solution. Given $a * b = \frac{ab}{2}, \forall\ a, b \in E$ .....(1)

Closure : Let $a, b \in E \Rightarrow ab$ is a multiple of 4

$\Rightarrow \frac{ab}{2}$ is a multiple of 2

$\Rightarrow \frac{ab}{2} \in E$

$\Rightarrow (a * b) \in E$

$\therefore$ E is closed.

Associativity : Let $a, b, c \in E$.

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

$= \frac{(ab)c}{4} = \left(\frac{ab}{2}\right) * c$

$= (a * b) * c$

So * is associative in E.

Identity Element : Let e be the identity element in E then, $e * a = a, \forall\ a \in E$

$\Rightarrow \frac{ea}{2} = 2$ [using (1)]

$\Rightarrow e = 2 \in E$

$\therefore$ 2 is the identity element in E.

Hence (E, *) is a monoid.

Example 15. How many binary operations are possible on a set A having n elements ?

Solution. We know that binary operations are defined from $A \times A$ to A. Now, there are n^2 ordered pairs in $A \times A$ and each of them will be assigned to any of the n elements of A. Hence there are n^{n^2} binary operations possible on the set A.

Example 16. How many commutative binary operations are possible on a set A having n–elements ?

Solution. There are n^2 ordered pairs in $A \times A$ out of which n^2–n ordered pairs are of the type (x, y) where $x \neq y$ and n ordered pairs are of the type (x, x). Since the binary operation is commutative so the pairs (x, y) and (y, x) where $x \neq y$ will take the same element while the pair of the type (x, x) will take any of the n elements of A. Hence the total number of commutative binary operations on the set A is given by

$$n^{\frac{n^2-n}{2}} \cdot n^n = n^{\frac{n^2-n}{2}+n} = n^{\frac{n(n+1)}{2}}$$

Example 17. Let $(\{x, y\}, \cdot)$ be a semigroup where $x \cdot x = y$ then show that

(i) $x \cdot y = y \cdot x$ (ii) $y \cdot y = y$.

Solution. (i) Given $x \cdot x = y$.....(1)

Now, LHS = $x \cdot y$

$= x \cdot (x \cdot x)$ [using (1)]

$= (x \cdot x) \cdot x$ [by associativity]

$= y \cdot x$ [using (1)]

= RHS

(ii) To show that $y \cdot y = y$

Since the set {x, y} is closed under the operation. So, we have two options

$x \cdot y = x$ or $x \cdot y = y$

If $x \cdot y = x$ then

LHS = $y \cdot y$

$= y \cdot (x \cdot x)$ [from (1)]

$= (y \cdot x) \cdot x$ [by associativity]

$= (x \cdot y) \cdot x$ [from part (i)]

$= x \cdot x$ [$\because$ we let $x \cdot y = x$]

= y = RHS [from (1)]

If $x \cdot y = y$ then,

LHS = $y \cdot y$

$= (x \cdot x) \cdot y$ [from (1)]

$= x \cdot (x \cdot y)$ [by associativity]

$= x \cdot y$ [$\because$ we let $x \cdot y = y$]

$= y$ [$\because x \cdot y = y$]

= RHS **Proved.**

Example 18. Let (S, *) be a semigroup such that for every $a \neq b$ in S, $a * b \neq b * a$. Then show that

(i) For every $a \in A$, $a * a = a$

(ii) For every $a, b \in A$, $a * b * a = a$

(iii) For every $a, b, c \in A$, $a * b * c = a * c$

Solution. Given that $a * b \neq b * a$ if $a \neq b$ .....(1)

$\Rightarrow a * b = b * a$ if $a = b$ .....(2)

(i) Let $a, b, c \in S$ then

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

on taking b= a and c = a, we get

$a * (a * a) = (a * a) * a$.....(3)

Let $a * a = x$ then (3) gives

$a * x = x * a \Rightarrow x = a$ [using (2)]

$\Rightarrow a * a = a.$ [$\because x = a * a$]

(ii) We have to show that $a * b * a = a$.

Consider $(a * b * a) * a = a * b * (a * a)$ (by associativity)

$= a * b * a$ (from part (i) $a * a = a$)

$= (a * a) * b * a$ ($\because a = a * a$)

$= a * (a * b * a)$ (by associativity)

put $a * b * a = x$, we get –

$x * a = a * x \Rightarrow x = a$ [using (2)]

$\Rightarrow a * b * a = a.$ [$\because a * b * a = x$]

(iii) We have to show that $a * b * c = a * c$

Since we have, $a * b * a = a$ [from part (ii)]

Now consider,

$$a * b * c * a * c = a * b * (c * a * c) = a * b * c \quad \text{[using (4)]} \qquad \text{.....(4)}$$

Also,

$$a * b * c * a * c = [a * (b * c) * a] * c = a * c \quad \text{[using (4)]} \qquad \text{.....(5)}$$

$\therefore$ (5) and (6) $\Rightarrow a * b * c = a * c.$ .....(6)

Example 19. If $(S_1, *)$ and $(S_2, *')$ are commutative semigroups, then prove that $(S_1 \times S_2, *")$ is also a commutative semigroup, where *" is defined as

$$(s_1, s_2) *" (s'_1, s'_2) = (s_1 * s'_1, s_2 *' s'_2)$$

where $s_1, s'_1 \in S_1$ and $s_2, s'_2 \in S_2$.

Solution. Since $S_1 \times S_2 = \{(s_1, s_2) : s_1 \in S_1, s_2 \in S_2\}$.

Closure : Let $(s_1, s_2), (s'_1, s'_2) \in S_1 \times S_2$

then $(s_1, s_2) *" (s'_1, s'_2) = (s_1 * s'_1, s_2 *' s'_2) \in S_1 \times S_2$

(since $s_1 * s'_1 \in S_1$ and $s_2 *' s'_2 \in S_2$)

So *" is closed in $S_1 \times S_2$.

Associativity : Let $(s_1, s_2), (s'_1, s'_2), (s"_1, s"_2) \in S_1 \times S_2$

Now, $(s_1, s_2) *" [(s'_1, s'_2) *" (s"_1, s"_2)]$

$= (s_1, s_2) *" (s'_1 * s"_1, s'_2 *' s"_2)$

$= [s_1 * (s'_1 * s"_1), s_2 *' (s'_2 *' s"_2)]$

$= [(s_1 * s'_1) * s"_1, (s_2 *' s'_2) *' s"_2]$ (since associativity hold in S_1 and S_2)

$= (s_1 * s'_1, s_2 *' s'_2) *" (s"_1, s"_2)$

$= [(s_1, s_2) *" (s'_1, s'_2)] * " (s"_1, s"_2)$

So associativity holds in $S_1 \times S_2$.

Commutativity : Let $(s_1, s_2), (s'_1, s'_2) \in S_1 \times S_2$ where $s_1, s'_1 \in S_1$ and $s_2, s'_2 \in S_2$.

Since S_1 and S_2 are commutative (given) so

$s_1 * s'_1 = s'_1 * s_1$ .....(1)

and $s_2 *' s'_2 = s'_2 *' s_2$ .....(2)

Now, (s_1, s_2) *" $(s'_1, s'_2) = (s_1 * s'_1, s_2 *' s'_2)$

$= (s'_1 * s_1, s'_2 *' s_2)$[using (1) and (2)]

$= (s'_1, s'_2)$ *" (s_1, s_2)

So, commutativity holds in $S_1 \times S_2$.

Thus, $(S_1 \times S_2, *")$ is a commutative semigroup.

Example 20. Let $A = \{0, 1\}$ and consider the semigroup $(A^*, \cdot)$ where $\cdot$ is the catenation. Define a relation R on this semigroup by α R β iff α and β have the same length. Prove that R is a congruence relation.

Solution. To prove that R is a congruence relation, we have to show that (i) R is an equivalence relation on A^* and (ii) If α R β, γ R $\delta \Rightarrow \alpha \cdot \gamma$ R $\beta \cdot \delta$.

(i) Reflexive : Let $\alpha \in A^*$ then α has the same length as itself so α R α, $\forall\ \alpha \in A^*$.

$\therefore$ R is reflexive.

Symmetric : Let α R $\beta \Longrightarrow$ length of α = length of β

$\Rightarrow$ length of β = length of α

$\Rightarrow \beta$ R α

$\therefore$ R is symmetric.

Transitive : Let α R β and β R γ then

length of α = length of β

and length of β = length of γ

$\Rightarrow$ length of α = length of β = length of γ

$\Rightarrow$ length of α = length of γ

$\Rightarrow \alpha$ R γ

$\therefore$ R is transitive.

Hence, R is an equivalence relation on A^*.

(ii) Let α R β and γ R δ

$\Rightarrow$ length of α = length of β.....(1)

and length of γ = length of δ.....(2)

Now, length of $\alpha \cdot \gamma$ = length of α + length of γ

$=$ length of β + length of δ[using (1) and (2)]

$=$ length of $\beta \cdot \delta$

$\Rightarrow \alpha \cdot \gamma$ R $\beta \cdot \delta$

Thus, R is a congruence relation on $(A^*, \cdot)$.

Example 21. Let $(M, *)$ be a semigroup and $a \in M$ such that the equations $a * u = x$ and $v * a = x$ have solutions in M for all $x \in M$. Show that $(M, *)$ is a monoid.

Solution. Given that, $a * u = x$

and $v * a = x$; $\forall\ x \in M$

Since $a \in M$, so if we take $x = a$ the above equations are also satisfied for some $u = e_r$ and $v = e_l$ i.e.,

$a * e_r = a$ and $e_l * a = a$.

Again, let $y \in M$ then $y * e_r = (v * a) * e_r = v * (a * e_r) = v * a = y$

and $e_l * y = e_l * (a * u) = (e_l * a) * u = a * u = y$

$\therefore$ $y * e_r = y$ and $e_l * y = y$

Hence e_r and e_l are right and left identity in M respectively.

So $e_r = e_l = e$

$\Rightarrow$ Identity element 'e' belongs to M

Thus, (M, *) is a monoid.

EXERCISE 8.1

1. Which of the following operations are commutative in R ?

   (i) $x * y = x + y$ (ii) $x * y = x - y$

   (iii) $x * y = xy + 2$ (iv) $x * y = x(y + 1)$

   (v) $x * y = x^y$

   [Ans. (i) Yes (ii) No (iii) Yes (iv) No (v) No]

2. Show that the set $S = \{1, 2, 3, 6, 9, 18\}$ is a semigroup for the operation defined by $a * b$ = LCM (a, b). Is it a monoid ?

   [Ans. Yes, identity element = 1]

3. Is the operation defined by $a * b = \frac{a}{b}$ in the set Q of rational numbers, a binary operation ?

   [Ans. No, check for $b = 0$]

4. Show that the power set of set $S = \{1, 2, 3\}$ is a monoid for

   (i) the operation forming the union

   (ii) the operation forming the intersection. Find the identity element in each case.

   [Ans. (i) Empty set ϕ, (ii) set S]

5. Let (S, *) be a commutative semigroup. Show that if $x * x = x$ and $y * y = y$, then

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

6. Let (S, *) be a semigroup and $a \in S$. Consider a binary operation o on S such that $x \circ y = x * a * y$, $\forall$ $x, y \in S$. Show that o is an associative binary operation on S.

   [Hint : $(x \circ y) \circ z = (x * a * y) \circ z = (x * a * y) * a * z = x * a * (y * a * z)$

   $= x * a * (y \circ z) = x \circ (y \circ z)$]

7. Let (S, *) be a monoid with identity e. If $ax = e$ and $ya = e$ have solutions in S, $\forall$ $a \in S$, then show that $y = x$.

   [Hint : $y = ye = y(a\ x) = (y\ a)\ x = ex = x$]

8. If (S, *) is a monoid with identity $e = a^o$, $a \in S$ and $T = \{a^i \mid i \in Z^+ \text{ or } i = 0\}$, then show that (T, *) is a submonoid of (S, *).

9. If (S, *) and (T, *') are monoids with identities e_S and e_T respectively, then show that $(S \times T, *'')$ is also a monoid, where *" is defined as (s_1, t_1) *" $(s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$, $s_1, s_2 \in S$ and $t_1, t_2 \in T$.

[Hint : Identity element of $S \times T$ is (e_S, e_T)]

10. Show that the set of integers Z is a monoid for the operation $a * b = a + b - ab$. Find the identity element.

[Hint : If e is the identity in Z then $a * e = a \Rightarrow a + e - a e = a \Rightarrow e(1 - a) = 0 \Rightarrow e = 0$ or $a = 1$ since a can take any value so $e = 0$]

[**Ans.** Identity element = 0]

11. Show that the set $K = \{-3, -1, 1, 3, 5, ...\}$ is not a semigroup for the operation addition.

12. Let $A = \{0, 1\}$ and consider the free semigroup A^* generated by A under the operation of catenation. Let N be the semigroup of all non–negative integers under the operation of ordinary addition.

(a) Verify that the function $f : A^* \to N$, defined by $f(\alpha)$ = the number of digits in α, is a homomorphism.

(b) Let R be the following relation on A^*,

$\alpha \, R \, \beta$ iff $f(\alpha) = f(\beta)$.

Show that R is a congruence relation on A^*.

8.6 COMPOSITION TABLE

A binary composition in a finite set can be shown in a tabular form known as composition table.

Let $S = \{a_1, a_2, ..., a_n\}$ is a finite set and '*' is a composition in S. We write the elements of S in a horizontal row as well as in a vertical column. The element $a_i * a_j$ associated to the ordered pair (a_i, a_j) is placed at the intersection of the row headed by a_i and the column headed by a_j.

*	a_1	a_2	a_3	...	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	$a_1 * a_3$	...	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	$a_2 * a_3$	...	$a_2 * a_n$
a_3	$a_3 * a_1$	$a_3 * a_2$	$a_3 * a_3$	...	$a_3 * a_n$
⋮	⋮	⋮	⋮	⋮	⋮
a_n	$a_n * a_1$	$a_n * a_2$	$a_n * a_3$	...	$a_n * a_n$

Remark 2.

(a) If all the entries in the composition table are the elements of S, then we say that S is closed.

(b) If i^{th} row of the table, headed by a_i, coincides with the top row of the table then a_i is the identity in S.

(c) If the table is symmetric about the leading diagonal i.e., entries in the first row coincides with the entries in the first column, entries in the second row coincides with the entries in the second column and so on, then we say that composition is commutative in S.

Example 22. $(S, \cdot)$ where $S = \{1, -1, i, -i\}$, is a monoid.

Closure : Since all the entries in the table are elements of S.

$\therefore$ S is closed.

·	1	–1	i	–i	(Top Row)
1	1	–1	i	–i	(First Row)
–1	–1	1	–i	i	
i	i	–i	–1	1	
–i	–i	i	1	–1	

Associativity : Since the multiplication of complex numbers is always associative so associativity holds in S.

Identity element : Since the first row of the table coincides with the top row and is headed by 1 so 1 is the identity element in S.

$\therefore$ (S, ·) is a monoid. It can be verify that (S, ·) is also commutative.

8.7 addition and multiplication modulo

8.7.1 Addition Modulo 'm'

Let a and b are any integers and m is a fixed positive integer, then addition modulo 'm' of a and b is defined by

$$a +_m b = r,\ 0 \le r < m$$

where r is the least non–negative remainder when (a + b) is divided by m.

Example 23.

(i) $15 +_5 7$ = remainder when (15 + 7 = 22) is divided by 5

= 2

(ii) $-23 +_3 3$ = remainder when (– 23 + 3 = – 20 = – 21 + 1) is divided by 3

= 1

8.7.2 Multiplication Modulo 'p'

Let a and b are any integers and p is a fixed positive integer, then 'multiplication modulo p' of a and b is defined by

$$a \times_p b = r,\ 0 \le r < p$$

where r is the least non–negative remainder when a · b is divided by p.

Example 24. (i) $8 \times_5 3$ = remainder when (8 × 3 = 24) is divided by 5.

= 4

(ii) $8 \times_5 (-3)$ = remainder when (8 × – 3 = – 24 = – 25 + 1) is divided by 5

= 1.

EXERCISE 8.2

1. Which of the following binary operations on A = {a, b, c, d} are commutative ?

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

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

[Ans. (i) No (ii) Yes]

2. Show that the set S = {a, b} is not a semigroup for the operation * defined as

*	a	b
a	b	b
b	a	a

[Hint. Associativity does not holds.]

3. Prove that the set A = {a, b} is a monoid for the operation * defined as

*	a	b
a	b	a
b	a	b

Find the identity element.

[Ans. b]

4. Let * be the operation on Z_8 defined by $a * b = a + b - a \cdot b$, where + and · are usual addition (mod 8) and multiplication (mod 8) respectively.

(i) Find 3 * 4 and 2 * – 5

(ii) Is $(Z_8, *)$ a semigroup ?

(iii) Is $(Z_8, *)$ a monoid ?

(iv) Is $(Z_8 *)$ commutative ?

[Ans. (i) 3, 7 (ii) Yes (iii) Yes, identity element = 0 (iv) Yes]

6. Which of the following tables defines a semigroup ?

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

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

[Ans. (i) No (ii) No, associativity does not hold]

8.8 Group

Definition : An algebraic structure (G, *) is called a group, if the binary operation * satisfies the following conditions :

(i) Closure property : If $a \in G, b \in G$ then $(a * b) \in G$

(ii) Associativity : If $(a * b) * c = a * (b * c)$, $\forall$ a, b, c, $\in G$

(iii) Existence of Identity : There exists a unique element $e \in G$ such that $a * e = a = e * a$, $\forall\ a \in G$. The element e is called the identity element.

(iv) Existence of Inverse : For every $a \in G\ \exists\ b \in G$ such that, $a * b = e = b * a$.

The element b is called the inverse of a and can be denoted by a^{-1}.

In other words, a monoid (S, *) is said to be a group if each element of S has its inverse in S.

Example 25. The set of integers Z is a group for the composition addition.

Example 26. The set of non–zero rational numbers Q is a group for the composition multiplication.

Example 27. The set Z^+ of positive integers is a monoid but not a group for composition multiplication because $2 \in Z^+$ but its inverse, i.e., $\frac{1}{2} \notin Z^+$

8.9 Abelian or Commutative Group

A group (G, *) is said to be abelian or commutative if $a * b = b * a$, $\forall$ a, b $\in$ G.

Example 28. (Z, +) is an abelian group.

Example 29. Let G be the set of all non–zero real numbers and let $a * b = \frac{ab}{2}$. Then show that (G, *) is an abelian group. **[Raj. 2003]**

Solution : Given $a * b = \frac{ab}{2}$, $\forall$ a, b $\in$ G

Closure : Let a, b $\in$ G

$\Rightarrow$ a and b are non–zero real numbers

$\Rightarrow$ ab is also a non–zero real number

$\Rightarrow \frac{ab}{2}$ is also a non–zero real number

$\Rightarrow \frac{ab}{2} \in G \Rightarrow (a * b) \in G$

$\therefore$ G is closed

Associativity : Let a, b, c $\in$ G then

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

Also, $(a * b) * c = \left(\frac{ab}{2}\right) * c = \left(\frac{ab}{2}\right)\frac{c}{2} = \frac{abc}{4}$ .....(1)

$\therefore$ (1) and (2) $\Rightarrow a * (b * c) = (a * b) * c$, $\forall$ a, b, c $\in$ G. .....(2)

So associativity holds in G.

Existence of Identity : Let e be the identity element in G then

$a * e = a$, $\forall$ a $\in$ G

$\Rightarrow \frac{ae}{2} = a$

$\Rightarrow e = 2 \in G$

$\therefore$ 2 is the identity element in G.

Existence of Inverse : Let b be the inverse of a $\in$ G then $a * b = 2$ (identity in G)

$\Rightarrow \frac{ab}{2} = 2 \Rightarrow b = \frac{4}{a} \in G$ ($\because a \neq 0$)

Since a is an arbitrary element so each element of G has its inverse in G.

Abelian : Let a, b $\in$ G then

$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$

$\Rightarrow a * b = b * a, \forall a, b \in G$

Therefore, $(G, *)$ is an abelian group.

8.10 Finite and Infinite Groups

A group G is said to be finite if it consists of a finite number of distinct elements, otherwise it is called an infinite group. The number of elements in a finite group is called the order of the group and is denoted by o(G). The infinite group is said to be of infinite order.

Example 30. $G = \{1, \omega, \omega^2\}$ is a finite group for composition multiplication and $o(G) = 3$.

Example 31. $(Z, +)$, $(R_0, \times)$ are infinite groups.

8.11 Elementary Theorems Based on Groups

Theorem 1. Let G be a group. Each element a in G has only one inverse in G. **[Raj. 2005]**

Proof. Let a be any element of a group G and let e be the identity element in G. If possible let b and c are two inverses of a, i.e.,

$ba = e = ab$ and $ca = e = ac$

Now, $b(ac) = be = b$ .....(1)

and $(ba)\, c = ec = c$ .....(2)

Since in a group, composition is associative so,

$b(ac) = (ba)c$

$\therefore$ (1) and (2) $\Rightarrow b = c$

Hence, inverse of each element of G is unique. **Hence proved.**

Theorem 2. Show that the left identity element and the right identity element in a group are same.

Proof. Let e_l be the left and e_r be the right identity element in a group G. Then,

$e_l e_r = e_r$ ($\because$ e_l is left identity) .....(1)

and $e_l e_r = e_l$ ($\because$ e_r is right identity) .....(2)

$\therefore$ (1) and (2) $\Rightarrow e_l = e_r$

Hence, the identity element in a group is unique. **Hence proved.**

Theorem 3. Let G be a group and let a, b and c be elements of G. Then

(1) $ab = ac \Rightarrow b = c$ (left cancellation law)

(2) $ba = ca \Rightarrow b = c$ (right cancellation law).

Proof. Let e be the identity element in G.

(1) Let $ab = ac$

multiplying both sides by a^{-1} from the left, we get –

$a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c$ (by associativity)

$\Rightarrow eb = ec$ (by definition of inverse)

$\Rightarrow b = c$

$\therefore$ Left cancellation law holds in G.

(2) Let $ba = ca$

multiplying both sides by a^{-1} from the right, we get –

$(ba)a^{-1} = (ca)a^{-1} \Rightarrow b(aa^{-1}) = c(aa^{-1})$ (by associativity)

$\Rightarrow be = ce \Rightarrow b = c$

$\therefore$ Right cancellation law holds in G. **Hence proved.**

Theorem 3. Let G be a group and a, b $\in$ G then,

(i) $(a^{-1})^{-1} = a$ (ii) $(ab)^{-1} = b^{-1}a^{-1}$

Proof. Let e be the identity element in G.

(i) Let a $\in$ G then there exists $a^{-1} \in$ G such that,

$a^{-1}a = e$

multiplying both sides by $(a^{-1})^{-1}$ from the left, we get

$(a^{-1})^{-1}[a^{-1}a] = (a^{-1})^{-1}e \Rightarrow [(a^{-1})^{-1}a^{-1}]\, a = (a^{-1})^{-1}$ (by associativity)

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

(ii) Let a, b $\in$ G then $\exists$ a^{-1}, $b^{-1} \in$ G such that

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

and $b^{-1}b = e = bb^{-1}$

Now, $(ab)(b^{-1}a^{-1}) = [(ab)b^{-1}]\, a^{-1} = [a(bb^{-1})]a^{-1} = (ae)a^{-1} = aa^{-1}$

$= e$ .....(1)

Also $(b^{-1}a^{-1})(ab) = b^{-1}[a^{-1}(ab)] = b^{-1}[(a^{-1}a)b]$

$= b^{-1}(eb) = b^{-1}b$

$= e$ .....(2)

$\therefore$ (1) and (2) $\Rightarrow (ab)(b^{-1}a^{-1}) = e = (b^{-1}a^{-1})(ab)$

If we let X = ab and $Y = b^{-1}a^{-1}$ then,

$XY = e = YX$

$\Rightarrow$ Y is the inverse of X (by definition of inverse)

$\Rightarrow X^{-1} = Y$

or, $(ab)^{-1} = b^{-1}a^{-1}$.

Hence the theorem.

Remark 3. If G is commutative, then $(ab)^{-1} = a^{-1}b^{-1}$.

Theorem 4. Let G be a group and a, b $\in$ G, then

(i) The equation ax = b has a unique solution in G.

(ii) The equation ya = b has a unique solution in G.

Proof. Let e be the identity element in G.

(i) Let $a \in G \Rightarrow \exists\ a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$

$\therefore\ a \in G, b \in G \Rightarrow a^{-1} \in G, b \in G \Rightarrow a^{-1}b \in G$ (by closure property)

Now substituting $a^{-1}b$ for x in the left hand side of the equation $ax = b$, we have

$a(a^{-1}b) = (aa^{-1})b = eb = b = RHS$

Thus $x = a^{-1}b$ is a solution of the equation $ax = b$ in G.

Now, we shall prove that solution is unique. Let us suppose that $x = x_1$ and $x = x_2$ are two solutions of the equation $ax = b$. Then

$ax_1 = b$

and $ax_2 = b$

$\Rightarrow\ ax_1 = ax_2 \Rightarrow x_1 = x_2$(by left cancellation law)

Thus, the solution is unique.

(ii) Since $a \in G \Rightarrow \exists\ a^{-1} \in G$ such that $aa^{-1} = e = a^{-1}a$

$\therefore\ b \in G, a^{-1} \in G \Rightarrow ba^{-1} \in G$ (by closure property)

Now substituting ba^{-1} for y in the left hand side of the equation $ya = b$, we have

$(ba^{-1})\ a = b(a^{-1}a) = be = b = RHS$

Thus, $y = ba^{-1}$ is a solution of the equation $ya = b$ in G.

Now, we shall show that the solution is unique. Let us assume that $y = y_1$ and $y = y_2$ are two solutions of the equation $ya = b$. Then

$y_1a = b$

and $y_2a = b$

$\Rightarrow\ y_1a = y_2a \Rightarrow y_1 = y_2$(by right cancellation law)

Thus, the solution is unique. **Hence proved.**

8.12 Composition Table for Groups

The composition table for a finite group can be constructed in a similar way as it was constructed for algebraic structures like semigroups and monoids in the previous chapter.

Remark 4. The composition table for a finite group contains each element of the group exactly once in each of its rows and columns.

Remark 5. Every row or column in the composition table of a group (G, *) is a permutation of the elements of G.

Example 32. Prove that the set of four bijective transformations f_1, f_2, f_3 and f_4 defined by $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$ and $f_4(x) = -\frac{1}{x}$ on the set of non–zero real numbers, form a group under the operation composition of functions.

Solution. The composition table for the given problem can be constructed as follows. Let $G = \{f_1, f_2, f_3, f_4\}$ and 'o' be the operation of composition of functions.

Now, $f_1 \circ f_2(x) = f_1[f_2(x)] = f_1[-x] = -x = f_2(x)$

$\Rightarrow f_1 \circ f_2 = f_2$

$$f_2 \circ f_3(x) = f_2[f_3(x)] = f_2\left[\frac{1}{x}\right] = -\frac{1}{x} = f_4(x)$$

$\Rightarrow f_2 \circ f_3 = f_4$ and so on.

$\therefore$ The table is as follows

$\circ$	f_1	f_2	f_3	f_4
$\boxed{f_1}$	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

(Top Row)

(First Row)

Closure : Since all the elements in the table are the elements of G, so G is closed.

Associativity : Since composition of functions is always associative, so associativity holds in G.

Identity element : As the first row of the table coincides with the top row and is headed by f_1, so f_1 is the identity element in G.

Existence of Inverse : From the table it is clear that

$f_1 \circ f_1 = f_1 \Rightarrow f_1^{-1} = f_1$; $f_2 \circ f_2 = f_1 \Rightarrow f_2^{-1} = f_2$

$f_3 \circ f_3 = f_1 \Rightarrow f_3^{-1} = f_3$; $f_4 \circ f_4 = f_1 \Rightarrow f_4^{-1} = f_4$

So, each element of G has its inverse in G.

Thus (G, o) is a group.

Further, the table is symmetrical about the leading diagonal, so (G, o) is an abelian group.

Example 33. Show that the Klien group $K_4 = \{e, a, b, c\}$ is a group for the operation defined by the following table

$\bullet$	e	a	b	c
$\boxed{e}$	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Solution. Given $K_4 = \{e, a, b, c\}$

Closure : Since all the elements in the table are the elements of K_4, so K_4 is closed.

Associativity : It can be easily verified that the operation is associative.

Identity element : Since first row of the table, headed by e, coincides with the top row so e is the identity element in K_4.

Existence of Inverse : From the table,

$e \cdot e = e \Rightarrow e^{-1} = e$; $a \cdot a = e \Rightarrow a^{-1} = a$

$b \cdot b = e \Rightarrow b^{-1} = b$; $c \cdot c = e \Rightarrow c^{-1} = c$

So, each element of K_4 has its inverse in K_4. Therefore. K_4 is a group for the operation given. Also, the table is symmetrical about the leading diagonal. Thus, the group K_4 is abelian.

Example 34. Prove that the set $G = \{0, 1, 2, ..., m - 1\}$ of m non–negative integers is a finite abelian group under the operation of addition modulo m.

Solution. Here operation is addition modulo m, i.e.,

$a +_m b = r, 0 \leq r \leq m - 1$

Closure : Let $a, b \in G$ then

$a +_m b = r \in G \quad (\because 0 \leq r \leq m - 1)$

$\therefore$ G is closed.

Associativity : Let $a, b, c \in G$ then

$(a +_m b) +_m c = (a + b) +_m c \quad [\because a +_m b = (a + b) \pmod m]$

= least non–negative remainder when $(a + b) + c$ is divided by m

= least non–negative remainder when $a + (b + c)$ is divided by m

$= a +_m (b + c)$

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

$\therefore$ Associativity holds in G.

Identity element : For an element $0 \in G$, we have

$0 +_m a = a = a +_m 0, \forall\ a \in G$

$\therefore$ 0 is the identity element in G.

Existence of Inverse : If $a \in G$ and $r \neq 0$ then $(m - a)$ is also an element of G. Now,

$a +_m (m - a)$ = least non–negative remainder when $a + (m - a)$ $(= m)$ is divided by m

$\Rightarrow a +_m (m - a) = 0 = (m - a) +_m a$

So, $(m - a)$ is the inverse of a.

Thus, each element of G has its inverse in G.

Therefore, G is a group for the composition addition modulo m.

Further, let $a, b \in G$ then,

$a +_m b = r$

= least non–negative remainder when $(a + b)$ is divided by m.

= least non–negative remainder when $(b + a)$ is divided by m.

$= b +_m a$

Hence, $(G, +_m)$ is an abelian group. **Hence proved.**

Example 35. Prove that $(Z_5, +_5)$ where $Z_5 = \{0, 1, 2, 3, 4\}$ and $+_5$ denotes addition modulo 5 is an abelian group.

Solution. The composition table for $(Z_5, +_5)$ is 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

Closure : All the entries in the table are the elements of Z_5, so Z_5 is closed.

Associativity : It can be easily verified from the table that the operation $+_5$ is associative in Z_5.

Identity element : Since first row of the table, headed by 0, coincides with the top row so 0 is the identity element in Z_5.

Existence of Inverse : From the table,

$0 +_5 0 = 0 \Rightarrow (0)^{-1} = 0$; $1 +_5 4 = 0 \Rightarrow (1)^{-1} = 4$

$2 +_5 3 = 0 \Rightarrow (2)^{-1} = 3$; $3 +_5 2 = 0 \Rightarrow (3)^{-1} = 2$ and

$4 +_5 1 = 0 \Rightarrow (4)^{-1} = 1$

So, each element of Z_5 has its inverse in Z_5.

Thus, $(Z_5, +)$ is a group.

Further, the table is symmetrical about the leading diagonal. Therefore, $(Z_5, +)$ is an abelian group of order 5.

8.13 Order of an Element

The order of an element $a \in G$ is defined as the least positive integer n, if one exists, such that

$a^n = e$ (identity of G)

Symbolically, we write $o(a) = n$.

If there exists no positive integer n such that $a^n = e$, then a is said to be of infinite order or of zero order.

Example 36. Find the order of each element in the group $(G, \cdot)$ where $G = \{1, -1, i, -i\}$.

Solution. Here identity element $e = 1$

Now, $(1)^1 = 1 \Rightarrow o(1) = 1$ [Compare with $a^n = e$]

$(-1)^2 = 1 \Rightarrow o(-1) = 2$

$(i)^4 = 1 \Rightarrow o(i) = 4$

$(-i)^4 = 1 \Rightarrow o(-i) = 4$.

8.14 Subgroup

Definition : A non–empty subset H of a group G is said to be a subgroup of G if the composition in G is also a composition in H and for this composition H itself is a group.

Since, every set is a subset of itself so 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 one element i.e., e, is also a subgroup of G. These two i.e., G and {e} are subgroups of any group G and they are called trivial or improper subgroups of G. A subgroup other than these two is called a proper subgroup.

Remark 6. The identity of a subgroup is the same as that of the group.

Remark 6(a). The inverse of any element of a subgroup is the same as it's inverse when it is treated as an element of the group.

Remark 6(b). The order of any element of a subgroup is the same as the order of the element regarded as a member of the group.

Example 37. The multiplicative group $\{1, -1\}$ is a subgroup of the multiplicative group $\{1, -1, i, -i\}$.

Example 38. The additive group of even integers is a subgroup of the additive group of all integers.

Theorem 6. A necessary and sufficient condition for a non–empty subset H of a group G to be a subgroup is that

$a \in H, b \in H \Rightarrow ab^{-1} \in H$, where b^{-1} is the inverse of b in G.

Proof. The condition is necessary

Let H be a subgroup of G and $a, b \in H$. We have to show that $ab^{-1} \in H$.

Since $b \in H \Rightarrow b^{-1} \in H$ ($\because$ H is a subgroup)

Now, $a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$ ($\because$ H is closed)

So, the condition is necessary.

The condition is sufficient

Given that, $a \in H, b \in H \Rightarrow ab^{-1} \in H$

We have to prove that H is a subgroup of G.

Identity element : $a \in H, a \in H \Rightarrow aa^{-1} \in H$

$\Rightarrow e \in H$ ($\because aa^{-1} = e$, identity of G)

$\therefore$ Identity element exists in H.

Existence of Inverse : Since $e \in H, a \in H \Rightarrow ea^{-1} = a^{-1} \in H, \forall a \in H$

So, each element of H has its inverse in H.

Closure property : Let, $a, b \in H \Rightarrow a \in H, b^{-1} \in H$

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

So, H is closed.

Associativity : The elements of H are also the elements of G. Since the composition in G is associative therefore, it must be associative in H.

Hence, H itself is a group. So, H is a subgroup of G. **Hence proved.**

Remark 7. If we denote the composition in G additively, the statement of the above theorem would have been, $a \in H, b \in H \Rightarrow a - b \in H$.

Remark 8. From Theorem 6 it is clear that if we want to prove that any set H is a subgroup of a group G then we have to show three conditions

(i) H is non–empty

(ii) H is a subset of G

(iii) $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Example 39. If H and K are two subgroups of a group G then $H \cap K$ is also a subgroup of G.

Solution. Given that H and K are subgroups of G. If e is the identity element in G then $e \in H$ and $e \in K \Rightarrow e \in H \cap K$.

So, $H \cap K$ is non–empty.

Again, let $a \in H \cap K \Rightarrow a \in H$ and $a \in K$

$\Rightarrow a \in G$ ($\because H \subseteq G$ and $K \subseteq G$)

So, $H \cap K \subseteq G$

Finally, let $a, b \in H \cap K \Rightarrow a, b \in H$ and $a, b \in K$

$\Rightarrow ab^{-1} \in H$ and $ab^{-1} \in K$($\because$ H and K are subgroups)

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

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

8.15 Group Homomorphism and Isomorphism

8.15.1 Group Homomorphism

Definition : Let (G, *) and (G', *') be two groups and let $f : G \to G'$ be a mapping, then f is called a group homomorphism if for all $a, b \in G$,

$f(a * b) = f(a) *' f(b)$.

Theorem 11. Let (G, *) and (G', *') be two groups and let $f : G \to G'$ be a homomorphism, then

(a) If e and e' be the identities in G and G' respectively, then $f(e) = e'$. **[Raj. 2001, MREC 2001]**

(b) If $a \in G$, then $f(a^{-1}) = [f(a)]^{-1}$ **[Raj. 2001, MREC 2001]**

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

(d) If $a \in G$, then $f(a^n) = [f(a)]^n$, $n \in Z$.

Proof. (a) Let $a \in G \Rightarrow f(a) \in G'$

Now, $e' *' f(a) = f(a)$ [$\because$ e' is identity in G']

$= f(e * a)$ [$\because$ e is identity in G]

$\Rightarrow e' *' f(a) = f(e) *' f(a)$[$\because$ f is a homomorphism]

or, $e' = f(e)$(by right cancellation law)

(b) Let $a \in G \Rightarrow a^{-1} \in G$

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

Since, $f(a) \in G'$ and G' is a group so $[f(a)]^{-1} \in G'$.

Now, multiplying both sides of (1) by $[f(a)]^{-1}$ from the left, we get

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

or, $[f(a)]^{-1} = ([f(a)]^{-1} *' f(a)) *' f(a^{-1})$

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

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

(c) Here $f(H) = \{f(h) | h \in H\}$

Given that H is a subgroup of G

$\Rightarrow e \in H \Rightarrow f(e) = e' \in f(H)$

so, f(H) is non–empty.

Again, let $a \in f(H) \Rightarrow \exists\ h \in H$ such that $a = f(h)$.

Now, $h \in H \Rightarrow h \in G \qquad (\because H \subseteq G)$

$\Rightarrow f(h) \in G' \Rightarrow a \in G' (\because a = f(h))$

$\therefore\ a \in f(H) \Rightarrow a \in G'$

so, f(H) is a subset of G'.

Finally, let $a, b \in f(H) \Rightarrow \exists\ h_1, h_2 \in H$ such that $f(h_1) = a$ and $f(h_2) = b$.

Now, $a *' b^{-1} = f(h)_1 *' [f(h_2)]^{-1} = f(h_1) *' f(h_2^{-1})$ [From part (b)]

$= f(h_1 * h_2^{-1}) \qquad [\because f \text{ is a homomorphism}]$

$= f(h) \in f(H) \qquad [\because h = h_1 * h_2^{-1} \in H]$

So, f(H) is a subgroup of G'.

(d) Let $a \in G$ then $a^n = a * a^{n-1}$

Now, $f(a^n) = f(a * a^{n-1})$

$= f(a) *' f(a^{n-1})$

$= f(a) *' f(a * a^{n-2}) = f(a) *' [f(a) *' f(a^{n-2})]$

$= [f(a)]^2 *' f(a^{n-2})$

by continuing this way, we get

$f(a^n) = [f(a)]^n$. **Hence the theorem.**

Example 40. Show that the mapping $f : (Z, +) \to (Z, +)$ defined by $f(n) = n + 1$, $n \in Z$, is not a homomorphism.

Solution : Let $x, y \in Z$ then,

$f(x + y) = x + y + 1$.....(1)

also, $f(x) + f(y) = (x + 1) + (y + 1) = x + y + 2$ .....(2)

(1) and (2) $\Rightarrow f(x + y) \neq f(x) + f(y)$

Hence, f is not a homomorphism.

Example 41. Show that the mapping $f : (Z, +) \to (Q_0, \cdot)$ defined by $f(x) = e^x$ is a homomorphism.

Solution : Let $x, y \in Z$ then,

$f(x + y) = e^{x+y} = e^x \cdot e^y$

$= f(x) \cdot f(y)$

Hence, f is a homomorphism.

Example 42. Show that the mapping $f : G \to G$ defined by $f(x) = e$, $\forall\ x \in G$, where e is the identity

element in G, is a homomorphism.

Solution : Let x, y ∈ G then

$f(xy) = e$ $(\because x, y \in G \Rightarrow xy \in G)$

$= e \cdot e$

or, $f(x\ y) = f(x)\ f(y)[\because x, y \in G \Rightarrow f(x) = e, f(y) = e]$

$\therefore$ f is a homomorphism.

8.15.2 Kernel of Homomorphism

Definition : If f is a homomorphism of a group G into a group G' then the set k of all those elements of G which are mapped onto the identity e' of G', is called the kernel of the homomorphism f.

Symbolically, $k = \{x \in G : f(x) = e'; e' \text{ is the identity in } G'\}$.

Example 43. Let $f : G \to H$ be a homomorphism from a group G to a group H. Prove that kernel f is a subgroup of G and image f is a subgroup of H.

Solution. Let e and e' be identities in G and H respectively. Then,

Ker $f = k = \{x \in G \mid f(x) = e'\}$ and,

Image $f = f(G) = \{f(x) : x \in G\}$

(i) To prove : k is a subgroup of G.

Since $f(e) = e' \Rightarrow e \in k \Rightarrow k$ is non empty.

Also, $x \in k \Rightarrow x \in G$ (by definition)

$\Rightarrow$ k is a subset of G.

Finally, let $a, b \in k \Rightarrow f(a) = e'$ and $f(b) = e'$

Now, $f(ab^{-1}) = f(a)\ f(b^{-1})$ [$\because$ f is homomorphism]

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

$= e'(e')^{-1} = e' \cdot e'$

or, $f(ab^{-1}) = e'$

$\Rightarrow ab^{-1} \in k$[by definition of k]

$\therefore$ $a, b \in k \Rightarrow ab^{-1} \in k$

Hence, k is a subgroup of G.

(ii) To prove : f(G) is a subgroup of H.

$f(G) = \{f(x) : x \in G\}$

Since, $e \in G \Rightarrow f(e) = e' \in f(G)$

So, f(G) is non–empty.

Also, let $f(x) \in f(G) \Rightarrow x \in G$

$\Rightarrow f(x) \in H$

so, f(G) is a subset of H.

Finally, let $h_1, h_2 \in f(G) \Rightarrow \exists\ x_1, x_2 \in G$ such that

$f(x_1) = h_1$ and $f(x_2) = h_2$

Now, $h_1h_2^{-1} = f(x_1)[f(x_2]^{-1} = f(x_1)\ f(x_2^{-1}) = f(x_1\ x_2^{-1})$

$= f(x) \in f(G)$ $[\because x = x_1x_2^{-1} \in G]$

$\therefore\ h_1, h_2 \in f(G) \Rightarrow h_1h_2^{-1} \in f(G)$.

Hence, f(G) is a subgroup of H.

Example 44. Show that the mapping $f : (R_0, \cdot) \to (R_0, \cdot)$ defined by $f(x) = x^2$, is a homomorphism. Find the kernel of f.

Solution : Let $x, y \in R_0$ then,

$f(x \cdot y) = (x \cdot y)^2 = x^2 \cdot y^2 = f(x) \cdot f(y)$

so, f is a homomorphism.

Since, the identity element in R_0 is 1 so the kernel of f consisting those elements whose image is 1.

Let $x \in$ kernel of f

$\Rightarrow\ f(x) = 1$

$\Rightarrow\ x^2 = 1 \Rightarrow\ x = \pm 1$

$\therefore$ ker. $f = \{-1, 1\}$.

Example. 45 If f be a homomorphism from G to G' with kernel k, show for $a, b \in G$,

$f(a) = f(b) \Rightarrow a^{-1}b \in k$.

Solution : To prove that $a^{-1}b \in k$, it is sufficient to show that $f(a^{-1}b) = e'$, where e' is the identity in G'. Also let e be the identity in G.

Given $f(a) = f(b)$

Now, $f(a^{-1}b) = f(a^{-1})\ f(b)$ $[\because$ f is a homomorphism$]$

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

$= f(a^{-1}a) = f(e)$ $[\because a^{-1}a = e]$

$= e'$ $[\because f(e) = e']$

$\Rightarrow a^{-1}b \in k$.

8.15.3 Group Isomorphism

Definition : Let $f : (G, *) \to (G', *')$ be a one–one mapping from a group G onto a group G' such that $f(a * b) = f(a) *' f(b), \forall\ a, b, \in G$

then f is called a group isomorphism from G to G' or we say that G is isomorphic to G'.
Symbolically, we write $G \cong G'$.

Working procedure to prove that G is isomorphic to G'

(i) Define a mapping $f : G \to G'$

(ii) Show that f is one–one

(iii) Show that f is onto

(iv) Show that f is a homomorphism i.e., $f(a * b) = f(a) *' f(b), \forall\ a, b \in G$.

Example 46. Let G be a group. Show that the function $f : G \to G$ defined by $f(a) = a^{-1}$ is an isomorphism if and only if G is abelian.

Solution : Let $f : G \to G$ is an isomorphism then we shall show that G is abelian.

Now, $f(ab) = f(a)\ f(b)$

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

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

multiplying both sides by b from the left as well as from the right, we get

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

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

Now, multiplying both sides by a from the left as well as from the right, we get

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

$\Rightarrow (aa^{-1})\ ba = ab\ (a^{-1}a) \Rightarrow e\ (ba) = (ab)e$

$\Rightarrow ba = ab \Rightarrow$ G is abelian.

Conversely, let G is abelian then we shall show that f is an isomorphism.

One–one : Let $f(a) = f(b)$, $a, b \in G$

$\Rightarrow a^{-1} = b^{-1} \Rightarrow aa^{-1} = ab^{-1} \Rightarrow e = ab^{-1}$

$\Rightarrow eb = (ab^{-1})\ b \Rightarrow b = a(b^{-1}b) \Rightarrow b = ae$

$\Rightarrow b = a$

$\therefore$ f is one–one.

Onto : Let $b \in G$ (codomain) then $\exists\ b^{-1} \in G$ (domain) such that, $f(b^{-1}) = (b^{-1})^{-1} = b$

So, each element of codomain has its preimage in domain.

$\therefore$ f is onto.

Homomorphism : Let $x, y \in G$ then,

$f(xy) = (xy)^{-1} = (yx)^{-1}$ [$\because$ G is abelian]

$= x^{-1}y^{-1}$

$= f(x)\ f(y)$

$\therefore$ f is a homomorphism.

Hence, f is an isomorphism from G to G.

Example 47. Show that the group $G = (Z, +)$ is isomorphic to the group $G' = (nZ, +)$, where n is a given integer.

Solution : Let us define a mapping $f : G \to G'$ such that $f(a) = na, \forall\ a \in Z$

One–one : Let $f(a) = f(b)$

$\Rightarrow na = nb \Rightarrow a = b$

$\therefore$ f is one–one.

Onto : Let $b \in G'$ then there exists $m \in Z$ such that $b = nm$.

Now, $f(m) = nm = b$, $m \in Z$

$\Rightarrow$ each element of G' has its preimage in G.

$\therefore$ f is onto.

Homomorphism :Let a, b ∈ G then,

$f(a + b) = n(a + b) = na + nb$

$= f(a) + f(b)$

$\therefore$ f is a homomorphism.

Hence, f is an isomorphism from G onto G' or $G \equiv G'$.

8.16 Permutation Group

As defined earlier in chapter 2, a permutation of degree n is a one–one mapping of a set S onto itself (i.e. bijection), where S is a finite set having n distinct elements. The number of elements in the finite set S is known as the degree of permutation.

If S is a finite set having n distinct elements then we have n! distinct arrangements of these elements of S. Hence, there will be n! distinct permutations of degree n.

If P_n (also denoted by S_n) is the set consisting of all permutations of degree n, then the set P_n is called the symmetric set of permutations of degree n.

For Example, if S = {1, 2, 3} then

$$P_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$$

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

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

Theorem 8 : Prove that the set P_3 of all permutations on three symbols 1, 2, 3 i.e., S = {1, 2, 3} is a finite non–abelian group of order 6 with respect to permutation multiplication as composition.

Proof : Let $P_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$

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

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

Now, composition table of P_3 is as follows

o	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_3	p_1	p_6	p_4	p_5
p_3	p_3	p_1	p_2	p_5	p_6	p_4
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_6	p_4	p_3	p_1	p_2
p_6	p_6	p_4	p_5	p_2	p_3	p_1

Closure : All the entries in the table are the elements of P_3. So, P_3 is closed.

Associativity : Since the composition of functions is always associative so, associativity holds in P_3.

Identity element : The first row of the table, headed by p_1, coincides with the top row. So, p_1 is the identity element in P_3.

Existence of Inverse : From the table, it is clear that

$p_1 \circ p_1 = p_1 \Rightarrow p_1^{-1} = p_1$; $p_2 \circ p_3 = p_1 \Rightarrow p_2^{-1} = p_3$

$p_3 \circ p_2 = p_1 \Rightarrow p_3^{-1} = p_2$; $p_4 \circ p_4 = p_1 \Rightarrow p_4^{-1} = p_4$

$p_5 \circ p_5 = p_1 \Rightarrow p_5^{-1} = p_5$; $p_6 \circ p_6 = p_1 \Rightarrow p_6^{-1} = p_6$

So, each element of P_3 has its inverse in P_3.

Hence P_3 is a group of order 6.

Further $p_2 \circ p_4 = p_6$ and $p_4 \circ p_2 = p_5$

$\Rightarrow p_2 \circ p_4 \neq p_4 \circ p_2$

So, the composition is not commutative.

Hence, P_3 is a non–abelian group of order 6. **Hence proved.**

Remark 9 : It is easy to see from the composition table of P_3 that $(\{p_1, p_2, p_3\}, \circ)$, $(\{p_1, p_4\}, \circ)$, $(\{p_1, p_5\}, \circ)$ and $(\{p_1, p_6\}, \circ)$ are all permutation groups of degree 3 and are called proper subgroups of P_3.

Remark 10 : In general, the set P_n (or S_n) of all permutations of n elements is a permutation group, called the symmetric group.

Theorem 9 : (Cayley's Theorem) : Every finite group G of order n is isomorphic to a permutation group of degree n.

Proof : Let G be a finite group of order n. Let $a \in G$, then for every x in G the product $ax \in G$. Now, we define a function f_a from G into G by

$f_a(x) = ax, \forall x \in G.$

Now, we show that f_a is a permutation.

One–one : Let $x, y \in G$ then,

$f_a(x) = f_a(y) \Rightarrow ax = ay \Rightarrow x = y$ (by left cancellation law)

$\therefore$ f_a is one–one.

Onto : Let $x \in G$ (codomain) then $\exists\ a^{-1} x \in G$ (domain) such that

$f_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})\ x = ex = x$

So, each element of codomain has its preimage in domain.

$\therefore$ f_a is onto.

Hence, f_a is a one–one function from G onto G. Thus, f_a is a permutation on G. Let G' be the set of all such permutations defined on G corresponding to every element of G i.e.,

$G' = \{ f_a : a \in G\}$.

Since, G has n elements so order of G' must be n. Now we shall show that G' is a group with respect to the operation composition of functions.

Closure : Let $f_a, f_b \in G'$ where $a, b \in G$. Now,

$(f_a \circ f_b)\ (x) = f_a\ [f_b(x)] = f_a(bx) = a(bx) = (ab)x$

$= f_{ab}(x), \forall x \in G$

$\Rightarrow f_a \circ f_b = f_{ab}$

Since, $ab \in G \Rightarrow f_{ab} \in G'$

Thus, G' is closed.

Associativity : Let $f_a, f_b, f_c \in G'$ where a, b, c, $\in$ G.

Then $f_a \circ (f_b \circ f_c) = f_a \circ (f_{bc}) = f_{a(bc)} = f_{(ab)c} = f_{ab} \circ f_c = (f_a \circ f_b) \circ f_c$

$\therefore$ Associativity holds in G'.

Identity element : If e is the identity of G, then $e \in G \Rightarrow f_e \in G'$. Now,

$f_a \circ f_e = f_{ae} = f_a$

and $f_e \circ f_a = f_{ea} = f_a$

$\Rightarrow$ $f_a \circ f_e = f_a = f_e \circ f_a$, $\forall f_a \in G'$

$\therefore$ f_e is the identity in G'.

Existence of Inverse : If $a \in G$ then $a^{-1} \in G \Rightarrow f_{a^{-1}} \in G'$

Now, $f_{a^{-1}} \circ f_a = f_{a^{-1}a} = f_e$

and $f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e$

$\Rightarrow$ $f_{a^{-1}} \circ f_a = f_e = f_a \circ f_{a^{-1}}$, $\forall f_a \in G'$

So, each element of G' has its inverse in G'.

Thus, G' is a group.

Next, we shall show that G is isomorphic to G'.

Let us define a function ϕ from G into G' by

$\phi(a) = f_a, \forall a \in G.$

Now, we show that ϕ is one–one, onto and homomorphism.

One–one : Let $a, b \in G$

Now $\phi(a) = \phi(b) \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x), \forall x \in G$

$\Rightarrow ax = bx \Rightarrow a = b$

$\therefore$ ϕ is one–one.

Onto : Let $f_a \in G'$ then $\exists a \in G$ such that

$\phi(a) = f_a$

$\Rightarrow$ each element of G' has its preimage in G'.

$\therefore$ ϕ is onto.

Homomorphism : Let $a, b \in G$ then,

$\phi(ab) = f_{ab} = f_a \circ f_b$

$= \phi(a) \circ \phi(b)$

$\therefore$ ϕ is a homomorphism.

Thus, G is isomorphic to G' i.e., $G \cong G'$. **Hence proved.**

Remark 11: The number of elements in P_n is n!, out of which $\frac{n!}{2}$ are even permutations and $\frac{n!}{2}$ are odd permutations. The set of even permutations, generally denoted by A_n, is called an **Alternating set** of permutations of degree n.

Example 48 : Show that the group $G = (\{1, \omega, \omega^2\}, \cdot)$ is isomorphic to the group $G' = (\{p_1, p_2, p_3\}, o)$ where

$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ are permutations.

Solution : The composition tables for G and G' are as follows

·	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

(For G)

o	p_1	p_2	p_3
p_1	p_1	p_2	p_3
p_2	p_2	p_3	p_1
p_3	p_3	p_1	p_2

(For G')

Now, we define a function $f : G \to G'$ such that $f(1) = p_1$, $f(\omega) = p_2$ and $f(\omega^2) = p_3$.

Then, f is one–one and onto both.

For Homomorphism,

$f(1 \cdot \omega) = f(\omega) = p_2 = p_1 \text{ o } p_2$ ($\because$ p_1 is identity)

$= f(1) \text{ o } f(\omega)$

Also, $f(1 \cdot \omega^2) = f(\omega^2) = p_3 = p_1 \text{ o } p_3 = f(1) \text{ o } f(\omega^2)$

and $f(\omega \cdot \omega^2) = f(\omega^3) = f(1) = p_1 = p_2 \text{ o } p_3$ [from the table]

$= f(\omega) \text{ o } f(\omega^2)$

Similarly, we can show that

$f(\omega \cdot 1) = f(\omega) \text{ o } f(1)$; $f(\omega^2 \cdot 1) = f(\omega^2) \text{ o } f(1)$ and

$f(\omega^2 \cdot \omega) = f(\omega^2) \text{ o } f(\omega)$

Thus, f is a homomorphism.

Hence, f is an isomorphism from G onto G', i.e., $G \cong G'$.

Example 49. Determine a permutation group which is isomorphic to the multiplicative group $G = \{1, -1, i, -i\}$.

Solution : Here we apply the Cayley's theorem to obtain the required permutation group. For that we choose one element of G and multiplying each element of G by that element to obtain a permutation. Since, G has four elements so we construct a permutation for each of the elements of G. So, the permutations are

$$p_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot 1 & -1\cdot 1 & i\cdot 1 & -i\cdot 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}$$

$$p_2 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot(-1) & -1\cdot(-1) & i\cdot(-1) & -i\cdot(-1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}$$

$$p_3 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot i & -1\cdot i & i\cdot i & -i\cdot i \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$$

$$p_4 = \begin{pmatrix} 1 & -1 & i & -i \\ 1\cdot(-i) & -1\cdot(-i) & i\cdot(-i) & -i\cdot(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$$

The set $G' = \{p_1, p_2, p_3, p_4\}$ is a group for the operation composition of functions.

Now, we define a mapping $f : G \to G'$ by $f(1) = p_1$, $f(-1) = p_2$, $f(i) = p_3$ and $f(-i) = p_4$. Then f is one–one and onto both. It can be easily proved that f is also a homomorphism from G onto G'.

Thus, f is an isomorphism from G onto G', i.e., $G \cong G'$.

Hence, $G' = \{p_1, p_2, p_3, p_4\}$ is the required permutation group.

ILLUSTRATIVE EXAMPLES

Example 50. Show that the set M of all 2×2 non–singular matrices over the set of integers Z, is a non–abelian group for the operation multiplication of matrices.

Solution. Closure : Let $M_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}, M_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$ are two non–singular matrices, i.e., $|M_1| \neq 0$ and $|M_2| \neq 0$, $M_1, M_2 \in M$

Also, M_1M_2 is a 2×2 matrix and $|M_1M_2| = |M_1|\,|M_2| \neq 0$

$\Rightarrow M_1M_2 \in M$

$\therefore$ M is closed.

Associativity : Since matrix multiplication is always associative so associativity holds in M.

Identity element : Since $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is a 2×2 matrix and $|I| \neq 0$, so $I \in M$ and $\forall\ M' \in M$ we have

$$M'I = M' = IM'$$

$\therefore$ I is the identity element in M.

Existence of Inverse : If $A \in M$ then $|A| \neq 0$ so A^{-1} exists and A^{-1} is also of order 2×2 with $|A^{-1}| \neq 0$ $\Rightarrow A^{-1} \in M$ such that

$$AA^{-1} = I = A^{-1}A,\ \forall\ A \in M$$

Thus, each element of M has its inverse in M.

Hence, M is a group for the operation multiplication.

Further, let $M_1 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$ and $M_2 = \begin{bmatrix} -2 & 0 \\ 3 & 4 \end{bmatrix}$ then $|M_1| \neq 0$ and $|M_2| \neq 0 \Rightarrow M_1, M_2 \in M$.

Now, $M_1M_2 = \begin{bmatrix} -5 & -4 \\ -1 & -4 \end{bmatrix}$ and $M_2M_1 = \begin{bmatrix} -2 & 2 \\ -1 & -7 \end{bmatrix}$

so $M_1M_2 \neq M_2M_1$

Therefore, M is a non–abelian group.

Example 51. Show that the set $G = R - \{-1\}$ is an abelian group for the operation defined by $a * b = a + b + ab$, $\forall\ a, b \in S$. Here R is the set of real numbers. **[Raj. 2004]**

Solution. First we show that the operation is well defined, i.e., $a \neq -1$, $b \neq -1$ then we must have $a * b \neq -1$ as $-1 \notin G$. Now, let if possible $a \neq -1$, $b \neq -1$ but $a * b = -1$, so

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

$\Rightarrow a + b + ab + 1 = 0$

$\Rightarrow (1 + a)(1 + b) = 0 \Rightarrow$ either $a = -1$ or $b = -1$

which is a contradiction. So our assumption that $a * b = -1$ was wrong, i.e., $a * b \neq -1 \Rightarrow a * b \in G$

$\therefore$ Operation is well defined and hence G is **closed** with respect to operation $*$.

Associativity : Let $a, b, c \in G$ then we have

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

$= a + b + c + bc + ab + ac + abc$

$= (a + b + ab) + c + (a + b + ab)\, c$

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

$= (a * b) * c$

So, associativity holds in G.

Identity element. Since $0 \in G$ and

$a * 0 = a + 0 + a \cdot 0 = a$ and $0 * a = 0 + a + 0 \cdot a = a$

i.e., $a * 0 = a = 0 * a$, $\forall\ a \in G$

so, 0 is the identity element in G.

Existence of Inverse : Let $a \in G$ and inverse of a is b(say) then,

$a * b = 0 \Rightarrow a + b + ab = 0$

or, $b(a + 1) = -a$

or, $b = \dfrac{-a}{a+1} \in G, a \neq -1$

$\therefore$ inverse of $a = \dfrac{-a}{a+1} \in G$

Thus, each element of G has its inverse in G.

Thus G is a group.

Further, $a * b = a + b + ab = b + a + ba$

$= b * a$, $\forall\ a, b \in G$

Therefore, G is an **abelian group.**

Example 52. Show that a group G is abelian iff $(ab)^2 = a^2b^2$, $\forall\ a, b \in G$.

Solution. Let G be abelian then we shall prove that $(ab)^2 = a^2b^2$.

Given, $ab = ba$, $\forall\ a, b \in G$ ($\because$ G is abelian)

Now, $(ab)^2 = (ab)(ab) = a(ba)\, b = a(ab)\, b$ ($\because$ $ab = ba$)

$= (aa)(bb)$

$= a^2b^2$

Converse : Let $(ab)^2 = a^2b^2$ then we have to show that G is abelian, i.e., ab = ba.

Now, $(ab)^2 = a^2b^2$

$\Rightarrow$ (ab) (ab) = (aa) (bb)

$\Rightarrow$ a(ba)b = a(ab)b

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

$\Rightarrow$ ba = ab, $\forall$ a, b $\in$ G(by right cancellation law)

So, G is abelian.

Example 53. If every element of a group G is its own inverse, then G is abelian.

OR

Let G be a group with identity e. Show that if $a^2 = e$, $\forall$ a $\in$ G, then G is abelian.

Solution. Let a, b $\in$ G then by given condition, we have

$a = a^{-1}$ and $b = b^{-1}$

or $a \cdot a = a^{-1} \cdot a$ and $b \cdot b = b^{-1} \cdot b$

or, $a^2 = e$ and $b^2 = e$, $\forall$ a, b $\in$ G .....(1)

Now, a, b $\in$ G $\Rightarrow$ ab $\in$ G

$\Rightarrow (ab)^2 = e$

or, (ab) (ab) = e

or, a(ba) b = e

Now, multiplying by a on the left and by b on the right of both sides, we get

$a^2(ba)b^2 = a(e)b = ab$

$\Rightarrow$ e(ba)e = ab [using (1)]

$\Rightarrow$ ba = ab, $\forall$ a, b $\in$ G

So, G is abelian.

Example 54. Prove that $(Z^*_7, \times_7)$ is an abelian group for multiplication modulo 7, where $Z^*_7 = \{1, 2, 3, 4, 5, 6\}$.

Solution. The composition table for Z^*_7, is as given below

$+_7$	1	2	3	4	5	6	(Top Row)
[1]	1	2	3	4	5	6	(First Row)
2	2	4	6	1	3	5	
3	3	6	2	5	1	4	
4	4	1	5	2	6	3	
5	5	3	1	6	4	2	
6	6	5	4	3	2	1	

Closure : All the entries in the table are the elements of Z^*_7, so Z^*_7 is closed.

Associativity. From the table it is clear that for all a, b, c, $\in Z^*_7$

$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$

So, associativity holds in Z^*_7.

Identity element : The first row of the table, headed by 1, coincides with the top row so 1 is the identity element in Z^*_7.

Existence of Inverse : From the table it is clear that

$1 \times_7 1 = 1 \Rightarrow (1)^{-1} = 1$; $2 \times_7 4 = 1 \Rightarrow (2)^{-1} = 4$

$3 \times_7 5 = 1 \Rightarrow (3)^{-1} = 5$; $4 \times_7 2 = 1 \Rightarrow (4)^{-1} = 2$

$5 \times_7 3 = 1 \Rightarrow (5)^{-1} = 3$; $6 \times_7 6 = 1 \Rightarrow (6)^{-1} = 6$

So, each element of Z^*_7 has its inverse in Z^*_7.

Hence $(Z^*_7, \times_7)$ is a group.

Further, the table is symmetrical about the leading diagonal.

Therefore, $(Z^*_7, \times_7)$ is an **abelian group**.

Example 55. Show that the set G = {A, B, C, D}

where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and $D = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, is an abelian group for matrix multiplication.

Solution. The composition table for G is as follows

•	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

Closure : All the entries in the table are the elements of G. So, G is closed.

Associativity : Since matrix multiplication is always associative, thus associativity holds in G.

Identity element : The first row of the table, headed by A, coincides with the top row therefore, A is the identity element in G.

Existence of Inverse : From the table,

$A \cdot A = A \Rightarrow A^{-1} = A$; $B \cdot B = A \Rightarrow B^{-1} = B$

$C \cdot C = A \Rightarrow C^{-1} = C$; $D \cdot D = A \Rightarrow D^{-1} = D$

So, each element of G has its inverse in G.

Hence G is a group.

Further, the table is symmetrical about the leading diagonal. So, composition is commutative.

Thus, G is an **abelian group**.

Example 56. Show that the set $G = \{2^n \mid n \in Z\}$ is a group for multiplication.

Solution. Here $G = \{2^n \mid n \in Z\}$.

Closure : Let $2^n, 2^m \in G$; $n, m \in Z$

then, $2^n \cdot 2^m = 2^{n+m} \in G$, $\because (n + m) \in Z$

$\therefore$ G is closed.

Associativity. Let $2^a, 2^b, 2^c \in G$; $a, b, c \in Z$ then,

$$2^a \cdot (2^b \cdot 2^c) = 2^a \cdot 2^{b+c} = 2^{a+(b+c)} = 2^{(a+b)+c} = 2^{a+b} \cdot 2^c$$

$$= (2^a \cdot 2^b) \cdot 2^c, \forall\ a, b, c \in Z$$

$\therefore$ Associativity holds in G.

Identity element : Since $0 \in Z \Rightarrow 2^0 \in G$

Now, for all $2^n \in G$, $n \in Z$

$$2^n \cdot 2^0 = 2^{n+0} = 2^n$$

and $2^0 \cdot 2^n = 2^{0+n} = 2^n$

$\Rightarrow 2^n \cdot 2^0 = 2^n = 2^0 \cdot 2^n, \forall\ 2^n \in G$

$\therefore$ 2^0 is the identity element in G.

Existence of Inverse : Let $2^n \in G$ then $n \in Z$

$\Rightarrow -n \in Z$

$\Rightarrow 2^{-n} \in Z$

Now, $2^n \cdot 2^{-n} = 2^0$ and $2^{-n} \cdot 2^n = 2^0$

$\therefore$ $2^n \cdot 2^{-n} = 2^0 = 2^{-n} \cdot 2^n, \forall\ 2^n \in G$

So, each element of G has its inverse in G.

Thus, G is a group.

Example 57. Show that the groups G and G' are isomorphic where $G = (Z_4, +_4)$ and $G' = (\{1, -1, i, -i\}, \cdot)$.

Solution. The composition tables for G and G' are as follows

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

For G

$\cdot$	1	-1	i	$-i$
[1]	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

For G'

Let us define a mapping $\phi : G \to G'$ such that $\phi(0) = 1$; $\phi(1) = i$; $\phi(2) = -1$; $\phi(3) = -i$. Then it is obvious that ϕ is one–one and onto.

Now, for homomorphism

$$\phi(0 +_4 0) = \phi(0) = 1 = \phi(0) \cdot \phi(0)$$

$$\phi(0 +_4 1) = \phi(1) = i = \phi(0) \cdot \phi(1)$$

$$\phi(0 +_4 2) = \phi(2) = -1 = \phi(0) \cdot \phi(2)$$

$$\phi(0 +_4 3) = \phi(3) = -i = \phi(0) \cdot \phi(3)$$

$\phi(1 +_4 1) = \phi(2) = -1 = \phi(1) \cdot \phi(1)$

$\phi(1 +_4 2) = \phi(3) = -i = \phi(1) \cdot \phi(2)$

$\phi(1 +_4 3) = \phi(0) = 1 = \phi(1) \cdot \phi(3)$

$\phi(2 +_4 2) = \phi(0) = 1 = \phi(2) \cdot \phi(2)$

$\phi(2 +_4 3) = \phi(1) = i = \phi(2) \cdot \phi(3)$

$\phi(3 +_4 3) = \phi(2) = -1 = \phi(3) \cdot \phi(3)$

Since, G and G' are abelian so,

$\phi(1 +_4 0) = \phi(1) \cdot \phi(0)$; $\phi(2 +_4 0) = \phi(2) \cdot \phi(0)$; $\phi(3 +_4 0) = \phi(3) \cdot \phi(0)$;

$\phi(2 +_4 1) = \phi(2) \cdot \phi(1)$; $\phi(3 +_4 1) = \phi(3) \cdot \phi(1)$; $\phi(3 +_4 2) = \phi(3) \cdot \phi(2)$

So, ϕ is a homomorphism from G onto G'.

Thus, ϕ is an isomorphism from G onto G'. i.e. $G \cong G'$.

Example 58. Let G be a finite group with identity e, and let a be an arbitrary element of G. Prove that there exists a non–negative integer n such that $a^n = e$.

Solution. Since $a \in G$ then by closure property in G, a, a^2, a^3, ... are the elements of G. Since G is finite, not all terms of this sequence can be distinct, i.e., for some $i \leq j$, $a^i = a^j$ then,

$$(a^{-1})^i (a^i) = (a^{-1})^i a^j$$

$\Rightarrow e = a^{j-i}$

Since, $j \geq i \Rightarrow j - i \geq 0 \Rightarrow n \geq 0$, where $j - i = n$ (say). Thus, there exists a non–negative integer n such that

$$a^n = e.$$

Example 59. Let G be the set of non–zero integers under the operation of multiplication, and let $H = \{3^n \mid n \in Z\}$. Is H a subgroup of G ?

Solution. Since, $H = \{3^n \mid n \in Z\}$ so if we take $n = -1$ then $3^{-1} \in H \Rightarrow \frac{1}{3} \in H$ but $\frac{1}{3} \notin G$

$\Rightarrow$ H is not a subset of G

Hence, H cannot be a subgroup of G.

Example 60. Let G be a group, and let $H = \{x \mid x \in G \text{ and } xy = yx \text{ for all } y \in G\}$. Prove that H is a subgroup of G.

Solution. Given $H = \{x \mid x \in G \text{ and } xy = yx, \forall y \in G\}$

Since, $ey = ye, \forall y \in G$ [e is the identity in G]

$\Rightarrow e \in H \Rightarrow$ H is non–empty.

Also, $x \in H \Rightarrow x \in G$ (by definition of H)

$\therefore$ H is a subset of G.

Let $a, b \in H$ then $ay = ya$ and $by = yb, \forall y \in G$

Now, $(ab^{-1})y = a(b^{-1}y) = a(yb^{-1})$ [$\because by = yb \Rightarrow b^{-1}(by)\, b^{-1} = b^{-1}(yb)\, b^{-1}$

$\Rightarrow e(yb^{-1}) = (b^{-1}y)e \Rightarrow yb^{-1} = b^{-1}y$]

$= (ay)b^{-1} = (ya)\, b^{-1} = y(ab^{-1})$

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

Hence, H is a subgroup of G.

Example 61. Let H and K be subgroups of a group G. Show that $H \cup K$ need not be a subgroup of G.

Solution. It is obvious that $H \cup K$ is a non–empty subset of G. Now, if we show that

$a, b \in H \cup K \nRightarrow ab^{-1} \in H \cup K$ then it proved that $H \cup K$ is not a subgroup of G. Let $a, b, \in H \cup K$ such that $a \in H$ but $a \notin K$ and $b \in K$ but $b \notin H$.

Now, $b \notin H \Rightarrow b^{-1} \notin H$ and $b \in K \Rightarrow b^{-1} \in K$

so, $a \in H, b^{-1} \notin H \Rightarrow ab^{-1} \notin H$.....(1)

also$a \notin K, b^{-1} \in K \Rightarrow ab^{-1} \notin K$.....(2)

(1) and (2) $\Rightarrow ab^{-1} \notin H \cup K$

So, $H \cup K$ is not a subgroup of G.

II Method

The above problem can also be solved by means of a counter example.

Let $P_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ be a permutation group for the operation permutation multiplication, where

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

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

Now, $H = (\{p_1, p_2\}, o\}$ and $K = (\{p_1, p_3\}, o\}$ are two subgroups of P_3 but $H \cup K = (\{p_1, p_2, p_3\}\ o)$ is not a subgroup of P_3 because $p_2, p_3 \in H \cup K$ but $p_2 \circ p_3 = p_6 \notin H \cup K$. So, $H \cup K$ is not closed with respect to operation permutation multiplication.

Hence $H \cup K$ is not a subgroup of P_3.

Remark 12. Let H and K are subgroups of a group G. Then $H \cup K$ is also a subgroup of G iff either $H \subseteq K$ or $K \subseteq H$.

Example 62. Let G be a group. Show that the function $f : G \to G$ defined by $f(a) = a^2$ is a homomorphism if and only if G is abelian.

Solution. Given $f : G \to G$ such that $f(a) = a^2$.

Let G is abelian $\Rightarrow ab = ba, \forall\ a, b \in G$.

Now, $a, b \in G$ then

$f(ab) = (ab)^2 = (ba)^2$ ($\because$ G is abelian)

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

So, f is a homomorphism.

Conversely, let f is a homomorphism i.e.,

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

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

$\Rightarrow a(ba)\ b = a(ab)b$

$\Rightarrow ba = ab$ [by left and right cancellation law]

$\therefore$ G is abelian.

Example 63. Let G be the group of integers under the operation of addition, and let G' be the group of all even integers under the operation of addition. Show that the function $f : G \to G'$ defined by $f(a) = 2a$ is an isomorphism.

Solution. Given, $f : G \to G'$ such that

$f(a) = 2a, \forall\ a \in G$

One–one : Let $a, b \in G$ and

$f(a) = f(b) \Rightarrow 2a = 2b \Rightarrow a = b$

$\therefore$ f is one–one.

Onto : Let $x \in G' \Rightarrow x$ is an even integer

$\Rightarrow \frac{x}{2}$ is an integer

$\Rightarrow \frac{x}{2} \in G$

Now, $f\left(\frac{x}{2}\right) = 2\left(\frac{x}{2}\right) = x$

So, each $x \in G'$ has its preimage in G.

Therefore, f is onto.

Homomorphism : Let $a, b \in G$ then,

$f(a + b) = 2(a + b) = 2a + 2b = f(a) + f(b)$

$\therefore$ f is a homomorphism.

Hence, f is an isomorphism from G onto G'.

Example 64. Let G be a group and let a be a fixed element of G. Show that the function $f_a : G \to G$ defined by $f_a(x) = a\ x\ a^{-1}$, for $x \in G$, is an isomorphism.

Solution. Given, $f_a : G \to G$ such that

$f_a(x) = a\ x\ a^{-1}, \forall\ x \in G$

One–one : Let $f_a(x) = f_a(y)$

$\Rightarrow a\ x\ a^{-1} = a\ y\ a^{-1} \Rightarrow xa^{-1} = ya^{-1}$ (by left cancellation law)

$\Rightarrow x = y$ (by right cancellation law)

$\therefore$ f_a is one–one.

Onto : Let $x \in G$ (codomain) and $a \in G \Rightarrow a^{-1} \in G$ (since G is a group), then by closure property in G, $a^{-1}\ x\ a \in G$.

Now, $f_a(a^{-1}\ x\ a) = a(a^{-1}\ x\ a)\ a^{-1} = (aa^{-1})\ x\ (aa^{-1}) = e\ x\ e = x$ [e is the identity element in G]

So, each $x \in G$ (codomain) has its preimage in G (domain).

Thus, f_a is onto.

Homomorphism : Let $x, y \in G$ then

$f_a(x\ y) = a(x\ y)a^{-1} = a[x(a^{-1}a)y]\ a^{-1}$

[$\because\ a^{-1}a = e$]

$= a[(xa^{-1})(ay)]\, a^{-1} = (a \times a^{-1})(a \, y \, a^{-1})$

$= f_a(x)\, f_a(y)$

$\therefore$ f_a is a homomorphism.

Hence, f_a is an isomorphism from G onto G.

Example 65. Let f and g be homomorphisms from a group (G, *) to a group (G', *'). Show that (H, *) is a subgroup of (G, *), where

$H = \{x \in G \mid f(x) = g(x)\}$.

Solution. Given, $H = \{x \in G \mid f(x) = g(x)\}$.

Let e and e' be the identities in G and G' respectively, then

$f(e) = e'$ and $g(e) = e'$

$\Rightarrow$ $f(e) = g(e)$, $e \in G$

$\Rightarrow$ $e \in H$ [by definition of H]

$\therefore$ H is non empty.

Let $x \in H \Rightarrow x \in G$[by definition of H]

$\Rightarrow H \subseteq G$

$\therefore$ H is a non–empty subset of G.

Further, let a, $b \in H$

$\Rightarrow f(a) = g(a)$ .....(1)

and $f(b) = g(b)$ .....(2)

Now, $f(a * b^{-1}) = f(a) *' f(b^{-1})$ [$\because$ f is a homomorphism]

$= f(a) *' [f(b)]^{-1}$

$= g(a) *' [g(b)]^{-1}$ [from (1) and (2)]

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

$= g(a * b^{-1})$ [$\because$ g is a homomorphism]

$\Rightarrow (a * b^{-1}) \in H$ [by definition of H]

Hence, H is a subgroup of G.

Example 66. Let G be a group and H and K are two subgroups of G. Show that if H is abelian and K is non–abelian then $H \cap K$ is an abelian subgroup of G.

Solution. We shall show that (i) $H \cap K$ is a subgroup of G, and (2) $H \cap K$ is abelian.

We proved earlier that $H \cap K$ is a subgroup of a group G. [Please refer Example 14]

Now, it remains to prove that $H \cap K$ is abelian.

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

$\Rightarrow ab = ba$ [$\because$ H is abelian]

So, each pair of elements of $H \cap K$ commutes.

Hence, $H \cap K$ is an abelian subgroup of G.

Example 67. If (G, *) is a group where $G = \{e, x, y\}$ and $o(G) = 3$, then show that $(x * y) = (x * y)^{-1}$.

Solution. The composition table for (G, *) is as follows :

*	e	x	y
e	e	x	y
x	x	a_{22}	a_{23}
y	y	a_{32}	a_{33}

Since, e is an identity in G so the first row and the first column in the table are obvious. Further, in second column x cannot be repeated so $a_{32} \neq x$ also, in third row y cannot be repeated so $a_{32} \neq y$ so $a_{32} = e$ and then $a_{33} = x$, $a_{22} = y$ and $a_{23} = e$

$\therefore$ The table is now constructed as

*	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

From the table, $(x * y) = e$.....(1)

Since $x, y \in G \Rightarrow x * y \in G$ [$\because$ G is a group]

$\Rightarrow (x * y)^{-1} \in G$[$\because$ G is a group]

Now, multiply both sides of (1) by $(x * y)^{-1}$ from the left, we have

$(x * y)^{-1} * (x * y) = (x * y)^{-1} * e$

or, $e = (x * y)^{-1}$ .....(2)

$\therefore$ (1) and (2) $\Rightarrow (x * y) = (x * y)^{-1}$.

Example 68. Let $f : G \rightarrow G'$ be a group homomorphism. Prove that f is one–one if ker (f) = {e}.

Solution. Let f is a one–one mapping and e, e' be the identities in G and G' respectively.

Also, let $a \in \ker(f) \Rightarrow f(a) = e'$ [by definition of ker(f)]

$\Rightarrow f(a) = f(e)$ [$\because f(e) = e'$]

$\Rightarrow a = e$ [$\because$ f is one–one]

$\therefore$ $a \in \ker(f) \Rightarrow a = e$ i.e., ker(f) has only one element e alone.

So, ker(f) = {e}.

Converse : Let ker(f) = {e}

Also, let $a, b \in G$ and $f(a) = f(b)$

$\Rightarrow f(a)\,[f(b)]^{-1} = f(b)\,[f(b)]^{-1}$

$\Rightarrow f(a)\,f(b^{-1}) = f(b)\,[f(b)]^{-1}$

$\Rightarrow f(ab^{-1}) = e'$ [$\because$ f is a homomorphism]

$\Rightarrow ab^{-1} \in \ker(f)$ [by definition of kernel]

$\Rightarrow ab^{-1} = e$ [$\because$ ker(f) = {e}]

$\Rightarrow (ab^{-1})b = eb \Rightarrow a(b^{-1}b) = b \Rightarrow ae = b$

or, $a = b$

$\therefore$ f is one–one.

Example 69. Let (G, *) be a group of even order. Show that there is an element a in G such that $a * a = e$, where e is the identity element in G and $a \neq e$.

Solution. Let order of G be 2n. We know that the inverse of the identity is the identity itself so $e = e^{-1}$. Now, we assume that no element of G, other than e, is its own inverse. Since, the number of elements in G other than e, is (2n – 1) i.e., odd, so if we make pairs of the elements and their inverses then we left with one element (say a) which does not has any option for its inverse other than itself. So, there exists one element $a \neq e$ in G which is its own inverse, i.e.,

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

Operating both sides by a, we get

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

Example 70. Let H_1 and H_2 be subgroups of a group G, neither of which contains the other. Show that there exists an element of G belonging neither to H_1 nor to H_2.

Solution. Given $H_1 \not\subseteq H_2$ and $H_2 \not\subseteq H_1$ .....(1)

Let if possible $H_1 \cup H_2 = G$.

Also let $x \in H_1$ and $y \in H_2 \Rightarrow x \in G, y \in G \Rightarrow xy \in G$ (by closure property)

Since $H_1 \cup H_2 = G$ and $xy \in G$

$\Rightarrow xy \in H_1$ or $xy \in H_2$

If $xy \in H_1 \Rightarrow x^{-1}(xy) = (x^{-1}x)y = ey = y \in H_1$ $(\because x \in H_1 \Rightarrow x^{-1} \in H_1)$

$\Rightarrow H_2 \subseteq H_1$ $(\because y \in H_2 \Rightarrow y \in H_1)$

which is a contradiction in view of (1).

If $xy \in H_2 \Rightarrow x^{-1}(xy)\, y^{-1} = x(yy^{-1}) = xe = y \in H_2$ $(\because y \in H_2 \Rightarrow y^{-1} \in H_2)$

$\Rightarrow H_1 \subseteq H_2$ $(\because x \in H_1 \Rightarrow x \in H_2)$

which is a contradiction in view of (1).

Thus, our assumption that $H_1 \cup H_2 = G$ was wrong i.e., $H_1 \cup H_2 \neq G$. Hence there exists at least one element in G which neither belongs to H_1 nor belongs to H_2.

Example 71. Let $S = \{x \mid x \text{ is real number and } x \neq 0, x \neq \pm 1\}$.

Consider the following functions $f_i : S \to S$, i = 1, 2, ..., 6

$$f_1(x) = x \quad , \quad f_2(x) = 1 - x \quad , \quad f_3(x) = \frac{1}{x},$$

$$f_4(x) = \frac{1}{1-x} \quad , f_5(x) = 1 - \frac{1}{x} \quad , \quad f_6(x) = \frac{x}{x-1}.$$

Show that $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ is a group under the operation of composition.

Solution. Given $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$.

Now, $f_1 \circ f_2(x) = f_1[f_2(x)] = f_1(1 - x) = 1 - x = f_2(x)$

$\Rightarrow f_1 \circ f_2 = f_2$

$$f_2 \circ f_3(x) = f_2[f_3(x)] = f_2\left(\frac{1}{x}\right) = 1 - \frac{1}{x} = f_5(x)$$

$\Rightarrow f_2 \circ f_3 = f_5$, and so on.

Thus, the composition table for the set S is as follows

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6	(Top Row)
$\boxed{f_1}$	f_1	f_2	f_3	f_4	f_5	f_6	(First Row)
f_2	f_2	f_1	f_5	f_6	f_3	f_4	
f_3	f_3	f_4	f_1	f_2	f_6	f_5	
f_4	f_4	f_3	f_6	f_5	f_1	f_2	
f_5	f_5	f_6	f_2	f_1	f_4	f_3	
f_6	f_6	f_5	f_4	f_3	f_2	f_1	

Closure : Since all the entries in the table are the elements of G, so G is closed.

Associativity : The composition of functions is always associative, so associativity holds in G.

Identity element : Since the first row of the table, headed by f_1, coincides with the top row so f_1 is the identity element of G.

Existence of Inverse : From the table,

$f_1 \circ f_1 = f_1 \Rightarrow f_1^{-1} = f_1$; $f_2 \circ f_2 = f_1 \Rightarrow f_2^{-1} = f_2$

$f_3 \circ f_3 = f_1 \Rightarrow f_3^{-1} = f_3$; $f_4 \circ f_5 = f_1 \Rightarrow f_4^{-1} = f_5$

$f_5 \circ f_4 = f_1 \Rightarrow f_5^{-1} = f_4$; $f_6 \circ f_6 = f_1 \Rightarrow f_6^{-1} = f_6$

Thus, each element of G has its inverse in G.

Hence, G is a group.

Also, $f_2 \circ f_3 = f_5$ and $f_3 \circ f_2 = f_4 \Rightarrow f_2 \circ f_3 \neq f_3 \circ f_2$

Therefore, G is a non–abelian group of order 6.

Example 72. Let (A, *) be a monoid such that for every x in A, $x * x = e$ (identity). Show that (A, *) is an abelian group. **[Raj. 2005]**

Solution. Given that (A, *) is a monoid. So to prove that (A, *) is a group it is remain to show that each element of A has its inverse in A.

Given $x * x = e$, $\forall x \in A$

$\Rightarrow x * x = e = x * x$, $\forall x \in A$

$\Rightarrow x^{-1} = x$ (by definition of inverse)

Since $x \in A \Rightarrow x^{-1} \in A$ $(\because x = x^{-1})$

Thus each element of A has its inverse in A.

So, (A, *) is a group.

Further, let $x, y \in A \Rightarrow x * y \in A$ (by closure property)

and $x * x$

$= e, y * y = e$ .....(1)

Now, $x * y \in A \Rightarrow (x * y) * (x * y) = e \Rightarrow x * (y * x) * y = e$

pre operating by x and post operating by y on both sides, we get

$x * [x * (y * x) * y] * y = x * (e) * y$

$\Rightarrow (x * x) * (y * x) * (y * y) = x * y$

$\Rightarrow e * (y * x) * e = x * y$ [using (1)]

$\Rightarrow y * x = x * y, \ \forall \ x, y \in A$

$\therefore$ (A, *) is an abelian group.

EXERCISE 8.3

1. Let G be a group with identity e. Show that if $x^2 = x$ for some x in G, then $x = e$.
2. Let G be an abelian group with identity e, and let $H = \{x \mid x^2 = e\}$. Show that H is a subgroup of G.
3. Show that the set {0, 1, 2} forms a group for the operation 'addition modulo 3'.
4. Show that the set H = {0, 2} is a subgroup of G = {0, 1, 2, 3} for addition modulo 4.
5. Let (I, +) be a group, where I is the set of all integers and + is an addition operation. Determine whether the following subsets of G are subgroups of G ?

   (i) The set G_1 of all odd integers. (ii) The set G_2 of all positive integers.

   [**Ans.** (i) No (ii) No]
6. Let $(A_1, *)$, where $A_1 = \{a, b, c\}$ and $(A_2, \cdot)$, where $A_2 = \{1, \omega, \omega^2\}$, are two algebraic structures as shown in the following figure.

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

·	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

   Show that the two algebraic structures are isomorphic.
7. Show that the group $G_1 = (\{0, 1, 2, 3\}, +_4)$ is isomorphic to the group $G_2 = (\{1, 2, 3, 4\}, \times_5)$.
8. Show that the mapping $f : G \to G$ defined by $f(x) = x^4$, is a homomorphism, where G is a group of non–zero real numbers under the operation multiplication.
9. Let (A, *) be a group. Show that for any a, b, c, d, a_1, b_1, c_1, d_1 in A, if

   $a * c = a_1 * c_1$, ; $a * d = a_1 * d_1$ and $b * c = b_1 * c_1$

   then show that $b * d = b_1 * d_1$.

[Hint : Note that $b * d = b * (c * c^{-1}) * (a^{-1} * a) * d$]

10. Show that the set of all $m \times n$ matrices is a group under addition of matrices.

11. Show that the set P(S), power set of a non–empty set S, is a group for $A * B = (A \cup B) - (A \cap B)$ where $A, B \in P(S)$.

12. Show that the mapping $f : G \to G$ defined by $f(x) = nx$, $n \in Z$, is a homomorphism where G is the group of integers for addition.

13. Show that the set G of all ordered pairs (a, b) of real numbers, where $a \neq 0$; under the operation defined as

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

is a non abelian group.

14. Prove that the set Q of rational numbers other than 1 forms an abelian group for the operation * defined as : $a * b = a + b - ab$.

15. Prove that the set $G = \{1, 2, ..., p - 1\}$ of $(p - 1)$ integers, p being prime, is a finite abelian group of order $p - 1$, under the operation multiplication modulo p.

16. Show that the following sets are isomorphic to each other

(i) $G_1 = (\{1, -1\}, \cdot)$(ii) $G_2 = (Z_2, +_2)$, where $Z_2 = \{0, 1\}$.

(iii) $G_3 = \left(\left\{\begin{bmatrix}1 & 2\\ 1 & 2\end{bmatrix}, \begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix}\right\}, 0\right)$

17. Find which of the following sets are groups under multiplication (mod 11).

(i) {1, 2, 3, 4, 5, 9}(ii) {1, 3, 5, 7, 8}

[Ans. (i) Yes (ii) No]

18. Define a subgroup. If H is any subgroup of a group G, then show that $H^{-1} = H$.

19. Prove that in an abelian group if an element a has order k and an element b has an order j and if k and j are relatively prime, then the element ab has the order kj.

20. Let $H_1, H_2, ..., H_k$ be the subgroups of a group G. Prove that $\bigcap_{i=1}^{k} H_i$ is also a subgroup of G.

21. Let G be an abelian group then show that $(ab)^n = a^n b^n$ for $n \in Z^+$ and $a, b \in G$.

22. Let A_n be the set of all even permutations in S_n. Show that A_n is a subgroup of S_n.

23. Let G be an abelian group and n be a fixed integer. Prove that the function $f : G \to G$ defined by $f(a) = a^n$, for $a \in G$, is a homomorphism.

24. Prove that the function $f(x) = |x|$ is a homomorphism from the group G of non–zero real numbers under multiplication to the group G' of positive real numbers under multiplication.

25. Let S be the set of all finite groups and define the following relation R on S :

G R G' iff G and G' are isomorphic.

Prove that R is an equivalence relation.

26. Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation $a^i a^j = a^r$, where $i + j \equiv r \pmod 6$. Prove that G and Z_6 are isomorphic.

27. Let Z be the group of integers under the operation of addition. Prove that the function $f : Z \times Z \to Z$ defined by $f(a, b) = a + b$ is a homomorphism.

28. Let H be a subgroup of R under addition. Define $G = \{2^a | a \in H\}$. Prove that G is a group under multiplication.

29. Define Dihedral group. Determine the elements of dihedral group formed by regular pentagon.

[**Ans.** D_5 = {I, (1 2 3 4 5), (1 3 5 2 4), (1 4 2 5 3), (1 5 4 3 2), (1) (25) (34), (2) (13) (45), (3) (24) (15), (4) (12) (35), (5) (14) (23)}]

30. Show that the four permutations I, (a, b), (c d), (a b) (c d) on four symbols a, b, c, d form a finite abelian group with respect to the permutation multiplication.

8.17 Product of Groups

Let $(G_1, *)$ and $(G_2, *')$ be two groups then the direct product of these two groups is the algebraic structure $(G_1 \times G_2, *")$, in which the binary operation $*"$ on $G_1 \times G_2$ is defined by

$$(a_1, a_2) *" (b_1, b_2) = (a_1 * b_1, a_2 *' b_2), \forall (a_1, a_2), (b_1, b_2) \in G_1 \times G_2.$$

Theorem 10. If $(G_1, *)$ and $(G_2 *')$ be two groups, then $(G, *")$ where $G = G_1 \times G_2$ is a group with operation $*"$ defined by

$$(a_1, a_2) *" (b_1, b_2) = (a_1 * b_1, a_2 *' b_2); a_1, b_1 \in G_1 \text{ and } a_2, b_2 \in G_2.$$

Proof. Closure property : Let $(a_1, a_2), (b_1, b_2) \in G$, then

$$(a_1, a_2) *" (b_1, b_2) = (a_1 * b_1, b_2 *' b_2) \in G_1 \times G_2 = G$$

$[\because a_1, b_1 \in G_1 \Rightarrow a_1 * b_1 \in G$

$a_2, b_2 \in G_2 \Rightarrow a_2 *' b_2 \in G]$

$\therefore$ G is closed.

Associativity : Let $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G$, then

$(a_1, a_2) *" [(b_1, b_2) *" (c_1, c_2)] = (a_1, a_2) *" [(b_1 * c_1, b_2 *' c_2)]$

$= [a_1 * (b_1 * c_1), a_2 *' (b_2 *' c_2)]$

$= [(a_1 * b_1) * c_1, (a_2 *' b_2) *' c_2]$

$= [(a_1 * b_1, a_2 *' b_2] *" (c_1, c_2)$

$= [(a_1, a_2) *" (b_1, b_2)] *" (c_1, c_2)$

$\therefore$ Associativity holds in G.

Identity element : If e_1 and e_2 be the identities in G_1 and G_2, respectively then

$$(e_1, e_2) \in G_1 \times G_2 = G.$$

Let $(a_1, a_2) \in G$, then

$$(a_1, a_2) *" (e_1, e_2) = (a_1 * e_1, a_2 *' e_2) = (a_1, a_2)$$

and $(e_1, e_2) *" (a_1, a_2) = (e_1 * a_1, e_2 *' a_2) = (a_1, a_2)$

$\therefore (a_1, a_2) *" (e_1, e_2) = (a_1, a_2) = (e_1, e_2) *" (a_1, a_2)$

$\Rightarrow (e_1, e_2)$ is the identity element in $G_1 \times G_2 = G$.

Existence of Inverse : Let $(a_1, a_2) \in G$ then $a_1 \in G_1$ and $a_2 \in G_2$

$\Rightarrow a_1^{-1} \in G_1$ and $a_2^{-1} \in G_2$

$\Rightarrow (a_1^{-1}, a_2^{-1}) \in G_1 \times G_2 = G$

Now, (a_1, a_2) *" $(a_1^{-1}, a_2^{-1}) = (a_1 * a_1^{-1}, a_2 *' a_2^{-1}) = (e_1, e_2)$

and (a_1^{-1}, a_2^{-1}) *" $(a_1, a_2) = (a_1^{-1} * a_1, a_2^{-1} *' a_2) = (e_1, e_2)$

$\therefore$ (a_1, a_2) *" $(a_1^{-1}, a_2^{-1}) = (e_1, e_2) = (a_1^{-1}, a_2^{-1})$ *" (a_1, a_2)

$\Rightarrow$ Inverse of (a_1, a_2) is (a_1^{-1}, a_2^{-1})

So, each element of G has its inverse in G.

Thus, (G, *") is a group. **Hence proved.**

8.18 Cyclic Group

Definition : A group G is said to be cyclic if there exists atleast one element $a \in G$, such that every element of G can be written as an integral power of a, i.e., for each $g \in G \; \exists \; n \in Z$ such that $g = a^n$. The element a is called the generator of the cyclic group G and then G can be written as G = [a].

Example 73. Show that the multiplicative group $G = \{1, -1, i, -i\}$ is cyclic. Find its generators.

Solution. Since, $G = \{1, -1, i, -i\}$

$= \{i^4, i^2, i^1, i^3\}$

so each element of G can be expressed as an integral power of $i \in G$. Thus, G is a cyclic group with generator i.

Also, $G = \{1, -1, i, -i\} = \{(-i)^4, (-i)^2, (-i)^3, (-i)^1\}$

$\Rightarrow -i$ is also a generator of G.

Hence, G is a cyclic group with two generators i and $-i$.

Example 74. Show that the multiplicative group $G = \{1, \omega, \omega^2\}$ is cyclic. Find its generators.

Solution. Since, $G = \{1, \omega, \omega^2\}$

$= \{\omega^3, \omega^1, \omega^2\}$ or $\{(\omega^2)^3, (\omega^2)^2, (\omega^2)^1\}$

So, each element of G can be expressed as an integral power of ω, or ω^2. Hence, G is a cyclic group with generators ω and ω^2.

Theorem 11. Every cyclic group is an abelian group.

Proof. Let G = [a] be a cyclic group generated by a. If $x, y \in G$, then

$x = a^r$ and $y = a^s$, for some $r, s \in Z$

Now, $xy = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = y\,x, \; \forall \; x, y \in G$

Thus, G is an abelian group. **Hence proved.**

Theorem 12. 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.

If $x \in G$, then

$x = a^r, r \in Z$

$= (a^{-1})^{-r} = (a^{-1})^s, -r = s \in Z$

$\Rightarrow$ each element of G can be expressed as an integral power of a^{-1}.

So, a^{-1} is also a generator of G. **Hence proved.**

Theorem 13. The order of a cyclic group is equal to the order of its generating element.

Proof. Let G be a cyclic group generated by a. Also assume that order of a is n, i.e., n is the least positive integer such that

$$a^n = e.$$

We shall show that G has exactly n distinct elements

$$a, a^2, a^3, ..., a^n = e = a^0. .....(1)$$

First we show that all the elements of (1) are distinct. If possible, let

$$a^i = a^j, 1 \leq j < i \leq n$$

$$\Rightarrow a^{i-j} = a^0 = e$$

Since, $0 < i - j < n$, so $a^{i-j} = e$ implies that the order of a is less than n, which is a contradiction. Thus, $a^i \neq a^j$.

Hence, all the n elements of (1) are distinct. Further, let $a^k \in G$ then by Euclidean algorithm, there exists two integers p and q such that

$$k = np + q, 0 \leq q < n.$$

$$\therefore a^k = a^{np+q} = a^{np} a^q = (a^n)^p a^q = e^p a^q = ea^q = a^q.$$

Since $0 \leq q < n$, so a^k $(= a^q)$ is one of the n elements in (1). Thus, each element of G is equal to some member of (1).

Therefore, G has exactly n elements, given in (1).

Hence, order of G = order of a = n

or $o(G) = o(a) = n$. **Hence proved.**

Theorem 14. If a finite group of order n contains an element of order n, the group must be cyclic.

Proof. Let G be a finite group of order n. Also suppose that $a \in G$ such that order of a is n. If H is a cyclic subgroup of G generated by a i.e., $H = \{a^i \mid i \in Z\}$, then the order of H must be equal to the order of its generator a i.e. $o(H) = o(a) = n$. Then H is a cyclic subgroup of G such that the number of elements in H is equal to the number of elements in G. Therefore, H = G and hence G itself is a cyclic group generated by a. **Hence proved.**

Example 75. Show that the group $G = (\{0, 1, 2, 3, 4, 5\}, +_6)$ is cyclic. Find the generators.

Solution. Given, $G = (\{0, 1, 2, 3, 4, 5\}, +_6) \Rightarrow o(G) = 6$. If there exists an element $a \in G$ such that $o(a) = o(G) = 6$ then G must be cyclic and a is the generator of G. Also, identity element of G is 0.

Now, $o(0) = 1$

$1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0 \Rightarrow o(1) = 6$

$2 +_6 2 +_6 2 = 0 \Rightarrow o(2) = 3$

$3 +_6 3 = 0 \Rightarrow o(3) = 2$

$4 +_6 4 +_6 4 = 0 \Rightarrow o(4) = 3$

$5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0 \Rightarrow o(5) = 6$

So, there are two elements 1 and 5 in G such that

$o(G) = o(1) = o(5) = 6$

Hence, G is cyclic and 1, 5 are the generators of G.

Example 76. Show that the group $G = (\{1, 2, 3, 4, 5, 6\}, \times_7)$ is cyclic. How many generators are there ?

Solution. Given, $G = (\{1, 2, 3, 4, 5, 6\}, \times_7)$

Here, $o(G) = 6$ and identity element = 1.

Now, $1^1 = 1 \Rightarrow o(1) = 1$

$2^3 = 2 \times_7 2 \times_7 2 = 1 \Rightarrow o(2) = 3$

$3^6 = 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 \times_7 3 = 1 \Rightarrow o(3) = 6$

$4^3 = 4 \times_7 4 \times_7 4 = 1 \Rightarrow o(4) = 3$

$5^6 = 5 \times_7 5 \times_7 5 \times_7 5 \times_7 5 \times_7 5 = 1 \Rightarrow o(5) = 6$

$6^2 = 6 \times_7 6 = 1 \Rightarrow o(6) = 2$

$\therefore$ $o(G) = o(3) = o(5) = 6$

So, G is cyclic and 3, 5 are two generators of G.

Remark 16. 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 m and n are relatively primes.

Example 77. How many generators are there of the cyclic group G = [a] of order 8 ?

Solution. Since, a is the generator of G so $o(a) = 8$.

$\therefore$ We can write $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

Now, 3 is prime to 8 $\Rightarrow$ a^3 is also a generator of G [see remark 13]

5 is prime to 8 $\Rightarrow$ a^5 is also a generator of G

7 is prime to 8 $\Rightarrow$ a^7 is also a generator of G.

Thus, G has four generators a, a^3, a^5 and a^7.

Theorem 13. If G is an infinite cyclic group then G is isomorphic to the additive group of integers.

Proof. Let G = [a] be the infinite cyclic group generated by a, then $G = \{a^m : m \in Z\}$. Also, let Z be the additive group of integers.

Now, we define a mapping $f : G \to Z$ such that

$f(a^m) = m, \forall\ m \in Z$

One–one : Let $f(a^m) = f(a^n) \Rightarrow m = n \Rightarrow a^m = a^n$

$\therefore$ f is one–one.

Onto : Let $x \in Z \Rightarrow a^x \in G$ such that

$f(a^x) = x, \forall\ x \in Z$

so each element of Z has its preimage in G.

$\therefore$ f is onto.

Homomorphism : Let $a^x, a^y \in G$ then

$f(a^x\ a^y) = f(a^{x+y}) = x + y = f(a^x) + f(a^y)$

$\therefore$ f is a homomorphism from G onto Z.

Hence, f is an isomorphism from G onto Z i.e.,$G \cong Z$. **Hence proved.**

Theorem 16. A cyclic group G with a generator of finite order n, is isomorphic to the additive group of residue classes modulo n.

Proof. Let G be a cyclic group generated by a and o(a) = n. We shall show that G has exactly n distinct elements

$a, a^2, a^3, ..., a^n = e = a^0$.....(1)

First, we show that all the elements of (1) are distinct. For this, if possible, let

$a^i = a^j$, $1 \le j < i \le n$

$\Rightarrow a^{i-j} = a^0 = e$

$\Rightarrow o(a) \le i - j < n$

which is a contradiction.

Thus, $a^i \neq a^j$ unless i = j.

So, all the n elements of (1) are distinct. Further, let $a^k \in G$ then by Euclidean algorithm, there exists p, $q \in Z$ such that

$k = np + q$, $0 \le q < n$

$\therefore a^k = a^{np+q} = a^{np}\, a^q = (a^n)^p\, a^q = e^p\, a^q = ea^q = a^q$.

Since, $0 \le q < n$ so a^k $(= a^q)$ is one of the n elements in (1). Thus, each element of G is equal to some member of (1). Therefore, G has exactly n elements given in (1).

Now, let Z_n be the group of residue classes modulo n.

By residue class we mean that if $a \in Z$ then the residue class of 'a' modulo n, denoted by [a], is $\{x : x \in Z$ and $x - a$ is divisible by n$\}$.

Here, Z_n be the collection of all such residue classes modulo n then,

$Z_n = \{[0], [1], [2], ..., [n-1]\}$

Consider a mapping $\phi : G \to Z_n$ defined as

$\phi(a^x) = [x]$, $\forall\ x \in Z$

First, we show that ϕ is well defined.

Let $x, y \in Z$ such that $a^x = a^y$.

Then we must show that $\phi(a^x) = \phi(a^y)$

Now, $a^x = a^y \Rightarrow a^{x-y} = a^0 = e \Rightarrow (x - y)$ is divisible by n $\quad [\because o(a) = n]$

$\Rightarrow x \equiv y \pmod n \Rightarrow [x] = [y]$

$\Rightarrow \phi(a^x) = \phi(a^y)$.

$\therefore$ ϕ is well defined.

One–one : Let $a^x, a^y \in G$ such that

$\phi(a^x) = \phi(a^y) \Rightarrow [x] = [y] \Rightarrow (x - y)$ is divisible by n

$\Rightarrow x - y = mn$, $m \in Z$

$\Rightarrow a^{x-y} = a^{mn} \Rightarrow a^x\, a^{-y} = (a^n)^m = e^m = e$

$\Rightarrow a^x = a^y \Rightarrow \phi$ is one–one.

Onto : Let $[x] \in Z_n$ then $x \in Z \Rightarrow a^x \in G$ and $\phi(a^x) = [x]$

So, each element of Z_n has its preimage in G.

$\therefore$ ϕ is onto.

Homomorphism : Let $a^x, a^y \in G$ then,

$$\phi(a^x\, a^y) = \phi(a^{x+y}) = [x + y] = [x] + [y]$$
$$= \phi(a^x) + \phi(a^y)$$

$\therefore$ ϕ is a homomorphism from G onto Z_n.

Hence, ϕ is an isomorphism from G onto Z_n i.e., G is isomorphic to Z_n. **Hence proved.**

8.19 Coset

Let G be a group and H be any subgroup of G. Also suppose that a be any element of G. Then the set

$Ha = \{ha : h \in H\}$ is called the **right coset** of H in G generated by a.

Similarly, the set $aH = \{ah : h \in H\}$ is called a **left coset** of H in G generated by a.

These cosets are also known as **residue classes modulo the subgroup.**

Remark 17. If G is abelian then H is abelian so $ah = ha, \forall h \in H$. Hence, every right coset will be equal to the corresponding left coset i.e. $aH = Ha$.

Remark 18. If e be the identity in G then $He = H = eH$. So, H itself is a right coset as well as left coset.

Remark 19. Since H is a subgroup of G so $e \in H$. Therefore, if aH is a left coset of H in G then $ae \in aH \Rightarrow a \in aH$. Hence, no left coset is empty. Similarly, no right coset is empty.

Remark 20. If the composition in G has been denoted additively, then the left coset of H in G generated by a is defined as

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

Similarly, the right coset can be defined as

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

Example 78. Find all the right cosets of a subgroup $H = 3.Z$ of a group $(Z, +)$ in Z. **[Raj. 2003]**

Solution. Here, $Z = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$

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

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

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

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

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

So H, H + 1 and H + 2 are the only distinct right cosets of H in Z. All these cosets partition the set Z into disjoint subsets such that

$Z = H \cup H + 1 \cup H + 2$

Since, the group $(Z, +)$ is abelian $\Rightarrow$ H is abelian, so every right coset is equal to the corresponding left coset i.e., $H + 1 = 1 + H$; $H + 2 = 2 + H$.

Theorem 17. If H is any subgroup of a group G and $h \in H$, then $Hh = H = hH$.

Proof. Here $Hh = \{h'h : h' \in H\}$

Now $h' \in H, h \in H \Rightarrow h'h \in H$ (by closure property)

so each element of Hh is the element of H

$\Rightarrow Hh \subseteq H$ .....(1)

Again, let $h' \in H$, then

$h' = h'e = h'(h^{-1}h) = (h'h^{-1})h \in Hh$ [$\because h \in H \Rightarrow h^{-1} \in H$

$\therefore h' \in H, h^{-1} \in H \Rightarrow h'h^{-1} \in H$]

$\Rightarrow h' \in Hh$

$\Rightarrow H \subseteq Hh$ .....(2)

(1) and (2) $\Rightarrow Hh = H$.

Similarly, we can prove that $hH = H$. **Hence proved.**

Theorem 18. If $a, b \in G$ and H be any subgroup of G, then

(i) $Ha = Hb \Leftrightarrow ab^{-1} \in H$ and (ii) $aH = bH \Leftrightarrow a^{-1}b \in H$.

Proof. (i) Since $a \in Ha$ [see remark 16]

and $Ha = Hb$ (given)

$\Rightarrow a \in Hb \Rightarrow ab^{-1} \in (Hb)\, b^{-1} = H(bb^{-1}) = He = H$

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

Conversely, let $ab^{-1} \in H \Rightarrow Hab^{-1} = H$ [$\because h \in H \Rightarrow Hh = H$]

$\Rightarrow (Hab^{-1})b = Hb \Rightarrow Ha(b^{-1}b) = Hb \Rightarrow Ha(e) = Hb$

$\Rightarrow Ha = Hb$.

(ii) Since $b \in bH$ and $aH = bH$ (given)

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

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

Conversely, Let $a^{-1}b \in H \Rightarrow a^{-1}bH = H$ [$\because h \in H \Rightarrow hH = H$]

$\Rightarrow a(a^{-1}b\ H) = aH \Rightarrow (aa^{-1})\ bH = aH \Rightarrow ebH = aH$

$\Rightarrow bH = aH$. **Hence proved.**

Theorem 19. Any two right (or left) cosets of a subgroup are either disjoint or identical.

Proof. Let H be a subgroup of a group G. Suppose that Ha and Hb are two right cosets of H in G such that they are not disjoint i.e., $Ha \cap Hb \neq \phi$. Then there exists atleast one element c such that $c \in Ha$ and $c \in Hb$.

Let $c = h_1a$ and $c = h_2b$, $h_1, h_2 \in H$

$\Rightarrow h_1a = h_2b \Rightarrow h_1^{-1}(h_1a) = h_1^{-1}(h_2b)$

$\Rightarrow (h_1^{-1}h_1)a = (h_1^{-1}h_2)b$

$\Rightarrow ea = (h_1^{-1}h_2)b \Rightarrow a = h_3b$, where $h_3 = h_1^{-1}h_2 \in H$

$\Rightarrow Ha = Hh_3b = Hb$ [$\because h_3 \in H \Rightarrow Hh_3 = H$]

$\Rightarrow$ Ha = Hb

$\Rightarrow$ Ha and Hb are identical, if they are not disjoint.

Thus, either $Ha \cap Hb = \phi$ or Ha = Hb.

Similarly, for left cosets aH and bH it can be proved that either $aH \cap bH = \phi$ or aH = bH. **Hence proved.**

Theorem 20. If H is a subgroup of a group G, then G is equal to the union of all right (or left) cosets of H in G i.e.,

$G = H \cup Ha \cup Hb \cup Hc \cup ....$, where a, b, c, ... are the elements of G.

Proof. Since, $Hx = \{hx : h \in H \text{ and } x \in G\}$

Now, $h \in H \Rightarrow h \in G$ $(\because H \subseteq G)$

$\therefore$ $h \in G, x \in G \Rightarrow hx \in G$ (by closure property in G)

$\Rightarrow$ $Hx \subseteq G$

$\therefore$ Each right coset of H in G is a subset of G

$\Rightarrow$ The union of all right cosets of H in G is also a subset of G i.e.,

$$\bigcup_{x \in G} Hx \subseteq G \qquad \text{.....(1)}$$

Also, if $x \in G$ then $x \in Hx$

$\Rightarrow$ each element of G is the element of some right coset of H in G.

$\Rightarrow$ x must belongs to the union of all right cosets of H in G.

$\Rightarrow$ G is a subset of the union of all right cosets of H in G i.e.,

$$G \subseteq \bigcup_{x \in G} Hx \qquad \text{.....(2)}$$

$\therefore$ (1) and (2) $\Rightarrow$ $G = \bigcup_{x \in G} Hx$

Similarly, it can be proved that $G = \bigcup_{x \in G} xH$. **Hence proved.**

8.19.1 Coset Decomposition of a Group

Let H be a subgroup of a group G. Then

(i) No right coset of H in G is empty.

(ii) Any two right cosets of H in G are either disjoint or identical.

(iii) The union of all right cosets of H in G is equal to G.

In view of above properties, we can say that the set of all right cosets of H in G determine a partition of G.

This partition is called the **right coset decomposition** of G with respect to the subgroup H. Similarly, we can also define the **left coset decomposition** of G.

8.19.2 Index of a Subgroup in a Group

Let H be a subgroup of a group G, then the number of distinct right (or left) cosets of H in G is called the index of H in G and is denoted by [G : H] or $i_G(H)$.

Theorem 21 (Lagrange's Theorem). The order of each subgroup of a finite group is a divisor of the order

of the group.

Proof. Let G be a finite group of order n and let H be a subgroup of G such that o(H) = m. Assume that $h_1, h_2, ..., h_m$ are the m elements of H. If $a \in G$ then Ha is a right coset of H in G and

$Ha = \{h_1a, h_2a, ..., h_ma\}$.

Ha has m distinct members, since $h_ia = h_ja \Rightarrow h_i = h_j$. So, each right coset of H in G has m distinct members. Also, two distinct right cosets of H in G are disjoint. Since G is finite so the number of distinct right cosets of H in G will be finite, say, equal to s. The union of all these s distinct right cosets of H in G will constitute G. Thus if $Ha_1, Ha_2, ..., Ha_s$ are the s distinct right cosets of H in G, then

$G = Ha_1 \cup Ha_2 \cup ..... \cup Ha_s$

$\Rightarrow |G| = |Ha_1| + |Ha_2| + ... + |Ha_s|$ [$\because$ two distinct right cosets are mutually disjoint]

$\Rightarrow$ number of elements in G

= number of elements in Ha_1 + number of elements in Ha_2 + ... + number of elements in Ha_s

$\Rightarrow o(G) = m + m + ... + m$ (s times) $= ms$

$\Rightarrow n = ms$

$\Rightarrow s = \frac{n}{m} \Rightarrow$ m is a divisor of n

$\Rightarrow$ o(H) is a divisor of o(G).

Hence the theorem.

Remark 18. The converse of Lagrange's theorem is not necessarily true.

Remark 19. Since s is the index of H in G and $m = \frac{n}{s} \Rightarrow$ s is a divisor of n.

Thus, the index of every subgroup of a finite group is a divisor of the order of the group.

Remark 20. If H is a subgroup of a finite group G, then the index of H in G = the number of distinct right (or left) cosets of H in G

$= s = \frac{n}{m}$

$= \frac{o(G)}{o(H)}$

Remark 21. The order of every element of a finite group is a divisor of the order of the group.

Remark 22. If G is a finite group of order n and $a \in G$, then $a^n = e$.

Theorem 23. Every group of prime order is cyclic.

Proof. Let G be a finite group of order p, where p is a prime number i.e., $p \neq 0$, $p \neq \pm 1$ and the only divisors of p are ± 1 and $\pm p$.

Since G is a group of prime order so G must have atleast 2 elements ($\because p \geq 2$). Then there must exists an element $a \in G$ such that $a \neq e$(identity element).

Since, $a \neq e \Rightarrow o(a) \geq 2$ [$\because$ identity is the only element whose order is 1]

Let o(a) = m. Also suppose that H be any cyclic subgroup of G generated by a, then o(H) = o(a) = m.

By Lagrange's theorem, m must divides p. But p is prime and $m \geq 2 \Rightarrow m = p$ and then H = G. Since H

is cyclic therefore G must be a cyclic group generated by a. **Hence proved.**

8.20 Normal Subgroup

Definition : Let G be a group and H be any subgroup of G, then H is said to be a normal subgroup of G if for every $x \in G$ and $h \in H$,

$$x\ h\ x^{-1} \in H.$$

Symbolically, we write $H \nabla G$.

Every group G has atleast two normal subgroups, namely G itself and the subgroup {e} i.e., having identity element alone. These two are called **improper normal subgroups**. The normal subgroup other than these two is called a **proper normal subgroup**.

The groups having only improper normal subgroups are called **simple groups.** In other words, a group having no proper normal subgroups is called a **simple group.**

Remark 23. Every group of prime order is simple because by Lagrange's theorem such a group has no proper normal subgroups.

Theorem 23. Every subgroup of an abelian group is a normal subgroup.

Proof. Let H be a subgroup of an abelian group G. Also let $x \in G$ and $h \in H$, then

$x\ h\ x^{-1} = x(hx^{-1}) = x(x^{-1}h)$ [$\because$ G is abelian]

$= (x\ x^{-1})h = eh$

$= h \in H$

$\Rightarrow x\ h\ x^{-1} \in H$

Hence, H is normal in G. **Hence proved.**

Remark 24. Since every cyclic group is abelian so the above theorem can also be stated as, Every subgroup of a cyclic group is a normal subgroup.

Theorem 24. A subgroup H of a group G is normal iff $x\ H\ x^{-1} = H, \forall\ x \in G$.

Proof. Here, $x\ H\ x^{-1} = \{x\ h\ x^{-1} : h \in H, x \in G\}$

First suppose that H is normal in G then

$x \in G, h \in H \Rightarrow x\ h\ x^{-1} \in H$

$\Rightarrow$ each element of $x\ H\ x^{-1}$ is the element of H

$\Rightarrow x\ H\ x^{-1} \subseteq H$ .....(1), $\forall\ x \in G$

Also, $x \in G \Rightarrow x^{-1} \in G$

$\therefore$ (1) $\Rightarrow x^{-1}H\ (x^{-1})^{-1} \subseteq H$[replacing x by x^{-1} in (1)]

$\Rightarrow x^{-1}\ H\ x \subseteq H$

$\Rightarrow x(x^{-1}\ H\ x)x^{-1} \subseteq x\ H\ x^{-1} \Rightarrow (xx^{-1})\ H(xx^{-1}) \subseteq x\ H\ x^{-1}$

$\Rightarrow e\ H\ e \subseteq x\ H\ x^{-1} \Rightarrow H \subseteq x\ H\ x^{-1}$ .....(2), $\forall\ x \in G$

$\therefore$ (1) and (2) $\Rightarrow x\ H\ x^{-1} = H, \forall\ x \in G$.

Conversely, Let $x\ H\ x^{-1} = H, \forall\ x \in G$

$\Rightarrow x\ H\ x^{-1} \subseteq H$

$\Rightarrow$ $x\,h\,x^{-1} \in H$; $x \in G$, $h \in H$

$\Rightarrow$ H is normal in G.

Hence the theorem.

Theorem 25. If f is a homomorphism of a group G into a group G' with kernel K, then K is a normal subgroup of G.

Proof. Let e and e' be the identities in G and G' respectively and let K be the kernel of f i.e.,

$K = \{x \in G \mid f(x) = e'\}$

First, we shall show that K is a subgroup of G. Since $f(e) = e' \Rightarrow e \in K \Rightarrow$ K is non–empty.

Also, $x \in K \Rightarrow x \in G$ (by definition of K)

$\Rightarrow K \subseteq G$ i.e., K is a subset of G.

Further, let $a, b \in K \Rightarrow f(a) = e'$ and $f(b) = e'$.

Now, $f(ab^{-1}) = f(a)\, f(b^{-1})$ [$\because$ f is a homomorphism]

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

$= e'$

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

$\therefore$ K is a subgroup of G.

Now, we shall show that K is normal in G.

Let $x \in G$ and $k \in K \Rightarrow f(k) = e'$

Now, $f(xkx^{-1}) = f(x)\, f(k)\, f(x^{-1})$ [$\because$ f is a homomorphism]

$= f(x)\, e'\, f(x^{-1}) = f(x)\, f(x^{-1})$

$= f(xx^{-1}) = f(e)$

$= e'$

$\Rightarrow xkx^{-1} \in K$ [by definition of K]

$\therefore$ K is a normal subgroup of G. **Hence proved.**

Theorem 26. Let N be a normal subgroup of a group G then show that every left coset is also a right coset.

Proof. Let N be a normal subgroup of G. Then for $n \in N$, $g \in G$, we have

$gng^{-1} \in N$

$\Rightarrow gng^{-1} = n'$, for some $n' \in N$

$\Rightarrow (gng^{-1})\, g = n'g \Rightarrow gn(g^{-1}g) = n'g \Rightarrow gn(e) = n'g$

$\Rightarrow gn = n'g$, $\forall$ n, $n' \in N$

$\Rightarrow \{gn \mid n \in N\} = \{n'g \mid n' \in N\}$

$\Rightarrow gN = Ng$ [by definition of left and right coset]

Hence every left coset is also a right coset. **Hence proved.**

Theorem 27. Let N be a normal subgroup of a group G and let R be the following relation on G :

a R b iff $a^{-1}b \in N$.

Then,(a)R is a congruence relation on G.

(b) N is the equivalence class [e] relative to R, where e is the identity of G. **[MREC 2001]**

Proof. Given, $aRb \Leftrightarrow a^{-1}b \in N$

(a) **Reflexive :** Since $e = a^{-1}a \in N$ [$\because$ N is a subgroup]

$\Rightarrow$ aRa

$\therefore$ R is reflexive.

Symmetric : Let $aRb \Rightarrow a^{-1}b \in N$

$\Rightarrow (a^{-1}b)^{-1} \in N$

$\Rightarrow b^{-1}(a^{-1})^{-1} = b^{-1}a \in N \Rightarrow bRa$

$\therefore$ R is symmetric

Transitive : Let aRb and bRc then

$a^{-1}b \in N$ and $b^{-1}c \in N$

Now, $a^{-1}b \in N, b^{-1}c \in N \Rightarrow (a^{-1}b)(b^{-1}c) \in N$ [by closure property]

$\Rightarrow a^{-1}(bb^{-1})c \in N$

$\Rightarrow a^{-1}(e)c \in N$

$\Rightarrow a^{-1}c \in N$

$\Rightarrow$ aRc

$\therefore$ R is transitive.

Thus, R is an equivalence relation on G.

Further, let aRb and cRd, a, b, c, d $\in$ G, then $a^{-1}b \in N$ and $c^{-1}d \in N$

Let $a^{-1}b = n_1$ and $c^{-1}d = n_2$ for some $n_1, n_2 \in N$

Now, consider $(ac)^{-1}bd = (c^{-1}a^{-1})bd = c^{-1}(a^{-1}b)d$

$= c^{-1}n_1 d$

$= c^{-1}d\,n'$ [$\because$ N is normal so $n_1 d = n'd$, for some $n' \in N$]

$= n_2 n' \in N$ [$n_2 \in N, n' \in N \Rightarrow n_2 n' \in N$]

$\Rightarrow (ac)^{-1}bd \in N$

$\Rightarrow$ ac R bd

Hence, R is a congruence relation on G.

(b) Let $x \in N \Rightarrow x^{-1}e = x^{-1} \in N$ ($\because$ N is a subgroup)

Now $x^{-1}e \in N \Rightarrow x\,R\,e \Rightarrow x \in [e]$

$\Rightarrow N \subseteq [e]$ .....(1)

Again, let $x \in [e] \Rightarrow x\,R\,e \Rightarrow x^{-1}e = x^{-1} \in N$

$\Rightarrow (x^{-1})^{-1} = x \in N$ ($\because$ N is a subgroup)

$\Rightarrow [e] \subseteq N$ .....(2)

$\therefore$ (1) and (2) $\Rightarrow N = [e]$

Hence the theorem.

Theorem 28. Let R be a congruence relation on a group G, and let H = [e], the equivalence class containing

the identity. Then H is a normal subgroup of G and for each $a \in G$, $[a] = aH = Ha$.

Proof. First we shall show that H is a subgroup of G.

Since $e \in [e] \Rightarrow e \in H$ $[\because H = [e]]$

$\therefore$ H is non–empty.

Also, let $h \in H \Rightarrow h \in [e] \Rightarrow h \, R \, e$

$\Rightarrow h \in G$ $[\because$ R is a relation on G$]$

$\therefore H \subseteq G$ i.e., H is a subset of G.

Further, let $a, b \in H$ then $a \in [e]$ and $b \in [e]$

$\Rightarrow [a] = [e]$ and $[b] = [e]$ (by property of equivalence classes)

Now, $[ab^{-1}] = [a]\,[b^{-1}] = [a]\,[b]^{-1} = [e]\,[e]^{-1} = [e]$

Since, $ab^{-1} \in [ab^{-1}] \Rightarrow ab^{-1} \in [e] \Rightarrow ab^{-1} \in H$

$\therefore$ H is a subgroup of G.

Again, let $x \in G$ and $h \in H$ then $[h] = [e]$ $[\because h \in H \Rightarrow h \in [e] \Rightarrow [h] = [e]$

Now, $[x\,h\,x^{-1}] = [x]\,[h]\,[x^{-1}] = [x]\,[e]\,[x^{-1}]$

$= [x]\,[x^{-1}] = [xx^{-1}] = [e]$

$\Rightarrow x\,h\,x^{-1} \in [e] \Rightarrow x\,h\,x^{-1} \in H$

Hence, H is a normal subgroup of G.

Finally, let $b \in [a] \Rightarrow [b] = [a] \Rightarrow [a]^{-1}\,[b] = [a]^{-1}[a]$

$\Rightarrow [a^{-1}]\,[b] = [e] \Rightarrow [a^{-1}b] = [e] \Rightarrow a^{-1}b \in [e]$

$\Rightarrow a^{-1}b \in H$ $[\because H = [e]]$

$\Rightarrow a(a^{-1}b) \in aH \Rightarrow (aa^{-1})b \in aH \Rightarrow eb \in aH$

$\Rightarrow b \in aH$

$\therefore b \in [a] \Rightarrow b \in aH$

$\Rightarrow [a] \subseteq aH$ .....(1)

Again, let $b \in aH \Rightarrow a^{-1}b \in a^{-1}(aH) = (a^{-1}a)\,H = eH = H$

$\Rightarrow a^{-1}b \in H \Rightarrow a^{-1}b \in [e] = [a^{-1}b] = [e]$

$\Rightarrow [a^{-1}]\,[b] = [e]$

$\Rightarrow [a]\,[a^{-1}]\,[b] = [a]\,[e] = [a]$

$\Rightarrow [aa^{-1}]\,[b] = [a] \Rightarrow [e]\,[b] = [a]$

$\Rightarrow [b] = [a] \Rightarrow b \in [a]$

$\therefore b \in aH \Rightarrow b \in [a]$

$\Rightarrow aH \subseteq [a]$ .....(2)

(1) and (2) $\Rightarrow [a] = aH$

Similarly, we can prove that $[a] = Ha$.

Hence, $[a] = aH = Ha$. **Hence proved.**

8.21 Quotient Group

Definition : Let G be a group and H be a normal subgroup of G, then the set $\frac{G}{H}$ of all right (or left) cosets of H in G i.e., $\frac{G}{H} = \{Ha \mid a \in G\}$ is a group for the operation multiplication of cosets defined by Ha Hb = Hab. This group $\frac{G}{H}$ is called the **quotient group** or **factor group** of G by H.

The identity element of the quotient group $\frac{G}{H}$ is H.

Example 79. Let G be a group and N is a normal subgroup of G. Let f be a mapping from G to $\frac{G}{N}$ defined by

$f(x) = Nx, \forall x \in G$

Then show that f is a homomorphism of G onto $\frac{G}{N}$ and kernel f = N.

Solution. Given $f : G \to \frac{G}{N}$ such that $f(x) = Nx, \forall x \in G$. We shall show that (i) f is an onto function, (ii) f is a homomorphism, and (iii) kernel f = N.

(i) f is onto : Let $b \in \frac{G}{N} \Rightarrow b = Na$ for some $a \in G$

$\left[\because \frac{G}{N} = \{Na : a \in G\}\right]$

Now, $f(a) = Na = b, a \in G$

$\therefore$ each element of $\frac{G}{N}$ has its preimage in G so f is onto.

(ii) f is a homomorphism : Let $a, b \in G$, then

$f(ab) = Nab = Na\ Nb$ [$\because$ Ha Hb = Hab]

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

$\therefore$ f is a homomorphism from G onto $\frac{G}{N}$.

(iii) Kernel f = N : Let K be the kernel of f. Since, the identity of $\frac{G}{N}$ is N so,

$K = \{y \in G : f(y) = N\}$

Let $k \in K \Rightarrow f(k) = N \Rightarrow Nk = N$ [by definition of f]

$\Rightarrow k \in N$ [$\because$ Hh = H $\Rightarrow$ h $\in$ H]

$\therefore K \subseteq N$ .....(1)

Again, let $n \in N$ then Nn = N [$\because$ h $\in$ H $\Rightarrow$ Hh = H]

We have, f(n) = Nn = N

$\Rightarrow n \in K$ [$\because$ f(x) = N $\Rightarrow$ x $\in$ K]

$\therefore$ $n \in N \Rightarrow n \in K$

$\Rightarrow N \subseteq K$ .....(2)

$\therefore$ (1) and (2) $\Rightarrow K = N$ i.e., Kernel f = N.

ILLUSTRATIVE EXAMPLES

Example 80. Let G be an abelian group and N is a subgroup of G. Show that $\frac{G}{N}$ is an abelian group.

Solution. Since, every subgroup of an abelian group is normal. So N must be normal in G. Then $\frac{G}{N}$ is defined and is a group for the operation coset multiplication.

Now, let Na, Nb $\in \frac{G}{N}$, then

NaNb = Nab = Nba [$\because$ a, b $\in$ G $\Rightarrow$ ab = ba]

= Nb Na

$\therefore$ $\frac{G}{N}$ is abelian.

Example 81. Let G be a group and let H = {x | x $\in$ G and xa = ax, $\forall$ a $\in$ G}. Show that H is a normal subgroup of G.

Solution. First we shall show that H is a subgroup of G.

Since, ae = ea $\Rightarrow$ e $\in$ H $\Rightarrow$ H is non–empty.

Let $x \in H \Rightarrow x \in G \Rightarrow H \subseteq G$

Also let x, y $\in$ H $\Rightarrow$ ax = xa and ay = ya, $\forall$ a $\in$ G .....(1)

$\Rightarrow x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1}$ and $y^{-1}(ay)y^{-1} = y^{-1}(ya)y^{-1}$

$\Rightarrow (x^{-1}a)(xx^{-1}) = (x^{-1}x)(ax^{-1})$ and $(y^{-1}a)(yy^{-1}) = (y^{-1}y)(ay^{-1})$

$\Rightarrow (x^{-1}a)e = e(ax^{-1})$ and $(y^{-1}a)e = e(ay^{-1})$

$\Rightarrow x^{-1}a = ax^{-1}$ and $y^{-1}a = ay^{-1}$.....(2)

Now, $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1})$ [using (2)]

$= (xa)y^{-1} = (ax)y^{-1}$ [using (1)]

$= a(xy^{-1})$ [by definition of H]

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

$\therefore$ H is a subgroup of G.

Now, we show that H is normal in G.

Let x $\in$ G and h $\in$ H $\Rightarrow$ ah = ha, $\forall$ a $\in$ G .....(3)

Consider $(x\ h\ x^{-1})a = (x\ h)(x^{-1}a) = (x\ h)(ax^{-1})$ [using (2)]

$= x(ha)x^{-1} = x(ah)x^{-1}$ [using (3)]

$= (xa)hx^{-1} = (ax)\ hx^{-1}$ [using (1)]

$= a(x\ h\ x^{-1})$ [by definition of H]

$\Rightarrow x\ h\ x^{-1} \in H$

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

Example 82. Show that the set $U_9 = \{1\ 2, 3, 5, 7, 8\}$ with an operation defined as multiplication modulo 9 i.e.,

$a \cdot b = 9m + c$

for all $a, b \in U_9$ and $c \in U_9$ is a cyclic group.

Find the order of various elements and subgroups generated by them. **[MNIT 2002]**

Solution. The composition table of U_9 for the given operation can be constructed as

•	1	2	4	5	7	8	(Top Row)
[1]	1	2	4	5	7	8	(First Row)
2	2	4	8	1	5	7	
4	4	8	7	2	1	5	
5	5	1	2	7	8	4	
7	7	5	1	8	4	2	
8	8	7	5	3	2	1	

Closure : All the entries in the table are the elements of U_9 so U_9 is closed.

Associativity : Since, multiplication of real numbers is always associative so associativity holds in U_9.

Identity element : Since, first row of the table, headed by 1, coincides with the top row so 1 is the identity element in U_9.

Existence of Inverse : From the table,

$1 \cdot 1 = 1 \Rightarrow (1)^{-1} = 1$; $2 \cdot 5 = 1 \Rightarrow (2)^{-1} = 5$

$4 \cdot 7 = 1 \Rightarrow (4)^{-1} = 7$; $5 \cdot 2 = 1 \Rightarrow (5)^{-1} = 2$

$7 \cdot 4 = 1 \Rightarrow (7)^{-1} = 4$; $8 \cdot 8 = 1 \Rightarrow (8)^{-1} = 8$

So each element of U_9 has its inverse in U_9.

Thus $(U_9, \cdot)$ is a group.

Now to prove that U_9 is a cyclic group, it is sufficient to show that there exists an element in U_9 whose order is same as that of U_9 (i.e., 6).

Since,

$1^1 = 1 \Rightarrow o(1) = 1$; $2^6 = 1 \Rightarrow o(2) = 6$

$4^3 = 1 \Rightarrow o(4) = 3$; $5^6 = 1 \Rightarrow o(5) = 6$

$7^3 = 1 \Rightarrow o(7) = 3$; $8^2 = 1 \Rightarrow o(8) = 2$

So, $o(2) = o(5) = o(U_9) = 6$

Thus, U_9 is a cyclic group with 2 generators 2 and 5.

Further, the subgroups generated by the elements of U_9 are –

Generated by $1 \rightarrow \{1\}$;

Generated by $2 \rightarrow \{1, 2, 4, 5, 7, 8\} = U_9$;

Generated by $4 \rightarrow \{1, 4, 7\}$

Generated by $5 \rightarrow \{1, 2, 4, 5, 7, 8\} = U_9$

Generated by $7 \rightarrow \{1, 4, 7\}$;

Generated by $8 \rightarrow \{1, 8\}$.

Example 83. Show that every abelian group is not necessarily cyclic.

Solution. To prove the given statement we can give a counter example.

Let G = {A, B, C, D}, where

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

Now, it can be easily verified that G is an abelian group for the composition matrix multiplication [Refer Example 31].

Further, the identity element in G is A.

Now, $A^1 = A \Rightarrow 0(A) = 1$; $B^2 = A \Rightarrow 0(B) = 2$

$C^2 = A \Rightarrow 0(C) = 2$; $D^2 = A \Rightarrow 0(D) = 2$

So, we see that there does not exists any element in G whose order is equal to the order of G (i.e. 4).

Hence, G is not a cyclic group.

Example 84. Let H be a subgroup of index 2 in a group G. Show that H is a normal subgroup of G.

Solution. Let H be a subgroup of index 2 in G. Then the number of distinct right (left) cosets of H in G is 2. Let $a \in G$ then if $a \in H$ we have

$aH = H = Ha$. $[\because\ h \in H \Rightarrow Hh = H = hH]$

If $a \notin H$, then the right coset Ha is distinct from H($\because a \in Ha$) and the left coset aH is distinct from H($\because a \in aH$). But index of H is 2 so the number of distinct right (left) cosets in right (left) coset decomposition of G will be 2. Thus, the cosets H, Ha and aH are such that $G = H \cup Ha = H \cup aH$.

Since H and Ha are distinct and also H and aH are distinct so we must have Ha = aH. Hence, we have $aH = Ha, \forall\ a \in G$.

Therefore, H is a normal subgroup of G.

Example 85. Let R be a congruence relation on a group (G, *) then the quotient set $\frac{G}{R}$ with operation defined by $[a] \circledast [b] = [a * b]$ is a group.

Solution. Here, $\frac{G}{R} = \{[a] : a \in G\}$

Closure : Let $[a], [b] \in \frac{G}{R}$, then

$[a] \circledast [b] = [a * b] \in \frac{G}{R}$ $\left[\because\ a, b \in G \Rightarrow a * b \in G \Rightarrow [a * b] \in \frac{G}{R}\right]$

$\therefore$ $\frac{G}{R}$ is closed.

Associativity : Let $[a], [b], [c] \in \frac{G}{R}$, then

$([a] \circledast [b]) \circledast [c] = [a * b] \circledast [c]$

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

$= [a * (b * c)]$[$\because$ a, b, c $\in$ G and associativity holds in G]

$= [a] \circledast [b * c]$

$= [a] \circledast ([b] \circledast [c])$

$\therefore$ Associativity holds in $\frac{G}{R}$.

Identity element : Since $e \in G \Rightarrow [e] \in \frac{G}{R}$.

Let $[a] \in \frac{G}{R}$, then

$[a] \circledast [e] = [a * e] = [a]$ [$\because$ e is identity in G)

and $[e] \circledast [a] = [e * a] = [a]$

$\therefore$ $[a] \circledast [e] = [a] = [e] \circledast [a]$

$\Rightarrow$ [e] is the identity in $\frac{G}{R}$.

Existence of Inverse : Let $a \in G \Rightarrow a^{-1} \in G \Rightarrow [a^{-1}] \in \frac{G}{R}$

Let $[a] \in \frac{G}{R}$, then

$[a] \circledast [a^{-1}] = [a * a^{-1}] = [e]$

and, $[a^{-1}] \circledast [a] = [a^{-1} * a] = [e]$

$\therefore$ $[a] \circledast [a^{-1}] = [e] = [a^{-1}] \circledast [a]$

$\Rightarrow$ $[a^{-1}]$ is the inverse of [a].

Hence, each element of $\frac{G}{R}$ has its inverse in $\frac{G}{R}$.

Therefore, $\frac{G}{R}$ is a group for the operation $\circledast$.

Example 86. Find the quotient group $\frac{G}{N}$ where $G = (\{1, -1, i, -i\}, \cdot)$ and $N = (\{1, -1\}, \cdot)$.

Solution. Since G is an abelian group and N is a subgroup of G so N must be normal in G.

Now, $\frac{G}{N} = \{Na : a \in G\}$

$\Rightarrow$ $\frac{G}{N} = \{N\cdot 1, N\cdot(-1), N\cdot i, N\cdot(-i)\}$

Also, $N\cdot 1 = \{1, -1\} = N\cdot(-1) = N$

$Ni = \{1\cdot i, -1\cdot i\} = \{i, -i\} = N(-i)$

$\therefore$ $\frac{G}{N} = \{N, Ni\}$

Now, the composition table of $\frac{G}{N}$ is as given below

•	N	Ni	(Top Row)
[N]	N	Ni	(First Row)
Ni	Ni	N	

Closure : Since every element of the table is the element of $\frac{G}{N}$ so $\frac{G}{N}$ is closed.

Associativity : Since multiplication of cosets is associative so associativity holds in $\frac{G}{N}$.

Identity element : The first row of the table, headed by N, coincides with the top row so N is the identity in $\frac{G}{N}$.

Existence of Inverse : From the table,

$N \cdot N = N \Rightarrow N^{-1} = N$; $Ni \cdot Ni = N \Rightarrow (Ni)^{-1} = Ni$

$\therefore$ each element of $\frac{G}{N}$ has its inverse in $\frac{G}{N}$.

Thus, $\frac{G}{N}$ is the required quotient group.

Example 87. Let P_3 be the symmetric group under composition operation and $P_3 = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ where, $p_1 = (1)\ (2)\ (3)$; $p_2 = (1, 2\ 3)$; $p_3 = (1\ 3\ 2)$; $p_4 = (1)\ (2\ 3)$; $p_5 = (1\ 3)\ (2)$; $p_6 = (1\ 2)\ (3)$.

Then show that $H = \{p_1, p_5\}$ is a subgroup of G and also compute all the distinct left cosets of H in G. Also show that H is not a normal subgroup of G.

Solution. It is obvious that H is a non–empty subset of P_3.

Also $p_1^{-1} = p_1$ and $p_5^{-1} = p_5$, then

$p_1, p_5 \in H \Rightarrow p_1 \circ p_5^{-1} = p_1 \circ p_5 = p_5 \in H$,

$p_5, p_1 \in H \Rightarrow p_5 \circ p_1^{-1} = p_5 \circ p_5 = p_5 \in H$,

$p_1, p_1 \in H \Rightarrow p_1 \circ p_1^{-1} = p_1 \circ p_1 = p_1 \in H$,

and $p_5, p_5 \in H \Rightarrow p_5 \circ p_5^{-1} = p_5 \circ p_5 = p_1 \in H$.

So for every $a, b \in H$ we have $ab^{-1} \in H$.

Thus, H is a subgroup of P_3.

Further, the left cosets of H in G are given as

$p_1H = H$ ($\because$ p_1 is the identity element)

$p_2H = \{p_2 \circ p_1, p_2 \circ p_5\} = \{p_2, p_4\}$

$p_3H = \{p_3 \circ p_1, p_3 \circ p_5\} = \{p_3, p_6\}$

$p_4H = \{p_4 \circ p_1, p_4 \circ p_5\} = \{p_4, p_2\} = p_2H$

$p_5H = \{p_5 \circ p_1, p_5 \circ p_5\} = \{p_5, p_1\} = H$

and, $p_6H = \{p_6 \circ p_1, p_6 \circ p_5\} = \{p_6, p_3\} = p_3H$

Thus, there are 3 distinct left cosets of H in G i.e., H, p_2H, p_3H.

Since, $Hp_2 = \{p_1 \circ p_2, p_5 \circ p_2\} = \{p_2, p_6\}$

$\Rightarrow p_2H \neq Hp_2$

Thus, H is not a normal subgroup of P_3.

Example 88. Show that every subgroup of a cyclic group is cyclic.

Solution. Let G = [a] is a cyclic group generated by a and H be a subgroup of G.

If H = G or {e} then H must be cyclic. So let H be a proper subgroup of G. Now, the elements of H are also integral powers of a i.e., if $a^r \in H$ then $a^{-r} \in H$. Therefore, H contains elements that have positive as well as negative integral powers of a. Let m be the least positive integer such that $a^m \in H$. Now, we shall show that $H = [a^m]$ i.e., H is a cyclic group generated by a^m.

Let $a^t \in H$ then by Euclidean algorithm, there exists integer q and s such that

$$t = m q + s, \ 0 \leq s < m.$$

Now, $a^m \in H \Rightarrow (a^m)^q \in H$ [by closure property]

$\Rightarrow a^{mq} \in H \Rightarrow (a^{mq})^{-1} \in H$

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

$\therefore a^t \in H, a^{-mq} \in H \Rightarrow a^t a^{-mq} = a^{t-mq} \in H$

$\Rightarrow a^s \in H$

Since, m is the least positive integer such that $a^m \in H$ and also $0 \leq s < m$ so s must be 0. Thus t = mq and

$$a^t = a^{mq} = (a^m)^q$$

Therefore, every element $a^t \in H$ can be expressed as an integral power of a^m.

Hence, $H = [a^m]$ is a cyclic subgroup of G.

Example 89. Show that the intersection of any two normal subgroups of a group is a normal subgroup.

Solution. Let H_1 and H_2 be two normal subgroups of a group G. Since H_1 and H_2 are subgroups of G, so $H_1 \cap H_2$ is also a subgroup of G [Refer example 14].

Now, let $x \in G$ and $h \in H_1 \cap H_2$, then $h \in H_1$, and $h \in H_2$.

$\therefore x \in G, h \in H_1 \Rightarrow x h x^{-1} \in H_1$ [$\because H_1$ is normal in G]

also, $x \in G, h \in H_2 \Rightarrow x h x^{-1} \in H_2$ [$\because H_2$ is normal in G]

$\therefore x h x^{-1} \in H_1, x h x^{-1} \in H_2 \Rightarrow x h x^{-1} \in H_1 \cap H_2$

Thus, $x \in G, h \in H_1 \cap H_2 \Rightarrow x h x^{-1} \in H_1 \cap H_2, \forall x \in G$

Hence, $H_1 \cap H_2$ is a normal subgroup of G.

Example 90. Let P_n be the symmetric group on n symbols. Show that the alternating set A_n is a normal subgroup of P_n.

Solution. We know that the alternating set A_n (set of even permutations) is a subgroup of P_n.

Let $\alpha \in P_n$ and $\beta \in A_n$, then β must be an even permutation while α may be odd or even.

If α is odd then α^{-1} is also odd. Now $\alpha\beta$ is odd and then $\alpha \beta \alpha^{-1}$ is even i.e., $\alpha \beta \alpha^{-1} \in A_n$.

If α is even then α^{-1} is also even. Now$\alpha\beta$ is even and then $\alpha \beta \alpha^{-1}$ is even i.e., $\alpha \beta \alpha^{-1} \in A_n$.

Thus $\alpha \in P_n, \beta \in A_n \Rightarrow \alpha \beta \alpha^{-1} \in A_n$.

Hence, A_n is normal in P_n.

Example 91. Let G_1 and G_2 be groups. Let $f : G_1 \times G_2 \to G_2$ be the homomorphism from $G_1 \times G_2$ onto G_2 defined as $f(g_1, g_2) = g_2$. Compute kerf.

Solution. Let e_1 and e_2 be the identities in G_1 and G_2 respectively. Then $(g_1, e_2) \in G_1 \times G_2$, $\forall\ g_1 \in G_1$.

Now, $f(g_1, e_2) = e_2$, $\forall\ g_1 \in G_1$

$\therefore$ Ker $f = \{(g_1, e_2) \mid g_1 \in G_1\}$.

Example 92. If H and K are two normal subgroups of G such that $H \cap K = \{e\}$, then show that every element of H commutes with every element of K.

Solution. Let $h \in H$ and $k \in K$ then we have to show that $hk = kh$.

Consider the element $hkh^{-1}k^{-1}$.

Since $h \in H \Rightarrow h^{-1} \in H$ and also $k \in K \Rightarrow k \in G$

Now, $k \in G, h^{-1} \in H \Rightarrow kh^{-1}k^{-1} \in H$ [$\because$ H is normal in G]

$\Rightarrow hkh^{-1}k^{-1} \in H$ [by closure property] .....(1)

Similarly, $h \in H \Rightarrow h \in G$ and $k \in K \Rightarrow k^{-1} \in K$

$\therefore\ h \in G, k \in K \Rightarrow hkh^{-1} \in K$ [$\because$ K is normal in G]

$\Rightarrow hkh^{-1}k^{-1} \in K$ [by closure property] .....(2)

$\therefore$ (1) and (2) $\Rightarrow hkh^{-1}k^{-1} \in H \cap K$

$\Rightarrow hkh^{-1}k^{-1} = e$ [$\because H \cap K = \{e\}$]

$\Rightarrow (hkh^{-1}k^{-1})k = ek$

$\Rightarrow hkh^{-1}(k^{-1}k) = k \Rightarrow hkh^{-1}e = k$

$\Rightarrow (hkh^{-1})h = kh \Rightarrow hk(h^{-1}h) = kh$

$\Rightarrow hke = kh$

or $hk = kh$.

Hence the result.

Example 93. If G is a finite group and H is a normal subgroup of G, then show that $o\left(\frac{G}{H}\right) = \frac{o(G)}{o(H)}$.

Solution. Since,

$$o\left(\frac{G}{H}\right) = \text{number of distinct right cosets of H in G}$$

$$= \frac{\text{number of elements in G}}{\text{number of elements in H}}$$

$$= \frac{o(G)}{o(H)}.$$

Example 94. Let f be a homomorphism from a group G_1 onto a group G_2 and let G_2 is abelian. Show that Ker(f) contains all elements of G_1 of the form $aba^{-1}b^{-1}$, where $a, b \in G_1$.

Solution. Let e_1 and e_2 be the identities in G_1 and G_2 respectively. Then $f(e_1) = e_2$. Also, Ker(f) = $\{x \mid f(x) = e_2$ and $x \in G\}$.

Now, $f(aba^{-1}b^{-1}) = f(a)\ f(b)\ f(a^{-1})\ f(b^{-1})$ [$\because$ f is a homomorphism]

$= f(b)\ f(a)\ f(a^{-1})\ f(b^{-1})$ [$\because$ G_2 is abelian]

$= f(b)\ f(aa^{-1})\ f(b^{-1}) = f(b)\ f(e_1)\ f(b^{-1})$

$= f(b)\ f(b^{-1}) = f(bb^{-1}) = f(e_1)$

$= e_2$

$\therefore\ aba^{-1}b^{-1} \in \text{Ker}\ (f)$.

Example 95. Let H be any subgroup of a group G. Prove that $aH = bH$ iff $Ha^{-1} = Hb^{-1}$, $\forall\ a, b \in G$.

Solution. Let $aH = bH$, then $a, b \in G \Rightarrow a^{-1}, b^{-1} \in G$.

Now, $aH = bH \Rightarrow a^{-1}(aH) = a^{-1}(bH) = (a^{-1}a)H = (a^{-1}b)H$

$\Rightarrow eH = a^{-1}bH \Rightarrow H = a^{-1}bH$

$\Rightarrow a^{-1}b \in H$ [$\because$ $hH = H \Rightarrow h \in H$]

$\Rightarrow Ha^{-1}b = H$ [$\because$ $h \in H \Rightarrow Hh = H$]

$\Rightarrow Ha^{-1}bb^{-1} = Hb^{-1}$

$\Rightarrow Ha^{-1} = Hb^{-1}$

Conversely : Let $Ha^{-1} = Hb^{-1}$

$\Rightarrow (Ha^{-1})b = (Hb^{-1})b = H(b^{-1}b) = He = H$

$\Rightarrow Ha^{-1}b = H \Rightarrow a^{-1}b \in H$ [$\because$ $Hh = H \Rightarrow h \in H$]

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

$\Rightarrow bH = aH$.

Example 96. Let G be a finite group and H be a subgroup of G such that $x^2 \in H$ for all $x \in G$. Show that H is a normal subgroup of G.

Solution. Let $x \in G$ and $h \in H$ then $xh \in G$ [$\because$ $H \subseteq G$]

$\Rightarrow (xh)^2 \in H$.

Also, $h \in H \Rightarrow h^{-1} \in H$ and $x \in G \Rightarrow x^{-1} \in G \Rightarrow x^{-2} \in H$

$\therefore\ h^{-1} \in H, x^{-2} \in H \Rightarrow h^{-1}x^{-2} \in H$

Now, $(xh)^2 \in H, h^{-1}x^{-2} \in H$

$\Rightarrow (xh)^2 (h^{-1}x^{-2}) \in H$[by closure property]

$\Rightarrow (xh)\ (xh)\ (h^{-1}\ x^{-2}) = x(hx)\ (hh^{-1})\ x^{-2} \in H$

$\Rightarrow (xhx)x^{-2} \in H \Rightarrow xh(xx^{-1})\ x^{-1} \in H$

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

$\therefore\ x \in G, h \in H \Rightarrow x\ h\ x^{-1} \in H$

Thus, H is a normal subgroup of G.

Example 97. Let G be a group and let $a \in G$ with $o(a) = n$, $n \in Z$. If $k \in Z$ and $a^k = e$, then prove that n divides k i.e., $n \mid k$.

Solution. Given $o(a) = n \Rightarrow$ n is the least positive integer such that $a^n = e$.

Now, $a^k = e$ (given), $k \in Z$.

By division algorithm there exist $q, r \in Z$ such that

$k = nq + r,\ 0 \le r < n$

$\Rightarrow a^k = a^{nq+r} = a^{nq}\, a^r = (a^n)^q\, a^r = e^q a^r = a^r$

$\Rightarrow a^k = a^r \Rightarrow a^r = e \qquad (\because a^k = e)$

Now, $0 \le r < n \Rightarrow a^r = e$ is only possible when $r = 0$.

Then, $k = nq,\ q \in Z$

$\Rightarrow q = \frac{k}{n}$

$\Rightarrow$ n divides k i.e., n|k.

EXERCISE 8.4

1. Show that the group $G = (\{1, 2, 3, 4\}, \times_5)$ is cyclic. How many generators are there ?
   [**Ans.** 2 and 3]
2. Let G be the group of all permutations of degree 3 on three symbols 1, 2, 3. Then $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where $f_1 = (1)$, $f_2 = (12)$, $f_3 = (23)$, $f_4 = (31)$, $f_5 = (1\ 2\ 3)$, $f_6 = (1\ 3\ 2)$. If $H = \{f_1, f_2\}$ then show that H is a subgroup of G and also find all the distinct right cosets of H in G.
   [**Ans.** H, Hf_3, Hf_4]
3. Show that the multiplicative group of n nth roots of unity is a cyclic group generated by $e^{\frac{2\pi i}{n}}$.
4. Show that every finite group of order less than six must be abelian.
5. (i) How many generators are there of the cyclic group of order 10 ?
   (ii) How many generators can a cyclic group of order 12 have ?
   [**Ans.** (i) a, a^3, a^7, a^9 (ii) $a, a^5, a^7\ a^{11}$]
6. How many elements of the cyclic group of order 6 can be used as generators of the group ?
   [**Ans.** Two i.e., a and a^5]
7. Show that the intersection of any collection of normal subgroups is itself a normal subgroup.
8. If H is a normal subgroup of G and K is a subgroup of G such that $H \subseteq K \subseteq G$. Show that H is also a normal subgroup of K.
9. If H is a subgroup of G and N is a normal subgroup of G, show that $H \cap N$ is a normal subgroup of H.
10. Show that $H = \{1, -1\}$ is a normal subgroup of $G\ (\{1, -1, i - i\}, \cdot)$.
11. Show that $A_3 = \{(1)\ (2)\ (3), (1\ 2\ 3), (1\ 3\ 2)\}$ is a normal subgroup of $S_3 = \{(1)\ (2)\ (3), (1\ 2\ 3), (1\ 3\ 2), (1\ 2)\ (3), (1)\ (2\ 3), (1\ 3)\ (2)\}$ under the operation of permutation multiplication.
12. Let N be a normal subgroup of a group G, and let R be the following relation on G :
    a R b if and only if $ab^{-1} \in N$
    Then (a) R is a congruence relation on G.
    (b) N is the equivalence class [e] relative to R, where e is the identity of G.
13. Prove that if G_1 and G_2 are abelian groups, then $G_1 \times G_2$ is an abelian group.
14. Let $G = Z_4$ where $Z_4 = \{[0], [1], [2], [3]\}$. For each of the following subgroups of H of G, determine all

the left cosets of H in G.

(a) $H = \{[0]\}$

(b) $H \{[0], [2]\}$

(c) $H = \{[0], [1], [2], [3]\}$.

[**Ans.** (a) $\{[0], \{[1]\}, \{[2]\}, \{[3]\}$,

(b) $\{[0], [2]\}, \{[1], [3]\}$

(c) $\{[0], [1], [2], [3]\}$

15. Let H be a subgroup of a group G. Show that every left coset aH of H has the same number of elements as H.

[Hint : Show that the function $f_a : H \to aH$ defined as $f_a(h) = ah$, for $h \in H$, is a bijection i.e., one-one and onto]

16. Let (G, *) be a group where $G = \{0, 1\}$. Also, let $H = \{1\}$ is a subgroup of G. Determine all the left costs of H in G.

[**Ans.** $\{1\}, \{0\}$]

17. Let (Z, +) be a group and $H = \{..., -4, -2, 0, 2, 4, ...\}$ be the subgroup of Z consisting of multiplies of 2. Determine all the left cosets of H in Z.

[**Ans.** H, 1 + H]

18. Let $G = (Z_9, +_9)$ and $H \{0, 3, 6\}$. Determine all the distinct left cosets of H in G.

[**Ans.** H, $1 +_9 H$, $2 +_9 H$]

19. If H be a cyclic subgroup of a group G and $x \in G$ then show that $x H x^{-1}$ is also cyclic.

[Hint : If $h \in H$ is a generator of H, then $x h x^{-1}$ is a generator of $x H x^{-1}$].

20. Show that two right cosets Ha, Hb are distinct iff the two left cosets $a^{-1}H$, $b^{-1}H$ are distinct.

[Hint : It is sufficient to show that $Ha = Hb$ iff $a^{-1}H = b^{-1H.}$].

❑❑❑