LECTURE NOTES

PROGRAMME – BCA

SEMESTER- IV

DISCRETE MATHEMATICS (BCA-401)

UNIT II

Unit-II

Algebraic Structures: Properties, Semi group, Monoid, Group, Abelian group, Properties of group, Subgroup, Cyclic group, Cosets, Permutation groups, Homomorphism, Isomorphism and Auto-morphism of groups.

In this chapter, we will study, binary operation as a function, and two more algebraic structures, semigroups and groups. They are called an algebraic structure because the operations on the set define a structure on the elements of that set. We also define the notion of a hornomorphism and product and quotients of groups and semigroup.

6.2 BINARY OPERATION

A binary operation on a set A is an everywhere defined function $f : A \times A \rightarrow A$ Generally operation is defined by $*$ *If* $*$ is binary operation on A then $a * b \in A \; \forall a, b \in A$

Properties of binary operation : - Let $*$ be a binary operation on a set A, Then $*$ satisfies the following properties for any a, b and c in A

1.	$a = a * a$	Identity property
2.	$a * b = b * a$	Commutative property
3.	$a * (b * c) = (a * b) * c$	Associative property

6.3 SEMIGROUP

A non-empty set S together with a binary operation $*$ is called as a semigroup if –

i) binary operation $*$ is closed

ii) binary operation $*$ is associative

we denote the semigroup by (S, $*$)

Commutative Semigroup :- A semigroup (S, $*$) is said to be commutative if $*$ is commutative i.e. $a * b = b * a \quad \forall a \in S$

Examples : 1) (z, +) is a commutative semigroup

2) The set P(S), where S is a set, together with operation of union is a commutative semigroup.

3) (Z, –) is not a semigroup
The operation subtraction is not associative

6.4 IDENTITY ELEMENT :

An element e of a semigroup (S, $*$) is called an identity element if $e * a = a * e = a \qquad \forall a \in S$

Monoid A non-empty set M together with a binary operation *defined on it, is called as a monoid if –

i) binary operation $*$ is closed

ii) binary operation $*$ is associative and

iii) (M, $*$) has an identity.

i.e. A monoid is a semi group that has an identity

6.5 GROUP

A a non-empty set G together with a binary operation $*$ defined on it is called a group if

(i) binary operation $*$ is close,

(ii) binary operation $*$ is associative,

(iii) (G, $*$) has an identity,

(iv) every element in G has inverse in G,

We denote the group by (G, $*$)

Commutative (Abelian Group : A group (G, $*$) is said to be commutative if $*$ is commutative. i.e. $a * b = b * a \ \forall a, b \in G$.

Cyclic Group : If every element of a group can be expressed as some powers of an element of the group, then that group is called as cyclic group.

The element is called as generator of the group.

If G is a group and a is its generator then we write $G = < a >$

For example consider $G = \{1, -1, i, -i\}$. G is a group under the binary operation of multiplication. Note that $G = < i >$. Because $a = \left\{i, i^2, i^3, i^4\right\} = \{i, -1, -i, 1\}$

6.6 SUBSEMIGROUP :

Let (S, $*$) be a semigroup and let T be a subset of S. If T is closed under operation $*$, then (T, $*$) is called a subsemigroup of (S, $*$).

Submonoid : Let (S, $*$) be a monoid with identity e, and let T be a non-empty subset of S. If T is closed under the operation $*$ and e $\in$ T, then (T, $*$) is called a submonoid of (S, $*$).

Subgroup : Let (G, $*$) be a group. A subset H of G is called as subgroup of G if (H, $*$) itself is a group.

Necessary and Sufficient Condition for subgroup : Let (G; $*$) be a group. A subset H of G is a subgroup of G if and only if $a * b^{-1} \in H$ $\forall a, b \in H$

6.7 PERMUTATION

Definition : A permutation on n symbols is a bijective function of the set $A = \{1,2,...n\}$ onto itself. The set of all permutations on n symbols is denoted by S_n. If α is a permutation on n symbols, then α is completely determined by its values $\alpha(1), \alpha(2) \ldots \alpha(n)$. We use following notation to denote $\alpha \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ \alpha(1) & \alpha(1) & \alpha(3) & ..... & \alpha(n) \end{pmatrix}$.

For example $\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$ denotes the permutation on the 5 symbols (1,2,3,4,5). α maps 1 to 5, 2 to 3, 3 to 1, 4 to 2 and 5 to 4.

Product of permutation : - Let A = {1,2,3,4}

Let $\alpha \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ and $\beta \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

Then $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Cycle - an element $\alpha \in s_n$ is called a cycle of lingth r if $\exists$ r symbols $i_1, i_2....i_n \alpha(i_1) = i_2, \alpha(i_2) = i_3 \ldots \alpha(i_n) = i_1$.

Example : Consider following permutation

i) $\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$. It can be expressed as a product of cycles -

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

Transposition :

A cycle of length two is called transposition.

For example following permutation can be expressed as a product of transpositions.

$\alpha\,(18\,3\,7)(2\,5)(4\,6)$

$\therefore \alpha\,(1\ 8)(1\ 3)(1\ 7)(2\,5)(4\,6)$

Even (odd) Permutation -

Let A {1, 2, ….n). A permutation $\alpha \in S_n$ is even or odd according to whether it can be expressed as the product of an even number of transpositions or the product of an odd number of transpositions respectively.

For example we can consider following permutation :

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

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

= odd no. of transpositions so α is odd permutation

Example 1 : Show that $*$ defined as $x * y = x$ is a binary operation on the set of positive integers. Show that $*$ is not commutative but is associative.

Solution : Consider two positive integers x and y. By definition $x * y = x$

which is a positive integer. Hence · is a binary operation.
For commutativity : $x * y = x$ and $y * x = x$. Hence $x * y \neq y * x$ in general

$\therefore$ $*$ is not commutative.

But $x * (y * z) = x * y = x$ and $(x * y) * z = x * z = x$. Hence $x * (y * z) = (x * y) * z$. $\therefore$ $*$ is associative

Example 2 : Let I be the set of integers and Z_m be the set of equivalence classes generated by the equivalence relation "congruent modulo m" for any positive integer m.

a) Write the sets Z_3 and Z_6

b) Show that the algebraic systems (Z_m, $+_m$) and (Z_m, $\times_m$) are monoids.

c) Find the inverses of elements in Z_3 and Z_4 with respect to $+_3$ and $\times_4$ respectively.

Solution : a) Z_3 for (Z_3,$+_3$) ={[0], [1], [2]}
Z_6 for (Z_6, $+_6$) = {[0], [1], [2], [3], [4], [5] }
Z_3 for (Z_3,$\times_3$) ={[0], [1], [2]}
Z_6 for (Z_6,$\times_6$) = {[0], [1], [2], [3], [4], [5] }

Example 3 : Determine whether the following set together with the binary operation is a semigroup, a monoid or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid determine whether it is commutative.

i) A = set of all positive integers. $a * b = \max\{a,b\}$ i.e. bigger of a and b [May-06]

ii) Set S = {1, 2, 3, 6, 12} where $a * b = G.C.D.(a,b)$

[Dec-03, May – 07]

iii) Set S ={1,2,3,6,9,18) where $a * b = L.C.M.(a,b)$ [Nov-06]

[April - 04]

iv) Z, the set of integers, where $a * b = a + b - ab$

v) The set of even integers E, where $a * b = \frac{ab}{2}$ [May-03]

vi) Set of real numbers with $a * b = a + b + 2$

vii) The set of all m×n matrices under the operation of addition.

Solution :

i) A = set of all positive integers. $a * b = \max\{a,b\}$i.e. bigger of a and b.

Closure Property: Since Max {a, b} is either a or b $\therefore$ $a * b \in A$. Hence closure property is verified.

Associative Property :

Since $a * (b * c) = \max\{\{a,b\},c\} = \max\{a,b,c\}$

$= \text{Max}\{a,\{b, c\}\} = (a.b).c$

$\therefore$ $*$ is associative.

$\therefore$ (A, $*$) is a semigroup.

Existence of identity : 1 $\in$ A is the identity because

1.a = Max{ 1,a}= a $\forall$ a$\in$A

$\therefore$ (A, $*$) is a monoid.

Commutative property : Since Max{a, b) = max{b, a) we have $a * b = b * a$Hence $*$ is commutative.

Therefore A is commutative monoid.

ii) Set S = { 1,2,3,6,12} where $a * b = G.C.D.(a,b)$

*	1	2	3	6	12
1	1	1	1	1	1
2	1	2	1	2	2
3	1	1	3	3	3
6	1	2	3	6	6

12	1	2	3	6	12

Closure Property : Since all the elements of the table ∈ S, closure property is satisfied.

Associative Property : Since
$a*(b*c) = a*(b*c) = a*GCD\{b,c\} = GCD\{a,b,c\}$

And $(a*b)*c = GCD\{a,b\}*c = GCD\{a,b,c\}$

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

$\therefore$ $*$ is associative.
$\therefore$ (S, $*$) is a semigroup.

Existence of identity: From the table we observe that 12 $\in$ S is the identity

$\therefore$ (S, $*$) is a monoid.

Commutative property : Since GCD{a,b}= GCD{b,a) we have

$a*b = b*a$. Hence $*$ is commutative.

Therefore A is commutative monoid

(iii) Set S ={ 1,2,3,6,9, 18} where $a*b$ =L.C.M. (a,b)

*	1	2	3	6	9	18
1	1	2	3	6	9	18
2	2	2	6	6	18	18
3	3	6	3	6	9	18
6	6	6	6	6	18	18
9	9	18	9	18	9	18
18	18	18	18	18	18	18

Closure Property : Since all the elements of the table $\in$ S, closure property is satisfied.

Associative Property : Since $a*(b*c) = a*LCM\{b,c\} = LCM\{a,b,c\}$

And $(a*b)*c = LCM\{a,b\}*c = LCM\{a,b,c\}$

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

$\therefore$ $*$ is associative.
$\therefore$ (S, $*$) is a semigroup.

Existence of identity : From the table we observe that 1 $\in$ S is the identity.

$\therefore$ (S, $*$) is a monoid.

Commutative property : Since LCM{a, b} = LCM{b, a} we have $a * b = b * a$. Hence $*$ is commutative.

Therefore A is commutative monoid.

(iv) Z, the set of integers where - a * b = a + b - ab

Closure Property : - $a, b \in z$ then $a + b - ab \in z \ \forall a, b$ so * is closure.

Associate Property : Consider $a, b \in z$

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= a + b - ab + c - (a + b - ab)\,c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc \qquad \textbf{(1)}\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * (b + c - bc) \\ &= a + b + c - bc - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc \qquad \textbf{(2)}\end{aligned}$$

From 1 & 2

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

$\therefore$ * is associative $\forall a, b, c \in z$

$\therefore$ (z, &) is a semigroup.

Existence of Identity : Let e be the identity element a * e = q

a + e - q.e = a

a + e - a.e = a

e (1-a) = 0

e = 0 or a = 1

But $a \neq 1$

E = 0

$\therefore$ $O \in Z$ is the identity element.

$\therefore$ (Z, *) is monoid.

Commutative property : $\forall a, b \in z$

a * b = a + b - ab

= b + a - ba

= b * a

$\therefore$ * is commutative

$\therefore$ (Z, *) is commutative monoid.

O$\in$Z is the identity

v) E = set of even integers. $a * b = \frac{ab}{}$

Closure Property : Since $\frac{ab}{2}$ is even for a and b even. $\therefore\ a*b\in E$. Hence closure property is verified.

Associative Property : Since $a*(b*c)=q*\left(\frac{bc}{2}\right)=\frac{abc}{4}=\frac{ab}{2}*c=(a*b)*c$

$\therefore$ $*$ is associative. $\therefore$ (E, $*$) is a semigroup.

Existence of identity : 2$\in$ E is the identity because $2*a=\frac{2a}{2}=$ a $\forall$ a $\in$ E

$\therefore$ (E, $*$) is a monoid.

Commutative property : Since $\frac{ab}{2}=\frac{ba}{2}$, we have $a*b=b*a$ Hence $*$ is commutative.

$\therefore$ (E,*) is commutative monoid.

(vi) -2$\in$A is identity

(vii) $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\in$ M is the identity

Example 4 : State and prove right or left cancellation property for a group.

Solution : Let (G, $*$) be a group.

(i) To prove the right cancellation law i.e. $a*b=c*b\Rightarrow a=c$

Let a, b, c$\in$G. Since G is a group, every element has inverse in G.

$\therefore$ $b^{-1}\in$ G

Consider $a*b=c*b$

Multiply both sides by b^{-1} from the right.

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

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

$\therefore$ $e*a=e*c$ $b*b^{-1}=e\in G$

$\therefore$ a = c e$\in$G is the identity

(ii) To prove the left cancellation law i.e. $a*b=c*b\Rightarrow a=c$

Let a, b, c$\in$G: Since G is a group, every element has inverse in G.

$\therefore$ $a^{-1}\in$G

Consider $a*b=a*c$

Multiply both sides by a^{-1} from the left

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

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

$\therefore \quad e * b = e * c$ $a^{-1} * a = e \in G$

$\therefore$ b = c e$\in$G is the identity

Example 5 : Prove the following results for a group G.

(i) The identity element is unique.

(ii) Each a in G has unique inverse a^{-1}

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

Solution : (i) Let G be a group. Let e_1 and e_2 be two identity elements of G.

If e_1 is identity element then $e_1e_2 = e_2e_1 = e2$..................... (1)

If e_2 is identity element then $e_1e_2 = e_2e_1 = e_1$................................(2)

$\therefore$ From (1) and (2) we get $e_1 = e_2$ i.e. identity element is unique.

(ii) Let G be a group. Let b and c be two inverses of a$\in$G.

lf b is an inverse of a then ab = ba = e.....................(1)

If c is an inverse of a then ac = ca = e.................... (2)

Where e $\in$ G be the identity element.

$\therefore$ From (1) and (2) we get ab = ac and ba = ca.

$\therefore$ b=c by cancellation law : i.e. inverse of a$\in$G is unique.

$\therefore$ inverse of $a \in G$ is unique.

(iii) Let G be a group. Let a, b $\in$ G.

Consider $(ab)(b^{-1}a^{-1})$

$= a(bb^{-1})a^{-1}$ Associative property

$= (ae)a^{-1}$ $bb^{-1} = e$, e$\in$G is identity

$= (ae)a^{-1}$ Associative property

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

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

Similarly we can prove $(b^{-1}a^{-1})(ab) = e$.

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

Example 6 : Let G be a group with identity e. Show that if $a^2 = e$ for all a in G, then every element is its own inverse [Nov.-05]

Solution : Let G be a group.

Given $a^2 = e$ for all $a \in G$.
Multiply by a^{-1} we get a^{-}
$^{1}a^{2} = a^{-1}e$
$\therefore \quad a = a^{-1}$
i.e. every element is its own inverse

Example 7 : Show that if every element in a group is its own inverse, then the group must be abelian. [Dec-02] [5]

OR

Let G be a group with identity e. Show that if $a^2 = e$ for all a in G, then G is abelian. [May-05]

Solution : Let G be a group.

$\therefore$ For $a \in G$, $a^{-1} \in G$

$\therefore$ Consider $(ab)^{-1}$

$\therefore$ $(ab)^{-1} = b^{-1}a^{-1}$ reversal law of inverse.

$\therefore$ $ab = ba$ every element is its own inverse

$\therefore$ G is abelian.

Example 8 : Let Z_n denote the set of integers (0, 1, .. , n-1). Let $\otimes$ be binary operation on Z_n such that $a \otimes b$ = the remainder of ab divided by n.

i) Construct the table for the operation $\otimes$ for n=4.

ii) Show that $(Z_n, \otimes)$ is a semi-group for any n.

iii) Is $(Z_n, \otimes)$ a group for any n? Justify your answer.

Solution : (i) Table for the operation $\otimes$ for n = 4.

⊗	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) To show that $(Z_n, \otimes)$ is a semi-group for any n.

Closure property : Since all the element in the table

$\in$ {0, 1, …, n-1}, closure property is satisfied.

Assiciative property : Since multiplication modulo n is associative, associative property is satisfied.

$\therefore$ $(Z_n, \otimes)$ is a semi-group

(iii) $(Z_n, \otimes)$ is not a group for any n.

If n = 4, 2^{-1} does not exist ($1 \in G$ is the identity.)

Example 9 : Show that a group (G, $*$) is abelian if and only if for a, b$\in$G, $(a*b)^2 = a^2 * b^2$ [Nov-06]

Solution : Step-1 : Given (G, $*$) is a group and for a, b$\in$G, $(a*b)^2 = a^2 * b^2$. To prove that (G, $*$) is abelian.

Given $(a*b)^2 = a^2 * b^2$

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

$\therefore$ $a*(b*a)*b = a*(a*b)*b$ Associative property

$\therefore$ $(b*a)*b = (a*b)*b$ Left cancellation law

$\therefore$ $b*a = a*b$ Right cancellation law

$\therefore$ (G, $*$) is abelian.

Step-2 : Assume that (G, $*$) is abelian.

To prove that a, b$\in$G, $(a*b)^2 = a^2 * b^2$

Consider $(a*b)^2$

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

$= a*(b*a)*b$ Associative property

$= a*(a*b)*b$ G is abelian

$= (a*a)*(b*b)$ Associative property

$= a^2 * b^2$

Example 10 : If (G, $*$) be an abelian group, then for all a, b$\in$G, show that $(a*b)^n = a^n * b^n$.

Solution : Given (G, $*$) is abelian. To prove that for all a, b$\in$G, $(a*b)^n = a^n * b^n$

We will use the method of induction. Let P(n) be the property that for all a, b$\in$G;

$(a*b)^n = a^n * b^n$

Step-I : Check that $P^{(1)}$ is true.

$(a*b)^1 = a^1 * b^1$

$a*b = a*b$ Hence P(1) is true.

Step-2 : Assume P(k) is true for some k∈N

$(a*b)^k = a^k * b^k$

Step-3: Prove P(k+1) is true. Consider

$*(a*b)^{k+1}$

$= (a*b)^k * (a*b) = (a^k * b^k) * (a*b)$ using step-2

$= a^k * (b^k * a) * b$ Associative property

$= a^k * (a * b^k) * b$ G is abelian

$= (a^k * a) * (b^k * b)$ Associative property

$= a^{k+1} * b^{k+1}$ ∴ P(k+1) is true.

Hence P(n) is true for every n∈N

Example 11 : Let α=(1 2 3 4)(6 5 7) and β=(2 4 3)(7 5) be permutations of the set {1,2,3,…..,7}. Express α as product of transposition. Find whether α ∘ β is an even permutation or not. [Dec-99][5]

Solution : Let a=(1 2 3 4)(6 5 7)

∴ α = (1 4)(1 3)(1 2)(6 7)(6 5)

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 5 & 6 \end{pmatrix} \text{o} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ & & & & & & \end{pmatrix}$$

$$\therefore \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 1 & 7 & 5 & 6 \end{pmatrix} = (1\,2)(5\,6)$$

∴α ∘ β is an even permutation.

Example 12 : Let A = { 1, 2, 3, 4, 5, 6} and P = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$ be permutation on A

a) Write P as a product of disjoint cycles.

b) Find P^{-1}.

c) Find the smallest positive integer k such that $P^k = 1_A$.

[May-02][4]

Solution: Let P = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 1 & 5 & 6 \end{pmatrix}$

(a) P = (1 2 4)(3)(5)(6)

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

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

∴ $P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}$

(c) $P^2 =$

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

$P^3 = p^2p =$

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

∴ Smallest k=3

Example 13 : Consider the group G = {1,2,3,4,5,6} under multiplication modulo 7. [Apr-04, May-06]

(i) Find the multiplication table of G

(ii) Find $2^{-1}, 3^{-1}, 6^{-1}$.

(iii) Find the order of the subgroups generated by 2 and 3.

(iv) Is G cyclic?

Solution : (i) Multiplication table of G

Binary operation $*$ is multiplication modulo 7.

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table we observe that $1 \in G$ is identity.

(ii) To find $2^{-1}, 3^{-1}, 6^{-1}$.

From the table we get $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

iii) To find the order of the subgroups generated by 2.

Consider $2^\circ = 1$ = Identity, $2^1 = 2$; $2^2 = 4$, $2^3 = 1$ = Identity

$< 2 > = \{2^1, 2^2, 2^3\}$

$\therefore$ Order of the subgroup generated by 2 =3

To find the order of the subgroups generated by 3.

Consider $3^\circ = 1$ = identity, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$ = Identity

$< 3 > = \{3^1, 3^2, 3^3, 3^4, 3^5, 3^6\}$

$\therefore$ Order of the subgroup generated by 3 = 6

(iv) G is cyclic because G = < 3 >.

Example 14 : Let $S=\{x|x$ is a real number and $x\neq 0$, $x\neq 1\}$. Consider the following functions $f_i : S\rightarrow S$, i=1,2,---,6 [Nov-05]

$$f_1(x) = x,\ f_2(x) = 1-x,\ f_3(x) = \frac{1}{x},\ f_4(x) = \frac{1}{1-x},\ f_5(x) = 1-\frac{1}{x},$$

$$f_6(x) = \frac{x}{x-1}$$

Show that G = $\{f_1, f_2, f_3, f_4, f_5, f_6)$ is a group under the operation of composition. Give the multiplication table of G.

Solution : (i) Multiplication table of G

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
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

(i) **Closure property :** Since all the elements in the table $\in$G, closure property is satisfied.

(ii) **Associative property :** Since composition of functions is associative, associative property is satisfied.

(iii) **Existence of identity :** From the table we observe that $f_1 \in G$ is the identity.

(iv) **Existence of inverse :** From the table we observe that

$f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_5$, $f_5^{-1} = f_4$, $f_6^{-1} = f_6$

i.e. every element of G has inverse in G. Hence G is a group.

Example 15 : Let G be an abelian group with identity e and let H = {x/x^2 = e). Show that H is a subgroup of G. [May-02, 03, May-07]

Solution : Let x, y$\in$H$\therefore$x^2 = e and y^2 = e $\therefore$ x^{-1} = x and y^{-1} = y

Since G is abelian we have xy = yx $\therefore$ xy^{-1} = yx

$$
\begin{aligned}
\text{Now } (xy^{-1})^2 &= (xy^{-1})(xy^{-1}) = (xy^{-1})(y^{-1}x) \\
&= (xy^{-1})(yx) = x(y^{-1}y)x \\
&= x(e)x \\
&= x^2 = e
\end{aligned}
$$

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

$\therefore$ H is a subgroup.

Example 16 : Let G be a group and let H = (x/x$\in$G and xy = yx for all y$\in$G}. Prove that H is a subgroup of G. [98][7]

Solution : Let x, z $\in$ H $\therefore$ xy = yx for every y$\in$G $\therefore$ x = yxy^{-1}.

Similarly zy = yz for every y$\in$G $\therefore$z = yzy^{-1}.

$$
\begin{aligned}
\text{Now consider } xz^{-1} &= (yxy^{-1})(yzy^{-1})^{-1} \\
&= yxy^{-1}\,yz^{-1}y^{-1} = yxz^{-1}y^{-1}
\end{aligned}
$$

$\Rightarrow$ (x.z^{-1})y = y(xz^{-1}) $\in$ H.

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

$\therefore$ H is a subgroup

Example 17 : Find all subgroups of (Z,$\oplus$) where $\oplus$ is the operation addition modulo 5. Justify your answer.

Solution:

$\oplus$	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

Example 18 : Let G be a group of integers under the operation of addition. Which of the following subsets of G are subgroups of G?

(a) the set of all even integers,

(b) the set of all odd integers. Justify your answer.

Solution:

a) Let H= set of all even integers.

We know, additive inverse of an even number is even and sum of two even integers is also even. Thus for $a,b \in H$ we have $ab^{-1} \in H$. Hence H is a subgroup of G.

b) Let K = set of all odd integers.

We know, additive inverse of an odd number is odd and sum of two odd integers is even.

Thus for $a,b \in K$ we have $ab^{-1} \notin K$.

Hence K is not a subgroup of G.

Example 19 : Let $(G, *)$ be a group and H be a non-empty subset of G. Show that $(H, *)$ is a subgroup if for any a and b in H, ab^{-1} is also in H.

[May-00) [3]

Solution :

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

$\therefore$ The identity element $\in$ H.

(ii) Let $e, a \in H$ $\therefore$ $ea^{-1} \in H$. i.e. $a^{-1} \in H$

$\therefore$ Every element has inverse $\in$ H.

(iii) Let $a, b \in H$. $\therefore$ $b^{-1} \in H$. $\therefore$ $a(b^{-1})^{-1} \in H$. i.e. $ab \in H$.

$\therefore$ Closure property is satisfied.

(iv) Every element in H is also in G. And G is a group. So associative property is satisfied by the elements of H. Hence associative property is satisfied by the elements of H.

Hence H is a group. But H is a subset of G. $\therefore$H is a subgroup of G.

Example 20 : Let H and K be subgroups of a group G. Prove that $H \cap K$ is a subgroup of G. [Dec-02] [5]

Solution : If H is a subgroups of a group G, then for any $a, b \in H$, $ab^{-1} \in H$.

Similarly, if K is a subgroups of a group G, then for any $a, b \in K$, $ab^{-1} \in K$.

Now if $a, b \in H \cap K$, $a, b \in H$ and $a, b \in K$. $\therefore$ $ab^{-1} \in H$ and $ab^{-1} \in K$. Hence $ab^{-1} \in H \cap K$.

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

6.8 PRODUCTS AND QUOTIENTS OF SEMIGROUPS:

In this section we obtain new semigroups from existing semigroups.

Theorem 6.1 :

If (S, $*$) and (T, $*'$) are semigroups, then (S × T, $*''$) is a semigroup, where $*''$ is defined by $(s_1,t_1) *''(s_2,t_2) = (s_1 * s_2, t_1 *' t_2)$

Theorem 6.2 :

If S and T are monoids with identities e_s and e_T, respectively, then, S × T is a monoid with identity (e_s, e_T)

Theorem 6.3 :

Let R be congruence relation on the semigroup (S, $*$). Consider the relation from S/R×S/R to S/R in which the ordered pair ([a], [b]) is, for a and b in S, related to [a $*$ b].

(a) $\otimes$ is a function from S/R×S/R to S/R, and as usual we denote $\otimes$ ([a],[b]) by [a] $*$ [b]. Thus $[a] \otimes [b]=[a*b]$.

(b) (S/R, $\otimes$) is a semigroup.

Proof : Suppose that ([a],[b]) = ([a'],[b']). Then aRa' and bRb', so we must have a $*$bRa' $*$b', since R is a congruence relation. Thus [a$*$b]=[a' $*$b']; that is, $\otimes$ is a function. This means that $\otimes$ is a binary operation on S/R.

Next, we must verify that $\otimes$ is an associative operation. We have $[a]\otimes([b]\otimes[c])=[a]\otimes[b*c]=[a*(b*c)]=[(a*b)*c]$ by associative property of $*$ in S

$$= [a*b] \otimes [c]$$

$$= ([a] \otimes [b]) \otimes [c],$$

Hence S/R is a semigroup. We call S/R the ***quotient semigroup*** or ***factor semigroup***. Observe that $\otimes$ is a type of "quotient binary relation" on S/R that is constructed from the original binary relation $*$ on S by the congruence relation R

Example 21 : Let Z be the set of integers, and Z_m, be the set of eduivalences classes generated by the equivalence relation "congruence modulo m" for any positive integer m.

Z_m, is a group with operation ⊕ where [a] ⊕ [b] = [a+b]

For Z_2 and Z_3 defined according to the above definition, write the multiplication table for the group $Z_2 \times Z_3$. [May-03] [5]

Solution : The multiplication table for the group $Z_2 \times Z_3$.

⊕	(0,0)	(0,1)	(0,2)	(1,0)	(1,1,)	(1,2)
(0,0)	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(0,2)	(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(1,0)	(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,1)	(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)
(1,2)	(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)

6.9 HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF SEMIGROUPS

Homomorphism : Let (S, ∗) and (T, ∗') be two semigroups. An everywhere defined function

f : S→T is called a homomorphism from (S, ∗) to (T, ∗') if

f(a ∗b) = f(a) ∗'f(b) ∀ a, b ∈ S

Isomorphism : Let (S, ∗) and (T, ∗') be two semigoups. A function

f : S → T is called a isomorphism from (S, ∗) to (T, ∗') if

(i) it is one-to-one correspondence from S to T (ii) f(a∗b) = f (a) ∗'f (b) ∀ a, b ∈ S

(S, ∗) and (T, ∗') are isomorphic' is denoted by $S \cong T$.

Automorphism : An isomorphism from a semigroup to itself is called an

automorphism of the semigoup. An isonorptism $f : s \to s$ is called automorphism.

6.10 HOMOMORPHISM, LSOMORPHISM AND AUTOMORNHISM OF MONOIDS :

Homomorphism : Let (M, ∗) and (M', ∗') be two monoids. An everywhere defined function f : M → M' is called a homomorphism from (M, ∗) to (M', ∗') if

f (a ∗ b) = f(a) ∗'f(b) ∀ a, b ∈ M

Isomorphism : Let (M, ∗) and (M', ∗') be two monoids. A function

f : M → M' is called a isomorphism from (M, ∗) to (M', ∗') if

(i) it is one-to-one correspondence from M to M’ (ii) f is onto.

(iii) f(a$*$b = f (a) $*$’f (b) $\forall$ a, b$\in$M

‘(M $*$) and (M’, $*$’) are isomorphic is denoted by M $\cong$ M’.

Automorphism : An isomorphism from a monoid to itself is called an automorphism of the monoid. An isomorphism $f : M \to M$ is called Automorphism of monoid.

6.11 HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF GROUPS :

Homomorphism : Let (G, $*$) and (G’, $*$’) be two groups. An everywhere defined function f : G $\to$ G’ is called a homomorphism from (G, $*$) to (G’, $*$’) if

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

Isomorphism : Let (G, $*$) and (G’, $*$’) be two groups. A function f : G$\to$G’ is called a isomorphism from (G, $*$) to (G’, $*$’) if

(i) it is one-to-one correspondence from G to G’ (ii) f is onto.

(iii) f(a $*$ b) = f (a) $*$’f (b) $\forall$ a, b$\in$G

‘(G, $*$) and (G’, $*$’) are isomorphic’ is denoted by G $\cong$ G’.

Automorahism: An isomorphism from a group to itself is called an automorphism of the group. An isomorphism $f : G \to G$ is called Automorphism.

Theorem 6.4 : Let (S, $*$) and (T, $*$’) be monoids with identity e and e’, respectively. Let f : S $\to$ T be an isomorphism. Then f(e) = e’.

Proof : Let b be any element of T. Since f is on to, there is an element a in S such that f(a) = b

Then $a = a * e$

$b = f(a) = f(a * e) = f(a) * f(e) = b *' f(e)$ (f is isomorphism) Similarly,

since $a = e * a$,

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

Thus for any ,b$\in$T,

$b = b *' f(e) = f(e) *' b$

which means that f(e) is an identity for T.

Thus since the identity is unique, it follows that f(e)=e’

Theorem 6.5: Let (S, $*$) and (T, $*'$) be monoids with identity e and e', respectively. Let f : S → T be a homomorphism. Then f(e) = e'.

Proof : It can be prove similarly like Theorem 6.4.

Theorem 6.6 : Let f be a homomorphism from a semigroup (S, $*$) to a semigroup (T, $*'$). If S' is a subsemigroup of (S, $*$), then

F(S') = {t ∈ T | t = f (s) for some s ∈ S},

The image of S' under f, is subsemigroup of (T, $*'$).

Proof : If t_1, and t_2 are any elements of F(S'), then there exist s_1 and s_2 in S' with

t_1= f(s_1) and t_2 = f(s_2).

Therefore,

$$t_1 * t_2 = f(s_1) * f(s_2) = f(s_1 * s_2) = f(s_2 * s_1) = f(s_2) * f(s_1) = t_2 * t_1$$

Hence (T, $*'$) is also commutative.

Example 22 : Let G be a group. Show that the function f : G → G defined by f(a) = a^2 is a homomorphism iff G is abelian. [98][6], [May-00] [4]

Solution :

Step-1 : Assume G is abelian. Prove that f : G → G defined by f(a) = a^2 is a homomorphism.

Let a,b∈G. ∴ f(a) = a^2 , f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

∴ f(ab)=$(ab)^2$

= (ab)(ab).

= a(ba)b associativity

= a(ab)b G is abelian

= (aa)(bb) associativity

= a^2b^2

= f(a)f(b) definition of f

∴ f is a homomorphism.

Step 2 : $\forall\ y = a^2 \in G\ \exists\ a \in G\ s\ t$

$f(a) = y = a^2$

∴f is onto.

Step-3 : Assume, f : G → G defined by f(a) = a^2 s a homomorphism. Prove that G is abelian.

Let a,b∈G. ∴ f(a) = a^2 , f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

$\therefore$ f(ab) = f(a)f(b) f is homomorphism

$\therefore$ $(ab)^2 = a^2 b^2$ definition of f

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

$\therefore$ a(ba)b = a(ab)b associativity

$\therefore$ ba = ab left and right cancellation taws

$\therefore$ G is abelian.

Example 23 : 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 $f_a(x) = axa^{-1}$ for $x \in G$ is an isomorphism. [Dec-O2][5]

Solution :

Step-1: Show that f is 1-1.

$f_a(x) = axa^{-1}$

Consider $f_a(x) = f_a(y)$ for $x, y \in G$

$\therefore$ $axa^{-1} = aya^{-1}$ definition of f

$\therefore$ x = y left and right cancellation laws

$\therefore$ f is 1- 1

Step 2 : $\forall\ y = axa^{-1} \in G\ \exists\ x \in G$ s.t.

$f_a(x) = a\,xa^{-1}$

$\therefore$ f is onto.

Step-3 : Show that f is homomorphism.

For $x, y \in G$

$f(x) = a * x * a^{-1}$, $f(y) = a * y * a^{-1}$ and $f(x * y) = a * (x * y) * a^{-1}$

Consider $f(x * y) = a * (x * y) * a^{-1}$ for $x, y \in G$

$\therefore$ $f(x * y) = a * (x * e * y) * a^{-1}$ $e \in G$ is identity

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

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

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

$\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 24 : Let G be a group. Show that the function f : G → G defined by $f(a) = a^{-1}$ is an isomorphism if and only if G is abelian. [May-03][4]

Solution :

Step-1: Assume G is abelian. Prove that f : G → G defined by $f(a) = a^{-1}$ is an isomorphism.

i) Let f(a)=f(b)

$\therefore a^{-1} = b^{-1}$ $\therefore a = b$ $\therefore$ f is 1- l.

ii) $\forall\, a \in G \Rightarrow a^{-1} \in G$

$\therefore x^{1} \in G$

$\Rightarrow f(x) = x^{-1}$

$\therefore$ f is onto.

iii) Let $a,b \in G$. $\therefore f(a) = a^{-1}$, $f(b) = b^{-1}$ and $f(ab) = (ab)^{-1}$ by definition of f.

$\therefore$ f(ab) = $(ab)^{-1}$

= $b^{-1}a^{-1}$ reversal law of inverse

= $a^{-1}b^{-1}$ G is abelian

= f(a)f(b) definition of f.

$\therefore$ f is a homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Step – 2 : Assume f : G → G defined by $f(a) = a^{-1}$ is an isomorphism. Prove that G is abelian.

Let $a, b \in G$ $\therefore f(a) = a^{-1}$, $f(b) = b^{-1}$ and $f(ab) = (ab)^{-1}$ by definition of f

$\therefore$ f(ab) = f(a)f(b) f is homomorphism

$\therefore$ $(ab)^{-1} = a^{-1}b^{-1}$ definition of f

$\therefore$ $b^{-1}a^{-1} = a^{-1}\, b^{-1}$ reversal law of inverse

G is abelian.

Example 25 : Define (Z, +) → (5Z, +) as f(x) = 5x, where 5Z=(5n : n ∈ Z). Verify that f is an isomorphism. [Dec-99j [S]

Solution:

Step -1 Show that f is 1-l.

Consider f(x) = f(y) for $x, y \in G$

$\therefore$ 5x = 5y definition of f

$\therefore$ x = y $\therefore$ f is 1-1

Step 2 : $\forall\, 5x \in G, \exists x \in G$

s.t. $f(x) = 5x$

$\therefore$ f is onto.

Step-3: Show that f is homomorphism.

For $x * y \in G$

f(x) = 5x, d(y) = 5y and f(x+y) – 5(x+y)

Consider f(x+y) = 5(x+y)   for x, y $\in$G

= 5x + 5y

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

$\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 26 : Let G be a group of real numbers under addition, and let G' be the group of positive numbers under multiplication. Let f : G → G' be defined by f(x) = e^x. Show that f is an isomorphism from G to G'

[May-06]

OR

Show that the group G = (R,+) is isomorphic to G' = (R^+, x) where R is the set of real numbers and R^+ is a set of positive real numbers.

Solution :

Step 1: Show that f is 1-1.

Consider f(x) = f(y)   for x,y$\in$G

$\therefore$ $e^x = e^y$ definition of f

$\therefore$ x = y $\therefore$ f is 1-1.

Step 2 : If $x \in G^1$, then log $x \in G$ and $f\left(.\log x\right) = e^{\log x} = x$ so f is onto.

Step-3 : Show that f is homomnrphism.

For x, y$\in$G

f(x) = e^x, f(y) = e^y and f(x+y) = $e^{(x+y)}$

Consider f(x + y) = $e^{(x + y)}$ for x, y $\in$G

= $e^x \times e^y$

$\therefore$ f(x + y) = f(x) × f(y) f is homomorphism.

Since f is 1-1 and homomorphasm, it is isomorphism.

Example 27 : Let G = {e, a, a^2, a^3, a^4, a^5} be a group under the operation of $a^i a^i = a^r$, where i + j $\equiv$ r(mod 6). Prove that G and Z_6 are isomorphic

[May-07]

Solution :

Step - I : Show that f is l-I.

Let $x = a^i$, and $y = a^j$.

Consider f(x) = f(y) for x, y $\in$ G

$\therefore$ $f(a^i) = f(a^j)$ definition of f

$\therefore$ $a^i = a^j$

$\therefore$ x = y f is 1-1.

Step-2 : Show that f is homomorphism.

Let x = a' and y = a' x, y $\in$ G

$f(a^i) = i$, $f(a^j)$ j and $f(x + y) = f(a^i\ a^j)$

Consider $f(x+y) = f(a^i a^j) = f(a')$ where i + j = r(mod 6)

= r

= i + j

= $f(a^i) + f(a^j)$

$\therefore$ $f(x \times y) = f(x) + f(y)$ $\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 28 : Let T be set of even integers. Show that the semigroups (Z, +) and (T, +) are isomorphic. [May-05]

Solution : We show that f is one to one onto .

Define f : (Z, +) → (T, +) as f(x) = 2x

1) Show that f is l-1

Consider f(x) = f(y)

$\therefore$ 2x = 2y

$\therefore$ x = y $\therefore$ f is 1-l.

2) Show that f is onto

y = 2x $\therefore$ x = y/2 when y is even.

$\therefore$ for every y$\in$T there exists x$\in$Z.

$\therefore$ f is onto.

$\therefore$ f is isomorphic.

3) F is homorphism

F (x + y) = 2 (x + y)

= 2x + 2y

= f(x) + f(y)

$\therefore$ f is honomorphism.

Example 29 : For the set A = {a,b,c} give all the permutations of A. Show that the set of all permutations of A is a group under the composition operation.

Solution : A={a,b,c}. S_3= Set of all permutations of A.

$$f_0 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad f_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad f_2 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$$f_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \quad f_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad f_5 = \begin{pmatrix} a & b & c \\ c & a & b` \end{pmatrix}$$

Let us prepare the composition table.

0	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_4	f_3	f_1
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	f_0
f_5	f_5	f_2	f_3	f_1	f_0	f_4

i) **Closure Property:** Since all the elements in the composition table $\in S_3$, closure property is satisfied.

ii) **Associative Property:** Since composition of permutations is associative, associative property is satisfied.

iii) **Existance of Identity:** From the table we find that fo is the identity

iv) **Existance of Inverse:** From the composition table it is clear that

$f_0^{-1} = f_0$, $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_5$, $f_5^{-1} = f_4$

∴ Every element has inverse in S_3. Hence S_3 is a group.

6.12 COSET AND NORMAL SUBEROUP:

Left Coset : Let (H, ∗) be a subgroup of (G, ∗). For any a ∈ G, the set of aH defined by $aH = \{a * h \,/\, h \in H\}$ is called the **left coset** of H in G determined by the element a∈G. The element a is called the representative element of the left coset aH.

Right Coset : Let (H, ∗) be a subgroup of (G, ∗). For any a ∈ G, the set of Ha defined by

$Ha = [h * a \,|\, h \in H]$

is called the **right coset** of H in G determined by the element $a \in G$. The element a is called the representative element of the right coset Ha.

Theorem 6.7: Let (H, $*$) be a subgroup of (G, $*$). The set of left cosets of H in G form a partition of G. Every element of G belongs to one and only one left coset of H in G.

Theorem 6.8 : The order of a subgroup of a finite group divides the order of the group.

Corollary : If (G, $*$) is a finite group of order n, then for any $a \in G$, we must have $a^n = e$, where e is the identity of the group.

Normal Subgroup : A subgroup (H, $*$) of (G, $*$) is called a normal subgroup if for any $a \in G$, aH = Ha.

Example 30 : Determine all the proper subgroups of symmetric group (S_3, o). Which of these subgroups are normal?

Solution : S = {1, 2, 3}. S_3 = Set of all permutations of S.
S_3 = {f_0, f_1, f_2, f_3, f_4, f_5 } where

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Let us prepare the composition table.

0	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_4	f_3	f_1
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	f_0
f_5	f_5	f_2	f_3	f_1	f_0	f_4

From the table it is clear that {f_0, f_1}, {f_0, f_2,}, {f_0, f_3) and {f_0, f_4, f_5} are subgroups of (S_3, 0): The left cosets of {f_0, f_1} are {f_0, f_1}, {f_2, f_5}, {f_3, f_4}. While the right cosets of {f_0, f_1} are {f_0, f_1}, {f_2, f_4}, {f_3, f_5}. Hence {f_0, f_1} is not a normal subgroup.

Similarly we can show that {f_0, f_2} and {f_0, f_1} are not normal subgroups.

On the other hand, the left and right cosets of $\{f_0, f_4, f_5\}$ are $\{f_0, f_4, f_5\}$ and $\{f_1, f_2, f_3\}$.

Hence $\{f_0, f_4, f_5\}$ is a nomal subgroup.

Example 31: Let S = {1, 2, 3}. Let G = S_3 be the group of all permutations of elements of S, under the operation of composition of permutations.

Let H be the subgroup formed by the two permutations $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Find the left coset of H in G. Is H a normal subgroup? Explain your notion of composition clearly. [Dec-02, Nov-06]

Solution : Let

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$\therefore$ H=$\{f_0, f_2\}$

<u>Left Cosets of H in G :</u>

$f_0H = \{f_0f_0, f_0f_2\} = \{f_0, f_2\}$ $\quad$ $f_1H = \{f_1f_0, f_1f_2\} = \{f_1, f_4\}$

$f_2H = \{f_2f_0, f_2f_2\} = \{f_2, f_0\}$ $\quad$ $f_3H = \{f_3f_0, f_3f_2\} = \{f_3, f_5\}$

$f_4H = \{f_4f_0, f_4f_2\} = \{f_4, f_1\}$ $\quad$ $f_5H = \{f_5f_0, f_5f_2\} = \{f_5, f_3\}$

<u>Right Cosets of H in G</u>

$Hf_0 = \{f_0f_0, f_2f_0\} = \{f_0, f_2\}$ $\quad$ $Hf_1 = \{f_0f_1, f_2f_1\}=\{f_1, f_3\}$

Since f_1 H $\neq$ Hf_1 , H is not a normal subgroup of G.

Example 32 : Consider the dihedral group (D_4, 0). Find the subgroup of D_4 generated by $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ Is it normal subgroup. Find the left cosets of D_4.

Solution: $\quad$ $D_4 = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ $\quad$ [Dec-99][6]

Example 33 : Define a normal sub-group. Let S_3 = Group of all permutations of 3 elements (say 1, 2, 3). For the following subgroups of S, find all the left cosets . Subgroup of A = {1,(1,2)}

Where I = identity permutation, (1, 2) is a transposition. Is A a normal subgroup. State a normal subgroup of the above group if it exists. [98][7]

Solution : $H = \{f_0, f_3\}$

The left cosets of H in G are as follow.

$f_0H = \{f_0, f_3\}$	$f_1H = \{f_1, f_5\}$	$f_2H = \{f_2, f_4\}$
$f_3H = \{f_3, f_0\}$	$f_4H = \{f_4, f_2\}$	$f_5H = \{f_5, f_1\}$

Consider a right coset $Hf_1 = \{f_1, f_4\}$

Since $f_1H \neq Hf_1$, H is not a normal subgroup of G.

6.13 UNIT END EXERCISES

1) Determine whether the set Q, the set of all rational number with the binary operation of addition is a group. If it is a group, determine if it abelian, specify the identity and the inverse of a general element.

2) If G is a set of all not-zero real numbers and $a * b = \frac{ab}{2}$, show that

(G, $*$) is an abelian group. [May-05]

3) Let G be a set of integers between 1 and 15 which are co-prime to 5. Find the multiplication table of G. Find 2^{-1}, 7^{-1}, 11^{-1}. Is G cyclic? [May-05]

4) Check whether it is an abelion group in each of the following cases-

i) R, set of real numbers where a * b = a + b +7

ii) 5 = Q × Q with operation defined as (a, b) * (c, d) = (ac, ad + b).

5) Determine whether the following sets along with the binary operation, form a group. If it is a group, state the identity, and the inverse of an element a. If it is not a group, state the reason why ?

[Oct-03]

i) Set is P(S) = set of all subsets of S where S is a non-empty set. The operation is that of union.

ii) Set of all non-zero real numbers, under the operation of multiplication.

6) Let H be a subgroup of a group G. Define the following [Oct-03]

i) Left coset of H in G.

ii) Right coset of H in G.

7) If G is a finite group then prove that $a^{|G|} = e$.