Date : / /
Page No.

Unit-3

Algebric Structure

↓

Semi group

↓

Monoid

↓

group

↓

Albelian group

$N = \{1, 2, 3, 4 \ldots \infty\}$ Decimal, -ve no, 0 are not Natural

$Z = $ { set of all integers } $-1.43, 3.14$ are not integers

$Q = $ { set of all rational no }

$R = $ { set of all Real no }

$C = $ { set of all complex no }

$\boxed{Q^* = Q - 0}$

Algebric structure

A non empty set S is called Algebraic structure w.r.t binary operation if $(a * b) \in S$ where $(a, b) \in S$

$*$ ↓ Binary operation

$*$ is closure operation on S

(1) $(N, +)$ $5 + 7 = 12$

$+ \rightarrow$ closure on N

Natural no

Natural no $= 0$ not a natural no

(2) $(N, \cdot) \rightarrow 2 \cdot 3 = 6$

Date : / /
Page No.

(3) $(N, -)$
$4-2 = 2$ $1-1=0$ No

(4) $(N, \div)$
$4 \div 2 = 2$ $3 \div 2 = 1.5$ No

(5) $(Z, +, \cdot, -, \div)$
$4+2=6$, $4 \cdot 2 = 8$, $4-2=2$, $3 \div 2$ = No

(6) $(R, +, \cdot, -, \div)$
yes, yes, yes, yes

(7) $(Q \div 0)$
$3/0 = \infty$ No

(8) $(Q^*, \div)$
yes

<u>Semi group</u>: An algebric structure $(S, *)$ is called semi group if it follows associative property

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

$\Rightarrow$ $(N, +)$ = yes

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

Date: / /
Page No.

$\Rightarrow (Z, *) = $ yes

$\Rightarrow (N, -) = $ No

Monoid: A Semigroup $(S, *)$ is called monoid if there exists an element $e \in S$ such that

$(a * e) = (e * a) = a \ \forall \ a \in S$

element e is called identity element of S w.r.t $*$

$\Rightarrow (N, \cdot)$

$3 \cdot e = 3$

$\boxed{e = 1}$

$\Rightarrow (Z, +)$

$\cdot 3 \oplus$ ~~e~~ $=$ $3 + e = 4$ $\qquad$ $3 + e = 3$

$e = 4 - 3$ $\qquad$ $\boxed{e = 0}$

$\boxed{e = 1}$

Group: A monoid $(S, *)$ with identity element 'e' is called a group if to each element $b \in S$ such that

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

then 'b' is called inverse of a denoted as a^{-1}

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

Date: / /
Page No.

$5 + \_\_ = e$

$e \to 5 + e = 5$
$5 + 0 = 5$
$e = 0$

$5 + (-5) = 0$

AS → Closure
SG → Associativity
Monoid → Identity

$\boxed{\text{Group} \to \text{Inverse}}$

$5 \cdot \_\_ = e$
$5 \cdot e = 5$
$e = 1$

$5 \cdot e = 1$
$e = \frac{1}{5}$

<u>Homomorphism Of Groups</u>: If (G, O) and (G', O') are two groups then a mapping function of such that $G \to G'$ is called homomorphism if

$f(a \, O \, b) = f(a) \, O' \, f(b) \ \forall \ a, b \in G$

$(G, O) \quad (G', O')$

Date: / /
Page No.

eg: $(G, +)$ $G \rightarrow$ set of real no
$(G', *)$ $G' \rightarrow$ set of non-zero number
$f(x) = 2^x$, $x \in G$, check if function is homorphism

Sol let $(a, b) \in G$
$f(a) = 2^a$, $f(b) = 2^b$

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

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

Isomorphism in Groups

If (G, O) & (G', O') are two groups, then a one-one onto bijective mapping such that $f: G \rightarrow G$ is called isomorphism from G to G' is f is homomorphism
also $\Rightarrow$ isomorphism
G f G'

G' elements mapped to only one element if G & each G element

$f(a.b) = f(a)$ $O' f(b)$ $\forall$ $a, b \in G$

Ex $(G, +) \longrightarrow G$, is a set of real no
$(G', *) \rightarrow G'$ is set of non-zero

$f(x) = 2^x$ $\forall$ $x \in G$
show that f is isomorphism
show that f is one-one, onto, homorphism
Prove that f is one-one

Date : / /
Page No.

Sol i) for One - one
let $x_1, x_2 \in G$ i.e $f(x_1) = 2^{x_1}$
$f(x_2) = 2^{x_2}$

$f(x_1) = f(x_2)$
$2^{x_1} = 2^{x_2}$
$x_1 = x_2$

$f: G \to G'$ is one - one

ii) for onto
$f(x) = 2^x$
let $f(x) = y$
$y = 2^x$
$\log_2 y = \log_2 2^x$

$\log_2 y = 2$

For onto - y do not have any value whose G' value is not available

An y non zero +ve value will always give real no.

iii) f is homomorphism

let $a, b \in G$
i.e $f(a) = 2^a$ and $f(b) = 2^b$

and $f(a+b) = 2^{a+b}$
$= 2^a \cdot 2^b$
$f(a+b) = f(a) \times f(b)$
$\therefore$ f is isomorphism.

Date : / /
Page No.

Abelian Group: A group $(G, *)$ is said to be abelian if $(a*b) = (b*a)\ \forall\ a, b \in G$

① $(Z, +)$

$10+7 = 7+10$

$-10+7 = 7+(-10)$

$-3 = -3$

② $(N, \cdot)$

It is not a abelian group because it is not a group

③ $(R^*, \cdot)$

It is an abelian group

Q Show that the set $\{1, 2, 3, 4, 5\}$ is not a group under addition & multiplication Modulo 6. Let $G = \{1, 2, 3, 4, 5\}$

6 sa kam hg

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

$0 \notin G$ Group is $(G, +_6)$ Not closed

$6 \overline{)7}$ 1
6
1

$6 \overline{)2}$ 0
0
2

$6 \overline{)18}$ 2
12

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

Date : / /
Page No.

Subgroup

A subset H of G is called a subgroup of G if H also forms a group under the operation $*$. Denoted by $H \subseteq G$ read as "H is a subgroup of G".

Basic properties of Subgroup:

① A subset H of the group G if and only if it is non empty and closed under products and inverse.

$\Rightarrow$ $a \in H$ and $b \in H$

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

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

② The identity of subgroup is the identity of the group.

③ The inverse of an element in a subgroup is the inverse of an element in the group.

④ The intersection of subgroups A and B is again a subgroup.

⑤ The Union of subgroups A and B may be or be a subgroup.

Q Let $G = \{1, -1, i, -i\}$ is a multiplicative group and $H = \{1, -1\}$ where $H \subseteq G$ then show that H is a subgroup.

Date : / /
Page No.

Sol

X	1	-1
1	1	-1
-1	-1	1

① Closure
② Associative
③ Identity element
④ Inverse.

⇒ Closure Property
In Which all elements Which follows Closure Property. $\{1, -1\}$

⇒ Associative Property

$(1 \times -1) \times 1 = 1 \times (-1 \times 1)$
$-1 = -1$

⇒ Identity Element
1 It is an identity Element
$1 \times 1 = 1$ $1 \times -1 = -1$ $e = 1$

⇒ Inverse Element
$1^{-1} = 1$
$-1^{-1} = -1$

So inverse element is Present

Cosets
let H be a subgroup of a Group G Whose Composition have been denoted multiplicative
let $a \in G$

$Ha = \{ha : h \in G\} \rightarrow$ Right Coset
$aH = \{ah : h \in G\} \rightarrow$ left Coset

Q ① Multiplicative Group $G = \{1, -1, i, -i\}$
$H = \{1, -1\}$

Right Coset

$H \cdot 1 = \{1, -1\}$
$H \cdot -1 = \{-1, 1\}$
$H \cdot i = \{i, -i\}$
$H \cdot -i = \{-i, i\}$

Left Coset

$1 \cdot H = \{1, -1\}$
$-1 \cdot H = \{-1, 1\}$
$i \cdot H = \{i, -i\}$
$-i \cdot H = \{-i, i\}$

Properties of Coset

① $H \cdot e = e \cdot H = H$
if e is the identity element

② $Hh = H \iff h \in H$

$H = \{1, -1\}$
$H \cdot 1 = \{1, -1\}$

③ If a and b are element of Group G

$Ha \cap Hb = \phi$ —— or $Ha = Hb$

$H \cdot 1 = \{1, -1\}$
$H \cdot i = \{i, -i\}$
$H \cdot 1 \cap H \cdot i = \phi$

$H \cdot 1 = H = \{1, -1\}$
$H \cdot -1 = H = \{-1, 1\}$

④ $a \in Ha$ {any element lies in the right coset}

$H \cdot 1 = \{1, -1\} = H$
$H \cdot -i = \{-i, i\} \neq H$

⑤ Order of the right coset is equal to order of subgroup is equal to order of left coset.

Date: / /
Page No.

$H = \{1, -1\}$

$H \cdot 1 = \{1, -1\} = H$

$H \cdot i = \{i, -i\} = H$

(6) In general $Ha \neq aH$

(7) $Ha = aH$, G is abelian group

(*) If the composition in the group G has been denoted additively, then

Right Coset $= H + a = \{h + a : h \in H\}$

left Coset $= a + H = \{a + h : h \in H\}$

Ex $(Z, +)$: addition group of integers

~~H = 3Z,+~~ $H = (3Z, +)$

$Z = \{-3, -2, -1, 0, 1, 2, 3, ----\}$

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

~~Z = 0~~

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

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

$H + 2 = \{-7, -4, -1, 2, 5, 8, 11, ---\}$

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

$H + 5 = \{-4, -1, 2, 5, 8, 11, 15 ---\}$

$H = H + 3$

$H + 2 = H + 5$

$H + 1$

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

Lagrange's Theorem

Statement: The order of each subgroup of a finite group is divisor of the order of group.

$O(H) \mid O(G)$

$O(G) \rightarrow$ order of group
$O(H) \rightarrow$ order of subgroup

let $O(G) = n \rightarrow$ elements of group
let $O(H) = m \rightarrow$ elements of subgroup

$\boxed{m/n}$ ie $n = Km$
↳ it means m divides n

$2/4 \Rightarrow 4 = 2^2$
↳ K

let $H = \{h_1, h_2, h_3, \ldots h_m\}$

Coset $a_1 \in G$
$Ha_1 = \{h_1a_1, h_2a_1, h_3a_1, \ldots h_ma_1\}$
$a_2 \in G$
$Ha_2 = \{h_1a_2, \ldots h_ma_2\}$
m coset can be formed
let K = distinct coset

$Ha_3 = \{h_1a_3 \ldots h_ma_3\}$
$\vdots$
$Ha_K = \{h_1a_K \ldots h_ma_K\}$

Date: / /
Page No.

$G = H \cup Ha_1 \cup Ha_2 \cdots \cup Ha_k$
= no of element in H + ... + no of element in Ha_k

$m + m + m + \cdots$ K times
$O(G) = K \cdot m$
$n = Km$
$m/n \to m$ divides n
Hence Proved.

Permutation and Permutation group

Let P be a finite set having n distinct element then a one-~~one~~ one, onto mapping from P to itself is called a Permutation of ~~[illegible]~~ degree n

Ex: $P = \{1, 2, 3\}$

$f : P \to P \Rightarrow$ Permutation

~~eg~~ $\sigma = (P_i) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$3! = 6 \to$ Total no of Permutation

$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

It is easy to verify that the Collection of all Permutation of a known empty set a forms a groups under the operation composition. This group is called a

Permutation group. It is denoted by S_n

$f : A \longrightarrow A, \quad A \neq \phi$

$S_n = \{ f_1 : f_1 : A \rightarrow A$ is a Permutation$\}$

(S_n, o) → Operation

↳ Permutation group

Identity Permutation

If each element of a Permutation is replaced by itself. Then it is called the identity Permutation and it is denoted by symbol I. For eg

$$I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

Equality Of Permutation

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

Eg: let f and g be given by

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

$f(1) = 2 = g(1) \qquad f(3) = 4 = g(3)$

$f(2) = 3 = g(2) \qquad f(4) = 1 = g(4)$

Date: / /
Page No.

Product of Permutations

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

$$fog = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}$$

Q Find the Product of two Permutation and Show that it is not Commutative

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

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

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}^{a_1 a_n}_{b_1 - b_n} \begin{pmatrix} 2 & 1 & 4 & 3 \\ 2 & 3 & 4 & 1 \end{pmatrix}^{b_1 - b_n}_{c}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^{a_1 - a_n}_{c_1 - c_n}$$

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

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

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

Date : / /
Page No.

Q $U = \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 6 \end{pmatrix}$

$V = \begin{pmatrix} 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 \end{pmatrix}$

find: UV, VU

$UV = \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 6 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 \end{pmatrix}$

$= \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 6 \end{pmatrix} \begin{pmatrix} 7 & 5 & 8 & 6 \\ 7 & 5 & 6 & 8 \end{pmatrix}$

$= \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 8 \end{pmatrix}$

$VU = \begin{pmatrix} 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 \end{pmatrix} \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 5 & 8 & 6 \end{pmatrix}$

$= \begin{pmatrix} 5 & 6 & 7 & 8 \\ 5 & 8 & 7 & 6 \end{pmatrix} \begin{pmatrix} 5 & 8 & 7 & 6 \\ 7 & 6 & 8 & 5 \end{pmatrix}$

$= \begin{pmatrix} 5 & 6 & 7 & 8 \\ 7 & 6 & 8 & 5 \end{pmatrix}$

Date: / /
Page No.

Normal Subgroup

let $G(x)$ be a group and H is a subgroup under the same binary operation $*$, then for any $a \in G$, if

$aH = \{a*h \mid h \in H\}$ $H \trianglelefteq G$ {Representation}
$Ha = \{h*a \mid h \in H\}$

then $aH = Ha$ {Left Coset = Right Coset}
that subgroup H is called as Normal subgroup of G
For abelian group $aH = Ha$
H = Normal subgroup $\forall\ a \in G$.

Improper / Trivial Normal subgroup =

$$\begin{cases} \{e\} & ea = ae\ \forall\ a \in G \\ \{G\} & Ga = aG\ \forall\ a \in G \end{cases}$$

Each group has two ~~one~~ normal subgroups -
$\{e\}$ and $\{G\}$
Other than $\{e\}$ and $\{G\}$ normal subgroups are called Proper Normal subgroups.

Q let H be a subgroup of G, then H is a normal subgroup if $aha^{-1} \in H\ \forall\ a \in G, h \in H$

Sol let H is a normal subgroup i.e. $aH = Ha$
We have to prove that $aha^{-1} \in H$

let $x \in aH$, $x \in Ha$

Date : / /
Page No.

$x = a * h$ — (1) $\quad x = h_1 * a$ — (2)

from (1) and (2)

$a*h = h_1 * a$
Multiply a^{-1} both on LHS & RHS

$(a*h)\,a^{-1} = (h_1 * a) * a^{-1}$
$= h_1 * (a * a^{-1})$
$= h_1 * e$
$(a*h) * a^{-1} = h_1$ & $h_1 \in H$

$(a*h) * a^{-1} \in H$
or
$aha^{-1} \in H \ \forall\ h \in H,\ a \in G$

let $aha^{-1} \in H$ and we have to prove that H is a normal subgroup $aH = Ha$

let $x = aH$ — (1)
$x = a*h = ah$
Multiply a^{-1} on both sides

$xa^{-1} = aha^{-1}$, here $aha^{-1} \in H$

So $xa^{-1} \in H$

Multiply a on both sides

$(xa^{-1})a \in Ha$
$x(a^{-1}a) \in Ha$
$xe \in Ha$ — (2)

Date: / /
Page No.

$x \in Ha$ - ②

From ① & ② $aH \subseteq Ha$

Hence $aH = Ha$

Factor / Quotient group

A group whose element are the coset of a normal group of a given group is called as Quotient or a factor group.

If G is a group and N is a Normal subgroup of G, then the set of all cosets of N in G forms a group. This group is called as quotient group or factor group of G relative to N.

It is denoted by G/N.

$G/N = \{ Na / a \in G \}$ or

$\{ aN / a \in G \}$

as $aN = Na$

Date: / /
Page No.

Cayley's theorem

Every group is isomorphic to a group of permutations.

V	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\lambda_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix} \quad \theta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)$$

$$\lambda_a = \begin{pmatrix} e & a & b & c \\ e & e & c & b \end{pmatrix} \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

$$\lambda_b = \begin{pmatrix} e & a & b & c \\ b & c & \cancel{a}e & a \end{pmatrix} \quad \theta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$

$$\lambda_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix} \quad \theta_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$

Hence G is isomorphic to the subgroup of S_4

$\{1, (12)(34), (13)(24), (14)(23)\} =$

$\{(12)(34), (13)(24)$