

Unit-3

Group theory (adherence of set theory)

Algebraic structure:-

on non empty set G along with a binary operator is called algebraic structure (or) algebraic system

Here it is written as $(G, *)$

where G is any set

$*$ is any binary operator

Ex:-

$(\mathbb{N}, +)$

$(\mathbb{Q}, -)$

$(\mathbb{R}, *x)$

Binary operator:-

Let S be any non empty set if $f: S \times S \rightarrow S$ is a mapping then f is called a binary operator in S .

→ we use the symbols $+, -, \times, \div, *, \oplus, \circ$ for binary operator

Ex:-

① define a binary operator $*$ as $a * b = ab$
for $a, b \in S$

② define a binary operator \circ as $a \circ b = a$
for $a, b \in S$

Properties:-

1) Closure :-

If $a * b \in S$ & $a, b \in S$ then we say that it satisfies the closure property.

2) Associative :-

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

3) exists^{ent}'s of identity :-

There $\Rightarrow a * e = e * a = a$

such that $\forall a \in S$

$$\begin{cases} (N, \times) \Rightarrow 1 \times a = a \times 1 = a \\ (Q, +) \Rightarrow 0 + a = a + 0 = a \end{cases}$$

4) exists^{ent}'s of inverse :-

If $b \in S \Rightarrow a * b = b * a = e$ for

any $a \in S$

$$\begin{cases} 1, 1 \Rightarrow 1 - 1 = 0 \\ 2 \times \frac{1}{2} \Rightarrow 1 \Rightarrow \text{multiplicative} = 1 \end{cases}$$

(additive = 0)

5) commutative commutative :-

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

Groupoid :-

An algebraic structure $(G, *)$ which satisfies only closure property is called groupoid.

Semi-group:-

An algebraic structure $(G, *)$ is said to be semi-group if it satisfy's closer, & associative property

Monoid:-

An algebraic structure $(G, *)$ is said to be monoid if it satisfy's closer, associative, exists of identity

* Group:-

An algebraic structure $(G, *)$ is said to a group if it satisfy's closer

1) closer $\Rightarrow a * b \in G \quad \forall a, b \in G$

2) associative $\Rightarrow (a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

3) exists of Identity

$$\exists e \in G \quad \Rightarrow a * e = e * a = a \quad \forall a \in G$$

4) exists of inverse

$$\exists e \in G \quad \Rightarrow a * b = b * a = e \text{ for any } a \in G$$

Abelian Group:-

A group is said to abelian group if it satisfy commutative property

10) Let 'S' be a non-empty set and ' \circ ' is the binary operator defined by $a \circ a = a$
 $\forall a, b \in S$ determine whether ' \circ ' is commutative & associative in S.

i) $a \circ b = a$

$$b \circ a = b$$

$$a \circ b \neq b \circ a$$

ii) $(a \circ b) \circ c = a \circ c = a$

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

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

20) Circled op ' \circ ' operation is defined on \mathbb{Q}

$$\text{as } a \circ b = a + b - ab \quad \forall a, b \in \mathbb{Q} \text{ is the}$$

operation ' \circ ' is binary operation in \mathbb{Q}

if so is it associative & commutative

i) $a \circ b = a + b - ab \in \mathbb{Q}$

ii) $(a \circ b) \circ c = (a + b - ab) \circ c$
 $= (a + b - ab) + c - (a + b - ab)c$
 $\Rightarrow a + b + c - ab - ac - bc + abc$

$$a \circ (b \circ c) \Rightarrow a \circ (b + c - bc)$$

$$a + (b + c - bc) - a(b + c - bc)$$

$$\Rightarrow a + b + c - bc - ab - ac + abc$$

iii) $a \circ b = a + b - ab$

$$b \circ a = b + a - ba$$

3Q) prove that $(P(S), \cap)$ is a semi-group
 where $P(S)$ is powerset of S and
 ' \cap ' insertion

i) if $A, B \in P(S)$

$$\Rightarrow A \cap B \in P(S)$$

it satisfy's closer

ii) we know that

$$(A \cap B) \cap C = A \cap (B \cap C)$$

so it satisfy's associative property

Hence it is a semi-group

4Q) determine whether (\mathbb{Q}, \circ) is semi-group
 where \mathbb{Q} is a set of rational numbers
 and binary operator is defined as

$$a \circ b = a - b + ab$$

i) if $a, b, c \in \mathbb{Q}$

$$\Rightarrow a \circ b \in \mathbb{Q}$$

$$\text{ii) } (a \circ b) \circ c \Rightarrow (a - b + ab) \circ c$$

$$\Rightarrow (a - b + ab) - c - (a - b + ab)c$$

$$\Rightarrow a - b - c - abc - bc - ac - bc + ac + bc$$

$$\Rightarrow a - b - c - 2ac - abc$$

$$\begin{aligned}
 a \circ (b \circ c) &\Rightarrow a \circ (b - c + bc) \\
 &\Rightarrow a - (b - c + bc) - a(b - c + bc) \\
 &\Rightarrow a - b - c - ab - ac - ab + bc \\
 &\quad - ab - ac \\
 &\Rightarrow a - b - c - 3ab - ac
 \end{aligned}$$

50) prove that (\mathbb{Q}, \cdot) is abelian group where
 \cdot is usual multiplication

i) $\forall a, b \in \mathbb{Q} \Rightarrow a \cdot b \in \mathbb{Q}$

ii) Associative

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in \mathbb{Q}$$

iii) Identity

$$\exists e \in \mathbb{Q} \ni a \cdot 1 = 1 \cdot a = a, \quad \forall a \in \mathbb{Q}$$

iv) Inverse

there is no inverse or $\forall b \in \mathbb{Q}$

$\therefore (\mathbb{Q}, \cdot)$ is not abelian group

but monoid

6) $(\mathbb{Q}, +)$

i) $\forall a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$

closed

ii) $a + (b + c) = (a + b) + c \quad \forall a, b, c \in \mathbb{Q}$

associative

iii) $\exists 0 \in \mathbb{Q} \ni a + 0 = 0 + a = a \quad \forall a \in \mathbb{Q}$ (Identity)

iv) $\exists -a \in \mathbb{Q} \ni a + (-a) = (-a) + a = 0$ for any

$a \in \mathbb{Q}$

(Inverse)

$$v) a+b = b+a \quad \forall a, b \in \mathbb{Q}$$

$(\mathbb{Q}, +)$ is $A \cdot G$

7) prove that $\{G_0 = \{1, \omega, \omega^2\}\}$ is a $A \cdot G$ with
representive multiplication where $1, \omega, \omega^2$ are
cubic root of unity

composition table (CT)

\cdot	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$$\therefore \omega^3 = 1$$

$$\omega^4 = \omega$$

i) Closure :-

All the values in the table are in G
so it satisfy closure

e) Associative :-

usual multiplication is associative so it
satisfy's associative

3) Identity :-

The value against 1, i.e 1st row & col
are same so Identity element is 1

4) Inverse :-

1 is 1

ω is ω^2

ω^2 is ω

5) commutative :-

the table is symmetric so it is commutative

8) show that $G_2 = \{1, -1, i, -i\}$ is a G with
respective multiplication where $i = \sqrt{-1}$

C. T

	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1) closer

2) associative

3) Identity

4) Inverse

$$1 \Rightarrow 1$$

$$-1 \Rightarrow -1$$

$$i \Rightarrow -i$$

$$-i \Rightarrow i$$

5) commutative

q) prove that a set \mathbb{Z} of all integers with
binary operation * defined by $a * b = ab + 1$

$\forall a, b \in \mathbb{Z}$ is an A.G

i) closer

$$a * b = ab + 1 \in \mathbb{Z} \quad \forall a, b \in \mathbb{Z}$$

ii) Associative

$$(a * b) * c = (a + b + 1) * c$$

$$= (a + b + 1) + c + 1$$

$$= a + b + c + 2$$

$$e a * (b * c) = a + (b + c + 1) * 1$$

$$= a + (b + c + 1) + 1$$

$$= a + b + c + 2$$

iii) Identity :-

$$a * e = a \Rightarrow a + e + 1 = a$$

$$\Rightarrow e = -1$$

iv) Inverse

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

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

$$\Rightarrow b = -2 - a$$

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

$$\in \mathbb{Z} \text{ & } a \neq -2$$

$\therefore -(a+2)$ is inverse of $a \in \mathbb{Z}$

v) Commutative :-

$$a * b = a + b + 1$$

$$b * a = b + a + 1$$

$$\therefore a * b = b * a$$

10) show that (\mathbb{Q}^+, \odot) is an AG where \mathbb{Q}^+ is all positive rational numbers & operator \odot is defined by $a \odot b = ab/3$

i) closure

$$a \odot b = ab/3 \quad \forall a, b \in \mathbb{Q}^+$$

ii) Associative

$$(a \odot b) \odot c = \left(\frac{ab}{3}\right) \odot c = \frac{abc}{9}$$

$$a \odot (b \odot c) = \frac{abc}{9}$$

iii) Identity

$$(a \odot e) = a \Rightarrow \frac{ae}{3} = a$$

$$e = 3$$

iv) Inverse

$$(a \odot b) = e$$

$$\Rightarrow \frac{ab}{3} = 3$$

$$\Rightarrow ab = 9$$

$$\Rightarrow b = 9/a$$

$$\Rightarrow a = 9/b$$

v) $(a \odot b) = \frac{ab}{3}$

$$(b \odot a) = \frac{ba}{3}$$

Addition modulo m:-

If a, b are any two integer & r is the least non-negative number obtained by dividing the ordinary sum $a+b$ by m then the addition modulo m of $a+b$ is r .

\rightarrow Symbolically $a +_m b = r \quad (0 \leq r < m)$

ex:-

$$3 +_5 2 = 5 = 0$$

$$m=5$$

$$7 +_5 2 = 4 \Rightarrow m=5$$

$$r=4$$

$$5) 9(1$$

$$\begin{array}{r} 5 \\ \hline 4 \end{array}$$

multiplication modulo p :-

If a & b are two integers and r is the least non-negative remainder obtained by dividing ordinary product of a and b by p then the multiplication modulo p of a & b is r

\rightarrow symbolically $a \times_p b = r \quad (0 \leq r < p)$

ex:-

$$5 \times_3 2 = 1$$

(Q) Show that set ' G_5 ' is AG where G_5 is the set of addition modulo 5

$$G_5 = \{0, 1, 2, 3, 4\}$$

$+_5$	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

so it is

closer \Rightarrow all the values are in G_2

$$\text{associative} \Rightarrow 1+5(3+54) = 1+52 = 3$$

$$\text{Identity} \Rightarrow (1+53)+54 = 4+54 = 3$$

(co) $1^{\text{st}} \text{ row} \& 1^{\text{st}} \text{ col}$ are same as in G_2

$$\text{Inverse} \Rightarrow 0^{-1} = 0$$

$$1^{-1} = 4$$

$2^{-1} = 3$ all the elements have

$$3^{-1} = 2$$
 inverses

$$4^{-1} = 1$$

commutative

the table is symmetric so set G_2 is commutative

\therefore set G_2 is $A\text{-Grp}$

12) show that the set G_2 of multiplication modulo

5 is an $A\text{-Grp}$

$$G_2 = \{1, 2, 3, 4\}$$

$\times 5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

So it is

closer:-

all the values are in G_2

associative

$$2 \times 5(3 \times 54) = 2 \times 52 = 4$$

$$(2 \times 53) \times 54 = 1 \times 54 = 4$$

Identity

$$c=1$$

Inverse

$$1^{-1} = 1$$

$$2^{-1} = 3$$

$$3^{-1} = 2$$

$$4^{-1} = 4$$

commutative

- the table is symmetric so set is commutative

commutative

\therefore set G is a group

- 13) $G_2 = \{1, 5, 7, 11, 13, 17\}$ x_{18} find construct
 composition table & find inverse of all elements

C-T:

x_{18}	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	13	1	7	5
17	17	13	11	7	5	1

$$\begin{aligned}
 121/18 &= 6.72 \\
 -6 \\
 \hline
 0.72 \times 18 & \\
 &= 13
 \end{aligned}$$

Inverse

$$1^{-1} = 1$$

$$5^{-1} = 11$$

$$7^{-1} = 13$$

$$11^{-1} = 5$$

$$13^{-1} = 7$$

$$17^{-1} = 17$$

iii) If G_2 is set of even numbers i.e
 $G_2 = \{ \dots, -4, -2, 0, 2, 4, \dots \}$ then prove
 that G_2 is a group with usual addition as
 an operator.

Sol) Let $a = 2x, b = 2y, c = 2z$

$$a, b, c \in G_2 \text{ & } x, y, z \in \mathbb{Z}$$

$$\text{i)} a+b = 2x+2y = 2(x+y) \in G_2$$

$$\begin{aligned}\text{ii)} a+(b+c) &= 2x + (2y+2z) \\ &= (2x+2y)+2z \\ &= (a+b)+c\end{aligned}$$

$$\text{iii)} a+c = a \quad c = 0 \in G_2$$

$$\text{iv)} a+d = 0 \Rightarrow d = -a \in G_2$$

$$\begin{aligned}\text{v)} a+b &= 2x+2y = 2(x+y) \\ &= 2(y+x) = 2y+2x \\ &= b+a\end{aligned}$$

15) State $G = \{x \mid x = 2^a 2^b \text{ for } a, b \in \mathbb{Z}\}$

under multiplication is Group

Let $x = 2^a \cdot 2^b$, $y = 2^c \cdot 2^d$, $z = 2^e \cdot 2^f$
 $x, y, z \in G$ & $a, b, c, d, e, f \in \mathbb{Z}$

i) $x \cdot y = 2^a \cdot 2^b \cdot 2^c \cdot 2^d$

$$= 2^{a+c} \cdot 2^{b+d}$$

$$a+c, b+d \in \mathbb{Z}$$

$$\therefore x, y \in G$$

ii) $x(y \cdot z) = 2^a \cdot 2^b (2^c \cdot 2^d \cdot 2^e \cdot 2^f)$

$$= (2^a \cdot 2^b \cdot 2^c \cdot 2^d) \cdot 2^e \cdot 2^f$$

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

iii) Let $e = 2^i \cdot 2^j \in G \Rightarrow a \cdot e = a$

$$\Rightarrow (2^a \cdot 2^b)(2^i \cdot 2^j) = 2^a \cdot 2^b$$

$$\Rightarrow 2^{a+i} \cdot 2^{b+j} = 2^a \cdot 2^b$$

$$\text{i.e } a+i=a \Rightarrow j=0$$

$$b+i=b \Rightarrow i=0$$

$\therefore e = 2^0 \cdot 2^0 \in G$ is an identity

iv) Let $y = 2^c \cdot 2^d \Rightarrow x \cdot y = 2^0 \cdot 2^0$

$$2^a \cdot 2^b \cdot 2^c \cdot 2^d = 2^0 \cdot 2^0$$

$$2^{a+c} \cdot 2^{b+d} = 2^0 \cdot 2^0$$

$$= a+c=0 \quad \& \quad b+d=0$$

$$c=-a \quad \& \quad d=-b$$

$\therefore 2^a \cdot 2^{-b}$ is inverse of $2^a \cdot 2^b$

Hence $-a, -b \in \mathbb{Q}$

$$2^{-a} \cdot 2^{-b} \in G_2$$

(Q) Show that a set of ordered pair (a, b) of real numbers for which $a \neq 0$ w.r.t the operator defined by $(a, b) * (c, d) = (ac, bc+d)$

is a group if this commutative

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

i) Clearly $a, b, c, d, \in \mathbb{Q}$

$$\Rightarrow ac, bc+d \in \mathbb{Q}$$

moreover since $a \neq 0$

$$c \neq 0 \Rightarrow ac \neq 0$$

$$\therefore (a, b) * (c, d) \in G$$

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

$$(a, b) * (ce, de+bc+f)$$

$$ace, bce + de + bc + f$$

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

$$= (ac, bc+d) * (e, f)$$

$$\Rightarrow (ace, bce + de + bc + f)$$

$$LHS = RHS$$

iii) Let $(a, b) * (c, d) = (ca, b)$

$$\Rightarrow (ac, bc + d) = (ca, b)$$

$$\therefore ac = ca \& bc + d = b$$

$$\Rightarrow c = 1 \& b + d = b \Rightarrow d = 0$$

$\therefore (1, 0) \in G_2$ is an identity

iv) $(a, b) * (x, y) = (1, 0)$

$$(ax, bx + y) = (1, 0)$$

$$ax = 1 \quad bx + y = 0$$

$$x = 1/a \quad y = -b/a$$

since $a \neq 0 \Rightarrow x \neq 0$

$\therefore (1/a, -b/a)$ is inverse

ele- of (a, b)

v) $(a, b) * (c, d) = (ac, bc + dd)$

$(c, d) * (a, b) = (ca, ad + b)$

$$\therefore bc + dd \neq ad + b$$

$(a, b) * (c, d) \neq (c, d) * (a, b)$

\therefore Hence it is not commutative

Sub-group:-

Let $(G, *)$ be a group & H be non-empty
subset of G . If $(H, *)$ is its self is a Group
then it is called subgroup of $(G, *)$

Ex:-

$(\mathbb{Q}, +)$ subgroup of $(\mathbb{R}, +)$

17) Let $G = \{1, -1, i, -i\}$, $H = \{1, -1\}$ check whether H is subgroup of G

i) closure

it statisfy's closure

$$\begin{array}{c|cc} & 1 & -1 \\ \hline 1 & 1 & -1 \\ i & -1 & 1 \end{array}$$

ii) it statisfy associative

iii) ~~et~~ identity 1 is in G

iv) inverse

$$\begin{aligned} 1^{-1} &= 1 \\ -1^{-1} &= -1 \end{aligned}$$

$\therefore H$ is a group

$\therefore H$ is a subgroup of G

18) prove that $H = \{0, 2, 4\}$ is a subgroup of \mathbb{Z}_6

($\mathbb{Z}_6 +_6$)

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

\mathbb{Z}_6	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

i) closure
it statisfy closure

ii) associative statisfy

iii) identity 0 is in \mathbb{Z}_6

iv) inverse

$$0^{-1} = 0$$

$$2^{-1} = 4$$

$$4^{-1} = 2$$

$\therefore H$ is a group

$\therefore H$ is a subgroup of \mathbb{Z}_6

17) Let S be a set of ordered pair (a, b) of real numbers such that also, binary operator ' \times ' is defined by $(a, b) \times (c, d) = (ac, bc+d)$ prove that (S, \times) gives (H, \times) is a subgroup of (S, \times) given that $H = \{(1, b) / b \in R\}$

i) $(1, a), (1, b) \in H$

$$(1, a) \times (1, b) = (1, a+b) \in H$$

ii) Associative
it also satisfy's associative

iii) $(1, b) \times (1, e) = (1, b)$

$$\Rightarrow (1, b+e) = (1, b)$$

$$\Rightarrow b+e = b$$

$$\Rightarrow e = 0$$

$\therefore (1, 0)$ is identity

iv) $(a, b)^{-1} = (1/a, -b/a)$

$$(1, b)^{-1} = (1, -b) \in H$$

$\therefore H$ is a group

$\therefore H$ is a subgroup of S .

order of an element:-

Let $(G, *)$ be a group and $a \in G$

then if there exists the least positive integer

$n \rightarrow a^n = e$ where e is the identity element in G then n is order of a
written as $O(a) = n$

Ex:-

$$G_2 = \{1, -1, i, -i\}$$

$$1^1 = 1 \quad O(1) = 1$$

$$1^2 = 1$$

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

$$(-1)^2 = 1 \checkmark \quad O(-1) = 2$$

$$i^1 = i \times$$

$$i^2 = -1 \times$$

$$i^3 = -i \times \quad O(i) = 4$$

$$i^4 = 1 \checkmark$$

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

$$(-i)^2 = +1 \times$$

$$(-i)^3 = i \times$$

$$(-i)^4 = 1 \checkmark$$

$$O(-i) = 4$$

order of a group:-

the order of a group is no. of elements in the group

Ex:-

1) $G_2 = \{1, -1, i, -i\}$

$$O(G_2) = 4$$

2) $(S^+, +_S)$

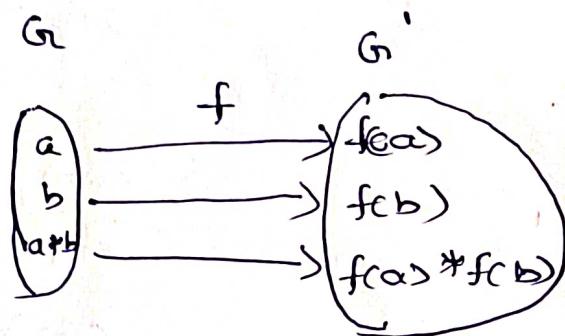
then $O(S^+, +_S) = 5$

functions of group:-

i) Homomorphism:-

A function $f: (G, *) \rightarrow (G', \cdot)$

is said to homomorphism if $f(a * b) = f(a) \cdot f(b)$ where $a, b \in G$ & $f(a), f(b) \in G'$



ii) Endomorphism:-

A homomorphism for a group G to itself is called endomorphism i.e

$$f: (G, *) \rightarrow (G, *)$$

iii) Monomorphism:-

A homomorphism $f: G \rightarrow G'$ is said to monomorphism if it is one-one function

iv) Epi morphism:-

A homomorphism $f: G \rightarrow G'$ is said to epi-morphism if it is onto function.

v) Isomorphisms

A homomorphism $f: G \rightarrow G'$ is said to be isomorphism if it is one-one & onto function.

vi) Automorphisms

An isomorphism f for G to its self is called automorphism.

- Q) Let $(\mathbb{Q}, +)$ be a group & $(G, *)$ be another group where $G = \{2^n | n \in \mathbb{Z}\}$. A function $f: \mathbb{Q} \rightarrow G$ defined by $f(n) = 2^n$ & prove that f is a homomorphism.

Let $n_1, n_2 \in \mathbb{Q} \rightarrow f(n_1) = 2^{n_1}, f(n_2) = 2^{n_2}$

$$f(n_1+n_2) = 2^{n_1+n_2} = 2^{n_1} * 2^{n_2}$$

$$= f(n_1) * f(n_2)$$

$\therefore f$ is homomorphism

- Q) Let $(\mathbb{Q}, *)$ defined by $G = \{1, -1, i, -i\} \in \mathbb{C}(\mathbb{Q}, +)$ be other group prove that $f: \mathbb{Q} \rightarrow G$ is homomorphism where $f(n) = i^n$ & prove

Let $n_1, n_2 \in \mathbb{Q} \rightarrow f(n_1) = i^{n_1}, f(n_2) = i^{n_2}$

$$f(n_1+n_2) = i^{n_1+n_2} = i^{n_1} * i^{n_2}$$

$$= f(n_1) * f(n_2)$$

$\therefore f$ is homomorphism