mood-book

UNIT-3

UNIT-3

Algebraic structures

Algebraic Systems and General properties

⇒ A system consisting of a non-empty set and one or more n-ary operations on the set is called an "Algebraic System".

→ An algebraic system will be denoted by $\{S, f_1, f_2, \ldots\}$

where
S is the non-empty set
$f_1, f_2 \ldots$ are n-ary (n number of) operations on S.

⇒ let $\{S,+\}$ here algebraic system operates $n=1$ operation i.e. Addition

→ $\{S,+,*\}$ " " " " with 2 operations

$n = 0, 1, 2$ → performs 2 operations.
0 → no operation
1 → unary operation

n starts from 0 (zero) but most algebraic systems do 1 or more operations)

→ we will mostly deal with algebraic systems with $n=0,1,$ and 2, containing one or two operations only.

General properties of Algebraic Systems:-

Let $\langle S,*,+\rangle$ be an Algebraic system where $*$ and $+$ are binary operations on S.

① Closure property:-

for any $a,b \in S$, $\boxed{a*b \in S}$

Ex:- If $a,b \in Z$, $a+b \in Z$ and $a*b \in Z$

where + and * are the operations of addition & multiplication.

② **Associative property:-**

for any $a, b, c \in S$, $\boxed{a*(b*c) = (a*b)*c}$

Ex:- If $a, b, c \in Z$

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

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

③ **Commutative property:-**

for any $a, b \in S$, $\boxed{a*b = b*a}$

Ex:- If $a, b \in Z$,

$a+b = b+a$ and

$a*b = b*a$

④ **Identity element:-**

There exists a distinguished element e, $e \in S$, such that for any element 'a', $a \in S$, then

$\boxed{a*e = e*a = a}$

The element $e \in S$ is called the identity element of S with respect to the operation '$*$'.

Ex:- '0' and '1' are the identity elements of 'Z' w.respect to the operations of addition and multiplication respecti-vely.

Since, for any element a, $a \in Z$

$a+0 = 0+a = a$

$a*1 = 1*a = a$

5 Inverse Element:-

For each element 'a', $a \in S$, there exists an element 'a^{-1}', $a^{-1} \in S$ such that $\boxed{a * a^{-1} = a^{-1} * a = e}$

The element a^{-1} is called the inverse of 'a' under the operation '*'.

'e' is called Identity element with respect to the operation '*'.

Ex:- for each $a \in Z$, $-a$ is the inverse of 'a' under the operation, since

$$a + (-a) = 0$$

where '0' is the Identity element of Z under addition

6 Distributive property:-

for any three elements $a, b, c \in S$,

$$\boxed{a * (b + c) = (a * b) + (a * c)}$$

In this case, the operation '*' is said to be distributive over the operation '+'.

for any 3 elements $a, b, c \in Z$

$$\boxed{\begin{gathered} a * (b + c) = (a * b) + (a * c) \\ a + (b * c) = (a + b) * (a + c) \end{gathered}}$$

7 Cancellation property:-

for any 3 elements $a, b, c \in S$ and $a \neq 0$,

$$\boxed{\begin{gathered} a * b = a * c \Rightarrow b = c \\ \& \\ b * a = c * a \Rightarrow b = c \end{gathered}}$$

Ex:- Cancellation property holds good for any $a, b, c \in Z$ under addition & multiplication.

(8) Idempotent property:-

An element a, $a \in S$ is called an Idempotent element with respect to the $*$,

If $\boxed{a * a = a}$

Ex:- $0 \in Z$ is an Idempotent element under addition $\boxed{a=0}$

$0+0=0$

$0,1 \in Z$ are idempotent element under multiplication $\boxed{a=0,1}$

$0 * 0 = 0$

$1 * 1 = 1$

Rough:-

(1) If closure + Associative Property satisfies then it is said Semigroup

(2) llly closure + Associative + Identity satisfies Monoid

(3) closure + Associative + Identity + Inverse Group

(4) closure + Associative + Identity + Inverse + Commutative satisfies Abelian Group (or) Commutative group

(5) Subgroup

$\langle G, * \rangle, \langle H, * \rangle$

$(H, *)$ Subgroup of $(G, *)$

- closure
- Asso
- Identity
- Inverse

S
*
<S,*> ① Clo
② A/So

Semi Group:-

Let S be a non-empty set and '*' be a binary operation on S, then algebraic system <S, *> is called a semi group Iff it satisfies the following properties.

(i) closure property:-

for any two elements a, b where a, b ∈ S then

$$\boxed{a * b \in S}$$

(ii) Associative property:-

for any 3 elements a, b, c where a, b, c ∈ S then

$$\boxed{a*(b*c) = (a*b)*c}$$

Ex:- E is the set of even positive numbers, (E, +), (E, *) are semi groups.

(N, +) is a semi group.

⇒ Prove (E, *) is a semi-group.

Suppose $E = \{2, 4, 6, 8, 10, 12 \ldots\}$

Take 2 elements a, b ∈ E a = 2, b = 4

Closure property:-

a, b ∈ E where a = 2, b = 4

a * b ∈ E i.e., 2 * 4 ∈ E

8 ∈ E (True)

closure property satisfied

Associative property:-

a, b, c ∈ E where a = 2, b = 4, c = 6

$a*(b*c) = (a*b)*c \Rightarrow 2*(4*6) = (2*4)*6$

$\Rightarrow 2*(24) = (8)*6$

$\Rightarrow 48 = 48 \in E$ (True)

Associative property satisfied.

S
+

Monoid:- $\langle S,+\rangle$ Closure, AVS, Identity

Let S be a non-empty set and '+' be a binary operation S, then the algebraic system $\langle S,+\rangle$ is called a monoid. Iff it satisfies the following properties.

(i) closure property:-

for any two elements a, b; such that

$$\boxed{a+b \in S \text{ where } a,b \in S}$$

(ii) Associative property:-

for any 3 elements $a,b,c \in S$, such that

$$\boxed{a+(b+c) = (a+b)+c}$$

(iii) Identity Element:-

There exists a distinguished element e, $e \in S$ such that → Identity element

$$\boxed{a+e = e+a = a, \ \forall a \in S}$$

(e=0 (Identity for addition op = 0) ele w.r.to

$a+0 = 0+a$

$a = a$

Ex:- $\langle W,+\rangle$ is a monoid

$\langle N,+\rangle$ is not a Monoid ($\because$ 0 missed in Natural no's)

Sol: where W = set of whole no's

$= \{0,1,2,3 \ldots\}$

N = set of Natural no's

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

Note:- A monoid is always a semi-group.

GROUP

Let S be a non-empty set and '+' be a binary operation on S, then the algebraic system $\langle S,+\rangle$ is called a Group iff it satisfies the following properties.

$S = \{0, 1, 2 \dots \infty\}$

(i) Closure property:-

For any 2 elements a,b; such that

$\boxed{a+b \in S \text{ where } a,b \in S}$

let $a=2$
$b=3$
$2+3 \in S$
$5 \in S$

(ii) Associative property:-

For any 3 elements $a,b,c \in S$, such that

$\boxed{a+(b+c) = (a+b)+c}$

let $a=2, b=3, c=4$
$2+(3+4) = (2+3)+4$
$2+7 = 5+4$
$9 = 9$

(iii) Identity Element:-

There exists a distinguished element e, $e \in S$ such that (Identity element)

$\boxed{a+e = e+a = a, \forall a \in S}$

let $a=2$
$2+0=0+2=2$ ($\because e=0$ for $+$ op)

e is the identity element w.r. to the addition operation

$\boxed{e=0}$

(iv) Inverse property:-

for any element 'a', $a \in S$, there exists an element 'a^{-1}', $a^{-1} \in S$, such that

$$\boxed{\begin{array}{c} a+a^{-1} = a^{-1}+a = e \\ \text{(or)} \\ a+(-a) = (-a)+a = e \end{array}}$$

where 'e' is the identity element.

let $a=2$
$a^{-1} = -2$
$2+(-2) = (-2)+2 = 0 = e$ $\boxed{\text{ex}}$

Ex:- $\langle I,+\rangle$ is a group
where I is the set of Integers
$I = \{-\infty, \dots -3,-2,-1,0,1,2,3 \dots \infty\}$

Ex: $\langle I, + \rangle$ is a Group

where I is the set of Integers

$I = \{-\infty \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots +\infty\}$

$\langle G, * \rangle$
$\langle H, * \rangle$ - Subgroup of G
- closure
- Asso
- Identity & Inverse.

Sub Group :-

Let $\langle G, * \rangle$ be a group. If H be a finite ~~set~~ subset of Group G, then H is a sub group of G if and only if it satisfies the following properties w.r.to the operation '$*$'.

$$H \subset G$$

(1) Closure property :-

Let a & b are 2 elements in H. i.e., $a, b \in H$ then

$$a * b \in H, \forall a, b \in H.$$

(ii) Associative property :-

Let a, b and c are 3 elements in H i.e., $a, b, c \in H$ then

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

(iii) Identity property :-

Let a is an element in H i.e., $a \in H$.

There exists a special element 'e' in H i.e., $e \in H$ where 'e' is an Identity element such that,

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

$$a * 1 = 1 * a = a \quad (\because e = 1)$$

($\because$ 1 is the Identity element w.r.to '$*$')

(iv) Inverse property :-

Let 'a' is an element in H, i.e., $a \in H$, then there exist its inverse a^{-1} is also in H i.e., $a^{-1} \in H$ such that.

$$a * a^{-1} = a^{-1} * a = e. \forall a \in H \quad (\because e = 1)$$

where e is an Identity ele. w.r.to '$*$'.

$\Rightarrow a^{-1}$ is the inverse of a.

$\boxed{\because \text{H satisfies 4 properties. Hence H is a SubGroup of G}}$

$\langle H, * \rangle$ is SubGroup of $\langle G, * \rangle$

Examples of SubGroups:-

1. $\langle Z, + \rangle$ is a sub Group of $\langle Q, + \rangle$
2. $\langle Q, + \rangle$ is a Sub Group of $\langle R, + \rangle$

$\because N \leq Z \leq Q \leq R \leq C$

N is the SubGroup of Z

Z is the SubGroup of Q

Q is the SubGroup of R

R is the SubGroup of C

where:

$N \rightarrow$ set of Natural no's

$Z \rightarrow$ set of integers no's

$Q \rightarrow$ set of rational no's

$R \rightarrow$ " " real no's

$C \rightarrow$ set of Complex no's

Ex:- Let $\langle G, * \rangle$ is a Group, $G = \{1, -1, i, -i\}$ and $\langle H, * \rangle$ is a SubGroup of $\langle G, * \rangle$. check wheather $\{1, -1\}$ is a SubGroup of G (or) not.

Sol:- $\langle G, * \rangle$ is a Group.

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

$\langle H, * \rangle$ is a SubGroup of $\langle G, * \rangle$

Here $H = \{1, -1\}$ is a sub Group, If it satisfies the following properties.

Composition Table:-

$*$	1	-1
1	1	-1
-1	-1	1

$1 \in H$

$-1 \in H$

(1) closure property:-

Let us take any 2 elements a & b, $a, b \in H$ then $a * b \in H$, $\forall a, b \in H$

for eg: $a = 1, b = -1$

$a * b \in H$

$1 * -1 \in H$

$-1 \in H$ $\therefore$ Closure property satisfied.

(ii) Associative property:-

Take any 3 elements a, b, c Here $a, b, c \in H$ then

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

for eg:- $a = 1, b = -1, c = 1$ ⟶ take 3 values from H $(H = \{1, -1\})$

$1 * (-1 * 1) = (1 * -1) * 1$

$1 * -1 = -1 * 1$

$-1 = -1 \quad \because -1 \in H$

∴ Associative property is satisfied.

(iii) Identity property:-

Take any element 'a', Here $a \in H$ then

$$a * e = e * a = a$$

where e is identity ele = 1 ($\because e = 1$ w.r.to Multipl)

for eg:- $a = -1, a \in H$

$-1 * 1 = 1 * -1 = -1 \in H$

∴ Identity property is satisfied.

(iv) Inverse property:-

Take any ele 'a'. Here $a \in H$. there exist an element a^{-1} in H i.e., $a^{-1} \in H$ then $a * a^{-1} = a^{-1} * a = e$

where e is the identity element its value is equal to '1'.

a inverse is a^{-1}

a^{-1} inverse is a

Ex:- let us take $a = 1$, where $a \in H$

Now its inverse is $a^{-1} = 1$ ($\because$ 1 inverse is 1, -1 inverse is -1)

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

$a * a^{-1} = 1$ ($\because e = 1$ w.r.to $*$)

$1 * a^{-1} = 1 \Rightarrow a^{-1} = \frac{1}{1} = 1 \Rightarrow \boxed{a^{-1} = 1}$

Ex②: let $a = -1$, where $a \in H$

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

$-1 * a^{-1} = 1$ ($\because e = 1$ w.r.to $*$)

$a^{-1} = \frac{1}{-1} \Rightarrow \boxed{a^{-1} = -1}$

Suppose $a = -1$, where $a \in H$

a inverse is $a^{-1} = -1 \in H$

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

$\Rightarrow -1 * -1 = -1 * -1 = e$

$\Rightarrow \boxed{1 = e}$

$\therefore$ Inverse Property is also satisfied.

$\therefore H = \{1, -1\}$ Satisfies 4 properties.

Hence $\langle H, * \rangle$ is a Sub Group of $\langle G, * \rangle$ where $H = \{1, -1\}$

=o=

Sub-Semi group :-

satisfies only closure property

Let S be a finite set $*$ is a binary operation $\langle S, * \rangle$ is said to be semi group iff it satisfies the following properties (i) closure property
(ii) Associative property

T be a finite set $*$ be a binary operation.

$T \subseteq S$

$\langle T, * \rangle$ is a sub semi group of $\langle S, * \rangle$ iff it satisfies

(i) closure property :-

for any 2 ele's in T i.e., $a, b \in T$ then $a * b \in T$

Ex(1) :- let us consider $\langle Z, + \rangle$ is a semi group

let $\langle Z_+, + \rangle$ is a Subsemigroup of $\langle Z, + \rangle$ iff it satisfies (i) closure property

for any 2 eles in Z_+ i.e., $a, b \in Z_+$ then $a+b \in Z_+$

let $a=2, b=3$. $a, b \in Z_+$

$a+b \in Z_+$

$2+3 \in Z_+$

$5 \in Z_+$

$\therefore \langle Z_+, + \rangle$ is subsemi group of $\langle Z, + \rangle$

The Semi-group formed by all +ve integers under addition operation is a sub-semi group of all integers.

Ex:- ② :- Under multiplication operation, the set E of all even integers forms a semi-group. this semigroup is a subsemigroup of $\langle Z, * \rangle$.

let $\langle Z, * \rangle$ is a semi-group.

$E \subseteq Z$ let $\langle E, * \rangle$ be a sub-semigroup of $\langle Z, * \rangle$ iff it satisfies

(i) closure property.

$E = \{2, 4, 6, 8, \ldots\}$

$Z = \{-\infty \text{ to } +\infty\}$

for any 2 ele's in E ie, $a, b \in E$ then

$a * b \in E$

$a = 4, b = 6$

$4 * 6 \in E$

$24 \in E$

$\therefore \langle E, * \rangle$ is a subsemigroup of $\langle Z, * \rangle$

Monoid < Closure, Asso, Identity   Submonoid < Closure & Identity

Sub-Monoid :- < closure ✓, Identity ✓

S is a finite set * is a binary operation.
<S, *> is said to be monoid iff it satisfies 3 properties

1. closure
2. Associative
3. Identity.

T is a finite set * is the binary operation.
T ⊆ S
<T, *> is submonoid of <S, *> iff it satisfies 2 properties

1. closure property :-

~~closure~~ for any a, b ∈ T then a * b ∈ T

2. Identity property :-

for any a, a ∈ T then their exist e ∈ T then
$e * a = a * e = a$

Ex :- <Z, +> is a sub-monoid of <Q, T>
where
Z is the set of all integers.
Q is the set of all rational numbers

NOTE :- Since every set is a subset of itself, it follows that every semigroup is a subsemigroup of itself & every monoid is a ~~subsemi~~monoid of itself

$\langle Q,+\rangle$ is a monoid

$\langle Z,+\rangle$ is a submonoid of $\langle Q,+\rangle$

Now $\langle Z,+\rangle$ satisfies 2 properties.

a) <u>Closure property</u>:-

for any 2 elements in Z i.e., $a,b \in Z$ then $a+b \in Z$

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

$a=-2, b=1$

$a,b \in Z$

$a+b \in Z$

$-2+1 \in Z$

$-1 \in Z$

$\therefore$ It satisfies closure property.

b) <u>Identity property</u>

for any element a, $a \in Z$, then there exist another ele e, $e \in Z$ then $a + e = e + a = a$

($\because e=0$ w.r.to add operation)

let $a=1, 1 \in Z$

$a+e = a+0 = 1+0 = 1 = a$

$\therefore$ It satisfies Identity property.

$\therefore \langle Z,+\rangle$ is a submonoid of $\langle Q,+\rangle$

$= \circ =$

In each of the following cases, a binary operation $*$ on a set $A = \{a, b\}$ is defined through a multiplication table. Determine whether $(A, *)$ is a semi-group or a monoid or neither.

7C

(1)

$*$	a	b
a	b	a
b	a	b

Sol:-

To check associative law

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

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

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

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

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

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

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

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

$\therefore$ $*$ is associative, so $(A, *)$ is a semi-group.

Identity

$a*b = a$

$b*a = a$

$b*b = b$

$b*b = b$

$\therefore$ b is an identity element

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

(ii)

$*$	a	b
a	a	a
b	b	b

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

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

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

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

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

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

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

$b*(b*b = b*b = (b*b)*b$ ✓

$\therefore (A, *)$ is semi group

$a*b = a$ No identity element
$b*a = b$

$\therefore$ Not Monoid.

(iii)

$*$	a	b
a	a	b
b	a	a

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

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

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

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

$b*(a*a) = \cancel{a*b*a = a = b*b = (a*b)*b}$ $b*a = a = a*a = (b*a)*a$

$b*(a*b) = b*b = a = b*b =$ ✗

$b*(b*a) =$

$b*(b*b)$

$\therefore (A, *)$ is not semi-group

$\therefore$ It is not monoid.

Abelian Group:- (or) Commutative Group:-

Let S be a non-empty set and '+' be a binary operation on S, then the algebraic system $<S,+>$ is called an Abelian Group iff it satisfies the following Properties.

(i) closure property:-

for any two elements a, b ; such that

$a+b \in S$ where $a,b \in S \rightarrow$ S be the set of integers

$S = \{-\infty \ldots +\infty\}$

$a,b \in S$ let $2,3 \in S$

$2+3 \in S$

$5 \in S$

(ii) Associative property:-

for any 3 elements $a,b,c \in S$, such that

$$\boxed{a+(b+c) = (a+b)+c}$$

let $a=3$, $b=4$, $c=5$

$3+(4+5) = (3+4)+5$

$3+9 = 7+5$

$12 = 12$

(iii) Identity element:-

There exist a distinguished element $e, e \in S$ such that (identity ele)

$$\boxed{a+e = e+a = a, \ \forall a \in S}$$

$a \in S$
$5 \in S$
$e \in S, e=0$

e is the Identity element w.r. to the addition operation ($0 \in S$) $(\because e=0)$

$5+0 = 0+5 = 5$

(iv)

(iv) Inverse property:-

for any element 'a', $a \in S$, there exists an element 'a^{-1}', $a^{-1} \in S$ such that.

$$\boxed{\begin{array}{c} a+a^{-1}=a^{-1}+a=e \\ \text{(or)} \\ a+(-a)=(-a)+a=e \end{array}}$$

where 'e' is the identity element

Ex:- let $a=+5$

$a^{-1}=-5$

$e=0$ ($\because$ identity ele $e=0$ w.r. to addition)

$5+(-5)=(-5)+5=0$

$=0$

(v) Commutative property:-

for any two elements a, b $a, b \in S$ such that

$$\boxed{a+b=b+a}$$

let $a, b \in S$

$a=3$

$b=4$

$3+4=4+3$

$7=7$

$\therefore \langle S,+\rangle$ is an Abelian Group. where S is the set of integers ($-\infty$ to ∞)

Ex:- Example problem on Abelian Group

Let G be the set of all non-zero real numbers and let $a*b=\frac{1}{2}ab$. S/T $\langle G,*\rangle$ is an abelian group.

Sol: Let G be the set of non-zero real no's.

$$a*b=\frac{1}{2}ab$$

$\langle G,*\rangle$ is said to be Abelian group.

Iff it satisfies the following properties.

(i) closure
(ii) Associative
(iii) Identity
(iv) Inverse
(v) Commutative

$\left.\begin{matrix}\text{(i)}\\\text{(ii)}\\\text{(iii)}\\\text{(iv)}\end{matrix}\right\}$ Group

(i) closure property:-

Let us consider any 2 elements $a,b\in G$ ~~then~~ then $a*b\in G$

a&b are 2 elements of G ie, $a,b\in G$ then $a*b=\frac{1}{2}ab\in G$

Ex:- Let $(2,3)\in G$

$$2*3=\frac{1}{2}(2*3)=\frac{1}{2}(6)=3\in G$$

$\therefore$ $*$ satisfies the closure property.
product

Ex②:- $(4,8)$

$$4*8=\frac{1}{2}(\cancel{4}^{2}*8)=16\in G.$$

(ii) Associative property:-

for any 3 elements of G ie, $a,b,c\in G$, then it satisfies

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

Let us consider LHS $= a*(b*c)$

$$= a*(\tfrac{1}{2}bc)$$
$$= \tfrac{1}{2}(\tfrac{1}{2}a(bc))$$
$$= \tfrac{1}{2}(\tfrac{1}{2}(ab)c) \quad (\because \text{Associative law})$$
$$= \tfrac{1}{2}(a*b)c$$

$\therefore$ $*$ satisfies Associative Property $= (a*b)*c = RHS$

(iii) Identity property:-

for any element a of G i.e, $a \in G$, there exist an Identity element e of G i.e, $e \in G$, then it satisfies.

$a * e = e * a = a$

where e is the identity element.

$a * e = \frac{1}{2} ae = \frac{1}{2} ea = a \quad (\because a * b = \frac{1}{2} ab)$

$\Rightarrow \frac{1}{2} \cancel{a} e = \cancel{a}$

$\therefore \boxed{e = 2}$

Identity element is 2

$a * e = \frac{1}{2} ae = \frac{1}{\cancel{2}} a.(\cancel{2}) = a$

$e * a = \frac{1}{2} ea = \frac{1}{\cancel{2}} \cancel{2} * a = a$

$\therefore \boxed{a * e = e * a = a}$

$\therefore *$ satisfies the Identity property.

(iv) Inverse property:-

for any element a of G, there exists an inverse of element 'a' is $a^{-1} \in G$, then it satisfies.

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

$a * a^{-1} = \frac{1}{2} aa^{-1} = e$

$\Rightarrow \frac{1}{2} a.a^{-1} = 2$

$\Rightarrow a.a^{-1} = 4$

$\Rightarrow \boxed{a^{-1} = 4/a}$

a^{-1} is the inverse of element 'a' where $a^{-1} = 4/a$

$\therefore a * a^{-1} = \frac{1}{2}(a.a^{-1}) = \frac{1}{\cancel{2}}(\cancel{a}.\frac{\cancel{4}^{2}}{\cancel{a}}) = 2 = e$

$\therefore a^{-1} * a = \frac{1}{2}(a^{-1}.a) = \frac{1}{\cancel{2}}(\frac{\cancel{4}^{2}}{\cancel{a}}.\cancel{a}) = 2 = e$

$\therefore a * a^{-1} = a^{-1} * a = e = 2$

$\therefore *$ satisfies the inverse property.

(v) Commutative property:-

for any 2 elements a, b of G i.e., $a, b \in G$, it satisfies

$a * b = b * a$

Let us consider LHS

$a * b = \frac{1}{2} ab$ $\quad (\because a * b = \frac{1}{2} ab)$

$= \frac{1}{2} ba$

$= b * a = RHS$

LHS = RHS

$\therefore *$ satisfies commutative property.

$\therefore *$ satisfies closure, Associative, Identity, inverse & commutative properties.

$\therefore$ Hence $\langle G, * \rangle$ is an Abelian Group (or) Commutative Group

=○=

Eg:-② on the set ~~of~~ Q of all rational no's the operation '$*$' is defined by $a * b = a + b - ab$. S/T $\langle Q, * \rangle$ is a commutative monoid (Abelian Group)

(i) closure property:- for any 2 ele's a, b in Q, i.e., $a, b \in Q$,

$a * b \in Q$

$a + b - ab \in Q$

Let $2, 3 \in Q$

$2 + 3 - 6 = -1 \in Q$ ✓

~~$\therefore \langle Q, * \rangle$ is abelian gp.~~

$\therefore *$ satisfies closure property.

(ii) Associative Property:

Let $a, b, c \in Q$

$\Rightarrow a * (b * c) = a * (b + c - bc)$

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

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

$= \cancel{a}(\cancel{b} + c - \cancel{bc}) - \cancel{a}(b + \cancel{c} - \cancel{ab})$

$= \cancel{a *}$

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

$= \underline{a+b-ab+c} - c(a+b-ab)$

$= \cancel{(a*b)+c-c}$

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

$= (a*b)*c$

$= RHS$

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

$\therefore$ '$*$' is associative.

<u>Identity property</u>:-

$a*e = e*a = a$

$a*e = a$

$a+e-ae = a$

$e-ae = a-a$

$e-ae = 0$

$e(1-a) = 0$

$\cancel{e(1-a)=0}$

$\boxed{e=0}$

$\cancel{a*e = a*0}$

$a*e = a+e-ae$

$= a+0-a(0)$

$= a$

$e*a = e+a-ea$

$= 0+a-0(a)$

$= a$

$\boxed{a*e = e*a = a}$ ✓

Inverse property:-

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

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

$a+a^{-1}-aa^{-1}=0$

$a^{-1}(1-a)=0-a$

$a^{-1}=\frac{-a}{(1-a)}$ (or) $\frac{a}{a-1}$

$a*a^{-1}=a+a^{-1}-a\times a^{-1}$

$=a+\frac{a}{a-1}-a*\frac{a}{a-1}$

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

$=\frac{\cancel{a^2}-\cancel{a}+\cancel{a}-\cancel{a^2}}{a-1}$

$=\frac{0}{a-1}=0$ ✓

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

$=\frac{a}{a-1}+a-\frac{a}{a-1}*a$

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

$=\frac{\cancel{a}+\cancel{a^2}-\cancel{a}-\cancel{a^2}}{a-1}$

$=\frac{0}{a-1}=0$ ✓

$a*a^{-1}=a^{-1}*a=0=e$

$\therefore$ '$*$' is inverse property.

Commutative property:-

$a*b=a+b-ab$
LHS
$=b+a-ab$
$=b*a$
$=$ RHS

'$*$' is Commutative

'$*$' satisfies Closure, Ass, Comm, Ident, Inverse

$\therefore \langle Q,*\rangle$ is abelian | commutative Group.

Ex:-(3):- If $\circ$ is an operation on Z defined by $x \circ y = x+y+1$
P/T $\langle Z, \circ \rangle$ is an Abelian Group.

$-\infty$ $\quad Z \quad 0 \quad \infty$

$\frac{1}{2} x \in Z$

Sol:- '$\circ$' is an operation on Z
Z is defined by $x \circ y = x+y+1$
$\langle Z, \circ \rangle$ is said to be Abelian Group.
iff it satisfies following properties
(i) closure
(ii) Associative
(iii) Identity
(iv) Inverse
(v) Commutative

Closure:- for any 2 elements x and y in Z, then $x \circ y \in Z$

$$x \circ y \in Z$$
$$x+y+1 \in Z$$

$\therefore$ '$\circ$' satisfies the closure property.

Associative:- let $x, y, z \in Z$

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y+z+1) \\ &= x+y+z+1+1 \\ &= (x+y+1)+z+1 \\ &= (x \circ y)+z+1 \end{aligned}$$

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

$\therefore$ '$\circ$' is associative

Identity:- $x \circ e = e \circ x = x$

(replace a with x)

$$a \circ e = a+e+1 = a$$
$$\Rightarrow e+1 = a-a$$
$$\Rightarrow e+1 = 0$$
$$\Rightarrow \boxed{e=-1} \in Z$$

$$x \circ e = x + e + 1$$
$$= x - 1 + 1$$
$$= x$$
$$e \circ x = e + x - 1$$
$$= -1 + x + 1$$
$$= x$$

$$x \circ e = e \circ x = x$$

Inverse property:-

$$\boxed{x \circ x^{-1} = x^{-1} \circ x = e}$$

$$x \circ x^{-1} = e$$
$$x \circ x^{-1} = -1 \quad (\because e = -1)$$
$$x + x^{-1} + 1 = -1$$
$$x + x^{-1} = -2$$
$$\boxed{x^{-1} = -2 - x}$$

$$x \circ x^{-1} = x + x^{-1} + 1$$
$$= x + x^{-1} + 1$$
$$= \cancel{x} - 2 \cancel{- x} + 1$$
$$= -1 = e$$

$$x^{-1} \circ x = x^{-1} + x + 1$$
$$= -2 - \cancel{x} + \cancel{x} + 1$$
$$= -1 = e$$

$\therefore$ $x \circ x^{-1} = x^{-1} \circ x = (-1) = e$

$\therefore$ 'o' satisfies Inverse property

Commutative property:-

$$x \circ y = x + y + 1$$
$$= y + x + 1$$
$$= y \circ x$$

$\therefore$ 'o' is commutative

$\therefore$ 'o' satisfies Closure, associative, Identity, Inverse, Commutative

$\langle Z, \circ \rangle$ satisfies abelian Group.

Generator (or) Generating Element

(13)

Let $\langle G, * \rangle$ be a group, an element 'a' is called Generator of $a \in G$ and $\forall a \in G$ can be represented using power of 'a' Such as $\{a^1, a^2, a^3, \dots\}$ with respect to '$*$'.

Rough: Let $\langle G, * \rangle$ a Group

$a, a \in G$

$\langle \{a^1, a^2, a^3, \dots\}, * \rangle$

when integral ~~it~~ Power of a generates all elements of G then a is called generating ele

when integral power of a doesnot generates all elem of G then a is not a generating ele

Ex:- $G = \{0, 1, 2, 3\}$

Let $a=0$ $\quad 0^1 = 0$	$1^1 = 1$
$0^2 = 0 \times 0 = 0$	$1^2 = 1 \times 1 = 1$
$0^3 = 0 \times 0 \times 0 = 0$	$1^3 = 1 \times 1 \times 1 = 1$
$0^4 = 0 \times 0 \times 0 \times 0 = 0$	$1^4 = 1 \times 1 \times 1 \times 1 = 1$
0 is not a generating ele	1 is not a generating ele

Ex:- let $Z=\{0,1,2,3\}$, find out all the generators for the group $\langle Z_4,+\rangle$ where $\langle Z_4,+\rangle$ is "Addition Modulo 4"

Sol:-

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Composition table

$\overset{r}{0} +_4 \overset{c}{0} = 0\%4 = 0$

$\overset{r}{0} +_4 \overset{c}{3} = 3\%4 = 3$ $4)3(0$, 0, 3

$\overset{r}{1}\overset{c}{3} \rightarrow 1+_4 3 = 4\%4 = 0$

$\overset{r}{3}\overset{c}{3} \rightarrow 3+_4 3 = 6\%4 = 2$ $4)6(1$, 4, 2

Finding Identity ele from the composition table.
here we have to identify which column no contains the elements in the same order as the elements in the set

Here $Z = 0,1,2,3$ ... 3rd coln order 3 0 1 2 ✗
2nd coln " 2 3 0 1 ✗
1st coln " 1 2 3 0 ✗
0 coln " 0 1 2 3 ✓

Now col '0' is zero is the identity element

∴ '0' is the identity ele

$$\boxed{a^n = e \Rightarrow a^n = 0}$$

(1)
$0^1 = 0$
$0^2 = 0+_4 0 = 0$
$0^3 = 0+_4 0+_4 0 = 0$
$0^4 = 0+_4 0+_4 0+_4 0 = 0$
∴ 0 is not a generator

$\Rightarrow$

(2)
$1^1 = 1$
$1^2 = 1+_4 1 = 2\%4 = 2$
$1^3 = 1+_4 1+_4 1 = 3\%4 = 3$
$1^4 = 1+_4 1+_4 1+_4 1 = 4\%4 = 0$
∴ 1 is generator (all elem's in Z set generated)

(3)
$2^1 = 2$
$2^2 = 2+_4 2 = 0$
$2^3 = 2+_4 2+_4 2 = 2$
$2^4 = 2+_4 2+_4 2+_4 2 = 0$
∴ 2 is not a generator [as it generates only 0 & 2 not 1 & 3]

$\Rightarrow$

(4)
$3^1 = 3$
$3^2 = 3+_4 3 = 2$
$3^3 = 3+_4 3+_4 3 = 9\%4 = 1$
$3^4 = 3+_4 3+_4 3+_4 3 = 12\%4 = 0$
∴ 3 is generator as it generates all eles in Z

$\therefore$ 1 and 3 are generators

$\langle Z_4, + \rangle$ Group contains 2 generators ie 1 & 3

$\langle Z_4, + \rangle$ is a cyclic group (it contains 2 generators ie 1 & 3)

A group becomes cyclic group iff it contains atleast one generat eles

=o=

Cyclic Group :-

A group $\langle G, * \rangle$ is said to be cyclic group, If it contains atleast one generator element.

Ex:- P/T $\langle G, * \rangle$ is a cyclic group where $G = \{1, \omega, \omega^2\}$

Sol:- $G = \{1, \omega, \omega^2\}$

composition table :-

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	ω^3
ω^2	ω^2	ω^3	ω^4

$\Rightarrow$

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$(\because \omega^3 = 1)$
$(\omega^4 = \omega^3 \cdot \omega = (1)\omega = \omega)$

$1^1 = 1$
$1^2 = 1 * 1 = 1$
$1^3 = 1 * 1 * 1 = 1$
$1^4 = 1 * 1 * 1 * 1 = 1$

$\therefore$ 1 is not a generator

$\omega^1 = \omega$
$\omega^2 = \omega * \omega = \omega^2$
$\omega^3 = \omega * \omega * \omega = \omega^3 = 1$
$\omega^4 = \omega * \omega * \omega * \omega$
$= \omega^3 * \omega$
$= 1 * \omega$
$= \omega$

$\therefore \omega$ is a generator

$(\omega^2)^1 = \omega^2$
$(\omega^2)^2 = \omega^4 = \omega^3 * \omega$
$\Rightarrow 1 * \omega$
$= \omega$
$(\omega^2)^3 = \omega^6 \Rightarrow \omega^3 * \omega^3$
$\Rightarrow 1 * 1 = 1$
$(\omega^2)^4 = \omega^8 = \omega^3 * \omega^3 * \omega^2$
$= 1 * 1 * \omega^2$
$= \omega^2$

$\therefore \omega^2$ is a generator

$\therefore \langle G, * \rangle$ contains 2 Generators $\langle \omega, \omega^2 \rangle$
$\therefore \langle G, * \rangle$ is a cyclic group

Ex:- (2) Prove that $\langle G, * \rangle$ is a cyclic group where $G = \{1, -1, i, -i\}$

Sol:- $G = \{1, -1, i, -i\}$

Composition table:-

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	i^2	$-i^2$
$-i$	$-i$	i	$-i^2$	i^2

$(\because i^2 = -1)$

$(-i^2 = -(-1) = 1)$

$\Rightarrow$

$*$	1	-1	i	-1
1	1	-1	i	-1
-1	-1	1	$-i$	i
i	i	-1	-1	1
$-i$	$-i$	i	1	-1

$1^1 = 1$

$1^2 = 1 \times 1 = 1$

$1^3 = 1 \times 1 \times 1 = 1$

$1^4 = 1 \times 1 \times 1 \times 1 = 1$

$\therefore 1$ is not a generator

$-1^1 = -1$

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

$-1^3 = -1 \times -1 \times -1 = -1$

$-1^4 = -1 \times -1 * -1 * -1$

$= 1 \times 1 = 1$

$\therefore -1$ is not a generator

$i^1 = i$ ✓

$i^2 = i \times i = i^2 = -1$ ✓

$i^3 = i \times i \times i = i^2 \times 1 = -1 \times i = -i$ ✓

$i^4 = i^2 \times i^2$

$= -1 \times -1 = 1$

$i^5 = i^2 \times i^2 \times i = -1 \times -1 \times i$

$= 1 \times i$

$= i$ ✓

$\therefore i$ is a generator

$(-i)^1 = -i$ ✓

$(-i)^2 = i^2 = -1$ ✓

$(-i)^3 = -i^3 = -i^2 \times i$

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

$(-i)^4 = i^2 \times i^2 = (-1) \times (-1) = 1$ ✓

$\therefore -i$ is a generator

$\therefore \langle G, * \rangle$ is a cyclic group because this group has 2 generators. (i.e., $i, -i$)

Order of an Element of a Group :-

Let $\langle G, * \rangle$ be a group, 'a' is an element of G i.e., $a \in G$, the order of an element 'a' is denoted by O(a),

$$\boxed{O(a) = n}$$

where 'n' is the smallest possible integer which satisfies the equation $a^n = e$, where 'e' is Identity element.

Note :- (1). Order of Identity element is always '1'.

(2) order of an element & its inverse is always same.

Ex:- Let $\langle Z_4, + \rangle$ is a group, find out the order of each element? $\langle Z_4, + \rangle$ is addition modulo 4.

Sol:- $\langle Z_4, + \rangle$ Addition modulo 4

Method① for findg set values $Z = \{0, 1, 2, 3\}$ (0%4, 1%4, 2%4, 3%4, 4%4 → 0)

0 % 4 = 0 | 1 mod 4 = 1 | 2 mod 4 = 2 | 3 mod 4 = 3

4 mod 4 = 0

llly 5 mod 4 = 1 | 6 mod 4 = 2 | 7 mod 4 = 2 ... 0, 1, 2, 3 ....

method② shortway for finding set values
Z_4 4−1=3 (0 to 3) {0, 1, 2, 3}
Z_7 7−1=6 (0 to 6) {0, 1, 2, 3, 4, 5, 6}
Z_n n−1 elements = {0, 1, ... n−1}

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

$0^1 = 0$ ✓
$0^2 = 0 +_4 0 = 0$ ✓
$0^3 = 0 +_4 0 +_4 0 = 0$ ✓
$a^n = e$
$0^n = 0$ ✓

+ − 0 identity ele (for addition identity ele is zero)
∗ − 1 Identity ele (for Multion identity ele is one)

$\therefore O(0) = 1$

(∵ Here Identity ele found at 1, 2, 3 among 1, 2 3 powers (1 is smallest)

O(0) = 1 read as Order of zero is 1

$1^1 = 1$

$1^2 = 1 +_4 1 = 2$

$1^3 = 1 +_4 1 +_4 1 = 3$

$1^4 = 1 +_4 1 +_4 1 +_4 1 = 0$ ✓ identity ele.

(for which value of n it generates zero)

A:- 4

$O(1) = 4$

$2^1 = 2$

$2^2 = 2 +_4 2 = 0$ ✓

$2^3 = 2 +_4 2 +_4 2 = 2$

$2^4 = 2 +_4 2 +_4 2 +_4 2 = 8 \% 4 = 0$ ✓

Here Identity ele found at 2 & 4 among 2 & 4 (2 is smallest)

$O(2) = 2$

$3^1 = 3$

$3^2 = 3 +_4 3 = 2$

$3^3 = 3 +_4 3 +_4 3 = 9 \% 4 = 1$

$3^4 = 3 +_4 3 +_4 3 +_4 3 = 12 \% 4 = 0$ ✓

$O(3) = 4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(which ~~col~~ number has the same order in set $Z = \{0, 1, 2, 3\}$?)

A:- column no. zero

Here column no is the identity ele

Ex②:- Let $\langle Z_6, + \rangle$ is a group, find out the order of each element ? $\langle Z_6, + \rangle$ is addition Modulo 6. (17)

Sol:- $\langle Z_6, + \rangle$ Additional Modulo.

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

Composition table:-

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

$\therefore$ Identity ele is '0'

$a^n = e$

$\Rightarrow a^n = 0$

$0^1 = 0$

$0^2 = 0 +_6 0 = 0$

$0^3 = 0 +_6 0 +_6 0 = 0$

$\boxed{O(0) = 1}$

$1^1 = 1$

$1^2 = 1 +_6 1 = 2 \% 6 = 2$

$1^3 = 1 +_6 1 +_6 1 = 3 \% 6 = 3$

$1^4 = 1 +_6 1 +_6 1 +_6 1 = 4 \% 6 = 4$

$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5 \% 6 = 5$

$1^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 6 \% 6 = 0$

$\boxed{O(1) = 6}$

$2^1 = 2$

$2^2 = 2 +_6 2 = 4 \% 6 = 4$

$2^3 = 2 +_6 2 +_6 2 = 6 \% 6 = 0$

$2^4 = 2 +_6 2 +_6 2 +_6 2 = 8 \% 6 = 2$

$2^5 = 2 +_6 2 +_6 2 +_6 2 +_6 2 = 10 \% 6 = 4$

$2^6 = 2 +_6 2 +_6 2 +_6 2 +_6 2 +_6 2 = 12 \% 6 = 0$

Among 3, 6 3 is Smallest

$\boxed{O(2) = 3}$

$3^1 = 3$

$3^2 = 3 +_6 3 = 6 \% 6 = 0$

$3^3 = 3 +_6 3 +_6 3 = 9 \% 6 = 3$

$3^4 = 3 +_6 3 +_6 3 +_6 3 = 12 \% 6 = 0$

$\boxed{O(3) = 2}$

$4^1 = 4$

$4^2 = 4 +_6 4 = 8 \% 6 = 2$

$4^3 = 4 +_6 4 +_6 4 = 0$

$\boxed{O(4) = 3}$

$5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$5^3 = 5 +_6 5 +_6 5 = 3$

$5^4 = 5 +_6 5 +_6 5 +_6 5 = 20 \% 6 = 2$

$5^5 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 25 \% 6 = 1$

$5^6 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0$

$\boxed{O(5) = 6}$

Example problem on Abelian Group, cyclic Group, Sub-groups in Group theory:

(1) Let $G = \{0,1,2,3,4,5\}$

(i) Prepare the composition table with respect to '$+_6$' (Addition Modulo 6)

(ii) P/T G is an Abelian Group.

(iii) Find the inverse of each and every element in G.

(iv) Is G is a cyclic group or not?

(v) Find the order of each and every ele in a Group.

(vi) find out the subgroups generated by each & every element in G.

Sol:-

(i) Composition table w.r.to Addition Modulo 6 ($+_6$)

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

$2 +_6 2 = 4 \% 6 = 4$

(iii) Inverse of each element in G:

Identity element for the above composition table is $\underline{0}$

Inverse of each element is

$0^{-1} = 0$ $\quad$ $3^{-1} = 3$

$1^{-1} = 5$ $\quad$ $4^{-1} = 2$

$2^{-1} = 4$ $\quad$ $5^{-1} = 1$

($\because$ Identify the Identity ele (zero) at 2nd row & write corresponding col^n no of found Identity ele (0) [zero])

(ii) P/T G is an Abelian group

To prove that G is an Abelian Group it satisfies the following properties:

① closure property:- for any 2 elements a,b;

$$a +_6 b \in G$$

let us take $a=2, b=3$

$$2 +_6 3 \in G$$
$$5 \in G$$

∴ It satisfies the closure property.

② Associative property:- for any 3 elements a,b,c;

$$(a +_6 b) +_6 c = a +_6 (b +_6 c)$$

let us take $a=2, b=3, c=4$

$$(a +_6 b) +_6 c) = a +_6 (b +_6 c)$$
$$(2 +_6 3) +_6 4 = 2 +_6 (3 +_6 4)$$
$$5 +_6 4 = 2 +_6 (7 \% 6)$$
$$\underset{(9\%6)}{5 +_6 4} = 2 +_6 (1)$$
$$3 = 3 \text{ (True)}$$

∴ It satisfies the Associative property.

③ Identity property:-

The identity element is $e=0$ (w.r to addition)

for any element a; $a \in G$

$$a +_6 e = e +_6 a = a$$

let us take $a=2$

$$2 +_6 0 = 0 +_6 2 = 2 \text{ (True)}$$

∴ It satisfies the Identity property

4) Inverse property:-

for each and every element in the Group G, Inverse of that element also exist in the Same Group G.

$0^{-1}=0$ $\quad 3^{-1}=3$

$1^{-1}=5$ $\quad 4^{-1}=2$

$2^{-1}=4$ $\quad 5^{-1}=1$

∴ It satisfies the Inverse property.

(5) Commutative property :-

for ~~ea~~any 2 elements $a, b; a, b \in G$ then

$a +_6 b = b +_6 a$

let us take ~~2 elements a,b∈~~ $a=3, b=4$

$a +_6 b = b +_6 a$

$3 +_6 4 = 4 +_6 3$

$7\%6 = 7\%6$

$1 = 1$ (True)

∴ It satisfies the Commutative property.

∴ Addition modulo satisfies the above 5 properties,

Hence $+_6$ is Abelian Group.

(iv) Is it a cyclic group or not?

To be a cyclic group, the Group must contain atleast one Generator element.

$\rightarrow 0^1 = 0$

$0^2 = 0 +_6 0 = 0$

$0^3 = 0 +_6 0 +_6 0 = 0$

$0^4 = 0 +_6 0 +_6 0 +_6 0 = 0$

$0^5 = 0 +_6 0 +_6 0 +_6 0 +_6 0 = 0$

$\therefore$ Ele '0' is not a Generator

$\rightarrow 1^1 = 1$

$1^2 = 1 +_6 1 = 2$

$1^3 = 1 +_6 1 +_6 1 = 3$

$1^4 = 1 +_6 1 +_6 1 +_6 1 = 4$

$1^5 = 1 +_6 1 +_6 1 +_6 1 +_6 1 = 5$

$1^6 = 1 +_6 1 +_6 1 +_6 1 +_6 1 +_6 1 = 0$

$\therefore$ Element '1' is a Generator

$\rightarrow 2^1 = 2$

$2^2 = 2 +_6 2 = 4$

$2^3 = 2 +_6 2 +_6 2 = 0$

$2^4 = 2 +_6 2 +_6 2 +_6 2 = 4$

$2^5 = 2 +_6 2 +_6 2 +_6 2 +_6 2 = 0$

$\therefore$ Ele '2' is not a Generator

$\rightarrow 3^1 = 3$

$3^2 = 3 +_6 3 = 0$

$3^3 = 3 +_6 3 +_6 3 = 3$

$3^4 = 3 +_6 3 +_6 3 +_6 3 = 0$

$3^5 = 3 +_6 3 +_6 3 +_6 3 +_6 3 = 3$

$3^6 = 3 +_6 3 +_6 3 +_6 3 +_6 3 +_6 3 = 0$

$\therefore$ Ele 3 is not a Generator

$\rightarrow 4^1 = 4$

$4^2 = 4 +_6 4 = 2$

$4^3 = 4 +_6 4 +_6 4 = 0$

$4^4 = 4 +_6 4 +_6 4 +_6 4 = 4$

$4^5 = 4 +_6 4 +_6 4 +_6 4 +_6 4 = 2$

$4^6 = 4 +_6 4 +_6 4 +_6 4 +_6 4 +_6 4 = 0$

$\therefore$ Ele '4' is not a Generator

$\rightarrow 5^1 = 5$

$5^2 = 5 +_6 5 = 4$

$5^3 = 5 +_6 5 +_6 5 = 3$

$5^4 = 5 +_6 5 +_6 5 +_6 5 = 2$

$5^5 = 5 +_6 5 +_6 5 +_6 5 +_6 5 = 1$

$5^6 = 5 +_6 5 +_6 5 +_6 5 +_6 5 +_6 5 = 0$

$\therefore$ Element 5 is a Generator.

$\therefore$ Here 1 and 5 are Generator

$\therefore$ G is a Cyclic group under $+_6$

(v) SubGroups Generated by each & every ele is:

$0 = \{0\}$

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

$2 = \{0, 2, 4\}$

$3 = \{0, 3\}$

$4 = \{0, 2, 4\}$

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

(V) Order of each & every ele in G :-

Order of an element 'a' is $O(a)$

$O(a) = n$

where n is the smallest possible integer which satisfies the equation $a^n = e$, where e is the ~~ser~~ Identity ele.

$\boxed{a^n = 0}$ $(\because e = 0)$

Refer (P.T.O) (iv) cyclic group Integral powers of $0^1, 0^2 \ldots$
←Back

$1^1, 1^2 \ldots 1^6$, $2^1 \ldots$, $3^1 \ldots$ $4^1 \ldots$ $5^1 \ldots$

$O(0) = 1$ (order of zero is 1)
$0^1 = 0$ ✓

$O(1) = 6$ (order of one is 6)
$1^6 = 0$ ✓

$O(2) = 3$ (order of 2 is 3)
$2^3 = 0$ ✓ (among 3, 6 → 3 is smallest)
$2^6 = 0$ ✗

$O(3) = 2$ ($3^2 = 0$ ✓ (among 2, 4, 6 → 2 is smallest)
$3^4 = 0$ ✗
$3^6 = 0$ ✗

$\|^{ly}$ $O(4) = 3$

$O(5) = 6$

—o—

Homomorphism in Group Theory :-

Rough

let $\langle G, * \rangle$

$\langle G', \Delta \rangle$

$f: G \to G'$ is said to be Homomorphism iff $\boxed{f(a*b) = f(a) \Delta f(b)}$ $\forall a, b \in G$

Let G and G' be any 2 groups with binary operations '$*$' and 'Δ' respectively, then a mapping $f: G \to G'$ said to be Homomorphism if

$$\boxed{f(a * b) = f(a) \Delta f(b), \ \forall a, b \in G}$$

Ex:- ①: Let $\langle Z, + \rangle$ be a group and $\langle G, * \rangle$ be another group, G can be defined as $G = \{2^n, n \in Z\}$

A function ~~from~~ $f: Z \to G$ by $f(n) = 2^n, \ \forall n \in Z$ S.T $f: Z \to G$ is a homomorphism.

Sol:- $\langle Z, + \rangle$ and $\langle G, * \rangle$ be two Groups

$$G = \{2^n, n \in Z\}$$

$f: Z \to G$ and $f(n) = 2^n, \forall n \in Z$

$n_1, n_2 \in Z \Rightarrow f(n_1) = 2^{n_1}$

$\Rightarrow f(n_2) = 2^{n_2}$

$f: Z \to G \Rightarrow f(n_1 + n_2)$

$f(n_1 + n_2) = 2^{n_1 + n_2} = 2^{n_1} * 2^{n_2} \ (\because a^m * a^n = a^{m+n})$

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

$$\therefore \boxed{f(n_1 + n_2) = f(n_1) * f(n_2)}$$

binary operation under Z binary operation under G

$\therefore f$ is homomorphism.

Ex(2):- let $\langle G, * \rangle$ be a group ~~by~~ defined by $G = \{1, -1, i, -i\}$ &

$\langle I, + \rangle$ be a group. P/T $f : I \to G$ is a homomorphism

where $f(n) = i^n \ \forall n \in I$

sol: $\langle G, * \rangle$. $G = \{1, -1, i, -i\}$

$\langle I, + \rangle$

$f : I \to G$ $f(n) = i^n, \forall n \in I$

~~$f(n) = i^n, \forall n \in I$~~

n_1 & n_2 are 2 elements in I ie, $n_1, n_2 \in I$

$$f(n_1) = i^{n_1}$$

$$f(n_2) = i^{n_2}$$

$$f(n_1 + n_2) = i^{n_1 + n_2} \quad (\because a^{m+n} = a^m * a^n)$$

$$= i^{n_1} * i^{n_2}$$

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

$$\boxed{f(n_1 + n_2) = f(n_1) * f(n_2)}$$

+ is binary operation w.r.to I

* is binary operation w.r.to G

$\therefore f : I \to G$ is a homomorphism.

Some more definitions:-

⇒ Let f be a homomorphism from $(S, *)$ to (H, o); if $f : S \to H$ is onto, then it is called "epimorphism."

⇒ If $f : S \to H$ is one-one, it is called as "monomorphism"

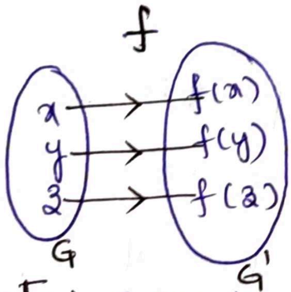
⇒ Let $(S, *)$ and (H, o) be 2 algebraic systems such that $S \subseteq H$, then a Homomorphism f from $(S, *)$ and (H, o) is called endomorphism.

Isomorphism in Group theory :-

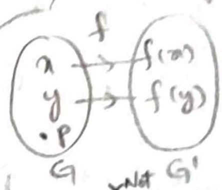
Let $\langle G, + \rangle$ and $\langle G', * \rangle$ are 2 Groups,
A function f mapping $f: G \to G'$ is called Isomorphism iff it satisfies the following 3 conditions.

(i) f is one-to-one
(ii) f is onto
(iii) f is homomorphism.

(i) **f is one-to-one** :- every element in G has image in G'

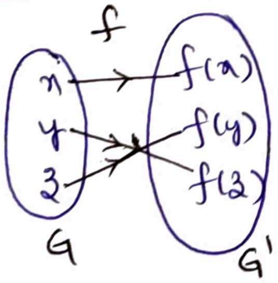


$\forall x, y, z \in G$
$\forall f(x), f(y), f(z) \in G'$

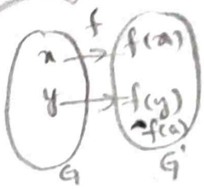


× Not one-one bcz P ele in G doesn't have image in G'

(ii) **f is onto** :- every ele in G' has particular preimage in G



f(x) has pre-image x
f(y) " " z
f(z) " " y

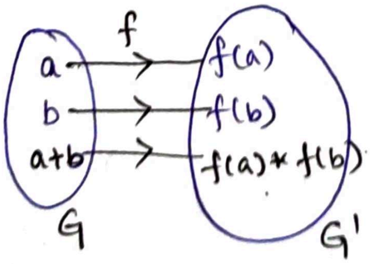


× Not onto bcz f(a) has no pre-image in G

$\forall x, y, z \in G$
$\forall f(x), f(y), f(z) \in G'$

(iii) f is homomorphism from $G \to G'$

$f(a+b) = f(a) * f(b), \forall a, b \in G$ & $f(a), f(b) \in G'$



$\therefore$ f satisfies the 3 conditions i.e., one-to-one, onto, Homomorphism

(P.T.O)

Hence, we can say that $f: G \to G'$ is called Isomorphism

$$G \cong G'$$

The symbol $\cong$ represents "Isomorphism" b/w two Groups $\langle G, + \rangle$ and $\langle G', * \rangle$

Example problem on Group Isomorphism

Ex:- Let R be the Additive group of real no's $\langle R, + \rangle$ and R^+ be the Multiplicative group of +ve real no's : $\langle R^+, * \rangle$ and a function f, $f: R \to R^+$ is defined by $f(x) = e^x$ $\forall$ ~~x∈~~ $x \in R$ then S|T $R \cong R^+$

Sol:- Let $\langle R, + \rangle$ & $\langle R^+, * \rangle$ are two groups f:R.

$f: R \to R^+$ is defined by $f(x) = e^x$, $\forall x \in R$

Now $f: R \to R^+$ is Isomorphism iff f satisfies the following properties.

(1) f is one-to-one
(2) f is onto
(3) f is Homomorphism

(1) f is one-to-one:-

Let us consider any 2 elements a, b

if $a, b \in R$ then $f(a) = f(b)$

$\Rightarrow e^a = e^b$ $\left(\because f(a) = e^a, \; f(b) = e^b \right)$

Apply log on both sides

$\log e^a = \log e^b$

$a \log e = b \log e$ $(\because \log e = 1)$

$\boxed{a = b}$ $(\because f(a), f(b) \in R^+$
$a, b \in R)$

Here a is image of f(a)
b " " " f(b)

$\therefore$ f is one to one

② **f is onto :-**

for any element c, $c \in R^+$, then there exist an element $\log c$, $\log c \in R$ then

$$f(\log c) = e^{\log c} = c$$

$\therefore$ for every ele in R^+, their exist an ele in R.

$\in R$ $\quad\quad$ $\in R^+$

③ **f is homomorphism :-**

for any 2 ele's a,b , $a,b \in R$ then

$$f(a+b) = e^{a+b}$$
$$= e^a * e^b \quad \left(\because \begin{array}{l} f(a) = e^a \\ f(b) = e^b \end{array}\right)$$
$$= f(a) * f(b)$$

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

$\therefore$ f is homomorphism

$f: R \to R^+$ satisfies the 3 conditions, Hence

$f: R \to R^+$ is Isomorphism

$\therefore R \cong R^+$

Ex:- let z be a group of Integers w.r.to the operation '+' ie $\langle Z,+\rangle$ is a group and G be a group w.r.to the operation '$*$' ie., $\langle G,*\rangle$ where $G=2^n, n\in Z$. Define $f: Z\to G$ by $f(n)=2^n$, $\forall n\in Z$

S/T f is Isomorphism.

Sol:- $\left.\begin{matrix}\langle Z,+\rangle\\ \langle G,*\rangle\end{matrix}\right\}$ are 2 groups

$G=2^n, n\in Z$

$f: Z\to G$ defined by $f(n)=2^n, \forall n\in Z$

A function $f: Z\to G$ is Isomorphism by satisfying the following

(i) f is one-to-one:-

for any 2 elements n_1 & n_2 where $n_1,n_2\in Z$ then

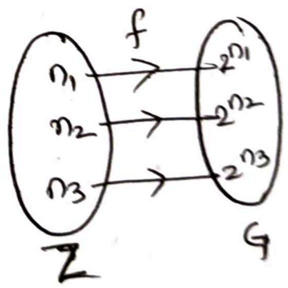
$f(n_1)=f(n_2)$ $\quad \left[\begin{matrix}\because f(n)=2^n\\ f(n_1)=2^{n_1}\\ f(n_2)=2^{n_2}\end{matrix}\right]$

$2^{n_1}=2^{n_2}$

Both sides bases are equal, then powers are also equal

$n_1=n_2$

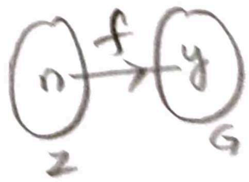
$\therefore$ f is one-to-one



(ii) f is onto:-

for any element $y, y\in G$ there exist atleast one element in Z, then $f(n)=f(2^n)=y$

n is one ele in Z $\therefore$ f is onto. y is ele in G and also



(iii) f is homo-morphism:-

for homo-morphism
$f(a+b)=f(a)*f(b)$

let us take 2 ele's n_1,n_2 where $n_1,n_2\in Z$

$f(n_1+n_2) = 2^{n_1+n_2} \quad (\because f(n) = 2^n)$

$= 2^{n_1} * 2^{n_2}$

$\cancel{f(n_1+n_2) = f(n_1) * f(n_2)}$

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

$\therefore f$ is Homomorphism.

$f: Z \to G$ is Homomorphism.

Example③ :-

Let $\langle G, * \rangle$ and $\langle G', (\text{mod } 3) \rangle$ be 2 groups where $G = \{1, \omega, \omega^2\}$ & $G' = \{0,1,2\}$ s/T $G \cong G'$

Sol:- $\langle G, * \rangle$ is a Group where $G = \{1, \omega, \omega^2\}$

$\langle G', (\text{mod } 3) \rangle$ is a Group where $G' = \{0,1,2\}$

To prove the isomorphism b/w 2 Groups G & G' ie, $G \cong G'$, the func $f: G \to G'$ satisfies 3 conditions.

(i) f is one-to-one :-

$*$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$(\because \omega^3 = 1)$

$\langle G, * \rangle$

mod3	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\langle G, \text{mod}_3 \rangle$

G'

$0 +_{mod_3} 0 = 0$

$1 \to 0, \ \omega \to 1, \ \omega^2 \to 2$

($\because$ 1 corresponding ele 0
ω " " 1
ω^2 " " 2)

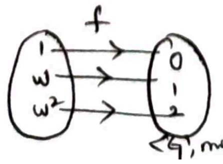
$0 +_{mod_3} 1 = 1 \text{ mod } 3 = 1$

$\because f(1) = 0, f(\omega) = 1 \quad f(\omega^2) = 2$

$0 +_{mod} 2 = 2 \text{ mod } 3 = 2$

$2 +_{mod} 2 = 4 \text{ mod } 3 = 1$

$1 +_{mod} 2 = 3 \text{ mod } 3 = 0$



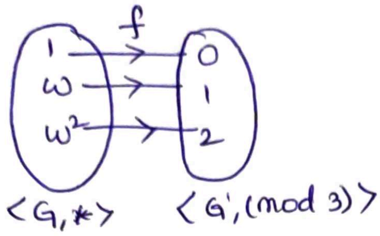
$\langle G, * \rangle$ $\quad$ $\langle G', \text{mod } 3$

$\therefore f$ is one-to-one.

(ii) f is onto :-

for every element $x, x \in G'$ then there exist an ele $x', x' \in G$

Hence f is onto.



$\therefore$ f is onto

(iii) f is homomorphism :-

for any 2 ele's $\omega, \omega^2 \in G$ then

$f(\omega * \omega^2) = f(\omega +_{mod\,3} \omega^2)$

$= f(\omega) +_{mod\,3} f(\omega^2)$

$= 1 +_{mod\,3} 2 = 3 \bmod 3 = 0$

$f : G \to G'$

$\downarrow \quad \downarrow$

$* \quad mod\,3$

$f(a*b) = f(a) \; mod_3 \; f(b)$

$a, b \in G$

$f(\omega * \omega^2) = f(\omega) +_{mod\,3} f(\omega^2)$

$\therefore$ f is homomorphism.

$\therefore$ f satisfies 3 conditions b/w G and G'

$\therefore G \cong G'$

= ∘ =

Theorem:-

In a Group $(G,*)$, Prove that the identity element is unique.

Proof:- let e_1 and e_2 are two identity elements in G

Now, $e_1 * e_2 = e_1$ — (1) ($\because e_2$ is the identity)

Again $e_1 * e_2 = e_2$ — (2) ($\because e_1$ is the identity)

from (1) and (2), we have

$$e_1 = e_2$$

$\therefore$ Identity element in a group is unique.

Theorem:- In a Group $(G,*)$. P/T the inverse of any element is unique.

Proof:- let $a, b, c \in G$ and e is the identity in G.

Let us suppose, Both b and c are inverse elements of a.

Now, $a * b = e$ —— (1) (since, b is inverse of a)

Again, $a * c = e$ —— (2) (since, c is also inverse of a)

from (1) and (2), we have

$$a * b = a * c$$

$\Rightarrow b = c$ (By left cancellation law)

In a group, the inverse of any element is unique.

Theorem:- In a Group $(G,*)$, if $(a*b)^2 = a^2*b^2$ $\forall a,b \in G$ then S/T G is abelian group.

(Hint Commutative prove ($ab=ba$ or $ba=ab$))

Sol: Proof:- Given that $(a*b)^2 = a^2*b^2$

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

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

$(b*a)*b = (a*b)*b$ (By left cancellation law)

$(b*a) = (a*b)$ (by right cancellation law)

Hence, G is abelian group.

Theorem:- In a Group $(G,*)$, P/T $(a*b)^{-1} = b^{-1}*a^{-1}$ $\forall a,b \in G$

proof:- Consider

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

$= a*(b*b^{-1})*a^{-1}$ (By Associative pro)

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

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

$= e$ (By inverse property)

$a*b=e$
(or) $a*a^{-1}=e$
Inverse of $a = b$
$\boxed{a^{-1}=b}$
IIIly:- $(\underbrace{a*b}_{a})^{-1} = \underbrace{b^{-1}a^{-1}}_{b}$
Here To prove $a^{-1}=b$
Multy$(a*b)$ LHS $\rightarrow$ prove e

IIIly we can S/T

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

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