GROUP THEORY

- **Groupoid** : A non-empty set G equipped with one binary operation is called groupoid.
  - G is closed for '*' under groupoid.
  - It is denoted by $(G, *)$
  - Ex :- $(N, +)$, $(Z, -)$, $(Q, \times)$, etc.

NOTE :- Groupoid is also called Quasi group.

- **Semi-group** : An algebraic structure $(G, *)$ is called a semi-group if the binary operation '*' satisfies associativity and closure property.

  [G1] $\rightarrow$ $(a*b)*c = a*(b*c)$ $a \in G$, $b \in G$, $c \in G$

  - Ex :- $(N, +)$, $(Z, +)$, $(Z, \times)$, $(Q, \times)$ are semi-groups but $(Z, -)$ is not because '−' is not associative.

- **Monoid** : A semi-group is called monoid if there exists an identity element 'e' such that:

  [G2] $e*a = a*e = a$, $a \in G$

  - Ex :- Semi-group $(N, \times)$ is monoid because 1 is the identity for multiplication.

- **Group :-** An algebraic structure of set G and a binary operation '$*$' defined in G, i.e., $(G,*)$ is called a group if $*$ satisfies the following postulates:

[G1] Closure : $a \in G,\ b \in G \Rightarrow a*b \in G.\ \forall\ a,b \in G$

[G2] Associativity : The composition $*$ is associative in G, i.e.

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

[G3] Existence of Identity : There exists an identity element e in G such that

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

[G4] Existence of Inverse : Each element of G is invertible, i.e., for every $a \in G$, there exists a^{-1} in G such that :

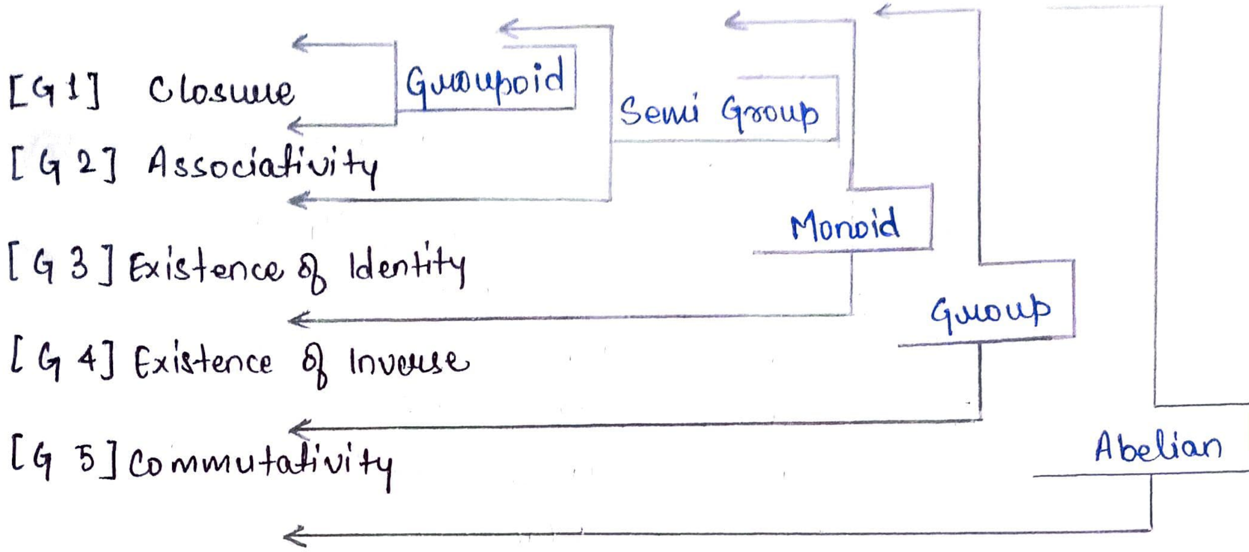
$$a*a^{-1} = a^{-1}*a = e \text{ (identity)}$$

- **Abelian / Commutative group** : A group $(G,*)$ is said to be abelian or commutative if $*$ is commutative also. A group $(G,*)$ is abelian if,

[G5] Commutativity : $a*b = b*a\ \ \forall\ a,b \in G$

- **Finite & infinite groups** :- A group $(G,*)$ is said to be finite if its underlying G is a finite set & a group which is not finite is called infinite group.

- **Order of group** :- No. of elements in finite group is called order of grp.
  - Denoted by $O(G)$.
  - If G is infinite group, then it is said to be of infinite order.



Mind map

* Properties of Group :-

① Uniqueness of Identity:

Theorem :- The identity element of group is unique.

Proof :- let $(G, *)$ be a group having two identities e and e'.

Since, e is the identity element of G,

$$\Rightarrow ae = ea = a \quad \forall a \in G \quad \text{---} (I)$$

Similarly, e' is the identity element of G,

$$\Rightarrow ae' = e'a = a \quad \forall a \in G \quad \text{---} (II)$$

As, eqn ① is true for $a \in G$ & $e' \in G$, so putting $a = e'$ in ①

$$\Rightarrow e'e = ee' = e' \quad \text{---} (III)$$

similarly, with eqn ②,

$$ee' = e'e = e \quad \text{---} (IV)$$

$\therefore$ from (III), (IV), it is proved that $e = e'$.

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

② Uniqueness of inverse :-

Theorem :- The inverse of an element in a group is unique.

Proof :- let a be any element of group $(G, *)$ which has two inverses b and c in group :-

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

$a^{-1} = c \Rightarrow ca = e = ac$

Now, $ba = e \Rightarrow (ba)c = ec$

$\Rightarrow b(ac) = c$

$\Rightarrow be = c$

$\Rightarrow b = c$

∴ the inverse of every element of a group is unique.

③ Theorem :- If G is a group, then for $a, b \in G$

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

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

i.e., the inverse of the product of two elements is the product of their inverses in reverse order.

Proof :- a) Since a^{-1} is the inverse of a, therefore

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

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

$\Rightarrow$ inverse of $a^{-1} = a$, i.e., $(a^{-1})^{-1} = a$

b) Since $a, b, a^{-1}, b^{-1}, ab, b^{-1}a^{-1}$ all are element of G,

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

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

$= aa^{-1}$

$= e$

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

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

$= b^{-1}b$

$= e$

∴ (ab) has $b^{-1}a^{-1}$ as its inverse.

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

(4) **Theorem:-** If a, b are elements of a group G, then equations $ax = b$ and $ya = b$ have unique solutions in G.

Proof:- $\because a \in G \Rightarrow a^{-1} \in G$ [by G3]

$\because a \in G \cdot b \in G \Rightarrow a^{-1}b \in G$ [by G1]

Now, $a(a^{-1}b) = (aa^{-1})b$

$= eb$

$= b$

Therefore, $x = a^{-1}b$ is a soln of eqn $ax = b$ in G.

Uniqueness:- let the eqn $ax = b$ have two soln, $x = x_1$ and $x = x_2$

then $ax_1 = b$ and $ax_2 = b$.

$\Rightarrow ax_1 = ax_2$

$\Rightarrow x_1 = x_2$ [by left cancellation law]

$\therefore$ soln of $ax = b$ is unique in G.

$\Rightarrow$ Similar steps to be taken for $ya = b$.

- **Subgroups :**

A non-empty subset H of a group G is called a subgroup of G if:

i) H is closed for the composition defined in G, i.e.;

$a \in H,\ b \in H \Rightarrow ab \in H$

ii) H itself is a group for the composition induced by G

- **Improper / Trivial subgroup :-**

Every group of order greater than 1 has atleast two subgroups which are :-

i) G (itself)

ii) $\{e\}$ i.e., group of identity alone.

These two subgroups are known as trivial / improper

- **Proper subgroup :-**

A subgroup other than that of trivial subgroups is know as proper subgroup;

• **Theorem 11:**

If H is a subgroup of G, then,

a) The identity of H is same as that of G,

b) The inverse of any element a of H is same as the inverse of same regarded as an element of G.

c) The order of any element a of H is same as the order of a in G.

Proof: a)

Let e and e' be identities of G and H respectively.

if $a \in H$, then $ae' = e'a = a$ —— (1)

Again, as $a \in H \Rightarrow a \in G$

So, $ae = ea = a$ —— (ii)

$\therefore$ from (1) & (2),

$ae' = ae$

Applying cancellation law,

$\Rightarrow e' = e$

b)

Let $a \in H$, b & c be inverse of a in G & H resp.

Let e be the identity element of G & H.

$ab = ba = e$ —(1) {$\because$ b is inv. of a $\rightarrow$ assumption}

similarly, $ac = ca = e$ —— (ii)

$\therefore$ from (1) & (ii),

$ab = ac$

By cancellation law,

$b = c$

Thus, the inverse of an element in H is same in H as that of G.

c) Let the order of $a \in H$ be m and n in H and G resp.
If e be the identity, then by definition of order

$a^m = e$ and $a^n = e \Rightarrow a^m = a^n$

$\Rightarrow a^m a^{-n} = a^n a^{-n} = a^0$

$\Rightarrow a^{m-n} = e$

$\Rightarrow m - n = 0$

$\Rightarrow m = n$

$\therefore$ The order of any elements of subgroup is same as that of subgroup and original group.

Theorem 2 :-

A non-void subset H of a group G is a subgrp iff : $\underline{a \in H, b \in H \Rightarrow ab^{-1} \in H}$

Proof :-

Let H be a subgroup of group G and $b \in H$
then $b \in H \Rightarrow b^{-1} \in H$ [by existence of inverse in G]

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

$\Rightarrow ab^{-1} \in H$ [by closure property in H]

Therefore, if H is a subgroup of G, then the condition is necessary.

Conversely :- Suppose given condition is true in H, then we shall prove that H will be a sub group.

$\therefore H \neq \phi$ $\qquad$ $\therefore$ let $a \in H$

Therefor, identity exists in H.

Again by same condition, $e \in H, a^{-1} \in H \Rightarrow ea^{-1} \in H = a^{-1} \in H$

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

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

H is closed for operation of G.

RING THEORY

- **Ring**:- The structure $(R, +, \times)$ consisting of a non void set R and two binary compositions, denoted by "+" and "×" or "·", is said to be a ring, if following axioms are satisfied:-

[R1] : $(R, +)$ is an abelian group

[R2] : $(R, \times)$ is a semi-group (i.e; closure & associative)

[R3] : $\forall\ a, b, c \in R$

$$a \times (b+c) = a\times b + a\times c \qquad \text{[left distributive law]}$$

$$(a+b)\times c = a\times c + b\times c \qquad \text{[Right distributive law]}$$

- **Types**:-

① **Ring with unity**:-

A ring $(R, +, \times)$ is said to be a ring with unity if its multiplicative identity exists (i.e; 1). i.e, if $\exists\ e \in R$ such that

$$ea = a = ae, \quad \forall a \in R$$

② **Commutative Ring**:-

A ring $(R, +, \times)$ is said to be a commutative ring if its multiplicative composition is also commutative, i.e, if

$$a\times b = b\times a, \quad \forall\ a, b \in R$$

③ **Commutative ring with unity**:-

A ring $(R, +, \times)$ possessing multiplicative identity and is commutative is called commutative ring with unity.

NOTE:- The set R consisting of single element 0 with two composition $(+)$ and $(\times)$ defined as: $0+0=0$ and $0\times 0 = 0$ is a ring called zero ring / Null ring / Trivial ring.

- **Properties of a ring:-**

a) $a \cdot 0 = 0 \cdot a = 0$

b) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

c) $(-a) \cdot (-b) = a \cdot b$

d) $a \cdot (b - c) = a \cdot b - a \cdot c$

e) $(b - c) \cdot a = b \cdot a - c \cdot a$

- **Special type of rings:-**

a) **zero divisors in a Ring :-** An element $a (\neq 0)$ of a ring R is said to be a zero divisor if there exists a non-zero b in R such that:

$$\boxed{a \times b = 0}$$

Ex In ring $[\{0,1,2,3,4,5\}, +_6, \times_6]$
2, 3 & 4 are zero divisors because
$2 \times_6 3 = 0$, $3 \times_6 2 = 0$, $4 \times_6 3 = 0$.

b) **Ring without zero divisors :-** A ring R is said to be a ring without zero divisors if it has no zero divisors,
i.e., $a, b \in R$ and $ab = 0$
$\Rightarrow a = 0$ or $b = 0$

Ex. Rings - $(Z, +, \times)$, $(Q, +, \times)$, $(R, +, \times)$, etc
are rings without zero divisors because there exists no two non-zero numbers such that their product is 0.

c) **Ring with zero divisors :-** A ring R is said to be ring with zero divisors if there exists $a, b \in R$ such that $a \neq 0$, $b \neq 0$, yet $a \cdot b = 0$.

Ex Ring:- $[\{0,1,2,3,4,5\}, +_6, \times_6]$ is with zero divisors.

$\Rightarrow$ $4 \times_6 3 = 0$, $4 \neq 0$ & $3 \neq 0$.

- **Integral Domain :-** A ring D is said to be an integral domain, if it is a commutative ring with unity and without zero divisors, i.e., a ring R is.

i) commutative

ii) with unity

iii) without zero divisors

NOTE :- In an integral domain, atleast two elements are required, because there must be atleast one non-zero element.

Thus, set $(D, +, \times)$ is called int. domain if it satisfies the following axioms for two defined binary comp. '+' & '×':

[ID₁] : $(D, +)$ is abelian group. $(\forall a, b, c \in D)$

[ID₂] : $(D, \times)$ is semi abelian group with unity, i.e.

✓ $a \times (b \times c) = (a \times b) \times c$ (Distributive)

✓ $\exists\, 1 \in D$ s.t $a \times 1 = 1 \times a = a$ (Identity)

✓ $a \times b = b \times a$ (commutative)

[ID₃] : Distributivity

[ID₄] : without zero divisors, i.e,

✓ $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

• **Field :-** A ring F is called a field, if it is:

i) Commutative

ii) with unity

iii) its every non-zero element is invertible, i.e., has multiplicative inverse.

Thus, a structure $(F, +, \times)$ containing atleast two elements is a field if it satisfies the following axioms :-

[F1] : $(F, +)$ is abelian group

[F2] : $(F_0, \times)$ is abelian group

[F3] : Distributivity

* **Unit elements in a ring with unity :-**

Let R be a ring with unity and 1 be the identity of second composition (i.e., $\times$), then any $a \in R$ is called unit element if there exists $b \in R$ such that $ab = 1 = ba$

i.e., b is inverse of a & vice-versa.