# Group Theory

## Binary operations →

Let A be a nonempty set. A binary operation $*$ on set A is a mapping from $A \times A \longrightarrow A$

ie for all $a, b \in A$, $a * b \in A$

ex:- ① + (additn) is a binary operatn on N

② − (sub) is not a binary operatn on N

$(2, 3, \; 2-3 = -1 \notin N)$

③ / (divisn) is not a binary operatn Z

$(2, 3, \; 2/3 \notin Z)$

If $*$ is a binary operation on 'A'. Then $*$ is said to be

① Commutative : $a * b = b * a \quad \forall\, a, b \in A$

② Associative : $a * (b * c) = (a * b) * c \quad \forall\, a, b, c \in A$

③ An elt 'e' in A is said to be an 'identity element' if

$a * e = e * a = a \quad \forall\, a \in A$

④ For $a \in A$, an elt $b \in A$ is said to be 'inverse' of a if $a * a^{-1} = a^{-1} * a = e$

⑤ closed : if $a * b \in A$ for $\forall\, a, b \in A$

Algebraic sys : A set along wd one or more operations

$(N, +)$ $(Z, +)$, $(Q, -)$

N → Natural nos  Z → Integers  Q → Rational nos  $Z^+$ → +ve integers

## Semigroup:

Let A be a nonempty set wd binary operation $*$. The $(A, *)$ is said to be a semigroup if it satisfies

i) closure law

ii) Associative law

ex:- $(N, +)$ is a semigroup

$(N, \cdot)$ is a semigroup

$(N, -)$ is not a semigroup

$(Z, -)$ is a semigroup

## Monoid:

$(A, *)$ is said to be a monoid if it satisfies

i) closure law

ii) associative law

iii) Identity law (ie there exists an identity elt)

ex:- $(N, +)$ is not a monoid ($\because$ (iii) law fails)

$(N, \cdot)$ is monoid

$(Z, +)$ is monoid

## Group:

$(A, *)$ is said to be a group if it satisfies

i) closure law

ii) Associative law

iii) Identity law

iv) Inverse law (every elt has its inverse in A)

ex:- $(N, \cdot)$ is not a group

$(Z, +)$ is a group

## Abelian group :-

i) closure law
ii) Associative "
iii) Identity "
iv) Inverse law
v) Commutative "

* $(\mathbb{Z}, +)$
* $(\mathbb{Z}, -)$
* $(N, +)$
* $(\mathbb{Q}, \cdot)$
* $(\mathbb{Q} - \{0\}, \cdot)$
* $(R, \cdot)$ ⟶ not a group ⟶ (Identity elt - 1 ✓ Inverse law fails as 0 has no inverse)
* $(R - \{0\}, \cdot)$ is a group
* set of all square matrices $(S_{n\times n}, \cdot)$
* Set of all invertible square matrices $(S'_{n\times n}, \cdot)$

## Properties of groups

Thm 1: In a group $(G, *)$, the identity element is unique

Thm 2 : In a group $(G, *)$, inverse of every element is unique

proof:- consider $a \in G$, if a has 2 inverses b & c

$$a * b = b * a = e \quad -①$$
$$a * c = c * a = e \quad -②$$

( ∵ a & b are inverse of each other, a & c " " " " )

consider $b = e * b$ (identity law)

$= (c * a) * b$ (frm ②)

$b = (c * a) * b$

$= c * (a * b)$ ($\because$ associative law)

$= c * e$ ($\because$ from ①)

$= c$ (identity law)

$\underline{\underline{b = c}}$,

Theorem 3: $(a^{-1})^{-1} = a$ for all $a \in G$ where $(G, *)$ is a group

Theorem 4: In a group $(G, *)$, $(a * b)^{-1} = b^{-1} * a^{-1}$ $\forall a, b \in G$

$(\mathbb{Z}, +)$
$(2+3)^{-1} = 5^{-1} = -5$
$3^{-1} + 2^{-1} = -3 - 2 = -5$

Proof:-

We've to P.T inverse of $(a * b)$ is $b^{-1} * a^{-1}$

(In gen, to prove $x$ is inverse of $y$, we must show $x * y = e$, $y * x = e$

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

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

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

$= a * a^{-1}$

$= e$

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

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

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

$= b^{-1} * b$

$= e$

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

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

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

$$= \underline{\underline{c^{-1}*b*a}}$$

**Theorem 5 :** In a group $(G,*)$

i) $a*b = a*c \Longrightarrow b=c$ (Left cancellation law)

ii) $a*b = c*b \Longrightarrow a=c$ (Right cancellation law)

$$\left( \begin{array}{l} \cancel{2}+3=\cancel{2}+x \\ 3=x \end{array} \right.$$

Proof:-

Given $a*b=a*c$, we've to prove $b=c$

operating on left by $a^{-1}$

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

$$(a^{-1}*a)*b = (a^{-1}*a)*c \qquad (\because \text{associative})$$

$$e*b = e*c \qquad (\because \text{Inverse})$$

$$\underline{\underline{b=c}} \qquad (\because \text{Identity law})$$

**Theorem 6 :** In a group $(G,*)$, the equations $a*x=b$ and $y*a=b$ $a,b\in G$ have unique soln

Proof:-

consider $a*x=b$

$$\left| \begin{array}{l} 2+x=8 \\ -2+2+x=8-2 \\ x=6. \end{array} \right.$$

Existence of the soln $\Rightarrow$

$$a*x=b$$

operating on left side by $a^{-1}$

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

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

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

$x = a^{-1} * b$

since $G$ is a group, $a^{-1} \in G$, $b \in G$, $a^{-1} * b \in G$

$\therefore x \in G$.

uniqueness of the soln :-

If $x_1$ & $x_2$ are the two solns of $a * x = b$

$a * x_1 = b$ & $a * x_2 = b$

$\cancel{a} * x_1 = \cancel{a} * x_2$

$x_1 = x_2$ ( left cancellation law)

Problems

1. Let $(\{a, b\}, *)$ be a semigroup. If $a * a = b$, then

P.T i) $a * b = b * a$

ii) $b * b = b$

$$\left\{\begin{array}{l} a * a \longrightarrow b \\ a * b \\ b * a \\ b * b \end{array}\right.$$

soln

i) $LHS = a * b$

$= a * (a * a)$ ($\because$ given)

$= (a * a) * a$ ($\because$ associative)

$= b * a$ ($\because$ given)

$= RHS$

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

$= a * (a * b)$ (associative law)

But $a * b$ can be either $a$ & $b$

Either $a * b = a$ & $a * b = b$

If $a*b=a \Rightarrow$

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

If $a*b=b \Rightarrow$

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

In both the cases, $b*b=b$.

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

soln

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

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

($\because$ using cancellatn laws)

(3) Let $G$ be a group in which every elt is inverse of itself. Then $G$ is abelian / Imp

soln

For all $a \in G$, $a*a=e$, $b*b=e$ $\quad (a*b)*(a*b)=e$

We've to P.T it is abelian gp ($\because$ commutative law)

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

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

OR

Given every elt is inverse of itself

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

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

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

$$= b * a$$

$$a * b = b * a$$

⑥ If a group $(G,*)$ has even no of elts, then S.T atleast one elt must be its own inverse.

soln

$$G = \{e, a_1, a_2, a_3 \cdots a_{2n-1}\}$$

w.k.t $e^{-1} = e$

For the rest, $a_1 \,\&\, a_2 \,|\, a_3 \,\&\, a_4 \,| \cdots a_{2n-3} \,\&\, a_{2n-2} \,|$ are inverses of each other

$a_{2n-1}$ is left, but it must have inverse in $G$

$$a_{2n-1}^{-1} = a_{2n-1}$$