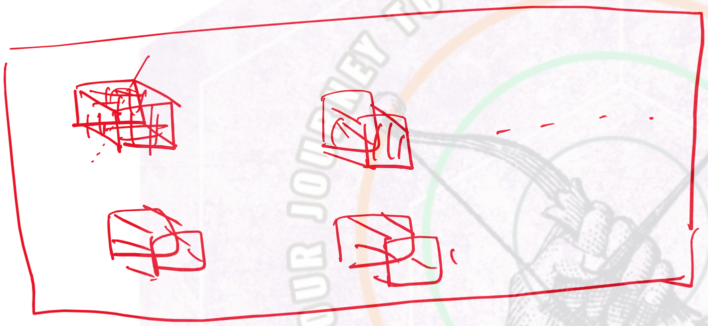
Group Theory (Math Minor sem V)

Lecture - 1

Group Theory is a part of Abstract Algebra.

Group $\Longleftrightarrow$ Symmetry.

S_4 D_6



Same image

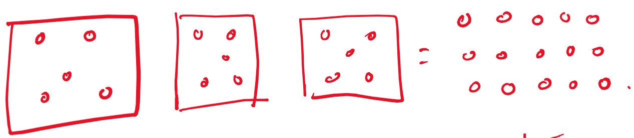
They all maintain symmetry.

3 (· · ·)

∘ ∘ ∘ + ∘ ∘ ∘ ∘ ∘ = ∘ ∘ ∘ ∘ ∘ ∘ ∘ ∘

$3 + 5 = 8$

$3 + 5 = 8$



3×5

15

Group (defⁿ)

A non-empty set G is said to form a group with respect to a binary composition '$\circ$' if

i) G is closed under the composition '$\circ$'

ii) $\circ$ is associative. $(a+b)+c = a+(b+c)$.

iii) There exist an element 'e' in G such that

$$e \circ a = a \circ e = a \quad \forall\, a \in G.$$

$e \rightarrow$ identity element of the group.

iv) For each element a in G, there exist an element a' in G such that

$$a' \circ a = a \circ a' = e.$$

$a' \rightarrow$ inverse of a.

$5 \times \frac{1}{5} = 1$

Examples group!

1) Consider the set $\mathbb{Z}$, $\circ \rightarrow +$

$(\mathbb{Z}, +) \rightarrow$ Group.

i) Closeness Property.

i) Closeness Property.

Let $a, b \in \mathbb{Z}$, The $a+b \in \mathbb{Z}$,

So, $\mathbb{Z}$ is closed under addition.

ii) Associative Property.

Addition is associative on $\mathbb{R}$

$\mathbb{Z} \subseteq \mathbb{R}$, Addition is associative in $\mathbb{Z}$.

iii) Identity Property.

$0 = 'e'$

$0 \in \mathbb{Z}$, $a \in \mathbb{Z}$

$0 + a = a + 0 = a$.

$\therefore$ '0' is the identity element.

iv) Inverse Property. $0 \to ?$

Let, $a \in \mathbb{Z}$, $a' = -a$. $\boxed{0 \to ?}$

$a + a' = 0 = 'e'$

So, $-a$ is the inverse of a.

$(\mathbb{Z}, +)$ is a Group. $\boxed{\text{PROVED.}}$

ii) Prove $(\mathbb{Q}, +)$ is a group.

$\mathbb{Q} \to$ Set of Rational no's

$\mathbb{Q} \rightarrow$ Set of Rational no's

Proof like above one only.

Similarly $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ forms a group.

Check whether $(\mathbb{Z}, \cdot)$ is a group or not?

$\cdot \rightarrow$ Multiplication.

Soln: $a, b \in \mathbb{Z}$ $\quad a \times b = c \in \mathbb{Z}$

i) Closeness ✓

ii) Associative ✓ $\qquad -1 \times \_ = -1$

iii) Identity $\rightarrow$ $1 \in \mathbb{Z}$; so identity exist ✓

iv) Inverse $\quad 1 \in \mathbb{Z}$

$1 \times 1 = 1 \qquad 1 \in \mathbb{Z}$.

$-1 \times \underline{1} = 1 \qquad a, -a +$

$\left.\begin{array}{l} a = -1, \; a' = -1 \\ a = 1, \; a' = 1 \end{array}\right\} \in \mathbb{Z}$.

$2 \times \frac{1}{2} = 1 (= e) \qquad \frac{1}{2} \notin \mathbb{Z}$?

So, $(\mathbb{Z}, \cdot)$ is not a group.

or, $\mathbb{Z}$ is not a group under multiplication.

Similarly $(\mathbb{Q}, \cdot)$; $(\mathbb{R}, \cdot)$; $(\mathbb{C}, \cdot)$ also

Similarly $(\mathbb{Q}, \cdot)$; $(\mathbb{R}, \cdot)$; $(\mathbb{C}, \cdot)$ also don't form a group.

Commutative Group or Abelian

A group $(G, \circ)$ is said to be a commutative or abelian group if '$\circ$' is commutative.

$a \circ b = b \circ a$.   e.g. $a + b = b + a$.
$a \times b = b \times a$.

Eg. $(\mathbb{Z}, +)$ $a + b = b + a$, $a, b \in \mathbb{Z}$.

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

Let $m \in \mathbb{Z}^+$, Then $m\mathbb{Z}$ denote the set of all integral multiples of m.

$$m\mathbb{Z} = \{0, \pm m, \pm 2m, \ldots\}.$$

$$2\mathbb{Z} = \{0, \pm 2, \pm 4, \pm 6, \ldots\}.$$

$$3\mathbb{Z} : \ldots .$$

Prove $(2\mathbb{Z}, +)$ is a commutative group.

Closeness Property.

i) Let $a, b \in 2\mathbb{Z}$, Then $a = 2p$, $b = 2q$.
$\forall\, p, q \in \mathbb{Z}$.

$\forall\, p, q \in \mathbb{Z}$.

$a + b = 2p + 2q$
$= 2(p+q) \in 2\mathbb{Z}$ since $p+q \in \mathbb{Z}$.

So, $2\mathbb{Z}$ is closed under $+$.

Associative Property

$2\mathbb{Z} \subseteq \mathbb{Z}$, so addition will hold on $2\mathbb{Z}$

iii) Identity Prop.

$0 \in 2\mathbb{Z}$ $\quad 0 + a = a + 0 = a \in 2\mathbb{Z}$.

iv) $a \in 2\mathbb{Z}$, then $-a \in 2\mathbb{Z}$

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

v) Commutativity $\qquad 2, 4 \in \mathbb{Z}$

$a, b \in 2\mathbb{Z}$ $\qquad 2+4 = 4+2$

$a + b = b + a$.

So, $(2\mathbb{Z}, +)$ is a commutative Group.

Note: $(m\mathbb{Z}, +)$ is a commutative group.

Some Important Theorems.

Th 1: A Group $(G, \circ)$ contains only one identity element.

Proof : Let e, f be two identity element in G.

$e \circ a = a \circ e = a$.

$f \circ a = a \circ f = a \quad \forall a \in G$.

$e \circ f = f \rightarrow$ when 'e' identity

$e \circ f = e \rightarrow$ when 'f' identity.

$\hookrightarrow \quad e = f$, this proves the uniqueness.

Thm: In a group $(G, \circ)$, each element has only one inverse.

Proof $\rightarrow$ Try yourself.

Note : $a^{-1} \rightarrow a$'s inverse

Cancellation Laws

In a group $(G, \circ)$ $\forall a, b, c \in G$.

i) $a \circ b = a \circ c$ implies $b = c$ (Left cancellation).

ii) $b \circ a = c \circ a$ implies $b = c$ (Right cancellation)

Proof : $a \in G$, $a^{-1} \in G$. '$\circ$' $\rightarrow$ associative.

$a \circ b = a \circ c$

$\Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$.

$\Rightarrow \underbrace{(a^{-1} \circ a)} \circ b = \underbrace{(a^{-1} \circ a)}_{e} c$

$\Rightarrow \underbrace{(a \circ a)}_{e} \circ b = \underbrace{(\quad)}_{e}$

$\Rightarrow e \circ b = e \circ c$.

$\Rightarrow b = c$. $\boxed{\text{PROVED}}$

ii) Proof the right cancellation.

Thm: $(G, \circ)$ $\forall a, b \in G$, each of the equations $a \circ x = b$ and $y \circ a = b$ has a unique sol^n in group G.

Proof: Since $a, b \in G$, $a^{-1} \circ b \in G$.

$a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b$ ($\circ$ is associative)

$= e_G \circ b$

$= b$.

$\Downarrow$

$a \circ x = b$

$x = a^{-1} \circ b$. is a sol^n of the eq^n $a \circ x = b$.

Let, x_1, x_2 be two sol^n of the eq^n.

$a \circ x = b$. Then

$a \circ x_1 = b$, $a \circ x_2 = b$

$\Rightarrow a \circ x_1 = a \circ x_2$

$\Rightarrow x_1 = x_2$ (By Left cancellation law)

$\Rightarrow x_1 = x_2$ (By Left cancellation law).

This proves the uniqueness.

$b \circ a^{-1} \in G$. $\quad (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a)$

$= b \circ e_G$

$= b$

$\Downarrow$

$y \circ a = b$.

$y = b \circ a^{-1}$ is a sol^n.

$y_1, y_2 \to$ unique.

use - right cancellation.

Thm: $(G, \circ)$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1} \ \forall a, b \in G$.

$(AB)^{-1} = B^{-1}A^{-1}$ (Matrix analogy).

$\Rightarrow$ Let, $a, b \in G$.

$a^{-1}, b^{-1}, a \circ b, b^{-1} \circ a^{-1} \in G$.

$(b^{-1} \circ a^{-1}) \circ (a \circ b) = [b^{-1} \circ (a^{-1} \circ a)] \circ b$.

$= (b^{-1} \circ e_G) \circ b$

$= b^{-1} \circ b = e_G \quad$ — (i)

Similarly,

$(a \circ b) \circ (b^{-1} \circ a^{-1}) = e_G$. $\quad$ — (ii).

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = e_G \quad \text{--- (ii)}$$

From (i) and (ii) ——

$$\underbrace{(b^{-1} \circ a^{-1})}_{\text{inverse}} \circ (a \circ b) = (a \circ b) \circ \underbrace{(b^{-1} \circ a^{-1})}_{\text{inverse}} = e_G$$

So, $(b^{-1} \circ a^{-1})$ is the inverse of $(a \circ b)$

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

PROVED.