Group Theory 4

29 September 2023 10:18

- A binary operation on a non-empty set G is a function
  $\mu : G \times G \to G$

- Generalized Associativity :- $a_1 * a_2 * \cdots * a_n$ needs no parantheses

Semigroup :- A semigroup $(G, *)$ is a non-empty set G equipped with an associative property

G be a semigroup then, for $a \in G$, $a^1 = a$ and for $n \geq 1$ we have $a^{n+1} = a * a^n$

$a^{mn} = \underbrace{a^m * a^m * \cdot * a^m}_{n \text{ times}}$ $\qquad a^{m+n} = a^n * a^m$

Group :- A group is a semigroup G containing an element e such that :-

(i) $e * a = a = a * e \quad \forall a \in G$

(ii) for every $a \in G$, $\exists$ an element $b \in G$ such that,
$a * b = e = b * a$

$S_X \to$ It holds associative property

$\to$ It is non-empty $\to$ so it is a semigroup

$\to \exists (1)(2)(3) \cdot (|X|)$ in S_X which is e, $e * a = a * e = a \quad \forall a \in S_X$

$\to \forall a \in S_X$, as a is a bijection, a^{-1} exists, which is b here
$a * b = b * a = e$ $\to$ it is a group

If $a*b = b*a$ holds $\forall a, b \in G$ then it is a abelian group (or semigroup)

- Concatenation is $(a_1, a_2, \dots, a_n) * (b_1, b_2, \dots, b_n) = (a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n) \in G$

  $(a_1, a_2, \dots)$ or $(b_1, b_2, \dots) \in G$

  $(a_i + b_i)^* \in G$ → semigroup $a_i * b_i \neq b_i * a_i$

  → So not abelian

Theorem:-
In a group G $\exists$ a unique element e with $e*a = a = a*e$ $\forall a \in G$.

Proof:- Suppose $\exists$ e, e' are two such elements

$e*a = a*e = a$ and $e'*a = a*e' = a$

$e = e*e' = e'$ $\Rightarrow\Leftarrow$ Hence unique

- In group G, $a \in G$ then $(a^{-1})^{-1} = a$

  $a^{-1} \in G$, $(a^{-1})^{-1} \in G$, $a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e$

  $a * a^{-1} = a^{-1} * a = e$ → By uniqueness, $a = (a^{-1})^{-1}$

- $a^{-n} = (a^{-1})^n$, $a^0 = e$

Theorem:- If G is a semigroup with an element e such that:-

(i) $e*a = a$ $\forall a \in G$ and

(ii) for each $a \in G$ $\exists$ an elements $b \in G$ with $b*a = e$

Then G is a group.

Proof:- $a = e*a$ $\forall a \in G$, $\exists b$ $b*a = e$

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

$b * a * a = b * (a * a) = e * a = \ldots$

$b * e * e = e$

Suppose $g * g = g$ then $\exists b'$ $b' * (g * g) = b' * g = e$

$b' * g * g = g \Rightarrow g = e$

$e * e = e$

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

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

$e * a = a \ \forall a \in G$ $\qquad a * b = e = b * a$

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

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

Hence G is a group

Q) In a group G, either of the equations $a * b = a * c$ and $b * a = c * a$ implies $b = c$.

Ans:- $a \in G$, $\exists d \in G$ $\quad a * d = e = d * a$

$d * a * b = d * a * c \Rightarrow b = c$

$b * a * d = c * a * d \Rightarrow b = c$

Q) A group in which $x * x = e \ \forall x \in G$ then G must be abelian. Prove it.

Ans:- $a * b = b * a \ \forall a, b \in G$ $\qquad a * a = e$
$\qquad b * b = e$

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

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

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

$e * b * a * b * b = a * b \Rightarrow b * a = a * b$

Q) Let G be a group, $a \in G$ and m, n are relatively prime

Q) Let G be a group, $a \in G$ and m, n are relatively prime integers. If $a^m = e$ show that $\exists\, b \in G$ such that $a = b^n$.

Ans :- <u>Hint</u> :- $nx + my = 1$ for some $x, y \in \mathbb{Z}$

$$a = a^1 = a^{my+nx} = a^{my} * a^{nx} = (a^m)^y * (a^n)^x$$
$$= (a^x)^n = b^n$$

$\Rightarrow \exists\, b$ such that $a = b^n$.