Chapter- 4 : Group Theory.

Let A be any non-empty set. A binary operation $*$ on A is a mapping from $A \times A \longrightarrow A$, i.e., $a*b \in A$, whenever $a, b \in A$.

Example : 1) On N, define $a*b = a+b$, $a, b \in N$
'+' is a binary operation.

2) On N, define $a*b = a-b$, $a, b \in N$.
'–' is not a binary operation.

3) Let $a, b \in Q$, $a*b = a+b-ab$.
Then '$*$' is a binary operation.

If $*$ is a binary operation on A, then we say
(i) $*$ is closure if $a*b \in A$, $\forall\, a, b \in A$.

(ii) $*$ is associative if $a*(b*c) = (a*b)*c$, for all $a, b, c \in A$.

(iii) An element $e \in A$ is called an identity element w.r.to $*$ if $a*e = e*a = a$, for all $a \in A$.

(iv) For $a \in A$, an element $b \in A$ is said to be inverse of a w.r.to $*$ if $a*b = b*a = e$, where e is an identity element. a^{-1}

(v) $*$ is commutative (abelian) if $a*b = b*a$ for $a, b \in A$.

Semigroup : Let A be a non-empty set with binary operation $*$. A is said to be a semigroup if the following properties are satisfied.

(i) closure
(ii) Associative

Example : $(N, +)$, $(N, \cdot)$

Monoid : Let A be a non-empty set with binary operation $*$. A is said to be a monoid if it satisfies the following properties.

(i) closure
(ii) Associative
(iii) Identity

Example : $(N, \cdot)$

Group : Let G be a non-empty set with binary operation $*$. G is said to be a group if it satisfies the following properties.

(i) Closure
(ii) Associative
(iii) Identity
(iv) Inverse

Note: we represent a group G & its binary operation $*$ as $(G, *)$.

Example : $(Z, +)$

Abelian group: A group $(G, *)$ is said to be abelian if it is commutative.

Example: $(\mathbb{Z}, +)$ is an abelian group.

$(\mathbb{Q} - \{0\}, \cdot)$ is an abelian group

Properties:

Theorem 1: In a group $(G, *)$, identity element is unique.

Proof: Let e_1 and e_2 be the 2 identity element of G.

As e_1 is an identity element and $e_2 \in G$

we have $e_2 * e_1 = e_1 * e_2 = e_2$ — (1) $a * e = e * a = a$

Also as e_2 is an identity element and $e_1 \in G$, then we have

$$e_1 * e_2 = e_2 * e_1 = e_1 \quad \text{— (2)}$$

From (1) & (2) $\Rightarrow$ $\underline{e_1 = e_2}$

Theorem 2: In a group $(G, *)$, inverse element is unique.

Proof: Let there are 2 inverses b and c of an element $a \in G$.

$$a * b = b * a = e \quad -(1)$$

$$a * c = c * a = e \quad -(2)$$

consider

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

$$= c * (a * b) \qquad \text{Associative}$$

$$= c * e$$

$$b = c \quad \Rightarrow \text{unique inverse}$$

Note: In a group $(G, *)$, $(a^{-1})^{-1} = a$ for all $a \in G$.