# Group Theory

Let $A$ be a non-empty set. A binary operation '$*$' on $A$ is a mapping from $A \times A \to A$.

i.e., $a * b \in A$ whenever $a, b \in A$

Eg: on $N$, define $a * b = a + b$, $a, b \in N$
'$+$' is a binary operation.

Eg: On $N$, define $a * b = a - b$, $a, b \in N$
'$-$' is not a binary operation

Eg: On $Q$, $a * b = a/b$, $a, b \in Q$
'$/$' is not a binary operation

Eg: But if $a * b = a/b$, $a, b \in Q \setminus \{0\}$
'$/$' is a binary operation.

Let $A$ be a non-empty set. If '$*$' is a binary operation on $A$, then we can say that,

(i) '$*$' is closure if $a * b \in A$, $\forall\, a, b \in A$

ii) '$*$' is associative if $a * (b * c) = (a * b) * c$, $\forall a, b, c \in A$

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

iv) For given $a \in A$, an element $b \in A$ is said to be inverse of '$a$' w.r.to '$*$' if
$a * b = b * a = e$, '$e$' identity element.

v) '$*$' is Commutative if $a * b = b * a$, $\forall a, b \in A$

**Semigroup**: Let A be a nonempty set with binary operation '$*$'.

$(A, *)$ is said to be a Semigroup if it satisfy the following properties:

(i) closure
ii) Associative

Eg: $(N, +)$, $(N, \cdot)$, $(Q, \cdot)$

**Monoid**: $(A, *)$ is said to be monoid if it satisfy the following properties;

(i) closure
ii) Associative
iii) identity

Eg: $(N, \cdot)$

**Group**: $(A, *)$ is said to be a group, if it satisfy the following properties;

(i) closure
ii) Associative
iii) identity
iv) inverse

Eg: $(Z, +)$ is a group

$(Z, \cdot)$ is not a group, because inverse does'nt exist.

Eg: Show that cube root of unity form a group under multiplication.

| $\cdot$ | 1 | $w$ | $w^2$ |
|---|---|---|---|
| 1 | 1 | $w$ | $w^2$ |
| $w$ | $w$ | $w^2$ | 1 |
| $w^2$ | $w^2$ | 1 | $w$ |

— closure & associative axioms satisfy
— identity element is '1'
— $w$ is inverse of $w^2$
Hence it forms a group.

**Abelian group**: $(A, *)$ is said to be an abelian group, if the following axioms are satisfied;

i) Closure
ii) Associative
iii) identity
iv) inverse
v) Commutative.

Eg: $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$

**Properties of a group:**

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

**Proof:** Let $e_1$ and $e_2$ be the two identity elements of $G$

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

$$e_1 * e_2 = e_2 * e_1 = e_2$$

$a, b, e$

$a * e = e * a = a$

$(\mathbb{Z}, +)$

$3 \in \mathbb{Z}$

$3 + (0) = 3$

ide

lly $e_2$ is an ~~et~~ identity elt, and $e_1 \in G$

$$e_1 * e_2 = e_2 * e_1 = e_1$$

$\Rightarrow e_1 = e_2$, identity elt in a group is unique.