Algebra-I
BA/B.Sc (NM) - III (Sem V)

Group (Definition) : Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $\langle G, * \rangle$ is called a group if it satisfies the following axioms

(i) $a * b \in G \quad \forall a, b \in G$ (Closure law)

(ii) $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$ (Associative property)

(iii) $\exists$ an element $e \in G$ such that

$$e * a = a * e = a \quad \forall a \in G.$$

then e is known as identity element of G w.r.t. the operation $*$.

(iv) For all $a \in G$, $\exists\, b \in G$ such that

$$a * b = b * a = e.$$

then b is called the inverse of a and is denoted by a^{-1}.

Note 1. If the operation $*$ is denoted by '$+$', the group is denoted by $\langle G, + \rangle$.

2. If the operation $*$ is denoted by '$\cdot$', the group is denoted by $\langle G, \cdot \rangle$.

Finite and Infinite Groups: If the set G is a finite, then it is called a finite group otherwise it is called an infinite group.

Order of a group: The order of a finite group $\langle G, * \rangle$ is defined as the number of distinct elements in G. It is denoted by $O(G)$ or $|G|$. If a group G has n elements, then $O(G) = n$.

The order of an infinite group is not defined or we say that the order is infinite.

Abelian and Non-abelian groups: A group $(G, *)$ is called an abelian group or Commutative group iff $a * b = b * a \quad \forall a, b \in G$.

If $a * b \neq b * a$, $\forall a, b \in G$, then the group $(G, *)$ is called a non-abelian group.

Semi-group: Let G be a non-empty set together with a binary operation $*$ defined on it such that

(i) $a * b \in G \quad \forall a, b \in G$

(ii) $(a * b) * c = a * (b * c) \quad \forall a, b, c \in G$

then G is called a semigroup.

Monoid: let $(G, *)$ be a semigroup such that $\exists$ an element $e \in G$ such that

$$a * e = a = e * a \quad \forall a \in G$$

then G is called a Monoid.

Examples

1.) Consider $\mathbb{N}$ = set of natural numbers under the binary operation '+'. then

(i) $a + b \in \mathbb{N} \quad \forall a, b \in \mathbb{N}$

$\therefore$ Closure property holds.

(ii) $(a+b) + c = a + (b+c) \quad \forall a, b, c \in \mathbb{N}$

$\therefore$ Associative property holds.

Hence $(\mathbb{N}, +)$ is a semigroup.

Note: $\nexists$ any element $e \in \mathbb{N}$ such that

$$a + e = a = e + a \quad \forall a \in \mathbb{N}.$$

and hence is not a group.

$\therefore$ $(\mathbb{N}, +)$ is not a monoid under the binary operation '+'.

2.) Consider $\mathbb{Z}$ = set of integers under the binary operation '+'.

Then

(i) $a + b \in \mathbb{Z} \quad \forall a, b \in \mathbb{Z}$.

(ii) $(a+b)+c = a+(b+c) \quad \forall a, b, c \in \mathbb{Z}$.

(iii) $\exists$ $0 \in \mathbb{Z}$ such that $a + 0 = a = 0 + a \quad \forall a \in \mathbb{Z}$.

(iv) For an element $a \in \mathbb{Z}$, there exist $-a \in \mathbb{Z}$ such that

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

Therefore, it satisfies all the properties of a group.

Hence ~~G,~~ $(\mathbb{Z}, +)$ is a group.

3.) $(\mathbb{Z}, \cdot)$ is a monoid but not a group.

Solution: (i) $a \cdot b \in \mathbb{Z} \quad \forall a, b \in \mathbb{Z}$

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in \mathbb{Z}$

(iii) $\exists$ an element $1 \in \mathbb{Z}$ such that

$$a \cdot 1 = 1 \cdot a = a.$$

For an element $a \in \mathbb{Z}$, $\nexists$ $\frac{1}{a} \in \mathbb{Z}$ such that

$$a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$$

Hence $(\mathbb{Z}, \cdot)$ is a monoid but not a group.

4. $(\mathbb{R}, +)$ is a group, where $\mathbb{R}$ = set of real numbers.

Solution: (i) $a+b \in \mathbb{R}$ $\forall a, b \in \mathbb{R}$

(ii) $(a+b)+c = a+(b+c)$ $\forall a, b, c \in \mathbb{R}$

(iii) $\exists$ an element $0 \in \mathbb{R}$ such that $a+0 = 0+a = a$.

(iv) For any element $a \in \mathbb{R}$, $\exists$ $(-a) \in \mathbb{R}$ such that

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

Therefore, it satisfies all the properties of a group.

Hence $(\mathbb{R}, +)$ is a group

5. $(\mathbb{R}, \cdot)$ is not a group under multiplication.

Solution: (i) $a \cdot b \in \mathbb{R}$ $\forall a, b \in \mathbb{R}$

(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall a, b, c \in \mathbb{R}$

(iii) $\exists$ an element $1 \in \mathbb{R}$ such that

$$a \cdot 1 = a = 1 \cdot a \quad \forall a \in \mathbb{R}.$$

$\therefore$ 1 is identity element of $(\mathbb{R}, \cdot)$.

(iv) For an element $a \neq 0 \in \mathbb{R}$, there exist $\frac{1}{a} \in \mathbb{R}$

such $a \cdot \frac{1}{a} = 1 = \frac{1}{a} \cdot a$.

$\Rightarrow$ $\forall a \neq 0 \in \mathbb{R}$, a has an inverse element $\frac{1}{a}$:

But there does not exist inverse of '0'.

Hence $(\mathbb{R}, \cdot)$ is a monoid but not a group.

Here we can note that in $(\mathbb{R}, \cdot)$, only '0' element does not have inverse. But there exist inverse of every element $a \neq 0 \in \mathbb{R}$. Hence $(\mathbb{R}, \cdot)$ to make a group, we can exclude $\{0\}$ from it. Let $\mathbb{R}^* = \mathbb{R} - \{0\}$ = set of non-zero real numbers.

Hence it can be easily checked that $(\mathbb{R}^*, \cdot)$ is a group.

6.) Show that the set $G = \{1, \omega, \omega^2\}$ of cube roots of unity forms a finite abelian group of order 3 under multiplication of complex numbers.