Unit - I

Advanced Abstract Algebra - I

Group: Suppose G be a non-empty set and $*$ be a binary operation then the algebraic structure $(G, *)$ is said to be a group if it satisfies the following conditions:

G1 - Closure: If $a, b \in G$ then $a * b \in G$.

G2 - Associative: For all $a, b, c \in G$, we have

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

G3 - Existence of identity: For all $a \in G$, there exists an element $e \in G$ such that

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

G4 - Existence of inverse: $\forall a \in G$ $\exists$ an element $a^{-1} \in G$ such that

$$a * a^{-1} = e = a^{-1} * a.$$

Abelian group: A group G is said to be abelian (or commutative) if it obeys the following:

G5 - $\forall a, b \in G$, we have

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

Definitions: Suppose A and B be the two sets. A relation from A to B is called a mapping (or a map or a function) from A to B if for each element x in A there is exactly one element y in B (called the image of x under f) such that x is in relation f to y.

If f is a mapping from A to B, we write

$$f : A \rightarrow B \quad \text{or} \quad A \xrightarrow{f} B.$$

Here A and B are respectively called the domain and codomain of the mapping f.

Suppose $x \in A$. If y is the image of x under f, we write $f(x) = y$ and we say f takes x to y, in symbols,

$$x \overset{f}{\longmapsto} y$$

or simply

$$x \longmapsto y.$$

Again, if $f(x) = y$, then x is called the preimage of y.

Composite mapping: Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$ be mappings. Then the mapping $h : A \rightarrow C$ given by

$$h(x) = g(f(x)) \text{ for all } x \in A$$ is called the composite of f followed by g and is denoted by $g \circ f$ (or gf). Thus,

$$g \circ f(x) = g(f(x)), \ \forall x \in A.$$

The mappings f and g are called factors of the composite.

One-one mapping (or 1-1 or injective):

A mapping $f: A \to B$ is called injective if for all $x_1, x_2 \in A$,

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

or equivalently, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Onto (or surjective): A mapping $f: A \to B$ is called surjective if for every $y \in B$, we have

$$y = f(x) \text{ for some } x \in A.$$

Bijective mapping: A mapping that is injective and surjective is said to be bijective.

If $f: A \to B$ is a bijective mapping, we may write

$$f: A \simeq B.$$

Note:

1. An injective mapping is also called injection.
2. A surjective mapping is also called surjection.
3. A bijective mapping is also called bijection or one-to-one correspondence.

Identity mapping:

A mapping $f: X \to X$ such that $f(x) = x \ \forall x \in X$ is called the identity mapping on X and is denoted by i_X or I_X.

Homomorphism: Suppose G and H be two groups. A mapping $\phi: G \to H$ is called a homomorphism (if ϕ preserves group operation) if for all $x, y \in G$,

$$\phi(xy) = \phi(x) . \phi(y).$$

Furthermore, if ϕ is bijective, then ϕ is called an isomorphism of G onto H and we write $G \simeq H$.

Special cases of isomorphism :-

1. If ϕ is just injective, i.e. 1-1, then ϕ is a monomorphism of G into H.
2. If ϕ is surjective, i.e. onto, then ϕ is called an epimorphism.
3. A homomorphism of G into itself is called an endomorphism of G.
4. An endomorphism of G that is both 1-1 and onto is called an automorphism of G.

OR

An isomorphism of a group G onto itself is called an automorphism.

OR

A mapping $\phi : G \to G$ is said to be automorphism if ϕ is 1-1, onto and homomorphism.