

Abstract Algebra

①

GROUPS

Let G be a non-empty set and $*$ be a binary operation defined on it, then the structure $(G, *)$ is said to be a group if the following axioms are satisfied:

(i) Closure property,

$$a * b \in G, \forall a, b \in G$$

(ii) Associativity

The operation $*$ is associative on G , i.e.

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

(iii) Existence of identity

There exists an element $e \in G$ such that

The element b is called the inverse

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

e is called identity of $*$ in G .

(iv) Existence of inverse

For each element $a \in G$, there exist an element $b \in G$ such that $a * b = b * a = e$. The element b is called the inverse of element a with respect to $*$ and we write

$$b = a^{-1}$$

Remarks

① When we say $*$ is a binary operation defined on a non-empty set G , it implies that G is closed for the binary operation $*$, i.e.

$$a \in G, b \in G \Rightarrow a * b \in G \quad \forall a, b \in G$$

② A group is not simply a set, but it is an algebraic structure.

③ Because of the associativity, the parenthesis can be dropped in products of more than two elements of a group and instead of writing $a * (b * c)$ or $(a * b) * c$ we may simply write $a * b * c$. The associative law can be extended to any finite number of elements.

Definition 2: - Group

A nonempty set of elements G is said to form a group if in G there is defined a binary operation, called the product and denoted by \cdot , such that

(i) $a, b \in G$ implies that $a \cdot b \in G$ (closed)

(ii) $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
(associative law)

(iii) There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$
(the existence of an identity element in G)

(iv) For every $a \in G$ there exists an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$
(the existence of inverse in G)

ABELIAN OR COMMUTATIVE GROUP

(G, \times) is said to be abelian or commutative group if $a \times b = b \times a, \forall a, b \in G$. The group which are not abelian are called non-abelian or non-commutative.

FINITE AND INFINITE GROUPS

group contains a finite number of elements, it is called a finite group. If the number of elements in a group is infinite, it is called an infinite group.

ORDER OF A GROUP

The number of elements in a finite group is called the order of the group. It is denoted by $O(G)$.

An infinite group is called a group of infinite order.

EXAMPLES OF GROUPS

- (i) The set \mathbb{Z} of integers is an infinite abelian group with respect to the operation of addition but \mathbb{Z} is not a group with respect to the multiplication.
- (ii) Let $G = \{1\}$, then G is an abelian group of order 1 with respect to multiplication.
- (iii) Let $G = \{0\}$, then G is an abelian group of order 1 with respect to addition.
- (iv) Let $G = \{1, -1\}$, then G is an abelian group of order 2 with respect to multiplication.