Group Theory

April 24, 2022

Definition 1 (Binary Operation) $* : A \to A$

Definition 2 *A non-empty set S w.r.t binary operation $*$ is called an algebraic structures. E.g, $S = \{1, -1\}$ is a structure under $\times$.*

Definition 3 *Let $(G, *)$ be an algebraic structures with binary operation $*$ then G is called a group if it satisfy the following properties :*

- *Closure property i.e, $\forall a, b \in G \; a * b \in G$*
- *There exist an identity element e s.t $a * e = e * a = a \; \forall a \in G$*
- *Every element $a \in G$ has an inverse $a^{-1} \in G$ s.t $a * a^{-1} = e$*
- *$*$ is Associative i.e, $\forall a, b, c \in G \; (a * b) * c = a * (b * c)$*

Example 1 *$(M_{m\times n}(\mathbb{R}), +)$ is a group.*

Example 2 *$G = \{M_{n\times n}(\mathbb{R}) | det(M) \neq 0\}$ is a non-singular matrix, $(G, \times)$ is a group.*

Definition 4 *A group is G is called Commutative or Abelian Group if it has commutative property i.e, $\forall a, b \in G \; a * b = b * a$*

Definition 5 *$(G, *)$ is a semigroup if it has - closure and Associativity.*

Definition 6 *$(G, *)$ is a monoid if it has - closure, Associativity and Identity element.*

Definition 7 *Let $(S, *)$ be a structure in which S is non-empty set and $*$ is a binary operation define on S. Such structure is called groupoid.*

Definition 8 *A group G is called a finite group if the no. of elements in G is finite.*

Definition 9 *The no. of elements in a group (finite or infinite) is called is called its order, denoted as $o(G)$ or $|G|$*

Example 3 *$G = \{1, -1, i, -i\} \implies o(G) = 4$*

Definition 10 *The order of an element $a \in G$ is the smallest $n \in \mathbb{Z}^+$ s.t $a^n = e$, if $a^n \neq e$ then a has infinite orders, denoted as $o(a) = n$ or $|a| = n$. For $+$ opereration $na = 0$.*

Example 4 *$G = \{1, -1, i, -i\}$ for $i \in G \implies o(i) = 4 \impliedby i^4 = (i^2)^2 = (-1)^2 = 1$*

Theorem 1 (Cancellation Law) *Let G be a group and $a, b, c \in G$ such that $a * b = a * c \implies b = c$*

Corollary 1 *A group G has a unique identity element.*

Corollary 2 *Any element of G has a unique inverse.*

Theorem 2 *If $a \in G$ then $(a^{-1})^{-1} = a$ and if $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$*

Definition 11 (Subgroup) *Let $(G, *)$ be a group and if $H \subseteq G$ then H is a subgroup of G if $(H, *)$ is a group.*

Example 5 *$2\mathbb{Z}$ is subgroup of $(\mathbb{Z}, +) \implies n\mathbb{Z} \subseteq \mathbb{Z}$*

Definition 12 *$g \in G$ is a generator of a group G if $G = \{g^n | n \in \mathbb{Z}\}$*

Example 6 *$1 \in \mathbb{Z}$ is a generator of $(\mathbb{Z}, +)$*

Definition 13 *A group G is finitely generated if $\exists\ g_1, g_2, \ldots g_k \in G$ s.t every element of G can be written as $g_1^{\alpha_1} \ldots g_k^{\alpha_k} \in G$ and $\alpha_1, \ldots \alpha_k \in \mathbb{Z}$*

Example 7

- $(\mathbb{Z}, +)$
- $G = \{\frac{a}{b} | a, b$ consist of prime $\leq r\}$ is finitely generated.