Group Theory

May 1, 2022

1 Groups, Semigroups, Monoids and Groupoid

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

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

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

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

Definition. *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. *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. *A group G has a unique identity element.*

Corollary. *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 $(ab)^{-1} = b^{-1}a^{-1}$*

2 Subgroups, Cosets and Normal Subgroup

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

Definition. *The trivial subgroup of any group is the subgroup $\{e\}$ consisting of just the identity element.*

Definition. *A proper subgroup of a group G is a subgroup H which is a proper subset of G i.e, $H \neq G$. Denoted as $H < G$*

Definition. *If H is a subgroup of G, then G is sometimes called an overgroup of H.*

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

Definition. *Let $(G, *)$ be a group and $H < G$, and $g \in G$ then -*

- *The left coset of H by g is $gH = \{gh | h \in H\}$*
- *The right coset of H by g is $Hg = \{hg | h \in H\}$*

Lemma. *Each coset of a subgroup H has the same size as H i.e, $|gH| = |H| = |Hg|$*

Remark. *Coset divides the finite group G in equals parts that is $G = H \cup g_1H \cup \cdots \cup g_kH$. Therefore,*

$$\begin{aligned} |G| &= |eH| + |gH| + \cdots + |g_kH| \\ &= k|H| \end{aligned}$$

Definition. *The no. of cosets (left or right) of H in G is called the index of H in G. Denoted as $[G : H]$. Therefore, we have a counting formula as*

$$|G| = [G : H] \times |H|$$

Remark. *The above serve as a proof of Lagrange's Theorem*

Theorem 3 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leq G$ then $o(H)|o(G)$*

Lemma. *The identity element and inverse of a subgroup is same as that of group.*

Theorem 4 (Two step subgroup test)**.** *Let $H \subseteq G$, H is a subgroup of G iff -*

- *$a \in H, b \in H \implies a * b \in H$*
- *$a \in H \implies a * a^{-1} \in H$*

Definition. *Let $H \leq G$ then using H we can form the cosets as $H, gH, g_2H \ldots$ if all these cosets form a group when $g^{-1}Hg \in H$ for any $g \in G$ then H is called the normal subgroup. Denoted as $H \trianglelefteq G$.*

Definition. *The cosets group is called a Factor or Quotient Group. Denoted as G/H*

Definition. *If the only normal subgroups of G are G and $\{e\}$ then G is called a simple group.*

Theorem 5. *Every subgroup of Abelian group is a normal subgroup*

Proof. Let $g \in G$ and $h \in H$ then

$$\begin{aligned} g^{-1}hg &= g^{-1}(gh) && \text{Since, } G \text{ is commutative} \\ &= (g^{-1}g)h \\ &= eh \implies h \in H \end{aligned}$$

□

Corollary. *Every subgroup of a cyclic group is also a normal subgroup*

3 Cyclic Group

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

Example 7.

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

4 Commutative Group

Definition (Partition of Integers)**.** *A multiset of positive integers that add to n is called a partition of n. The no.of partitions of k is denoted as $p(k)$.*

Example 8. *$p(3) = 3 \iff \{3, 1+2, 1+1+1\}$ ($1+2$ is same as $2+1$)*

Theorem 6 (Fundamental Theorem of Finite Abelian Group)**.** *The no. of Abelian groups of order n is the product of no. of partitions of n_i, where n_i is obtained from the prime factorization of n*

$$n = p_1^{n_1}.p_2^{n_2} \dots p_k^{n_k}$$

5 Homomorphism and Isomorphism