Group Theory

May 2, 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 ×.

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 $G = H \cup g_1 H \cup \cdots \cup g_k H$. Therefore,*

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

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 Homomorphism and Isomorphism

Definition. Let $(G, *)$ and $(H, \bullet)$ be a two group such that $f : G \to H$ is a homomorphism if $\forall a, b \in G$

$$f(a * b) = f(a) \bullet f(b)$$

Remark. *Homomorphism means same shape that is if G is homomorphic to H that means G and H has similar structure.*

Theorem 6. *Let $f : G \to H$ be a group homomorphism and e_G and e_H be the identities of respective group then $f(e_G) = e_H$.*

Proof. Let $g \in G$ then,

$$\begin{aligned} g * e_G &= g \\ f(g * e_G) &= f(g) \\ f(g) \bullet f(e_G) &= f(g) \\ h \bullet f(e_G) &= h \\ h^{-1} \bullet h \bullet f(e_G) &= h^{-1}h \implies f(e_G) = e_H \end{aligned}$$

□

Theorem 7. *Let $f : G \to H$ be a group homomorphism and let g^{-1} be the inverse of $g \in G$ and h^{-1} for $h \in H$ then $f(g^{-1}) = h^{-1}$*

Proof. Let $g \in G$ then,

$$\begin{aligned} g * g^{-1} &= e_G \\ f(g * g^{-1}) &= f(e_G) \\ f(g) \bullet f(g^{-1}) &= e_H \\ h \bullet f(g^{-1}) &= e_H \\ h^{-1} \bullet h \bullet f(g^{-1}) &= e_H \bullet h^{-1} \\ f(g^{-1}) &= h^{-1} \end{aligned}$$

□

Definition. Let $f : G \to H$ be a group homomorphism then the kernal of f,

$$ker(f) = \{g \in G \mid f(g) = e_H\}$$

Definition. If $f : G \to H$ is bijective then it is *isomorphism.*. Written as $G \cong H$

Example 6. $\mathbb{Z} \cong \mathbb{Z}_2$

Lemma. If $f : G \to H$ is isomorphism then $f^{-1} : H \to G$ is also an isomorphism

Lemma. If $G \cong H$ then G is commutative iff H is commutative

Corollary. If $G \cong H$ then G is cyclic iff H is cyclic

Lemma. $H \cong (\mathbb{Z}, +)$ where $H = \{\ 2^n \mid n \in \mathbb{Z}\}$

Proof. Define $f(n) = 2^n$ then $f(a + b) = 2^{a+b} \implies 2^a * 2^b = f(a) * f(b)$ □

4 Cyclic Group

Definition. Let G be a group, $a \in G$ if all the elements of G are in the form $a^n \in G$ for some $n \in \mathbb{Z}$ (*that is,* $G = \{a^n \mid n \in \mathbb{Z}\}$) then G is called a *cyclic group.* $a \in G$ is a generator of a group G. Denoted as

$$G =< a >= \{\dots a^{-2}, a^{-1}, e, a^1, a^2 \dots\}$$

Example 7. $1 \in \mathbb{Z}$ *is a generator of* $(\mathbb{Z}, +)$

Lemma. If a is the generator of G then a^{-1} is also a generator.

Lemma. Every cyclic group is Abelian.

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 8.

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

5 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 9. $p(3) = 3 \impliedby \{3, 1+2, 1+1+1\}$ *(*$1+2$ *is same as* $2+1$*)*

Theorem 8 (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*

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