Abstract Algebra
Summer of Science

Swayam Chube
Mentor: Shourya Pandey

July 19, 2021

Introduction

In this brief presentation I shall focus mainly on **Group Theory** and some powerful results related to it.
Topics which I hope to cover are:

- Cosets and Lagrange's Theorem
- Orbit-Stabilizer Theorem
- Cauchy's Theorem
- Fundamental Theorem of Finite Abelian Groups

I would have liked to include the three Sylow Theorems but that would inflate the running time of the presentation to more than 15 minutes.

Definition of a Group

Definition (Binary Operation)

Let G be a set. A binary operation on G is simply a function $\star\colon G \times G \to G$.

Definition (Group)

Let G be a set and $\star$ be a binary operation defined on G. Then the ordered pair $(G, \star)$ is said to be a *group* if

1. $\forall\ a, b, c \in G,\ a \star (b \star c) = (a \star b) \star c$. Associativity.
2. $\exists\ e \in G$ such that $\forall\ a \in G,\ a \star e = a = e \star a$. Existence of the Identity.
3. $\forall\ a \in G, \exists\ b \in G$ such that $a \star b = e = b \star a$. Existence of Inverses.

Henceforth, I shall abuse notation and use the phrase "G is a group" to refer to "$(G, \star)$ is a group" and ab to refer to $a \star b$.

Properties of Groups

Theorem

Let G be a group. Then,

- *The identity element is unique.*
- *Left and Right cancallation laws hold true. That is, $ab = ac \implies b = c$ and $ba = ca \implies b = c$.*
- *$\forall\ a \in G$, the inverse a^{-1} is unique.*
- *$\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$*

Orders and Subgroups

Definition (Order of a Group)

The *order* of a group is equal to the number of elements in it. We use $|G|$ to denote the order of a group G.

Definition (Order of an Element)

The order of an element g in a group G is equal to the smallest positive integer n (if it exists) such that $g^n = e$. If no such n exists, g is said to have infinite order. The order of an element g is denoted by $|g|$.

Definition (Subgroup)

$H \subseteq G$ is said to be a subgroup of G if $(H, \star)$ is a group.

More Definitions and a Theorem

Definition (Center of the Group)

Let G be a group. The *center* $Z(G)$ is defined as follows

$$Z(G) = \{a \in G \mid ax = xa \quad \forall x \in G\}$$

Further, $Z(G)$ is a subgroup of G.

Definition

Let G be a group and $a \in G$. The *centralizer* of a in G, $C(a)$ is defined to be the set of all elements in G that commute with a. For all $a \in G$, $C(a)$ is a subgroup of G.

Theorem

The order of each element in a finite group is finite.

Cyclic Groups

Definition

Let G be a group. G is said to be cyclic if there exists $a \in G$ such that

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Theorem (Fundamental Theorem of Cyclic Groups)

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$

Cosets

Definition

Let G be a group and let H be a non-empty subset of G. For any $a \in G$, denote the set $\{ah \mid h \in H\}$ by aH and similarly denote the set $\{ha \mid h \in H\}$ by Ha and the set $\{aha^{-1} \mid h \in H\}$ by aha^{-1}. When H is a subgroup of G, the set aH is called the left coset of H in G containing a and Ha is called the right coset of H in G containing a. a is then called the coset representative of aH or Ha. We use $|aH|$ or $|Ha|$ to denote the number of elements in aH or Ha respectively.

Properties of Cosets

Theorem

Let H be a subgroup of G and let $a, b \in G$. Then,

- $aH = H$ *if and only if* $a \in H$
- $aH = bH$ *if and only if* $a \in bH$
- *Either* $aH = bH$ *or* $aH \cap bH = \emptyset$
- $|aH| = |bH|$

Lagrange's Theorem

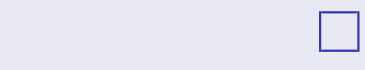
Theorem (Lagrange, 1770)

If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Furthermore, the number of distinct cosets(left or right) of H in G is $|G|/|H|$.

Proof.

Let $a_1H, a_2H, \cdots, a_nH$ denote the distinct left cosets of H in G. Due to the previous theorem, we know that all the above cosets must be disjoint and must have equal number of elements. Furthermore, every element must be a member of exactly one left coset.

$$n|H| = \sum_{i=1}^{n} |a_iH| = |G|$$



Permutation Groups

Definition (Permutation Group)

A permutation of a set A is a bijective function $\sigma : A \to A$. A *permutation group* of a set A is a set of all permutations of A, which form a group under the binary operation of composition.

Orbits and Stabilizers

Definition (Stabilizer of an element)

Let G be a group of permutations of a set S. For each $i \in S$, let

$$\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$$

be the *stabilizer* of i in G.

Definition

Let G be a group of permutations of a set S. For each $i \in S$, let

$$\text{orb}_G(i) = \{\phi(i) \mid \phi \in G\}$$

be the orbit of i under G. We use $|\text{orb}_G(i)|$ to denote the number of elements in $\text{orb}_G(i)$.

Guess what comes next...

Orbit-Stabilizer Theorem

Theorem

Let G be a finite group of permuattions of a set S. Then, for any $i \in S$,

$$|G| = |\operatorname{orb}_G(i)||\operatorname{stab}_G(i)|$$

Proof.

Consider the mapping $\Phi : G \to S$ which maps $\phi \operatorname{stab}_G(i) \mapsto \phi(i)$. Show now that Φ is a well defined bijection. This would then imply that the number of distinct left cosets of $\operatorname{stab}_G(i)$ in G is equal to $|\Phi(G)|$ which is nothing but $|\operatorname{orb}_G(i)|$. $\square$

Normal Subgroup and Factor Group

Definition (Normal Subgroup)

A subgroup H of a group G is said to be *normal* if $aH = Ha$ for all $a \in G$. We denote this by $H \lhd G$.

Theorem

Let G be a group and let H be a normal subgroup of G. The set

$$G/H = \{aH \mid a \in G\}$$

is a group under the operation $(aH)(bH) = (ab)H$. This group is called a Factor Group or Quotient Group.

Cauchy's Theorem

Theorem

Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.

Proof.

The proof is by induction on $|G|$. If the order of an element x is equal to n which is not prime, then simply take x^{n/p_i} where p_i is a prime dividing n and that would have prime order. Now let $g \in G$ have prime order q. If $q \neq p$, take the group $\overline{G} = G/\langle g \rangle$. Now since p divides $|\overline{G}|$, show that there exists $h\langle g \rangle$ of order p. Then, we would have $h^p\langle g \rangle = \langle x \rangle$ or $h^p \in \langle g \rangle$. If $h^p \neq e$, then y^p has order r and h^r has order p. □

Direct Products

Definition (External Direct Product)

Let $G_1, G_2, \cdots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \cdots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is the set of all n-tuples for which the i-th component is an element of G_i and the operation is componentwise.

Definition (Internal Direct Product)

We say that G is the *internal direct product* of H and K and write $G = H \times K$ if H and K are normal subgroups of G and

$$G = HK = \{hk \mid h \in H,\ k \in K\} \qquad \text{and} \qquad H \cap K = \{e\}$$

Fundamental Theorem of Finite Abelian Groups

Theorem (Fundamental Theorem of Finite Abelian Groups)

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

The proof of the above theorem requires four lemmas. I shall not go over their proofs but I will show how they come together to prove the Fundamental Theorem of Finite Abelian Groups.

The First Two

Lemma

Let G be a finite Abelian group of order $p^n m$ where p is a prime that doesn't divide m. Then $G = H \times K$ where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$.

Lemma

Let G be an Abelian group of prime power order and let a be an element of maximum order in G. Then G can be written int the form $\langle a \rangle \times K$.

The Last Two

Lemma

A finite Abelian gorup of prime power order is an internal direct product of cyclic groups.

Lemma

Suppose that G is a finite Abelian group of prime power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H and K are nontrivial cyclic subgroups with monotonically decreasing orders, then $m = n$ and $|H_i| = |K_i|$ for all i.

Putting It All Together

Let G be a finite Abelian group of order $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Then, from Lemma 1, we can write G as an internal product of $G(p_1) \times G(p_2) \times \cdots \times G(p_k)$. Where $G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$. But, from Lemma 3, we have that each of these $G(p_i)$ is an internal direct product of cyclic groups. And uniqueness is now guaranteed by Lemma 4. This completes the proof. ■

Lemma 2 is used in the proof of Lemma 3.