Abstract Algebra Notes

Yusif Mehdiyev

February 2025

Contents

Part I

Group Theory

1 Introduction to Groups

When I started studying this subject, I though Abstract Algebra was a field about theoretical mathematics, which of course I was wrong.

Abstract Algebra, especially Groups, study the natural structure of life (or mathematical objects) in general (or in abstract) view. Symmetries, Permutations, Rotations are part of the study of the Group Theory and many scientists (and mathematicians obviously) such as modern Physicists and Chemists heavily use this subject. [1]

§1.1 Definition of Groups

Group Theory is fairly new subject and through the history had subject to evolutionary process. Naturally it had many different definitions and properties depending on these definitions. The modern definition is as follows,

Definition. Let G be a set. A **Binary Operation** on G is a function that inputs a pair of elements in G to another element of G.

Example 1.1.1
Addition and Multiplication are Binary Operations in $\mathbb{Z}$.

Definition. A **Group** $(G, *)$ is a set with a binary operation on G that satisfies

1. Closure: $\forall x, y \in G$, $x * y \in G$.
2. Associativity
3. Identity (neutral): $\exists e \in G$ such that $x * e = x \ \forall x \in G$.
4. Inverse: $\forall x \in G$, $\exists x^{-1} \in G$ such that $x * x^{-1} = e$.

Example 1.1.2
There are several Groups we are already familiar with: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are all groups under addition. The identity element is 0 and the inverses are simply $-a$ $\forall a \in G$.

Example 1.1.3
$(\mathbb{Q}^+, *)$ is a Group with identity 1. Clearly the inverse of $\frac{m}{n} \in G$ is $\frac{n}{m}$.

[1] This is what I understood from stuff I have read in the internet

Example 1.1.4

Addition of finite integers modulo n or $(\mathbb{Z}_n, +_{\mod n})$ is a group. We denote this as $\mathbb{Z}_n$. For the specific case $n = 5$, we have

$$\{0, 1, 2, 3, 4\} \in \mathbb{Z}_n$$

Identity element is 0. We also call specific groups like these **Cyclic Groups**. We will learn about them later.

Example 1.1.5

A set of rotations and reflections of n-gon where $n \geq 3$ is a group with composition as operation. We call this **Dihedral Group** and denote this group as D_n. For $n = 3$, D_n consists of rotating $0°, 120°, 240°$ and reflecting about three bisects. There are total 6 elements of D_3.

Example 1.1.6

The $n \times n$ **general linear group** is the group of all invertible $n \times n$ matrices under multiplication of matrices. Notation is,

$$GL_n = \{n \times n \text{ invertible matrices } A\}$$

This is true since identity matrix I is invertible and multiplication of matrices outputs another invertible matrix.

We also donate $GL_n(\mathbb{R})$ to show if whether we are working on Reals or Complex matrices.

Example 1.1.7

Set of **permutations** of a set T under operation composition is a group. Remember that permutations are bijective functions such that

$$f : T \to T$$

Composition of functions are associative (this is a very well known fact).

Another specific case of permutations, which show itself in the nature and mathematics very often:

Example 1.1.8

The set of permutations of indices $\{1, 2, \ldots, n\}$ with operation composition is a group. In short,

$$S_n \text{ is the group of permutations of } \{1, 2, \ldots, n\}$$

Then, the number of elements of the group, **the order** of S_n, denoted as $|S_n|$ is equal to $n!$. It turns out that S_n have many nice properties. We will study them further in next sections (for organization of notes).

Remark. General Linear Groups and Symmetric Groups are very important in Group Theory. This is mainly because these groups are often **subgroups** of other groups.

§1.2 Elementary Properties of Groups

Now we will list very elementary properties and theorems of the groups with proofs (of course).

Definition 1.2.1. The number of elements of a group G is called **order** of G and is notated as $|G|$. If the set is infinite, then $|G| = \infty$.

The order of an element $g \in G$ is also has means as the smallest positive integer n such that $g^n = e$. If no such n exists, then $|g| = \infty$.

Theorem 1.2.2

In the group G, identity is unique.

Proof. Suppose otherwise. If both e_1, e_2 are distinct identity elements, then

$$e_1 = e_1 * e_2 = e_2$$

Which is a clear contradiction. □

Group theory heavily studies the groups under binary operations $+$ and $\cdot$. In order to make notation more clear and easier, we use (for multiplication)

$$a \cdot b = ab, e = 1, a^n = aaa \dots a$$

and for addition,

$$a + b, e = 0, -a = a^{-1}, na = a + a + \dots + a$$

Usually groups with addition operations are **commutative**. Primary reason is mathematicians do not like seeing $a + b \neq b + a$. We also have a specific name for such groups

Definition. A Group is **abelian** if it is commutative.

Theorem 1.2.3

(Cancellation Law) in a group G, cancellation holds,

$$ba = ca \Rightarrow b = c \ \wedge \ ab = ac \Rightarrow b = c$$

Proof. Multiply by a^{-1} from right and left respectively. □

Theorem 1.2.4

In the group G, inverses are unique.

Proof. Suppose otherwise. If both b and c are inverses of a, then

$$a * b = a * c = e$$

Cancelling a gives $b^{-1} = c^{-1}$ □

Theorem 1.2.5

For all a, b elements of a group, [a]

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

[a] Notice how this theorem looks very familiar for Linear Algebra's inverse theorem. No surprise here, invertible matrices under multiplication is a group.

Proof. We have

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

□

§1.3 Subgroups, Additive Groups of Integers

Definition. If a set H is subset of a group G and is also a group, then we call H as **subgroup** of G, notated as $H \leq G$. If it is a proper subgroup (that is, if it is not a set consisting of only identity nor equal to G) we write $H < G$.

To check whether if H is subset of G, we have to check 3 properties excluding the associativity. This makes sense, since associativity is more of a property of the structure of operations we are working with.

Example

The set of all multiples of $a \in \mathbb{Z}$ under addition,

$$\mathbb{Z}a = \{n \in \mathbb{Z} \mid n = ka,\ k \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}^+$ under addition, or $\mathbb{Z}a \leq \mathbb{Z}^+$ [a]

[a] here $\mathbb{Z}^+$ means set of integers under operation addition, not positive integers

Proof. clearly $0 \in \mathbb{Z}a$. The inverse of $a \in \mathbb{Z}a$ would be simply $-a \in \mathbb{Z}a$. Lastly, it is closed since $ka + ta = a(k + t) \in \mathbb{Z}a$. □

Theorem 1.3.1

Let H be a subgroup of $\mathbb{Z}^+$. Then $H = \{0\}$ or $H = \mathbb{Z}a$ where a is the smallest positive integer in H.

Proof. The case when $H = \{0\}$. Is trivial. Assume non-zero element $a \in H$. Then $-a \in H$ or in other terms a smallest positive integer a must exist. Then, since H is a subgroup, $2a \in H, 3a \in H, \ldots, ka \in H$. Or in other terms

$$\mathbb{Z}a \leq H$$

Now, we will show that $H \leq \mathbb{Z}a$. If $n \in H$, it is clear that either $n \in \mathbb{Z}a$ or $n = qa + r$ for $0 < r \leq a - 1$. However, then $n - qa = r \in H$. Since a is the smallest integer, the condition

$$0 < r < a - 1 \wedge r \in H \wedge r \geq a$$

is impossible, hence contradiction, which means $r = 0$ is the only possible case, hence the result. □

This theorem has interesting consequences, one of them being this theorem:

Theorem 1.3.2

The set of the combinations of all integer combinations of $ra + sb$ of a and b is a subgroup of Z^+ under addition. In fact, if $d = \gcd(a, b)$, this group is $\mathbb{Z}d$. In short,

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b = \{n \in Z \mid ra + sb \text{ for some integers r, s}\}$$

We say $\mathbb{Z}d$ is **generated** by a and b, since it is the smallest group containing both a and b.

Corollary 1.3.3

A pair of integers a and b are relatively prime iff $\exists r, s$ such that

$$sa + rb = 1$$

In other words, iff $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$ then a, b are relatively prime.

Another useful subgroup is $\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b \leq \mathbb{Z}$. The variable m is in fact equal to $\text{lcm}(a, b)$.

Theorem 1.3.4

Let a, b be non-zero integers and let $m = \text{lcm}(a, b)$. Then,

$$\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$$

Corollary 1.3.5

Let a, b be integers. Then,

$$ab = \text{lcm}(a, b) \cdot \gcd(a, b)$$

2 Cyclic Groups

§2.1 Definition of Cyclic Groups

There are some special kind groups that can be constructed with only one element of the group. In other words,

Definition 2.1.1. A group G is called **cyclic** if there is a element $a \in G$ such that

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

We call this a the **generator** of G. There can be multiple generators for the same cyclic group G. We write $\langle a \rangle$ to notate this group of a. a^n may be distinct for all n or loop through like a circle (that is where name comes from).

Example 2.1.2

$\mathbb{Z}$ under addition is a cyclic group with generators 1 and -1. In fact, if a is a generator then also is a^{-1}.

Example 2.1.3

The set $\mathbb{Z}_n$ is a cyclic group. $\langle 1 \rangle$ and $\langle n-1 \rangle$ are generators. In fact, for any $\gcd(x, n) = 1$, $\langle x \rangle$ is true.

§2.2 Elementary Properties of Cyclic Groups

Theorem 2.2.1

All cyclic groups are abelian.

Proof. This is direct consequence of definition of powers. For any element in a cyclig group G, we can write them as a^s where a is a generator. Then,

$$a^s * a^t = a^{s+t} = a^{t+s} = a^t * a^s$$

□

Now we will study deeply about the properties of cyclic groups.

Theorem 2.2.2

Let $\langle a \rangle$ be a cyclic group G. Then,the powers $a^i = a^j$ for $i \geq j$ iff $n | i - j$

Proof. For $i = j$, this is clearly true. assume $i > j$. Then by division algorithm, we can write

$$i - j = qn + r$$

Where $n = |a|$. Then, for $a \in G$ we have,

$$a^{qn+r} = a^{qn} * a^r = (a^n)^q * a^r = a^r$$

We know that $a^r = e$ iff $r = 0$, hence we are done. Converse is trivial □

Recall the definition of the order of the element in G. We have a neat relationship,

Corollary 2.2.3

$\forall a \in G$, $|a| = |\langle a \rangle|$.

This actually directly comes from definitions.

Another trivial but useful corollary,

Corollary 2.2.4

$a^k = e$ only and only if $n|k$.

Proof. Using Theorem 2.1.5, we know $a^k = a^0$ iff $n|k - 0$. Hence we are done. □

Theorem 2.2.5

Let $|a| = n$ in a group (hence group is cyclic) and let k be a positive integer. Then, $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n, k)$

Proof. For the first statement, let $d = \gcd(n, k)$. Then $k = dk'$. However,

$$a^k = (a^d)^{k'} \in \langle a^d \rangle \Rightarrow \langle a^k \rangle \leq \langle a^d \rangle$$

In other direction, we know that we can write $d = ns + kt$. Then,

$$a^d = a^{ns+kt} = a^{ns}a^{kt} = a^{kt} = (a^k)^t \in \langle a^k \rangle \Rightarrow \langle a^d \rangle \leq \langle a^k \rangle$$

Hence $\langle a^k \rangle = \langle a^d \rangle$.

For second statement, we will use the fact that $(a^d)^{n/d} = e$ or $|a^d| = n/d$. Then using the first statement,

$$|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = |a^{\gcd(n,k)}| = n/\gcd(n, k)$$

□

3 Permutations

§3.1 Definition of Permutations

Definition. **Permutations** are functions from the set to itself that are also bijective.

Permutation group is set of composition of permutation functions. We use arrays to express the permutations. That is,

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \alpha(1) & \alpha(2) & \alpha(3) & ... & \alpha(n) \end{pmatrix}$$

Example 3.1.1

The permutations that shift everything to left by one can be written as

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

That is, $\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 4, \alpha(4) = 1$.

Composition of permutations are also simple. If γ and β are permutations, then is also $\gamma\beta$ and $\beta\gamma$.Note that permutation groups are **not necessarily abelian**.

Example 3.1.2

Symmetric group S_3 is set of permutations of $\{1, 2, 3\}$ under composition. Then,

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Other permutations are then

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad \alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \alpha^2\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Notice that there are two kinds of permutations: Rotation in cycle or Changing only between two elements (Transposition). The permutation of first kind is usually notated as ρ_i where i is the number of elents you rotate to the left. Meanwhile, second kind is notated as μ_i where i is the stationary element. Therefore,

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Then we can show all permutations with combinations of μ_2 and ρ_1

§3.2 Cycle Notation

Take ρ_2 in S_2. When we look at the elements, we see that

$$1 \to 3 \to 2 \to 1$$

Similarly for μ_1, we can again see that

$$1 \to 1; \quad 2 \to 3 \to 2$$

The idea is very simple, we can show any permutations in combinations of these cycles. ρ_2 itself is a cycle and we can donate it as $(1,3,2)$. μ_1 can be shown as $(1)(2,3)$.

Example 3.2.1

In S_7, there is a permutation $(2,5,4,3)(1,6)(7)$. It is equivalent to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 2 & 3 & 4 & 1 & 7 \end{pmatrix}$$

If there is an elementary cycle like (7) here, we do not write it. Then our permutation is just $(2,5,4,3)(1,6)$.

We can multiply the permutations using this notation. (We read it from right to left).

Example 3.2.2

$$\rho_2\mu_1 = (1,3,2)(2,3)$$

Notice that the cycles are not **disjoint**. This means that $2 \to 3 \to 2$. (we read it from right to left). Doing this for other elements, we see that

$$\rho_2\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \mu_2 = (1,3)$$

Theorem 3.2.3

Every permutation of a finite set can be written as multiplication of disjoint cycles.

Proof. We are permutating $A = \{1, 2, 3, \ldots, n\}$ with σ. Define

$$O_a = \{y = ga | g \in G\}$$

That is, this set (which is called **Orbit**) is basically the set of elements

$$a, \sigma(a), \sigma^2(a), \ldots, \sigma^{n-1}(a), \sigma^n(a) = a$$

This set is trivially finite since otherwise A would not be finite. Then notice that if $O_i \cap O_j \neq \emptyset$, $O_i = O_j$. Basically if there is an common elements residing in both orbits, then after permutating the element in each orbit for some m, n times, we will get the same element, hence the orbits are equal. The unique orbits are just our disjoint cycles!

We can also think orbits at everything that can be reached from x by an action of something in G. □

Theorem 3.2.4 (Commutativity of Disjoint Cycles)

Disjoint cycles are commutative.

Proof. Trivial, let α, β be disjoint cycles. Then $\forall a_i, b_i$ in these cycles respectively, we have

$$\alpha(\beta(a_i)) = \alpha(a_i) = a_j$$
$$\beta(\alpha(a_i)) \ = \beta(a_j) = a_j$$

Simply, β do not affect any a_i. □

Definition 3.2.5. We say that the permutation σ has **order of n** if $\sigma^n(a) = a$.

Theorem 3.2.6 (Order of a Permutation)

The order of disjoint cycles is equal to least commont multiple of length of cycles

Proof. For each disjoint cycle, we know that their order is their length (since they are just a cycle). If $a_1, a_2, \ldots, a_n$ are the orders of each these disjoint cycles, it is trivial that $\text{lcm}(a_1, \ldots, a_n)$ properly cycles through the each disjoint cycle. □

§3.3 2-cycles (Transpositions)

2-cycles are, as the name suggests, cycles with 2 elements. The examples are $(1, 2); (5, 9)(3, 7)$ or whatever you think. They are called **transpositions** since only two elements are moving while others are stationary. They are useful (we would not study them otherwise)

Theorem 3.3.1 (Permutations in transposition notation)

Any permutations can be written with transposition cycles

Proof. Every permutation can be written in multiplication of disjoint cycles. Let one disjoint cycle be $(a_1, \ldots, a_i)$. Then,

$$(a_1, \ldots, a_i) = (a_1, a_i) \ldots (a_1, a_3)(a_1, a_2)$$

We can do this for other disjoint cycles, hence we are done. □

§3.4 Parity of a Permutation

The integers can be logically divided into two distinc pairs of odd and even integers. Notice that an operation on two odd integers give even integer, in parallel an operation on odd and an even integer gives an odd integer. Following this, we can similarly divide the permutations into **odd and even** permutations.

Definition 3.4.1. Parity of Permutations A permutation σ's' parity is equal to the parity of the number of transposition compositions.

With this definition, the function sgn that sends each permutation to its sign, that is,

$$S_n \to \{-1, 1\}$$

is a homomorphism similar to parity of the integers.

Theorem 3.4.2

The set of even permutations A_n in S_n is a subgroup of S_n. Moreover,

$$|A_n| = \frac{n!}{2}$$

This is true because in a group, number of odd and even permutations are equal(except in trivial cases of course).

4 Cosets

We already know $\mathbb{Z}$ is a group under addition. The set of even numbers under addition is also a subgroup of $\mathbb{Z}$. However, we cannot say the same thing for the odd integers. But, the odd integers are just one shift of the even integers! We basically call such sets that look like groups but not as **cosets** of a group.

Definition 4.0.1. Let G be a group and H be a group such that $H \leq G$. Then, **left cosets** are defined as,

$$aH = \{ah | h \in H\}$$

Similarly, right cosets are defined with the set Ha etc. Number of Left cosets, **index** of a subgroup H in G is are shown as $|G : H|$.

To get the left cosets of a subgroup H, we just shift it witch each element $g \in G$.

We have already seen the examples of cosets through the mathematics. The points in a unit circle. We can also see that all the left (or right) cosets circle through the entiretiy of the group G. More precisely, their union gives G.

Theorem 4.0.2

Lagrange's Theorem If G is a finite group and H is a subgroup of G, Then $|H|$ divides G. In fact, number of left or right cosets are equal to the number $|G|/|H|$. That is,

$$|G : H| = \frac{|G|}{|H|}$$

Corollary 4.0.3

Groups of prime orders are cyclic

Proof. let a be an element of the group. Then $|\langle a \rangle| \mid |G|$. But $|G|$ is prime, hence $|\langle a \rangle| = |G| \Rightarrow$ G is cyclic. □

§4.1 Orbits and Stabilizers

Definition 4.1.1. Stabilizer The stabilizer of an element i in G are set of elements in G such that does not change i, that is it **stabilizes it** as name suggests. Basically the set of elemetns such that,

$$\sigma(i) = i$$

We write this set as $\text{stab}_G(i)$.

Definition 4.1.2. Orbit We have already talked about this, we usually notate it as $O_{G,i}$ or $\text{orb}_G(i)$.

Theorem 4.1.3

Orbit-Stabilizer Theorem Let G be a group in S_n. Then $\forall i \in G$,

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

§4.2 External Direct Products

This concept is similar to other direct products across the mathematics. For example, $\mathbb{Z}^2$ is set of 2-tuple integers (a, b). Similarly, for all the groups,

Definition 4.2.1. External Direct Products Let $\{G_i\}$ be collection of groups. **External Direct Products** of this collection written as

$$G_1 \oplus G_2 \oplus \ldots \oplus G_n = (g_1, g_2, \ldots, g_n) | G_i \in G_i$$

Example 4.2.2

$\mathbb{R}^2, \mathbb{R}^3$ and other $\mathbb{R}^n$ that we have studied in Linear Algebra, Calculus and Physics are examples.

The operations, our definitions of orbits, cycles etc are all component wise redefined.

§4.3 Normal Subgroups

A normal Subgroup H of a group G is a normal subgroup if left and right cosets are equal