Abstract Algebra Notes

Joseph 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 test