Abstract Algebra Notes

Joseph Mehdiyev

February 2025

Contents

Part I

Group Theory

1 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 Introduction to 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

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

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

$(\mathbb{Q}^+, *)$ 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

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

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.

§1.2 Elementary Properties of Groups

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

Theorem 1.2.1

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 1.2.2

(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. $\square$

Theorem 1.2.3

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 $b^{-1} = c^{-1}$ $\square$

Theorem 1.2.4

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

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

$\square$