Notes on Abstract Algebra

Harry Luo

Lecture notes from Math 541 Modern Algebra I, Fall 2025.

Rerference:

- Dummit and Foote, Abstract Algebra, 3rd edition
- lectures by prof. Mikhail Ivanov

Contents

Chapter 1 3
Chapter 2 4
Midterm 1 Cutoff 4
2.4 *Subgroup generated by subsets of a group* 4
2.5 *Lattice of subgroups of a Group* 5
Chapter 3 7
3.1 *Quotient Groups* 7
3.2 *Cosets and Lagrange Theorem* 9
3.3 9
3.5 9
Chapter 4 10
4.1 10
4.2 10
4.3 10
4.4 10
Chapter 5 11
5.1 11
5.2 11
Mitterm 2 Cutoff 11

Chapter 1

Chapter 2

Midterm 1 Cutoff

Midterm 2 coverage: 2.4, 2.5, 3.1, 3.2, 3.3, 3.5, 4.1, 4.2, 4.3, 4.4, 5.1, 5.2

2.4 *Subgroup generated by subsets of a group*

Given a group G and a subset $A \subset G$, we can construct the smallest subgroup of G that contains A. This is called the **subgroup generated by A**. It's analogous to the span of a set of vectors in linear algebra, where we look for the smallest subspace containing a given set of vectors.

There are two equivalent ways to define the subgroup generated by a subset A of a group G:

- **Top-down: an intersection of subgroups.**

  We can think of the subgroup generated by A as the smallest subgroup of G that contains A. *Smallest* implies taking an intersection of all subgroups containing A.

  We first need to verify that the intersection of subgroups is indeed a subgroup.

  > ***Proposition***
  >
  > Let $\mathcal{A}$ be a collection of subgroups of a group G. The intesection $\bigcap_{H \in \mathcal{A}} H$ is also a subgroup of G.
  >
  > **Proof:** Identity is in every subgroup,so it's in the intersection.
  >
  > If x, y in the intersection, then x, y are in every subgroup in $\mathcal{A}$. Since each subgroup is closed under the group operation, xy^{-1} is in every subgroup, hence in the intersection. □

  This proposition allows us to define the subgroup generated by A as an intersection of subgroups.

  > **Definition**
  >
  > Let G be a group and $A \subset G$ be a subset in G.The **subgroup generated by G** , denoted $\langle A \rangle$, is the intersection of all subgroups of G that contain A.
  >
  > $$\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subset H}} H. \tag{1}$$

todo: we can draw a venn diagram here.

- **Bottom-up: Words in Generators.**

  The first definition was clear but not constructive. We want to know what the elements of $\langle A \rangle$ actually look like. We can describe an equivalent subgroup using "words" formed from elements of A and their inverses.

  Notice that for a subgroup H to contain A, it must be closed under group operation and taking inverses. This means H must contain all elemenets in A, all their inverses, and all finite products of these elements. This leads to the following definition:

  > **Definition**
  >
  > The subgroup generated by a subset $A \subset G$, is the set of all finite products of elements of A and their inverses.
  >
  > $$\langle A \rangle = \{a_1^{e_1} a_2^{e_2} ... a_n^{e_n} \mid n \in \mathbb{Z}^+, a_i \in A, e_i = \pm 1\}. \tag{2}$$

These products $a_1^{\varepsilon_1}...a_n^{\varepsilon_n}$ are often called words in the genrators A.

After defining the subgroup generated by a subset A, we define a **Finitely generated group** as follows:

> **Definition**
>
> A group G is finitely generated if there exists a finite set A such that $G = \langle A \rangle$.

Example:
1. $D_{2n} = \langle r, s \rangle$
2. $Q_8 = \langle i, j \rangle$
3. S_n :
   - $S_1 = \{e\} = \langle e \rangle$,
   - $S_2 = \{e, (12)\} = \langle (12) \rangle$,
   - $S_n = \langle (1\ 2), (1\ 2...n) \rangle$
4. $$\mathrm{GL}_2(\mathbb{R}) = \langle \underbrace{\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)}_{\text{swap}}, \underbrace{\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)}_{\text{add}}, \underbrace{\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right)}_{\text{multiply}} \rangle \tag{3}$$

2.5 *Lattice of subgroups of a Group*

We can draw a lattice diagram to visualize the structure of a group by showing its subgroups and their inclusion relationships.

The key idea is to find subgroups **generated by small subsets** (starting with single elements, then pairs or small combinations),and then arrange them by order and inclusion to form the partial order.

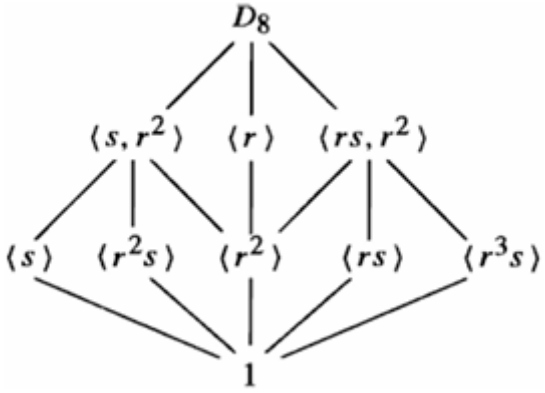
We will center this method around an example.

Consider D_8. Recalling the dihedral symmetry $sr^{-i} = r^i s$, we can write

$$\begin{aligned} D_9 &= \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle \\ &= \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}. \end{aligned} \tag{4}$$

We can categrozite them as subgroups generated by subsets of D_8.
- order 1:
$$\{e\} = \langle e \rangle \tag{5}$$
- order 2:
$$\langle r^2 \rangle = \{e, r^2\}, \quad \langle s \rangle = \{e, s\}, \quad \langle sr \rangle = \{e, sr\}, \quad \langle sr^2 \rangle = \{e, sr^2\}, \quad \langle sr^3 \rangle = \{e, sr^3\}. \tag{6}$$
- order 4:
$$\begin{aligned} \langle r \rangle &= \{e, r, r^2, r^3\}, \\ \langle r^2, s \rangle &= \{e, r^2, s, sr^2\}, \\ \langle r^2, sr \rangle &= \{e, r^2, sr, sr^3\}. \end{aligned} \tag{7}$$
  In particular, notice that $\langle r^2, sr^2 \rangle = \langle r^2, s \rangle$, and that $\langle r^2, sr^3 \rangle = \langle r^2, sr \rangle$, so we only have 3 distinct subgroups of order 4.
- order 8 is the whole group:
$$D_8 = \langle r, s \rangle \tag{8}$$

Putting this all together, we can draw the lattice diagram of D_8 :


D_8
$\langle s, r^2 \rangle$
$\langle r \rangle$
$\langle rs, r^2 \rangle$
$\langle s \rangle$
$\langle r^2 s \rangle$
$\langle r^2 \rangle$
$\langle rs \rangle$
$\langle r^3 s \rangle$
1

Chapter 3

3.1 *Quotient Groups*

The Big picture: homomorphisms and Fibers

Imagine a homomorphism $\varphi : G \to H$. This map "collapses" G onto H by identifying certain elements of G that map to the same element in H. The preimage of each element in H under φ is called a **fiber**. These fibers partition G into disjoint subsets.

For X_a the fiber over $a \in H$, and X_b the fiber over $b \in H$, define their product as the fiber over ab:

$$X_a X_b = X_{ab}. \tag{9}$$

This new operation on the fibers turns the set of fibers into a group, called a **quotient group**.

Kernel and Cosets

The most important fiber is that over the identity element e_H in H.

> **Definition: Kernel**
>
> If $\varphi : G \to H$ is a homomorphism, the **kernel** of φ is the set of elements in G that map to the identity e_H in H:
>
> $$\ker(\varphi) = \{g \in G |\ \varphi(g) = e_H\}. \tag{10}$$

The kernel is a subgroup of G, and it has a special structure as follows

> ***Proposition***
>
> Let $\varphi : G \to H$ be a homomorphism. Then
>
> 1. $\varphi(e_G) = \varphi(e_H)$.
> 2. $\varphi(g^{-1}) = \varphi(g)^{-1}\ \forall g \in G$.
> 3. $\ker(\varphi) \leq G$.
> 4. The image $\mathrm{im}(\varphi)$ is a subgroup of H.

Next, we define **cosets**, which are understood as neighboring copies of a subgroup within the larger group.

> **Definition: Coset**
>
> For any subgroup $N \leq G$, and any element $g \in G$, the set
>
> $$gN = \{gn \mid n \in N\} \tag{11}$$
>
> is called a **left coset** of N in G. The element g is called a **representative** of the coset gN. Similarly, $Ng = \{ng |\ n \in N\}$ is a right coset.

A crucial link between fibers, kernels and cosets is established by the following proposition:

> ***Proposition***
>
> Let $\varphi : G \to H$ be a homomorphism and $K = \ker(\varphi)$ be its kernel. Let X be the fiber of $a \in H$. For any $u \in X$ (i.e. $\varphi(u) = a$), then $X = uK = \{uk |\ k \in K\}$ is a left coset of Kernel.

Normal Subgroups and Quotient Groups

The fibers of a homomorphism partition the group into cosets of the Kernel. The group of these cosets forms the **quotient group**.

> **Definition: Operation on Cosets**
>
> Let $K = \ker(\varphi)$. The set of fibers is denoted by G/K. We define a kinary operation on G/K as follows:
>
> $$(uK)(vK) = (uv)K, \quad \forall uK, vK \in G/K. \tag{12}$$

In the particular case where this operation is well-defined, i.e. for a different u', v', we still have $(u'v')K = (uv)K$, we say that K is a **normal subgroup** of G.

> **Definition: Normal subgroup**
>
> a Subgroup N of a group G is called a **normal subgroup** if $\forall g \in G$, and $n \in N$,
>
> $$gng^{-1} \in N \quad \Leftrightarrow gNg^{-1} = N. \tag{13}$$
>
> Denote this N as $N \trianglelefteq G$. The elements gng^{-1} is the **conjugate** of n by g.

It's clear that onjugating a normal subgroup by any element of the group leaves the subgroup unchanged.

It can be proven that a normal subgroup has several equivalent characterizations:

> ***Theorem***
>
> Let $N \leq G$. The following are equivalent:
>
> $$\begin{aligned} &1. N \trianglelefteq G. \\ &2. \forall g \in G, gN = Ng. \\ &3. (un)(vm)N = (uv)N \quad \forall u, v \in G, \text{and } \forall n, m \in N. \\ &4. N = \ker(\varphi) \text{ for some homomorphism } \varphi. \end{aligned} \tag{14}$$

This theorem is the cornerstone of the section. It tells us that the subgroups we can "quotient by" are precisely the normal subgroups, which are precisely the kernels of homomorphisms.

If $N \trianglelefteq G$, the set of left cosets of N in G, denoted G/N, forms a group under the operation $(uN)(vN) = (uv)N$. A quotient group is then defined as follows

> **Definition: Quotient Group**
>
> Let $N \trianglelefteq G$ be a normal subgroup. The **quotient group** G/N is the set of left cosets of N in G with the operation defined by
>
> $$(uN)(vN) = (uv)N, \quad \forall u, v \in G. \tag{15}$$
>
> Its set-builder representation is thus
>
> $$G/N = \{gN \mid g \in G\} \tag{16}$$

3.2 *Cosets and Lagrange Theorem*

This section builds on homomorphisms and normal subgroups (Section 3.1) to explore cosets of a subgroup $H \leq G$. Cosets provide a way to "slice" G into equal-sized pieces, leading to powerful counting results. The main tool is Lagrange's Theorem, which relates subgroup orders to the group's order.

Cosets Partition the Group.

Recall, for any subgroup $H \leq G$ and any element $g \in G$, the set $gH = \{gh \mid h \in H\}$ is called a **left coset** of H in G. These form a partition of G.

> ***Proposition***
>
> Let G be a group and $H \leq G$. THen there exists distinct elements $g_1, g_2, ..., g_k \in G$ for some finite k, such that:
>
> 1. $$G = \bigcup_i g_i H \tag{17}$$
>
> (Cosets partition G, and their union covers G.)
>
> 2. $$g_i H \cap g_j H = \emptyset, (i \neq j) \tag{18}$$
> 3. $$|gH| = |H| \ \forall g \in G. \tag{19}$$

Core Insight: Cosets are "translates" of H that tile G without overlap. The number k of cosets is called the index of H in G.

> **Definition: Index of a subgroup**
>
> The index of $H \leq G$, denoted $|G : H|$. is the number of distinct left cosets of H in G. (the "size" of the quotient group).
>
> For finite G,
>
> $$|G : H| = \frac{|G|}{|H|}. \tag{20}$$

Lagrange theorem then follows naturally from the properties of cosets:

> ***Theorem***
>
> Lagrange's Theorem :
>
> Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$, i.e., $|G| = |H| \cdot |G : H|$.

Main Corollaries

Lagrange's Theorem has immediate consequences for elements, small groups, and normality.

3.3

3.5

Chapter 4

4.1

4.2

Groups acting on themselves by left multiplication – ***Cayley's Theorem***

- Le

4.3

4.4

Chapter 5

5.1

5.2

Mitterm 2 Cutoff