Midterm 1 Cutoff

Midterm 2 coverage: 2.4, 2.5, 3.1, 3.2, 3.3, 3.5, 4.1, 4.2, 4.3, 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.
>
> $$\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subset H}} H. \tag{1}$$

- **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.
>
> $$\langle A \rangle = \{a_1^{e_1} a_2^{e_2} ... a_n^{e_n} \mid n \in \mathbb{Z}^+, a_i \in A, e_i = \pm 1\}. \tag{2}$$

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 :
   - $S_1 = \{e\} = \langle e \rangle$,
   - $S_2 = \{e, (12)\} = \langle (12) \rangle$,
   - $S_n = \langle (1\ 2), (1\ 2 \ldots n) \rangle$
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: $\{e\} = \langle e \rangle$
- order 2:

$$\langle r^2 \rangle = \{e, r^2\}, \quad \langle s \rangle = \{e, s\}, \quad \langle sr \rangle = \{e, sr\}, \quad \langle sr^2 \rangle = \{e, sr^2\}, \quad \langle sr^3 \rangle = \{e, sr^3\}. \tag{5}$$

- order 4:

$$\begin{aligned} \langle r \rangle &= \{e, r, r^2, r^3\}, \\ \langle r^2, s \rangle &= \{e, r^2, s, sr^2\}, \\ \langle r^2, sr \rangle &= \{e, r^2, sr, sr^3\}. \end{aligned} \tag{6}$$

  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:

$$D_8 = \langle r, s \rangle \tag{7}$$

Putting this all together, we can draw the lattice diagram of D_8 seen below.

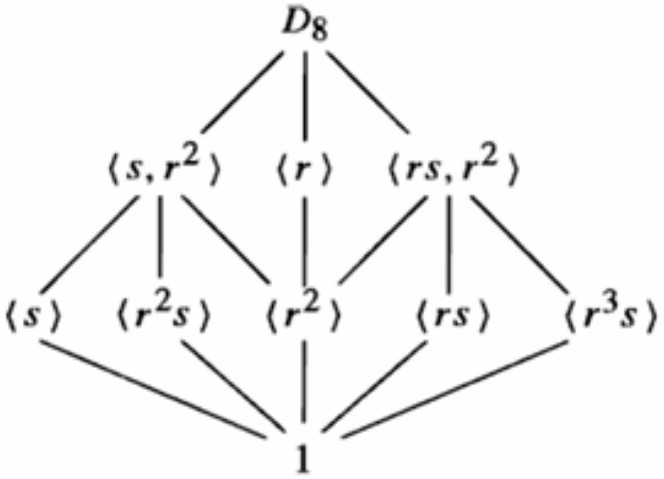

Figure 1: lattice of D_8.

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:

$$X_a X_b = X_{ab}. \tag{8}$$

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:
>
> $$\ker(\varphi) = \{g \in G |\ \varphi(g) = e_H\}. \tag{9}$$

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
>
> $$gN = \{gn \mid n \in N\} \tag{10}$$
>
> 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:

$$(uK)(vK) = (uv)K, \quad \forall uK, vK \in G/K. \tag{11}$$

In the particular case where this operation is well-defined, i.e. for a different $u' \in uK, v' \in vK$, 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 $n \in N$,

$$gng^{-1} \in N \quad \Leftrightarrow gNg^{-1} = N. \tag{12}$$

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:

$$\begin{aligned} &1. N \trianglelefteq G. \\ &2. \forall g \in G, gN = Ng. \\ &3. (un)(vm)N = (uv)N \quad \forall u, v \in G, \text{and } \forall n, m \in N. \\ &4. N = \ker(\varphi) \text{ for some homomorphism } \varphi. \end{aligned} \tag{13}$$

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

$$(uN)(vN) = (uv)N, \quad \forall u, v \in G. \tag{14}$$

Its set-builder representation is thus

$$G/N = \{gN \mid g \in G\} \tag{15}$$

In the quotient group, each element is a coset, and the group is "zoomed out" with respect to a normal subgroup. The group operation is defined by $aN \cdot bN = ab\ N$, and the identity is $e_G N = N$.

This section can be thus summarized as:

If $N \trianglelefteq G$, then $G/N = \{gN \mid g \in G\}$ with operation $aN \cdot bN = ab\ N$.

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. $$G = \bigcup_i g_i H \tag{16}$$

   (Cosets partition G, and their union covers G.)

2. $$g_i H \cap g_j H = \emptyset, (i \neq j) \tag{17}$$

3. $$|gH| = |H|\ \forall g \in G. \tag{18}$$

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,

$$|G : H| = \frac{|G|}{|H|}. \tag{19}$$

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.,
>
> $$|G| = |H| \cdot |G : H| \ . \tag{20}$$

Main Corollaries

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

> ***Corollary: Order of an element divides group order.***
>
> If G is finite and $g \in G$, then $|g|$ divides $|G$.

> **Proof:** Let $H \leq G$ and $H = \langle g \rangle$. Then $|H| = |g|$. By Lagrange, $|H|$ divides $|G|$, so $|g|$ divides $|G|$. □

> ***Corollary: Groups of prime order are cyclic.***
>
> If $|G| = p$ is prime, then G is cyclic, i.e., $G \cong Z_p$

> **Proof:** The subgroups are only $\{e\}$ (order 1) and G itself (order p) both divides p. Let $g \in G \setminus \{e\}$, $\langle g \rangle \leq G$, then by Lagrange theorem, $|g|$ divides p, so $|g| = p$. Thus $G = \langle g \rangle \simeq Z_p$ is cyclic. □

> ***Corollary: Subgroups of index 2 are normal.***
>
> If $H \leq G$ with $|G : H| = 2$, then $H \trianglelefteq G$.

> **Proof:** There are only two left cosets: H and gH for some $g \in G \setminus H$. And only two right cosets H, Hg. Since both left cosets and right cosets partition G, they must match, i.e. $gH = Hg (\forall g \in G.)$ Therefore by Equation 13, $H \trianglelefteq G$ □

3.3 *The Isomorphism Theorems*

The Isomorphism Theorems formalize the relationship between homomorphisms, kernels, and quotient groups established in Sec 3.1.

For purpose of exam, we focus on the First Isomorphism Theorem, while understanding the 3rd theorem statement. The proof to 1st and 3rd are omitted; The 2nd and 4th are omitted (they are so hard!)

The First Isomorphism Theorem

The First isomorphism theorem states that if we map G to H via a homomorphism φ, then the image of φ is isomorphic to the quotient of G by the kernel of φ.

> ***Theorem: First Isomorphism Theorem***
>
> Let $\varphi : G \to H$ be a homomorphism, then $\ker(\varphi) \trianglelefteq G$ and
>
> $$G/\ker(\varphi) \simeq \mathrm{Im}(\varphi). \tag{21}$$

There are several important corollaties to this theorem:

> ***Corollary: 1***
>
> φ is injective iff $\ker(\varphi) = \{e_G\}$.

Proof: If $\ker(\varphi) = e_G$, then $G/\ker(\varphi) = G \simeq \operatorname{Im}(\varphi)$ so φ is bijective. Conversely, if φ is injective, then $|\ker(\varphi)| = 1$, so $\ker(\varphi) = \{e_G\}$. □

> ***Corollary: 2***
>
> If G finite, then $|G : \ker(\varphi)| = |\operatorname{Im}(\varphi)|$.

Proof: By Lagrange theorem, $|G : \ker(\varphi)| = |G| \ / \ |\ker(\varphi)|$. By First Isomorphism theorem, $|G/\ker(\varphi)| = |\operatorname{Im}(\varphi)|$. □

> ***Corollary: 3***
>
> If φ is surjective ($\operatorname{Im}(\varphi) = H$), then $G/\ker(\varphi) \simeq H$.

Proof: Trivial.□

> ***Corollary: 4***
>
> If φ is injective, then $G \simeq \operatorname{Im}(\varphi)$.

Proof: Trivial.□

The Third Isomorphism Theorem
The Third Isomorphism Theorem deals with nested quotients. It can be memorized as "invert and cancel" as one would do with fractions.

> ***Theorem: Third Isomorphism Theorem***
>
> Let G be a group, and let $H \trianglelefteq G, K \trianglelefteq G, H \leq K$. Then $K/H \trianglelefteq G/K$, and
>
> $$G/H \Big/ K/H \simeq G/K. \tag{22}$$

3.5 *Transpositions and the Alternating Group*

We establish a fundamental property of permutations: each one has a "parity" (even or odd). Thi sidea is formalized by constructing a homomorphism from S_n to $\{\pm 1\}$. The kernel of this map, the set of even permutations, is the **Alternating Group A_n.**

Transpositions as Genrator of S_n.
Recall a permutation can be written as a product of cycles (not nessessarily disjoint) in many non-unique ways.

Definition: Transposition

A Transposition is a 2-cycle (ij).

Every permutation can be beilt from transpositions. In fact:

Proposition

The symmetric group S_n is generated by transpositions.

$$S_n = \langle (ij) \mid 1 \leq i \leq j \leq n \rangle \tag{23}$$

Proof: Since evvery permutation can be written as product of disjoint cycles, it suffices to show that eveyr cycle can be written as a product of transpositions. Indeed, for any k- cycle,

$$(a_1 a_2 ... a_k) = (a_1 a_k)(a_1 a_{k-1})...(a_1 a_2). \tag{24}$$

□

Note that this decomposition is not unique. For example, $(123) = (13)(12)$ but also $(123) = (21)(23)$. However, the parity of the number of transpositions is an invariant, as we will now prove.

The `sign` homomorphism.

To formalize the idea of parity, we construct a homomorphism from S_n to the multiplicative group $\{\pm 1\}$.

To construct, recall that S_n acts on $P[x_1, x_2, ..., x_n]$ s.t.

$$\sigma \cdot P[x_1, x_2, ..., x_n] = P\left[x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}\right]. \tag{25}$$

Consider polynomial in n variables

$$\Delta_n \equiv \prod_{1 \leq i \leq j \leq n} (x_i - x_j). \tag{26}$$

For example,

$$\begin{aligned} \Delta_4 &= (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4), \\ (12)\Delta_4 &= (x_2 - x_1)(x_2 - x_3)(x_2 - x_4)(x_1 - x_3)(x_1 - x_4)(x_3 - x_4) = -\Delta_4; \\ (123)\Delta_4 &= (x_2 - x_3)(x_2 - x_1)(x_2 - x_4)(x_3 - x_1)(x_3 - x_4)(x_1 - x_4), = \Delta_4. \end{aligned} \tag{27}$$

Definition: The sign function

Using Δ_n, define sign as

$$\text{sign } (\sigma) = \frac{\sigma(\Delta_n)}{\Delta_n} = \pm 1. \tag{28}$$

A permutation σ is called even if $\text{sign}(\sigma) = +1$, and odd if $\text{sign}(\sigma) = -1$.

Theorem: Sign homomorphism

The sign map is a surjective homomorphism from S_n to $\{\pm 1\}$. That is,

$$\text{sign}(\tau\sigma) = \text{sign}(\tau)\text{sign}(\sigma). \tag{29}$$

Proof:

$$\text{sign}(\tau)\ \text{sign}(\sigma) = \frac{(\tau\sigma)\Delta_n}{\Delta_n} = \frac{\tau(\sigma(\Delta_n))}{\Delta_n}\frac{\sigma(\Delta_n)}{\Delta_n} = \text{sign}(\tau)\text{sign}(\sigma). \tag{30}$$

Proof for surjectivity is omitted.□

The alternating group A_n.
For even permutation σ , $\text{sign}(\sigma) = 1$. We exploit this to define the alternating group.

Definition: Alternating group A_n

$$A_n = \ker(\text{sign}) \tag{31}$$

is the subgroup of S_n consisting of even permutations

Since A_n is the kernel of a homomorphism, it's a normal subgroup of S_n. Thus by first isomorphism theorem,

$$S_n/A_n \simeq \text{Im}(\text{sign}) = \{\pm 1\}. \tag{32}$$

This immediately tells us the index and order of A_n.

$$|S_n : A_n| = \frac{|S_n|}{|A_n|} = |\,\text{Im}(\text{sign})| = 2 \quad \Rightarrow \quad |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}. \tag{33}$$

There are only two cosets of A_n, the even permutations (A_n itself) and the odd permutations ($(12)A_n$). In other words,

$$\begin{aligned} \sigma \in A_n &: \text{even} \\ \sigma \in S_n - A_n &: \text{odd}. \end{aligned} \tag{34}$$

Therefore, the transposition (ij) is odd.
- Even permutation = prod. of even number of transpositions.
- Odd permutation = prod. of odd number of transpositions.

equivalently,

$$(a_1 a_2 ... a_k) = \begin{cases} \text{odd} & k \text{ even} \\ \text{even} & k \text{ odd}. \end{cases} \tag{35}$$

Example

Consider the following permutation

$$\begin{aligned} &\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 1 & 5 & 9 & 3 & 7 & 8 \end{pmatrix} \\ &= (124)(36987)(5) = (12)(24)(36)(69)(98)(87) \end{aligned} \tag{36}$$

There are even number (6) of transpositions, so it's an even permutation.

Alternative Characterization of sign.
The sign of a permutation can also be determined by counting the number of times a larger number precedes a smaller number in the image of the permutation.

Definition: Inversion

Spcifically, consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & \dots & n \\ a_1 & a_2 \dots & a_i & a_j & \dots a_n \end{pmatrix} \tag{37}$$

For each $a_i > a_j, (i < j)$, inversion happens once. $\text{sign}(\sigma) =$ parity of number of inversions.

Example

consider the lower line of permutation to be

$$2, 4, 6, 1, 5, 9, 3, 7, 8. \tag{38}$$

Fix 2, found 1 preceeding element bigger that 2, inversion +1. Fix 4, found 2 preceeding elements bigger than 4, inversion +2. Repeat the process for all elements, we find 10 inversions. So it's a even permutation.

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