Math493: Honors Algebra I

Yanzhi Li

December 23, 2025

Abstract

This course is **a basic introduction on finite group theory** and **representation theory**, containing my personal thoughts as well as lecture notes. My course instructor is Mircea Mustață.

Contents

Chapter 1

Group Actions

1.1 Introduction

We now lay our focus to group actions, group actions are useful because we can endowed the **symmetric structure** of a group into other mathematical objects through group actions, specifically:

- often groups acts on various mathematical structure, such as sets, topological spaces, manifolds, etc.
- It will be of great significance for us to consider the actions of a group on itself via **conjugation**.

Definition 1.1.1. Let's fix a group G and a set X, an **action** (say also a left action of) G on X is a map:

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

such that the following holds:

$$ex = x \quad \forall\, x \in X$$
$$g(hx) = (gh)x \quad \forall\, g, h \in G,\ x \in X$$

We now introduce an **equivalent formulation** for group action:
Recall that:

$$S_X = (\{\text{bijections } X \to X\}, \circ)$$

is a group.

Definition 1.1.2. Now suppose we have the action of G on X as above, we may define a map $\varphi : G \to S_X$ as follows: for every $g \in G$, $\varphi(g)$ which written as φ_g is the map:

$$\varphi_g : X \to X, \varphi_g(x) = gx$$

It is easy to see that by inheritance of the existance of inverses in G, φ_g is a bijection. In particular, one can see that it is actually a **group homomorphism**.

And the following conclusion is easy to deduce:

Conclusion 1.1.1.

$$\{\textbf{Actions of } G \textbf{ on } X\} \leftrightarrow \{\textbf{Group Homomorphism } G \to S_X\}$$

forms a **bijection**.

We then give some examples of group actions:

Example. Given any set X, we have the identity, **trivial** group action given by the group homomor-

phism:

$$S_X \xrightarrow{Id} S_X$$

which is equivalent to the action of S_X on X by:

$$S_X \times X \to X \ , \ (f, x) \mapsto f(x)$$

Example. If $n > 3$ and P_n be the regular n-gon, we then have a group homomorphism:

$$D_{2n} \to S_{P_n}$$

which leads to an action of D_{2n} on P_n

> **Note.** See that in this case D_{2n} preserve the distance structure within the regular n-gon.

Example. The group $GL_n(\mathbb{C})$ acts on $\mathbb{C}^n$ via:

$$(A, u = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}) \mapsto Au$$

which represent the matrix as **linear transformation**. Such corresponds to the group homomorphism:

$$GL_n(\mathbb{C}) \to S_{\mathbb{C}^n}$$
$$A \mapsto \text{corresponds linear transformation on } \mathbb{C}^n$$

Example. (Cayley's Theorem) Define an action of G on itself by:

$$G \times G \to G$$
$$(g, h) \mapsto g \cdot h$$

which acts by the natural left multiplication. Note such corresponds to a group homomorphism:

$$G \xrightarrow{\varphi} S_G$$

And we shall have:

> **Proposition 1.1.1.** (Cayley) φ is always injective

In particular, if G is finite, G is then **isomorphic** to a subgroup of S_n.

$$G \cong \text{Im}(\varphi) \subseteq S_G$$

The proof is immediate by showing $\ker(\varphi) = \{e\}$ by cancellation.

Example. Suppose $H \leq G$, we have:

$$G \times (G/H)_l \to (G/H)_l$$
$$(g, ah) \mapsto gaH$$

easy to see such is a group action after checking well-definedness. Such action is induced by the action of group on itself, note H here is **not necessarily normal**.

Example. (Group action by **Conjugation**) The following will be the most interesting example for us. First recall we have an **automorphism** given by $g \in G$:

$$\alpha_g : G \to G \ , \ \alpha_g(x) = gxg^{-1}$$

Moreover, observe $Aut(G) \leq S_G$, so we have a group homomorphism:

$$G \to Aut(G) \leq S_G$$
$$g \mapsto \alpha_g$$

We can understand $Aut(G)$ as those **permutation that preserve the group structure**.
In particular, by our discussion, we get an action of G on itself:

$$(g, x) \mapsto gxg^{-1}$$

1.2 Orbits and Orbits-Stablizer Theorem

Definition 1.2.1. Write $x \sim y$ for $x, y \in X$, if $\exists\, g \in G$, s.t. $gx = y$.

Lemma 1.2.1. Such gives us a equivalent relation, directly check by **reflexive, symmetric, transitive**.

Conclusion 1.2.1. We get a partition of X into equivalence classes, called **orbits**. If $x \in X$, then the corresponding equivalence classes is given by:

$$\{gx \mid g \in G\}$$

which is denoted by **Gx** or **O(x)**.

Notation. X/G denotes the sets of the orbits of X.

Definition 1.2.2. The action of G on X is <u>transitive</u> if X has only one orbits, which is:

$$\forall\, x, y \in X,\ \exists\, g \in G\ s.t.\ gx = y$$

Example. The action given by the left multiplication of G on itself is **transitive**.

Example. Induced by above example, the action of G on the **set of left cosets** of H is also transitive.

Definition 1.2.3. For every $x \in X$, the <u>stablizer</u> of $x \in G$ is given by:

$$Stab_G(x) = \{g \in G \mid gx = x\}$$

namely those elements in G that doesn't move the position of x.

Lemma 1.2.2. $Stab_G(x) \leq G$ being a subgroup.

Example. Consider the action of G on itself by conjugation, the orbits of $a \in G$ is called the

conjugate class of a. Two elements of G are conjugate of each other if they lie in the same conjugate class (**same orbit**).

What is the stablizer in this case?

$$Stab_G(x) = \{y \in G \mid yxy^{-1} = x\} =: C_G(x)$$

which is the centralizer of x in G.

Note. $C_G(x) = G$ iff $x \in Z(G)$

Remark. Consider the conjugacy classes of S_n, then $\sigma, \tau \in S_n$ are conjugate of each other if and only if when they written as **product of disjoint cycles**, then # of k-cycle for both of them is the **same** for all k (**they have same cycle type**).

We now introduce Orbit-Stablizer theorem.

Theorem 1.2.1. If G acts on X, then for every $x \in X$:

$$\#O(x) = (G : Stab_G(x))$$

In particular, if G is finite group, then

$$\#O(x) \mid |G|$$

Proof. Define a map:

$$f : (G/Stab_G(x))_l \longrightarrow O(x)$$
$$f(gStab_G(x)) = gx$$

- Well-defineness + injectivity:

$$\begin{aligned} & g_1 Stab_G(x) = g_2 Stab_G(x) \\ \Leftrightarrow\ & g_2^{-1} g_1 \in Stab_G(x) \\ \Leftrightarrow\ & (g_2^{-1} g_1)x = x \\ \Leftrightarrow\ & g_2^{-1}(g_1 x) = x \\ \Leftrightarrow\ & g_1 x = g_2 x \end{aligned}$$

- Surjectivity:

$$\begin{aligned} & y \in O(x) \\ \Rightarrow\ & y = gx \\ \Rightarrow\ & y = f(gStab_G(x)) \end{aligned}$$

So we see f is a bijection. The first isomorphism theorem direct yields the result. ■

Note. When the action is transitive, with X being finite, we have:

$$\#O(x) = (G : Stab_G(x)) = |X|$$

In particular, transitive means there is only one orbits.

Proposition 1.2.1. If G acts on X, then:

$$|X| = \sum_{i \in I} (G : Stab_G(x))$$

where x_i are a system of representative for the orbits of G in X.

Proof. We have a partition:

$$X = \bigsqcup_{i \in I} O(x) \Rightarrow \#X = \sum \#O(x_i)$$

with:

$$\#O(x_i) = (G : Stab_G(x_i))$$

■

Example. (**Class Equation: A important special case**) Consider the action of $G \times G \to G$ by **conjugation**, with G be finite group:

$$|G| = \sum_{i \in I} (G : C_G(x_i))$$
$$\Rightarrow |G| = |Z(G)| + \sum_{i \in I'} (G : C_G(x_i))$$

where I' runs over indices such that $(G : C_G(x_i)) > 1$.

Such results direct yields from the fact that elements in $Z(G)$ attains its centralizer (stablizer) to be the whole group.

Note. Such only works for actions by **conjugation!**

We now give an application for orbits-stablizer theorem, which is important when we study the construction of groups.

Definition 1.2.4. If p be prime number, and G be group, if $|G| = p^n$ for some $n \geq 1$, then we say G is a p-group.

Proposition 1.2.2. If G is a p-group, then:

$$Z(G) \neq \{e\}$$

Proof. Since $p \mid |G|$ and $(G : Stab_G(x)) \mid |G| = p^n$, then:

$$p \mid (G : C_G(x_i))$$

whenever this is > 1, then class equation yields that:

$$p \mid |Z(G)|$$

■

Corollary 1.2.1. If p prime, $|G| = p^2$, then G is an abelian group.

To proof this we need first a lemma:

Lemma 1.2.3. For all group G, if $G/Z(G)$ is cyclic, then G is abelian.

Proof. By cyclic property, first suppose that $xZ(G)$ is a generator of $G/Z(G)$, then there exists

$i, j \in \mathbb{Z}$, such that:

$$\begin{aligned} aZ(G) &= x^i Z(G) \\ bZ(G) &= x^j Z(G) \\ \Leftrightarrow a &= x^i a' \\ b &= x^j b' \qquad \text{for some } a'b' \in Z(G) \\ \Rightarrow ab &= x^i a' x^j b' = x^{i+j} a' b' \\ ba &= x^j b' x^i a' = x^{i+j} b' a' \\ \Rightarrow ab &= ba \qquad \text{since } a', b' \in Z(G) \end{aligned}$$

■

We now give proof to **Corollary** 1.2.1:

Proof. We know that:

$$Z(G) \neq \{e\}$$

Then by **Lagrange's theorem**, see that either $Z(G) = G$ or $|Z(G)| = p$.

If $Z(G) = G$, we already done! Now suppose that $|Z(G)| = p$, now observe that every subgroup of $Z(G)$ is a **normal subgroup** of G by definition.

In particular, we then consider the group $G/Z(G)$, this is of order p, so it is cyclic. Then by **Lemma** 1.2.3, see that G is abelian, contradict to the fact that $Z(G) \neq G$ ↯. ■

Chapter 2

Sylow's Theorem

Sylow's Theorem is important when we want to understand and classify the category of finite groups, simply by looking on the order of such finite group. Further, it lays foundation and gives tools for us when we want to understand the structure of the building blocks of finite group (simple group).

2.1 Cauchy's Theorem

Our motivation to study Cauchy's Theorem, as well as Sylow's Theorem, in the first place, is we want to give a partial inverse to **Lagrange's theorem**. Recall that Lagrange's theorem implies that:

Proposition 2.1.1. If G is a finite group, with order n, then $\forall\, x \in G$, it satisifies that:

$$|x| \mid n$$

In general, the converse of this statement is not true, in particular:

$$\exists\, q \mid |G|, \text{ but there exists no } g \in G, \text{ s.t. } |g| = q$$

for example we can take $q = |G|$, but G is **not a cyclic group**.

So we give partial converse of this statement by stating **Cauchy's Theorem** and later Sylow's theorem.

Theorem 2.1.1. (**Cauchy**) If G is a finite group and p is a prime integer, s.t. $p \mid |G|$, then $\exists\, g \in G$, $|g| = p$.

We first proof for the case when G is **abelian group**, then one can easily derive the general cases by invoking $\mathbf{Z}(\mathbf{G})$ of any group.

Proof. We reason by deviding cases for abelian and non-abelian group:

- When G is **abelian**: We argue by contradiction, suppose that $|x| \neq p,\ \forall x \in G$, in this case see that $p \nmid |x|,\ \forall x \in G$, otherwise if $|x| = m,\ p \mid m \Rightarrow |x^{\frac{m}{p}}| = p \lightning$.

  Let $N = \text{lcm}\{|x| \mid x \in G\}$, use prime factorization of N see that $p \nmid N$. Now suppose $g_1, \ldots, g_n$ are the elements of G, we define:

$$f : \underbrace{\mathbb{Z}/N\mathbb{Z} \times \ldots \times \mathbb{Z}/N\mathbb{Z}}_{n \text{ times}} \longrightarrow G$$
$$f(a_1 + N\mathbb{Z}, \ldots, a_n + N\mathbb{Z}) = g_1^{a_1} \ldots g_n^{a_n}$$

  one can easily check the well-definedness of such map. The point is G be an abelian group makes

this map a group homomorphism:

$$\begin{aligned} f((a_1+N\mathbb{Z},\dots,a_n+N\mathbb{Z})+(b_1+N\mathbb{Z},\dots,b_n+N\mathbb{Z})) &= f(a_1+b_1+N\mathbb{Z},\dots,a_n+b_n+N\mathbb{Z}) \\ &= g_1^{a_1+b_1}\dots g_n^{a_n+b_n} \\ &= (g_1^{a_1}\dots g_n^{a_n})(g_1^{b_1}\dots g_n^{b_n}) \quad \text{By } G \text{ is abelian} \\ &= f((a_1+N\mathbb{Z},\dots,a_n+N\mathbb{Z})) \\ &+ f((b_1+N\mathbb{Z},\dots,b_n+N\mathbb{Z})) \end{aligned}$$

so f indeed be a group homomorphism. One should then see that f is clearly surjective by taking:

$$g_i = f(0,\dots,\overset{i}{1},\dots,0)$$

By fundemental isomorphism theorem:

$$G \cong (\mathbb{Z}/N\mathbb{Z})^n/\ker(f) \Rightarrow |G| = \frac{|\mathbb{Z}/N\mathbb{Z}|^n}{|\ker(f)|}$$

And by Lagrange theorem:

$$|G| \mid |(\mathbb{Z}/N\mathbb{Z})^n| = N^n$$

however, since $p \mid |G|$, but $p \nmid N$, hence $p \nmid N^n$, leading to contradiction $\lightning$.

- When G is **non-abelian**: We argue by induction on $|G|$.
  - Base case: If $|G| = p \Rightarrow G$ is cyclic, then we are done.
  - Inductive case: we assume we know the assertion for all G', such that $p \mid |G'|$, with $|G'| < |G|$, and prove the assertion for G. Note that if there exists $H \leq G$, with $H \neq G$, but $p \mid |H|$, then by the induction hypothesis we are done.
    Hence, may assume: $\forall\, H \leq G,\ H \neq G,\ p \mid H$. Then by Lagrange theorem: $|G| = |H| \cdot (G : H) \Rightarrow p \mid (G : H)$. By class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{d} (G : C_G(x_i))$$

    where x_i runs over a system of representatives of conjugacy classes with ≥ 2 elements. By our assumptions, we saw:

$$p \mid (G : C_G(x_i)),\ p \mid |G| \Rightarrow p \mid |Z(G)|$$

    Since among all subgroups of G, **only itself** can be divided by p, so this means that:

$$Z(G) = G$$

    so we see G is abelian and yields back to the case we've proven before.

■

2.2 Sylow's First Theorem

With the help of Cauchy's theorem, we now give proof to Sylow's first theorem.

Definition 2.2.1. If G is finite group, p prime integer, s.t. $p \mid |G|$ and $p^m \mid |G|$, $p^{m+1} \nmid |G|$, then a subgroup of G with order p^m is called a p-Sylow subgroup of G.

Theorem 2.2.1. (**Sylow's First Theorem**) If G is a finite group and p is a prime integer, if $p \mid |G| \Rightarrow G$ contains a p-Sylow subgroup.

Note. Sylow's first theorem actually implies Cauchy's theorem.
If $H \leq G$ be a p-Sylow subgroup and $g \in H \backslash \{e\} \Rightarrow |g| = p^r \Rightarrow \left|g^{p^{r-1}}\right| = p$.
However, we will **use** Cauchy's theorem to prove Sylow's theorem.

Proof. We argue by induction on $|G|$.

- Base case: $|G| = p$, the assertion is clear, G is its own p-Sylow subgroup.
- Inductive case: Assume that we know the theorem for all groups G', s.t. $p \mid |G'|$, and $|G'| < |G|$, we want to show the assertion for G.

  Suppose that $p^m \mid |G|$, but $p^{m+1} \nmid |G|$, then there are two cases:

  - If there is a **proper subgroup** H of G, s.t. $p^m \mid |H|$, then by induction hypothesis, H contains a p-Sylow subgroup, and this is also a p-Sylow subgroup of G.
  - If **for all proper subgroup** H of G, $p^m \nmid |H|$, then p^m has to **divide the index of such subgroup**. Then by class equation:

$$|G| = |Z(G)| + \sum_{i=1}^{d} \underbrace{(G : C_G(x_i))}_{\geq 2 \text{ hence divided by } p.}$$

  And see that:

$$p \mid |G| \Rightarrow p \mid |Z(G)|$$

  By Cauchy's theorem for the abelian group $Z(G)$, there exists $x \in Z(G)$, s.t. $|x| = p$. Since $x \in Z(G) \Rightarrow \langle x \rangle$ is a normal subgroup of G. Now consider: $G' := G/\langle x \rangle$

  - If $m = 1$, then we are done! Since $\langle x \rangle$ is a p-Sylow subgroup of G.
  - If $m \geq 2$, see that $|G'| = \frac{|G|}{p} < |G|$ is divisible by p , so we apply induction on G', see that G' contains a p-Sylow subgroup, which is of the form: $H/\langle x \rangle$ for some subgroup H of G. Notice that:

$$|H/\langle x \rangle| = p^{m-1} \Rightarrow |H| = p^{m-1} \cdot p = p^m$$

■

by prime factorization, $G = p^m \cdot (\cdots)$, so see $|G'| = \frac{|G|}{p} = p^{m-1} \cdot (\cdots)$

Appendix