Math493: Honors Algebra I

Yanzhi Li

December 25, 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

Part I

Finite Group Theory

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:

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

■

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

2.3 Sylow's Second and Third Theorem

Sylow's Second theorem basically tells us how the p-Sylow subgroup of G relate to each other, and Sylow's third theorem tells us the possible number of each p-Sylow subgroup can take. Before diving into the proof, we need to dig more intuition on what group actions can do, i.e. how it **permute the endian sets**.

2.3.1 More on Group Action

Example. Suppose G is a group acting on a set X:

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto gx$$

If $cP(X)$ is the set of all subsets of X, we then get an **induced group action**:

$$\begin{aligned} G \times \mathcal{P}(X) &\longrightarrow \mathcal{P}(X) \\ (g, A) &\longmapsto gA = \{ga \mid a \in A\} \end{aligned}$$

and its clear that such satisfy the group action properties, we get a group action of G acting on $\mathcal{P}(X)$.

Important exmaple: If in this case we consider the action on G acting on itself by conjugation, we can get a correspond action of G on $\mathcal{P}(G)$:

$$(g, A) \longmapsto gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

Note. If A is a subgroup of G, then gAg^{-1} is also a subgroup of G .

the conjugation map is a group **automorphism**

Remark. If H is a p-Sylow subgroup of G and $\sigma : G \to G$ be an automorphism, then $\sigma(H)$ will also be a p-Sylow subgroup, in particular, **every conjugation** of H which is p-Sylow subgroup will also be a p-Sylow subgroup.

2.3.2 Sylow's Second and Third Theorem

Theorem 2.3.1. (**Sylow's Second Theorem**) If H is a p-Sylow subgroup of G, K is **any p-subgroup** of G, then there exists $a \in G$, s.t. $K \subseteq aHa^{-1}$.

In particular: if K is a p-Sylow subgroup, too. Then H, K are conjugate of each other: $K = aHa^{-1}$ for some $a \in G$.

Theorem 2.3.2. (**Sylow's Third Theorem**) If we denote:

$$n_p = \#p\text{-Sylow subgroups of } G$$

Then we have:

$$\begin{cases} n_p \equiv 1 (\mathrm{mod} p) \\ n_p = (G : N_G(H)) \Rightarrow n_p \mid (G : H) \end{cases}$$

with:

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

where H is a p-Sylow subgroup of G.

Note. $N_G(H)$ will be the largest subgroup of G in which H is a normal subgroup.

Note. The assertion:

$$n_p = (G : N_G(H)) \Rightarrow n_p \mid (G : H)$$

is derived from Lagrange's theorem:

$$\begin{aligned} H \leq N_G(H) \leq G \\ \Rightarrow (G : H) = \frac{|G|}{|H|} = \frac{|G|}{|N_G(H)|} \cdot (N_G(H) : H) \\ \text{And } (G : N_G(H)) = \frac{|G|}{|N_G(H)|} \end{aligned}$$

We shall prove both of the theorem at the same time.

Proof. We've seen in **Example** , G has an action on $\mathcal{P}(G) = \{T \mid T \leq G\}$ by conjugation: $(g, T) \to gTg^{-1}$. We now define:

$$\mathcal{S} = \{H = H_1, H_2, \ldots, H_r\}$$

which is the collection of the orbits of H with respect to such action. By **Orbit-Stablizer Theorem** 1.2.1:

$$\begin{aligned} r &= (G : Stab_G(H)) \\ Stab_G(H) &= \{g \in G \mid gHg^{-1} = H\} = N_G(H) \\ \Rightarrow r &= (G : N_G(H)) \end{aligned}$$

Now suppose we have a p-subgroup K of G, the action of G on $\mathcal{P}(G)$ then induces an action of K on $\mathcal{P}(G)$, and we shall have the canonical injective homomorphism:

$$K \cap N_G(H) \Big/ K \cap H \hookrightarrow N_G(H) \Big/ H$$

For the right hand side, see that:

$$\left| N_G(H) \Big/ H \right| = \frac{|N_G(H)|}{|H|} \left| \frac{|G|}{|H|} = \frac{|G|}{p^m} \right.$$

Note that $\frac{|G|}{p^m}$ is relatively primed to p.

For the left hand side, it attains a non-negative order (can be 0), since K is a p-group, it should attain its order to be **power of p** by **Lagrange's Theorem**.

Now since it is a injective homomorphism, it attains a trival kernel, so by **Lagrange's theorem + first isomorphism theorem**:

$$\left| K \cap N_G(H) \Big/ K \cap H \right| \left| \left| N_G(H) \Big/ H \right| \right.$$

But notice that the right hand side is coprime with p but left hand side divides p, this leads to:

$$\left| K \cap N_G(H) \Big/ K \cap H \right| = 1 \Rightarrow K \cap N_G(H) = K \cap H \tag{2.1}$$

Now suppose $I \subseteq \{1, \ldots, r\}$ are those such that $\{H_i \mid i \in I\}$ which gives a system of representatives for the orbits of the K action on $\mathcal{S}$, then by class equation:

$$r = |\mathcal{S}| = \sum_{i \in I} (K : \underbrace{Stab_K(H_i)}_{= K \cap Stab_G(H_i) = K \cap H_i \text{ by } 2.1}) \tag{2.2}$$

Now we want to prove:

$$(K : K \cap H_i) \Leftrightarrow K \subseteq H_i \tag{2.3}$$

If it is not the case, then $(K : K \cap H_i)$ is divisible by p since K is a p-group. First take $K = H$, since $|H| = |H_i|$, $\forall i$, we have $H \leq H_i \Leftrightarrow i = 1$. Hence by **Equation** 2.2, $r \equiv 1 (\mathrm{mod} p)$.

Suppose that K is an arbitrary p-group, if $K \not\subseteq H_i$, $\forall i \in I \Rightarrow p \mid r$ by **Equation** 2.2, which contradicts to $r \equiv 1 (\mathrm{mod} p)$. Hence there exists i, s.t. $K \subseteq H_i = aHa^{-1}$ for some $a \in G$, such yields **Sylow's Second Theorem**.

In particular, we see $\mathcal{S} = \{p\text{-Sylow subgroups of } G\} \Rightarrow r = n_p$:

$$\begin{aligned} \Rightarrow n_p &\equiv 1 (\mathrm{mod} p) \\ n_p = r &= (G : N_G(H)) \end{aligned}$$

which yields **Sylow's Third Theorem**. ■

Note. All p-Sylow subgroups are conjugate to each other.

Remark.

$$n_p = 1 \Leftrightarrow H \trianglelefteq G$$

We state a small proposition that is helpful when we analyze the group structure along with Sylow's Theorem, it is also the midterm problem of this course.

Proposition 2.3.1. Let $H, K \trianglelefteq G$, and $H \cap K = \{e\}$, then:

$$\begin{aligned} H \times K &\longrightarrow HK \\ (h, k) &\longmapsto hk \end{aligned}$$

is a group isomorphism.

We now give two applications of Sylow's Theorem, and give proof to the second one.

Proposition 2.3.2. Let G be a group such that: $|G| = pq$ where p, q are primes, let P_p and P_q be two the p, q-Sylow subgroups of G respectively, satisfying $P_p, P_q \trianglelefteq G$, and if $p < q,\ q \not\equiv 1 (\bmod p)$, we have:

$$G \cong {\mathbb{Z}} \Big/ {pq\mathbb{Z}}$$

and thus G is **cyclic** and thus abelian.

Proposition 2.3.3. Suppose G be a group with order $30 = 2 \cdot 3 \cdot 5$, then:

1. there is a subgroup $H \leq G$ of order 15.
2. $n_5(G) = 1,\ n_3(G) = 1$.

Proof. Let H be a 5-Sylow subgroup of G and K be a 3-Sylow subgroup of G. See that $|H \cap K| = 1$ since it has to divide both 3 and 5.

If $H \trianglelefteq G$, then by **second isomorphism theorem**, see that $HK \leq G$ and:

$$\begin{aligned} {HK} \Big/ {H} &\cong {K} \Big/ {H \cap K} \cong K \\ \Rightarrow |HK| &= |H| \cdot |K| = 15 \end{aligned}$$

Similarly we will get a subgroup of order 15 if K is normal.

Then suppose that both H, K are not normal subgroups of G. By **Sylow's Third Theorem**:

$$\left.\begin{array}{l} n_3(G) \left| \dfrac{|G|}{5} = 6 \right. \\ n_3(G) \equiv 1 (\bmod 5) \end{array}\right\} \Rightarrow n_5(G) = 6 \quad (n_5(G) \neq 1 \Leftrightarrow H \not\trianglelefteq G)$$

And similarly we have $n_3(G) = 10$.

Notice that the intersection of any 2 distinct 5-Sylow subgroups is the identity, since any of these subgroups is generated by elements that are not the identity. We then have $6 \times 4 = 24$ elements of order 5 in G, and similarly we get $10 \times 2 = 20$ elements of order 3. Since $24 + 20 > 30$, such leads to contradtiction $\lightning$.

Thus we reach to the conclusion that there exists subgroup G' of G of order 15, and since $(G : G') = 2 \Rightarrow G' \trianglelefteq G$. Now since $|G'| = 3 \times 5$ and $5 \not\equiv 1 (\bmod 3)$, by **Proposition** 2.3.2, G' is cyclic thus abelian.

By Sylow's second theorem, $n_5(G') = n_3(G') = 1$, and it should deduce that $n_3(G) = n_5(G) = 1$:

Say A is a 5-Sylow subgroup of G', it should also be a 5-Sylow subgroup of G. Now if A' is another 5-Sylow subgroup of G, by Sylow's Second theorem, there exists $g \in G,\ A' = gAg^{-1}$. Since G' isi abelian, $A \trianglelefteq G' \trianglelefteq G \Rightarrow A' = gAg^{-1} \subseteq gG'g^{-1} = G' \Rightarrow gAg^{-1}$ is also a 5-Sylow subgroup of G' and hence equal to A. ∎

2.4 Simple Group

"Simple groups are the basic **building blocks** of groups". Given a group $H \trianglelefteq G$, if we understand H, G/H, we can then hope to get some information of G, and thus to decompose such idea, we obtain the concept of **simple group**.

Definition 2.4.1. A group G, (**not necessarily finite**), is simple. if the following:

1. $G \neq \{e\}$
2. whenever $H \trianglelefteq G$, we have either $H = \{e\}$ or $H = G$.

In particular, there is **no** interesting normal subgroup of G.

We shall give an overview of classifying some good types of groups, but now we already seen that cyclic group and abelian groups give us good enough property. We may ask what will happen to an abelian group if it is also simple.

Proposition 2.4.1. If G is abelian, then G is simple **if and only if** $G \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. May assume that $G \neq \{e\}$, since G is abelian, it means that every subgroup of G is normal subgroup. Hence G is simple if and only if G has no non-trivial subgroups.

Equivalently: $\forall\, x \in G$, $x \neq e$, we have $G = \langle x \rangle$. This is ok if $G \cong \mathbb{Z}/p\mathbb{Z}$.

Conversely: suppose G satisfying $G = \langle x \rangle$, in particular, see that G is cyclic, so $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$. Clearly $\mathbb{Z}$ does not satisfy generated by any element of it: e.g. $\langle 2 \rangle \neq \mathbb{Z}$. So $G \cong \mathbb{Z}/n\mathbb{Z}$, $n \geq 2$. If p prime, and $p \mid n$, this implies:

$$\left.\begin{array}{l} \left|\frac{n}{p}\right| = p \\ \langle \frac{n}{p} \rangle = G \text{ by assumption} \end{array}\right\} \Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$$

■

We shall give some examples of it.

Example. $n \geq 3$, Dihedral groups, see that:

$$D_{2n} \neq \text{ simple groups}$$

since

$$\langle \sigma \rangle \trianglelefteq D_{2n}$$

because it has index 2.

Example. $n \geq 3$, S_n is not simple as $A_n \trianglelefteq S_n$.

Example. If p, q prime integers, $|G| = p^2 q \Rightarrow G$ is not simple.

Proof. **Sketch of Proof:** Consider whether $Z(G) = G$, if $Z(G) = G$, then by **Proposition** 2.4.1, it is not simple. If they are not equal, use Sylow's theorem to deduce that it cannot happen that $n_q \neq 1 \neq n_p$. ■

2.4.1 Special simple groups

We now give an important theorem, which gives us a big type of simple finite groups.

Theorem 2.4.1. For every $n \geq 5$, A_n is simple.

Proof. We will proceed by induction on $n \geq 5$.

- **Base case ($\mathbf{n = 5}$)**: $|A_5| = 2^2 \cdot 3 \cdot 5 = 60$. Suppose H be the non-trivial **normal** subgroup of A_5, we want to deduce a contradiction.
  - If $\mathbf{5 \big| |H|}$: notice that $n_5(H) = n_5(G)$ by similar reasoning as we've done in **Proposition** 2.3.3: (Sylow's Second theorem + $H \trianglelefteq G$).
    See that:
    $$\left.\begin{aligned} n_5(G) &\equiv 1 (\mathrm{mod} 5) \\ n_5(G) &\Big| \frac{|G|}{5} = 12 \end{aligned}\right\} \Rightarrow n_5(G) = 1 \text{ or } 6$$
    - If $n_5(G) = n_(H) = 6$: then H contains more than 24 elements of order 5. And by $|H| \big| |G|$, $|H| = 30$. By **Proposition** 2.3.3, see that $n_5(H) = 1$, leads to contradiction $\lightning$.
    - If $n_5(G) = n_5(H) = 1$: then G only has 4 elements of order 5 in G, but $G = A_5$, these are precisely the 5-cycles (They have sign to be 1). But we have $4 \times 3 \times 2 \times 1$ such cycles, in A_5 $\lightning$.

    So we reach the conclusion that we cannot have $5 \big| |H|$.
  - Since $|H| \big| 60$ and $\gcd(5, |H|) = 1 \Rightarrow |H| \big| 12 \Rightarrow |H| \in \{2, 3, 4, 6, 12\}$. The main idea is to try to **contract to the acse of 2,3,4**.
    - If $|H| = 6$, then:
      $$\left.\begin{aligned} n_3(H) &\equiv 1 (\mathrm{mod} 3) \\ n_3(H) &\Big| \frac{|H|}{3} = 2 \end{aligned}\right\} \Rightarrow n_3(H) = 1$$
      Again by sylow's second theorem + $H \trianglelefteq G \Rightarrow n_3(H) = n_3(G) = 1 \Rightarrow G$ has a 3-Sylow subgroup that is normal.
    - If $|H| = 12$, then:
      $$\left.\begin{aligned} n_3(H) = n_3(G) &\equiv 1 (\mathrm{mod} 3) \\ n_3(H) = n_3(G) &\Big| \frac{12}{3} = 4 \end{aligned}\right\} \Rightarrow n_3(H) = n_3(G) = 1 \text{ or } 4$$
      - If $n_3(G) = 1$, then replacing H by a 3-Sylow subgroup get a normal subgroup of G or order 3.
      - If $n_3(G) = n_3(H) = 4$, we have $4 \times 2 = 8$ elements of order 3 in H, thus we get 3 elements of order different from 1 and 3 in H.
        Since $|H| = 12$, it has a subgroup P with 4 elements (a 2-Sylow subgroup), thus P is the unique 2-Sylow subgroup of H, and thus be a unique 2-Sylow subgroup of G. So we repalce H by P and get a normal subgroup of G with 4 elements.
    - Hence assume $|H| \in \{2, 3, 4\}$, thus $|G \,/\, H| \in \{30, 20, 15\}$.

      Claim. $G \,/\, H$ contains a normal subrgoup with 5 elements, then this has to be of the form $K \,/\, H$ where $K \trianglelefteq G$, $H \subseteq K \Rightarrow 5 \big| |K|$, which contradicts to **the initial case!**

      Let $\overline{G} = G \,/\, H$:
      - If $\left|\overline{G}\right| = 30$, then by **Proposition** 2.3.3, $n_5(\overline{G}) = 1$, and we get a normal subgroup with 5 elements.
      - If $\left|\overline{G}\right| = 20$, then $n_5(\overline{G}) \equiv 1 (\bmod 5)$ and $n_5(\overline{(G)}) \big| \frac{20}{5} = 4 \Rightarrow n_5(\overline{G}) = 1$, conclusion the same.

· If $\left|\overline{G}\right| = 15$, then similarly as the case just proved, $n_5(\overline{G}) = 1$, conclusion the same.

So the claim holds and the base case is done.

- **Inductive case**: Suppose that $n \geq 6$ and we know that A_{n-1} is simple.

  Suppose that H is non-trivial normal subgroup of $A_n = G$. For $i \in [n]$, let:

$$G_i = \{\sigma \in G \mid \sigma(i) = i\} \cong A_{n-1} \tag{2.4}$$

  Note that if $\alpha \in S_n$, then:

$$\alpha G_i \alpha^{-1} = G_{\alpha(i)} \tag{2.5}$$

  Since **Formula** 2.4 is clear, if $i = 1 \Rightarrow$ it follows for all i by taking some α, s.t. $\alpha(i) = 1$.

  We now consider $H \cap G_i$ be normal subgroup of G_i, with G_i being simple group by **IH**, there is only two possibilities:

  1. $H \cap G_i = \{e\}$
  2. $H \cap G_i = G_i \Rightarrow G_i \subseteq H$

  – If there exists i, s.t. $G_i \subseteq H$, then for every j, if $\sigma \in G$ is s.t. $\sigma(i) = j$, then by **Formula** 2.5 and $H \trianglelefteq G$, $G_j \subseteq H \Rightarrow \langle G_1, \ldots, G_n \rangle \subseteq H$.

  But $\langle G_1, \ldots, G_n \rangle = A_n$ by the fact that every $\sigma \in A_n$ are product of even number of transposition of the form $(ij)(kl)$, and if $q \neq i, j, k, l \Rightarrow (ij)(kl) \in G_q$.

  – If $G_i \cap H = \{e\}$, $\forall\ i$: then if $\sigma, \sigma' \in H$, s.t. $\sigma(i) = \sigma'(i)$ for some i, then $\sigma(\sigma')^{-1} \in H \cap G_i \Rightarrow \sigma = \sigma'$.

  Suppose $\sigma \in H, \sigma \neq e$

  * In the decomposition of σ into disjoint cycles, there is a cycle of order ≥ 3:

$$\sigma = (a_1 a_2 a_3 \ldots) \ldots$$

    Let $\alpha \in A_n$, s.t. $\alpha(a_1) = a_1, \alpha(a_2) = a_2, \alpha(a_3) \neq a_3$, there must exsist such α, since $n \geq 6$. then:

$$\sigma' = \alpha\sigma\alpha^{-1} = (a_1 a_2 \alpha(a_3) \ldots) \ldots \in H \text{ by normality of } H$$

    See that $\sigma(a_1) = \sigma'(a_1)$ but $\sigma(a_2) \neq \sigma'(a_2)$, leading to contradiction $\lightning$.

  * The decomposition of σ into disjoint cycles only has transpositions, by Induction hypotheis, it can't fix any elements as $G_i \cap H = \{e\}$, $\sigma \in H$.

$$\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6) \ldots$$

    Take $\alpha \in A_n$, s.t. $\alpha = (a_1 a_2)(a_3 a_5)$, and let $\sigma' = \alpha\sigma\alpha^{-1}$, see that $\sigma'(a_1) = a_2 = \sigma(a_1)$, $\sigma'(a_3) = a_6 \neq \sigma(a_3) \Rightarrow \sigma \neq \sigma'$, leading to contradiction $\lightning$.

■

Remark. A_4 is **not** simple group!

$$H = \{e, (12)(34), (13)(24), (14)(23)\} \trianglelefteq a_4$$

Note that H is isomorphic to the **Klein group**. See that H is a normal subgroup since **conjugation preserves the cycle type decomposition** and the element of H that are $\neq e$ are **precisely the one** that decomposition as product of 2 disjoint cycles.

Remark. Elementary to check: if $|G| < 60$, G is simple $\Rightarrow G \cong \mathbb{Z}/p\mathbb{Z}$, p prime.

2.4.2 Classification of Finite Simple Groups

There exists an **explicit classification** of finite simple groups!

1. $\mathbb{Z}/p\mathbb{Z}$, p primes.
2. A_n, $n \geq 5$
3. 12 series of "finite groups of Lie types".
   For example: $\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z})$ or more generally $\mathrm{PSL}_n(\mathbb{F}_q)$.
$$\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) = \{A \in M_n(\mathbb{Z}/p\mathbb{Z}) \mid \det A = 1\}$$
$$\mathrm{PSL}_n(\mathbb{Z}/p\mathbb{Z}) = \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z}) \Big/ \{A = \lambda I_n \mid \lambda \in \mathbb{Z}/p\mathbb{Z},\ \lambda^n = 1\}$$
4. 26 "sporaolic examples".

   The largest one: the Monster
   has order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
   $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$
   $\sim 8 \cdot 10^{53}$
   This can be embedded as a subgroup of $GL_n(\mathbb{C})$, $n = 196,883$

2.5 Semidirect Product

General Motivation: Suppose G be a group, $N \trianglelefteq G$, s.t. we understand N and G/N, what can we say about G? In general, not much. However, in particular cases when we have $G \xrightarrow{\pi} G/N$ and there is a section of π to be a group homomorphism: $s : G/N \to G$, s.t. $\pi \circ s = Id$, then we can completely describe G if we know one more piece of data.

The external semidirect product is built by two separate independent group, while the internal semidirect product is to decompose an existing group at hand.

2.5.1 External Semidirect Product

Definition 2.5.1. Suppose N, H be two groups, and we have a group homomorphism
$$\varphi : H \to \mathrm{Aut}(N)$$
We define an operation $\star$ on $\mathbf{N} \times \mathbf{H}$ by:
$$(n_1, h_1) \star (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$$
Such defines a group, denoted as $N \rtimes H$, which is called the **external semidirect product** of N and H with respect to φ.

Left for the reader to check that it is indeed a group, checking associativity, existence of identity and existence of inverses are not hard.

Note.
- If $\varphi : H \to \mathrm{Aut}(N)$, $h \mapsto Id$, we recover the usual group structure on $N \times H$, namely the direct product.
- We have a map $H \to N \rtimes_\varphi H$, $h \mapsto (e_N, h)$, this is a group homomorphism, it is clearly injective, with image to be:
$$H' = \{(n, h) \in N \rtimes_\varphi H \mid n = e_N\}$$
Similarly, we have $N \to N \rtimes_\varphi H$, $n \mapsto (n, e_H)$, which is also a group homomorphism, injective,

with image to be:

$$N' = \{(n, h) \in N \rtimes_\varphi H \mid h = e_H\}$$

In fact this is a normal subgroup of $N \rtimes_\varphi H$, can be verified by proving:

$$(n', h')^{-1} \star (n, e) \star (n', h') \in N'$$

- We can also prove the following claim by checking:

$$(e_N, h) \star (n, e_H) \star (e_N, h)^{-1} = (\varphi_h(n), e_H)$$

> **Claim.** via the isomorphism $N \cong N'$, $H \cong H'$, the morphism:
>
> $$\begin{aligned} H' &\to \mathrm{Aut}(N') \\ g &\mapsto (n \mapsto gng^{-1}) \end{aligned}$$
>
> is given by φ.

- We have a group homomorphism:

$$\begin{aligned} N \rtimes H &\to H \\ (n, h) &\mapsto h \end{aligned}$$

This is surjective group homomorphism, with the kernel to be $N' \cong N \Rightarrow N \rtimes_\varphi H \,/\, N' \cong H$.

- We have a section given by:

$$H \to N \rtimes_\varphi H$$

> **Definition 2.5.2.** (**Section of a Group Extension**) Let explicit the short exact sequence:
>
> $$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} H \longrightarrow 1$$
>
> A homomorphism $s : H \to G$ is called a **section** (or a splitting) of the extension if it satisfies:
>
> $$\pi \circ s = \mathrm{id}_H$$
>
> where id_H represents the identity map on H.
>
> If such a section exists, we say the extension *splits*, and G is isomorphic to the semidirect product $N \rtimes H$.

2.5.2 Internal Semidirect Product

> **Definition 2.5.3.** Suppose G be any group, and H, N be subgroups of G with $N \trianglelefteq G$ normal. And define:
>
> $$\begin{aligned} \varphi : H &\to \mathrm{Aut}(N) \\ h &\mapsto \varphi_h \\ \varphi_h(n) &= hnh^{-1} \qquad \text{ok since } N \trianglelefteq G \end{aligned}$$
>
> We get a map $N \rtimes_\varphi H \xrightarrow{\alpha} G, (n, h) \mapsto nh$. And we claim it is a **group homomorphism**, with the operation defined as:
>
> $$(n_1, h_1) \star (n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$$
>
> One should easily verify that.
> We define G to be the **internal semidirect product** of its subgroups N, H if α is an isomorphism.

We then give a more straightforward equivalence of this definition.

Proposition 2.5.1. Let H, N, G be as in the definition, G is the internal semidirect product of N, H if and only if:

1. $N \trianglelefteq G$
2. $G = N \cdot H$
3. $H \cap N = \{e\}$

Proof. α is isomorphism if and only if it is injective and surjective. It is surjective if and only if $G = N \cdot H$ (This is subgroup since $N \trianglelefteq G$). It is injective if and only if:

$$\begin{aligned}\ker(\alpha) &= \{(n, h) \mid n \in N,\ h \in H,\ nh = e\} \\ &= \{(n, n^{-1}) \mid n \in H \cap N\} \\ &= \{e\}\end{aligned}$$

■

Chapter 3

Classification of Finite Groups

Finite group theory is already a well-studied field, people are already been able to classify different types of groups in finite order with good or relatively good property, and decompose the finite group into the building blocks, namely the simple groups. We've studied simple groups before, so in this chapter we shall introduce how we will decompose the finite groups into simple factors through **Jordan-Hölder theorem**. We will then introduce some special groups with relatively good properties, which are built by abelian groups. A small glimpse of it will be:

$$\text{cyclic} \subseteq \text{abelian} \subseteq \textit{nilpotent} \subseteq \text{solvable}$$

and we will also try to dig some more property of p-group.

3.1 Composition Series and Jordan-Hölder Theorem

Definition 3.1.1. (**Composition Series**) Given a group G, a composition series of G is given by a sequence of subgroups:

$$\{e\} \leq N_r \leq N_{r-1} \leq \ldots \leq N_0 = G$$

such that $\forall\, i \in [r-1]$:

1. $N_{i+1} \trianglelefteq N_i$
2. $N_i \,/\, N_{i+1}$ are simple groups

We call r to be the length of the series, and the $N_i \,/\, N_{i+1}$ to be the simple factors in the series

> **Note.** Some trivial case worth noting:
>
> - $r = 0 \Leftrightarrow G = \{e\}$
> - $r = 1 \Leftrightarrow G$ is simple

Definition 3.1.2. If G has a composition series, then G has finite length.

Proposition 3.1.1. Every finite group has finite length

Proof. **Sketch of proof**: proof by induction on $|G|$, and **glue the composition series** of N and $G \,/\, N$ if there exists $N \trianglelefteq G$. ■

Theorem 3.1.1. (**Jordan-Hölder Theorem**) Given two composition series for G, denoted as:

$$\{e\} = N_r \leq \ldots \leq N_1 \leq N_0 = G$$
$$\{e\} = N'_s \leq \ldots \leq N'_1 \leq N'_0 = G$$

Then:

- $r = s$
- and
$$N_{r-1}/N_r, \ldots, N_0/N_1$$
$$N'_{s-1}/N'_s, \ldots, N'_0/N'_1$$
are pairwise isomorphism, after possibly reordering.

> **Note.** This is basically stating that the **simple factors** are the **building blocks**.

We need a lemma to proof the original theorem.

Lemma 3.1.1. If G has a composition series, $N \trianglelefteq G$, then N has a composition series.

Proof. (**Proof of Lemma 3.1.1**) Suppose we start with a composition series of G, and consider for N:
$$\{e\} = N \cap G_r \leq \ldots \leq N \cap G_1 \leq N \cap G_0 = N$$
Now what can we say about the following injective map?
$$N \cap G_i / N \cap G_{i+1} \hookleftarrow G_i / G_{i+1}$$
By normality of N in G, see:
$$N \cap G_i / N \cap G_{i+1} \subseteq G_i / G_{i+1}$$
With the image of the map also normal in G_i / G_{i+1}, and since the simple factor is simple:

- either $N \cap G_i / N \cap G_{i+1} = \{e\}$
- or $N \cap G_i / N \cap G_{i+1} = G_i / G_{i+1}$

Then **After removing repeated factors, i.e. Those** $\{\mathbf{e}\}$, we get a composition series of N. ■

Proof. (**Proof of Jordan-Hölder Theorem**) We shall proceed the proof by induction on the shortest length of a composition series of G, in particular, our aim is to see that if G has a composition series with length r, then all composition series of G should have length r and the pairwise isomorphism statement holds.

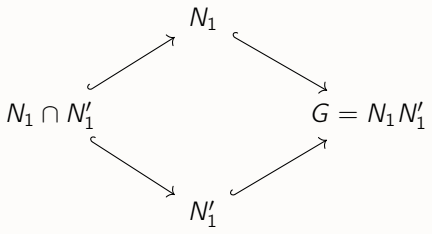
- **Base case**: If this is 0: $G = \{e\}$, which is trivial, if this is 1, then G is simple, every composition series should have length to be 1, also trivial.
- **Inductive case**: Suppose $r \leq s$, and we assume by Induction we know the theorem for those groups that admit a composition series with length $r - 1$, then there are two cases:
  - $N_1 = N'_1$: we then get a composition series for those two subgroups, and we can apply induction hypothesis see that $r - 1 = s - 1$ and the pairwise isomorphism statement also holds and call a day.
  - $N_1 \neq N'_1$: We then look at what we can say about $N_1 N'_1$?
    First note that $N_1 \not\subseteq N'_1$, otherwise:
    $$\{e\} \neq N'_1/N_1 \trianglelefteq G/N_1 \textbf{ (Simple)} \quad \lightning$$
    Similarly, $N'_1 \not\subseteq N_1$.
    Then $N_1 \subseteq N_1 N'_1 \trianglelefteq G$, since both N_1, N'_1 are normal subgroups.

Since $G \,/\, N$ is simple, then either $N = N_1 N_1' \Rightarrow N_1' \subseteq N_1 \not\downarrow$ or $N_1 N_1' = G$, clearly the latter case.

Hence $G = N_1 N_1'$, then by the second isomorphism theorem:

$$G \Big/ N_1 = N_1 N_1' \Big/ N_1 \cong N_1' \Big/ N_1 \cap N_1' \Rightarrow G \Big/ N_1' \cong N_1 \Big/ N_1 \cap N_1'$$

We then want to use a composition series of $N_1 \cap N_1'$ to apply induction.



and by the second isomorphism theorem:

$$\begin{aligned} N_1 \Big/ N_1 \cap N_1' &\cong G \Big/ N_1' \\ N_1' \Big/ N_1 \cap N_1' &\cong G \Big/ N_1 \end{aligned} \tag{3.1}$$

And in particular, groups on the **LHS** are **simple**.

Since $N_1 \cap N_1' \subseteq G$ and G has a composition series, then by **Lemma** 3.1.1, $N_1 \cap N_1'$ also has a composition series, and in particular $N_1 \cap N_1' \trianglelefteq G$.

We now choose one such composition series:

$$\{e\} = N_t'' \leq \ldots \leq N_1'' \leq N_0'' = N_1 \cap N_1'$$

Then we obtain four kinds of composition series for G:

1. $\{e\} = N_r \leq \ldots \leq N_2 \leq N_1 \leq G$
2. $\{e\} = N_t'' \leq \ldots \leq N_1'' \leq N_1 \cap N_1' \leq N_1 \leq G$
3. $\{e\} = N_t'' \leq \ldots \leq N_1'' \leq N_1 \cap N_1' \leq N_1' \leq G$
4. $\{e\} = N_s' \leq \ldots \leq N_2' \leq N_1' \leq G$

Since N_1 has a composition series of length $r-1$, by **IH**, the **first and second** series satisfy the condition of the theorem.

By **Formula** 3.1, the **second and third** series satisfy the condition in the theorem.

By N_1' has a composition series of length $r-1$, by **IH**, the **third and fourth** series satisfy the condition in the theorem.

Thus the **first and fourth** series satisfy the condition of the theorem.

■

Remark. If G being finite, and:

$$\{e\} = G_r \leq \ldots \leq G_1 \leq G = G_0 \text{ is a composition series.}$$

Then induction on i + Lagrange theorem gives us:

$$|G_i| = \prod_{j=i}^{r-1} \left| G_j \Big/ G_{j+1} \right|$$
$$\text{by } |G_i| = |G_{i+1}| \cdot \left| G_i \Big/ G_{i+1} \right|$$
$$\Rightarrow |G| = \prod_{i=0}^{r-1} \left| G_i \Big/ G_{i+1} \right|$$

Remark. If G is abelian and finite, then since any of its subgroup will be normal, then given a composition series denoted as above, we have:

$$\left| G_i \Big/ G_{i+1} \right| = \text{ prime integer}$$

In fact we will see later this is an **equivalent** definition for a group to be **nilpotent**.

Proof. **Sketch of Proof**: This directly yields by doing prime factorization on $|G|$ and matching the size of the simple factor on the prime number and combined with **Proposition** 2.3.2. ■

Example. Both $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ have simple factors $\mathbb{Z}/2\mathbb{Z}$ twice, in particular this tells us simple factors aare not unique properties to a group, it is only related to $|G|$, **just like the prime numbers to a particular integers**.

3.2 Solvable and Nilpotent Groups

As we stated before, those two kinds of groups are built out of abelian groups, and both of them are classes of groups that characterized by such fact. Without making confusion we state the definition of characterized group here.

Definition 3.2.1. A group $H \leq G$ is called characterized if $\forall\ \varphi \in \mathrm{Aut}(G)$, $\varphi(H) = H$. Denoted as $H \mathrm{char} G$.

3.2.1 Solvable Group

Definition 3.2.2. A group G is solvable if there exists a **finite** sequence of subgroups

$$\{e\} = G_r \leq \ldots \leq G_1 \leq G_0 = G$$

such that:

- $G_{i+1} \trianglelefteq G_i$ for all $i \in [\![0, r-1]\!]$.
- G_{i+1}/G_i is abelian for all $i \in [\![0, r-1]\!]$.

Remark. This notation is important in both representation theory and Galois theory.

Proposition 3.2.1. Let G be a group, $N \leq G$, then:

1. If G is solvable $\Rightarrow$ N is solvable.
2. If $N \trianglelefteq G$, G is solvable $\Rightarrow$ G/N is solvable.

3. If $N \trianglelefteq G$, $N, G/N$ is solvable $\Rightarrow G$ is solvable.

Proof. **(First statement)**: Suppose we have a sequence of subgroups as stated in the definition of solvable group. If $N \leq G$, we get a corresponding sequences of subgroups in N:

$$\{e\} = N \cap G_r \leq \ldots \leq N \cap G_1 \leq N = N \cap G_0$$

Easy to see that $N \cap G_{i+1} \trianglelefteq N \cap G_i$. Moreover, we have an injective group homomoprhism:

$$\begin{aligned} {N \cap G_i}\Big/{N \cap G_{i+1}} &\to {G_i}\Big/{G_{i+1}} \\ x(N \cap G_{i+1}) &\mapsto xG_{i+1} \end{aligned}$$

In particular, if G is solvable, then have such sequence with all G_i/G_{i+1} abelian, and thus have $N \cap G_i / N \cap G_{i+1}$ abelian for all i, thus N is solvable, which yields the first statement.

Note. Abelian property is **carried through** by the injective group homomorphism.

(Second Statment): Suppose we have a sequence of subgroups as stated in the defintion of solvable group for G. Consider $\forall i$, that $N \subseteq G_iN \leq G$ (It is a subgroup by the normality of N).

Since $G_{i+1} \trianglelefteq G_i \Rightarrow G_{i+1}N \trianglelefteq G_iN$, we then get a sequence of subgroups of G/N given by:

$$\{e\} = {G_rN}\Big/{N} \subseteq {G_{r-1}N}\Big/{N} \subseteq \ldots \subseteq {G_0N}\Big/{N} = {G}\Big/{N}$$

with:

$${G_{i+1}N}\Big/{N} \trianglelefteq {G_iN}\Big/{N}$$

By the third isomorphism theorem:

$${G_iN}\Big/{N}\Big/{G_{i+1}N}\Big/{N} \cong {G_iN}\Big/{G_{i+1}N} \leftarrow {G_i}\Big/{G_{i+1}} \quad \text{gp. hom. by abelian group}$$

$$\underbrace{g \cdot G_{i+1}N \leftarrow\!\shortmid g \cdot G_{i+1}}_{\text{This is surjective} \Rightarrow G_{i+1N}/G_iN \text{ is abelian.}}$$

which yields the second statement.

(Third Statement): Suppose we have two sequences of subgroups as in the definition of solvable groups:

$$\begin{aligned} N_0 = \{e\} \subseteq N_1 \subseteq \ldots \subseteq N_r = N \\ \{e\} = {N_r}\Big/{N} \subseteq {N_{r+1}}\Big/{N} \subseteq \ldots \subseteq {N_{r+s}}\Big/{N} = {G}\Big/{N} \end{aligned}$$

The third isomorphism theorem tells us the sequence of subgroups

$$N_0 \subseteq \ldots \subseteq N_r \subseteq N_{r+1} \subseteq \ldots \subseteq N_{r+s} = G$$

satisfy the condition to make G solvable. ■

We shall give some examples to commonly seen solvable groups.

Example. Every abelian group G is solvable.

Example. D_{2n} is solvable since $\exists\, H \leq D_{2n}$ with H abelian, take $H = \langle \sigma \rangle$, see that H is normal and $D_2n/H \cong \mathbb{Z}/2\mathbb{Z}$.

Example. If G is simple, but non-abelian, then G is not solvable. For example A_n, $n \geq 5$ is not solvable.

Example. By **Proposition** 3.2.1, $S_n,\ n \geq 5$ is not solvable.

Example. S_4 is solvable, take K to be the Klein group, and we have the sequences as:

$$\{e\} \leq K \leq A_4 \leq S_4$$

where:

$$K \cong {\mathbb{Z}}/{2\mathbb{Z}} \times {\mathbb{Z}}/{2\mathbb{Z}}$$
$${A_4}/{K} \cong {\mathbb{Z}}/{3\mathbb{Z}}$$
$${S_4}/{A_4} \cong {\mathbb{Z}}/{2\mathbb{Z}}$$

Definition 3.2.3. (Commutator) Given G be a group, define:

$$[G, G] = \langle [g, h] \mid g, h \in G,\ [g, h] = ghg^{-1}h^{-1} \rangle$$

to be the commutator of G. See that $[G, G] \trianglelefteq G$ and

$$G^{ab} := {G}/{[G, G]} \text{ is abelian.}$$

We can then construct recursively a sequence of subgroups of G:

- $G^{(0)} = G,\ G^{(1)} = [G, G]$.
- If $G^{(n)}$ is constructed, then $G^{(n+1)} = [G^{(n)}, G^{(n)}] \trianglelefteq G^{(n)}$

Thus defined a series for G.
We now give an equivalent definition for solvable groups.

Proposition 3.2.2. G is solvable if and only if there exists n, s.t. $G^{(n)} = \{e\}$.

Proof. The "($\Leftarrow$)" part is clear by definition, so we only care about "($\Rightarrow$)" part.
Suppose we have:

$$\{e\} = N_r \leq \ldots \leq N_1 \leq N_0 = G$$

s.t.

- $N_{i+1} \trianglelefteq N_i,\ \forall\ i \in [\![0, r-1]\!]$.
- $N_i \,/\, N_{i+1}$ abelian.

It is enough to show that for $i \in [\![0, r-1]\!]$, we have $G^{(i)} \subseteq N_i$, then when $i = r \Rightarrow G^{(r)} = \{e\}$.
We argue by induction on $i \geq 0$:

- **Base case**: ok when $i = 0$.
- **Inductive case**: Suppose $i \leq r-1$ and we know the assertion for i:

$$G^{(i+1)} = \underbrace{[G^{(i)}, G^{(i)}] \subseteq [N_i, N_i]}_{\text{By induction, } G^{(i)} \subseteq N_i} \subseteq N_{i+1}$$

The last inclusion needs further explanation:

$${N_i}/{N_{i+1}} \text{ is abelian}$$
$${N_i}/{[N_i, N_i]} \text{ is the largest abelian group for the quotient}$$

■

3.2.2 Nilpotent Group

Definition 3.2.4. (Nilpotent Group) Let G be any group, we define a sequence of subgroups $\{Z_i(G)\}_{i\geq 0}$ as follows:

$Z_0(G) = \{e\}$

- $Z_1(G) = Z(G)$
- If $Z_i(G) \leq G$ is constructed, consider:

$$Z\left(G \Big/ Z_i(G)\right) = Z_{i+1}(G) \Big/ Z_i(G)$$

for some $Z_{i+1}(G) \trianglelefteq G$ and containing $Z_i(G)$.

The group G is nilpotent if there exists n, s.t. $Z_n(G) = G$.

We then give some examples for nilpotent groups.

Example. nilpotent group is solvable group, since

$$Z\left(G \Big/ Z_i(G)\right) = Z_{i+1}(G) \Big/ Z_i(G) \text{ is abelian.}$$

Example. abelian groups are nilpotent: $Z(G) = G = Z_1(G)$.

Example. $S_3 \cong D_6$ is solvable but not nilpotent, since $Z(S_3) = \{e\}$ but $S_3 \neq \{e\}$.
In particular, S_3, S_4 are solvable, but not nilpotent.

Proposition 3.2.3. A group G is nilpotent if and only if there exists a sequence of subgroups:

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_r = G$$

s.t.

1. $G_i \trianglelefteq G,\ \forall\ i \in [\![0, r-1]\!]$.
2. $G_i \,/\, G_{i+1} \subseteq Z\left(G \,/\, G_{i-1}\right),\ \forall\ i \in [\![1, r]\!]$.

Proof. **Sketch of Proof**: One direction is trivial. The other direction can be treated by prove $G_i \subseteq Z_i(G),\ \forall\ i \in [\![0, r]\!]$ by induction on i. ■

Proposition 3.2.4. Let $N \leq G$, then:

1. G nilpotent $\Rightarrow N$ is nilpotent.
2. $N \trianglelefteq G$, G is nilpotent $\Rightarrow G \,/\, N$ is nilpotent.
3. If $\mathbf{N \leq Z(G)}$ and $G \,/\, N$ is nilpotent $\Rightarrow G$ is nilpotent.

Note. If we just know $N \trianglelefteq G$ nilpotent and $G \,/\, N$ nilpotent $\not\Rightarrow G$ nilpotent.

Proof. Almost the same as what we have done for solvable group in **Propositpion** 3.2.1. Using the

characterization via sequences of subgroups by taking:

$$\{G_i \cap N\}_{i\in I} \text{ for } N$$
$$\left\{G_iN \Big/ N\right\}_{i\in J} \text{ for } G \Big/ N$$

We give more assertion for the **third statement**:

If $\{e\} = G_0 / N \leq G_1 / N \leq \ldots \leq G_r / N = G / N$ as characterization of G / N being nilpotent, then

$$\{e\} \underbrace{\leq N}_{\text{Since } N\subseteq Z(G)} = G_0 \leq G_1 \leq \ldots \leq G$$

satisfies the characterization of G being nilpotent group. ■

We now look at what p-group has.

Proposition 3.2.5. If G is a p-group, then G is nilpotent.

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

- **Base case**: If $|G| = p \Rightarrow G \cong \mathbb{Z} / p\mathbb{Z} \Rightarrow$ nilpotent.
- **Inductive case**: We've proven $Z(G) \neq \{e\}$ before in **Proposition** 1.2.2, it follows that:

$$\left|G \Big/ Z(G)\right| < |G|$$

and

$$\left|G \Big/ Z(G)\right| \Big| |G| \Rightarrow G \Big/ Z(G) = \{e\} \text{ or a p-group.}$$

If $G = Z(G)$ then G is abelian thus nilpotent. Otherwise we apply induction hypothesis on $G / Z(G)$ and learn that it is nilpotent. By **Proposition** 3.2.4, G is nilpotent.

■

We now give several equivalent definition to nilpotent groups to strengthen the intuition. It is actually strict for some groups to be nilpotent or even solvable.

Theorem 3.2.1. Let G be a finite group, $p_1, p_2, \ldots, p_r$ are the primes in the prime factorization of $|G|$. Let P_i be the p_i-Sylow subgroup of G, then the following are equivelent:

1. G is nilpotent.
2. For every $H \lneq G$, we have $H \subsetneq N_G(H)$.
3. $P_i \trianglelefteq G$, $\forall\, i$.
4. $G \cong P_1 \times \ldots \times P_r$.

Lemma 3.2.1. Frattini's Argument If G is a finite group with normal subgroup H, and if P is a Sylow p-subgroup of H, then

$$G = N_G(P)H$$

in particular, by applying it to $N_G(N_G(P))$, one can show that

$$N_G(N_G(P)) = N_G(P)$$

whenever G is a fnite group and P is a Sylow p-subgroup of G.

Proof. The main idea is to show: $\mathbf{1} \Rightarrow \mathbf{2} \Rightarrow \mathbf{3} \Rightarrow \mathbf{4} \Rightarrow \mathbf{1}$.

- ($\mathbf{1} \Rightarrow \mathbf{2}$): Proceed by induction on $|G|$. If $|G| = 1$, things are clear. For the inductive step, If $Z(G) \not\subseteq H \Rightarrow \exists\ a \in Z(G) \backslash H$, and so $a \in N_G(H) \backslash H$.

  If $Z(G) \subseteq H$, take $\overline{G} = G \,/\, Z(G) \supsetneq \overline{H} = H \,/\, Z(G)$. Since G is nilpotent, then $|Z(G)| > 1 \Rightarrow \left|\overline{G}\right| < |G|$. Note that $\overline{G}$ is nilpotent by **Prposition** 3.2.4. We now apply induction for $\overline{H}$ and obtain: $\overline{H} \subsetneq N_{\overline{G}}(\overline{H}) \Rightarrow \exists\ aZ(G) \in H \,/\, Z(G),\ a \notin H$, s.t. $aZ(G)\overline{H}a^{-1}Z(G) = \overline{H} \Rightarrow aHa^{-1} = H$, such completes the induction step.

- ($\mathbf{2} \Rightarrow \mathbf{3}$): By **Frattini's Argument** 3.2.1, $N_G(N_G(P_1)) = N_G(P_i),\ \forall\ i$, by condition in 2, $N_G(P_i) = G \Leftrightarrow P_i \trianglelefteq G$.

- ($\mathbf{3} \Rightarrow \mathbf{4}$): One shall utilize **Proposition** 1.2.2 for this. We show by induction on n, $n \in [\![1, r]\!]$, that:

$$P_1 \times \cdots \times P_n \to P_1 \cdots P_n \text{ is an isomorphism.} \tag{3.2}$$

  Note that $P_1 \cdots P_n \trianglelefteq G$ since $P_i \trianglelefteq G\ \forall\ i$.

  If this is ok, take $n = r$, since

$$|P_1 \times \cdots \times P_r| = |G| \Rightarrow P_1 \cdots P_r = G$$

  and yields the result. We now try to proceed the inductive step:

  We have $P_1 \cdots P_n \trianglelefteq G$ and $P_{n+1} \trianglelefteq G$ and $P_1 \cdots P_n \cap P_{n+1} = \{e\}$. By

$$|P_1 \dots P_n \cap P_{n+1}| \;\middle|\; \left.\begin{array}{l} |P_1 \dots P_n| = \prod_{i \le n} |P_i| \\ |P_{n+1}| \end{array}\right\} \text{relatively prime}$$

  By lagrange theorem and our previous proposition, such holds:

$$\begin{gathered} (P_1 \cdots P_n) \times P_{n+1} \to P_1 \cdots P_n P_{n+1} \text{ is an isomorphism.} \\ (a, b) \mapsto ab \end{gathered}$$

  And thus:

$$(P_1 \times \cdots \times P_n) \times P_{n+1} \xrightarrow[\text{By IH}]{\sim} (P_1 \cdots P_n) \times P_{n+1} \to P_1 \cdots P_n P_{n+1} \text{ is an isomorphism.}$$

  The composition is also an isomorphism.

- ($\mathbf{4} \Rightarrow \mathbf{1}$): Since we know that each P_i is nilpotent by being a p_i-group, it is enough to show the following lemma:

> **Lemma 3.2.2.** (structrual theorem) If G, H are nilpotent group, then $G \times H$ is still nilpotent.

Proof. Check that:

$$Z(G \times H) = Z(G) \times Z(H)$$

then:

$$G \times H \Big/ Z(G \times H) \cong \left(G \Big/ Z(G)\right) \times \left(H \Big/ Z(H)\right)$$

And apply induction on i:

$$Z_i(G \times H) = Z_i(G) \times Z_i(H)$$

and if $i \gg 0$:

$$Z_i(G) = G$$
$$Z_i(H) = H$$
$$\Rightarrow Z_i(G \times H) = G \times H$$

■

■

3.3 Free groups

In this section, we will give some introduction on the free groups and more generally we hope to grab some idea of **free objects** in Category Theory.

We shall start with the **forget functor**. Suppose that $\mathcal{C}$ is a category consisting of "sets with extra structure", then the forget functor is given by:

$$G_{\text{forget}} : \mathcal{C} \to \underline{\text{Sets}}$$

Its easy to understand that the forget functor is to strip off the extra structure on the sets and leaving only its basic set structure, for example, we can view a vector space as a bunch of elements forming a set.

The main idea is to see the **free functor** is the **left adjoint** of the **forget functor**.

Given a set S, the **free object corresponding** to S is an object $F(S) \in \text{Ob}(\mathcal{C})$, such that there is a **functorial bijection** for all $X \in \text{Ob}(\mathcal{C})$:

$$\text{Hom}_{\mathcal{C}}(F(S), X) \cong \text{Hom}_{\underline{\text{Sets}}}(S, G_{\text{forget}}(X))$$

Or say the following diagram is commutative:

$$\begin{array}{ccc} \text{Hom}_{\mathcal{C}}(F(S), X) & \xrightarrow{\sim} & \text{Hom}_{\underline{\text{Sets}}}(S, G_{\text{forget}}(X)) \\ \Big\downarrow{\scriptstyle f_*=(u \mapsto f \circ u)} & & \Big\downarrow \\ \text{Hom}_{\mathcal{C}}(F(S), X') & \xrightarrow{\sim} & \text{Hom}_{\underline{\text{Sets}}}(S, G_{\text{forget}}(X')) \end{array}$$

where f is any **morphism** from X to X' here. Or $f \in \text{Hom}_{\mathcal{C}}(X, X')$.

It maybe helpful to understand it with an example in vector spaces and corresponding bases:

Example. Let $\mathcal{C} = \text{Vect}_{\mathbb{R}}$ with $S \in \text{Ob}(\text{Sets}) \to F(S) =$ vector spaces with a basis indexed by S

In this case, see that every object in Vect is isomorphic to $F(S)$, for some S, i.e. **every object in the category of vector spaces is free**.

> **Note.** This probably give us some sense that why Linear Algebra is easier to study than group theory. Objects in vector space category are all free, so we just count things in terms of basis to classify all of them. But in groups, not every groups are free, so in general it is more complex to study.

Intuition. In short, $F(S)$ are free objects **generated** by S under some rule.

3.3.1 Construction of Free Groups

We introduce the construction of free groups in this section.

Fix a set S, let S^{-1} be a set in **bijection** with S, written as:

$$S \to S^{-1}$$
$$g \mapsto g^{-1}$$

Notation. For $x \in S^{-1}$, s.t. $x = a^{-1}$, write $x^{-1} = a$.

Consider a **separate** element, denoted as 1, by notation, $1^{-1} = 1$. We will work with:

$$T = S \sqcup S^{-1} \sqcup \{1\}$$

Definition 3.3.1. A word in T is a sequence $(x_1, x_2, \ldots)$, such that:

$$\begin{cases} x_n = 1, \text{ for } n \gg 0 \\ x_n \in T \ \forall \ n \geq 1 \end{cases}$$

Notation. Use the notation $1 = (1, 1, \ldots)$, to refer the empty word.

A reduced word $(x_1, x_2, \ldots)$ is a word, s.t.:

1. For every $n \geq 1$, $x_{n+1} \neq x_n^{-1}$, unless $x_n = x_{n+1} = 1$.
2. If $x_n = 1$, then $x_p = 1$, $\forall\ p \geq n$.

Definition 3.3.2. **(Free Group)** Define $F(S) = \{\text{reduced word on } T\}$.

Define an operation $\star$ on $F(S)$ as follow "concatenation", given:

$$x = (x_1, x_2, \ldots, x_m \neq 1, 1, 1, \ldots)$$
$$y = (y_1, y_2, \ldots, y_n \neq 1, 1, 1, \ldots)$$

consider

$$z = (x_1, \ldots, \underbrace{x_m, y_1}_{\text{inverse?}}, \ldots, y_n, 1, 1, \ldots)$$

This is reduced unless $x_m = y^{-1}$, and if this is the case, simply remove both of them and repeat and after finite times later, we get **a reduced words**, which is $x \star y$.

Note. Note that:

$$1 \star y = y \text{ if } m = 0$$
$$x \star 1 = x \text{ if } n = 0$$

It is straightforward but tedious to prove associativity for it. It has identity 1 and every element have inverses:

$$x = (x_1, \ldots, x_m \neq 1, 1, \ldots)$$
$$x^{-1} = (x_m^{-1}, \ldots, x_1^{-1}, 1, \ldots)$$

So $(F(S), \star)$ is a group and is called the free group on the set S.

Note. If we defined with **word**, the condition existence of inverses will failed, but we can define monoid with it. The reduced word give us equivalence relation so we can guarantee the uniqueness of inverse elements.

Notation. We will then follow the followin notation later:

1. $(x_1, x_2, \ldots, x_m, 1, \ldots) = x_1 x_2 \cdots x_m$
2. $x_1 x_1 x_2 x_3^{-1} x_3^{-1} x_3^{-1} = x_1^2 x_2 x_3^{-3}$
3. $x_i \in S$ or S^{-1}

Note. Every $x \in F(S)$ is (finite) product of element in S or inverses of such elements, so $F(S)$ is generated by S.

Proposition 3.3.1. (Universal Property) For every group G, the map:

$$\{\text{gp. hom. } F(S) \to G\} \to \{\text{functions } S \to G\} \text{ is bijective}$$
$$f \mapsto f|_S$$

Explicitly: $\forall$ map $\varphi : S \to G$, there exists a **unique** group homomorphism $f : F(S) \to G$, s.t. $f(s) = \varphi(s)$, $\forall\, s \in S$.

Proof. Prove exsistence and uniqueness separately.

- Uniqueness follows by the fact that S generates $F(S)$. Specifically, let H be a group and $A \subseteq H$ such that $H = \langle A \rangle$. Let $f, g : H \to G$ be group homomorphism such that $f|_A = g|_A \Rightarrow f = g$. **If they map the same on the generator, then they map the same on the whole group**.
- Existence: Define:
$$f : F(S) \to G$$
$$f(x_1, x_2, \ldots, x_m \neq 1, 1, \ldots) = u(x_1) \cdots u(x_m)$$
where
$$u(x_i) = \begin{cases} \varphi(x_i), & x_i \in S \\ \varphi(x_i^{-1})^{-1}, & x_i^{-1} \in S \end{cases}$$
The idea of define u here is to maintain the group structure after the mapping of generator. Check that f is a group homomoprhism and $f|_S = \varphi$.

■

Example. $\#S = 1 \Rightarrow F(S) \cong \mathbb{Z}$. To see it, use the universal property.

$$\{\text{gp. hom.: } \mathbb{Z} \to G\} \to G \cong \{\text{functions } S \to G\} \text{ is bijection.}$$
$$f \mapsto f(1)$$
$$f(n) = (f(1))^n$$

Remark. Given two sets S, S' and a map $\varphi : S \to S'$, the **universal property** of the free group $F(S)$ implies:

$$\exists!\ \text{group homomorphism } F(\varphi) : F(S) \to F(S')$$

such that the following diagram is **commutative** (think: sending basis elements to basis elements):

$$\begin{array}{ccc} S & \xrightarrow{\varphi} & S' \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle\iota'} \\ F(S) & \xrightarrow{F(\varphi)} & F(S') \end{array}$$

This construction gives a **functor** F from the category of Sets to the category of Groups:

$$\begin{aligned} F : \underline{\text{Sets}} &\to \underline{\text{Gps}} \\ S &\rightsquigarrow F(S) \\ (\varphi : S \to S') &\rightsquigarrow (F(\varphi) : F(S) \to F(S')) \end{aligned}$$

To verify F is a functor, we need to check two conditions:

1. **Identity:** $F(\mathrm{Id}_S) = \mathrm{Id}_{F(S)}$ for all sets S.
2. **Composition:** For $\psi : S' \to S''$ and $\varphi : S \to S'$,

$$F(\psi) \circ F(\varphi) = F(\psi \circ \varphi)$$

Consider the following diagram consisting of two adjacent squares:

$$\begin{array}{ccccc} S & \xrightarrow{\varphi} & S' & \xrightarrow{\psi} & S'' \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle\iota'} & & \downarrow{\scriptstyle\iota''} \\ F(S) & \xrightarrow{F(\varphi)} & F(S') & \xrightarrow{F(\psi)} & F(S'') \end{array}$$

- By the definition of $F(\varphi)$ and $F(\psi)$, both the left square and the right square are commutative. This implies the outer rectangle is also commutative.
- By the uniqueness part of the universal property for $F(S)$, the composition $F(\psi) \circ F(\varphi)$ must be the unique homomorphism that satisfies the defining property of $F(\psi \circ \varphi)$.
- Therefore, $F(\psi) \circ F(\varphi) = F(\psi \circ \varphi)$.

Remark. In particular, since F is a functor, if φ is a bijection, then $F(\varphi)$ is a group isomorphism, this states that $F(S)$ **only depends on the cardinarlity** of S **up to isomorphism**.

> **Notation.** So we denote $F_n = F(S)$, when $\#S = n$.

Theorem 3.3.1. (Schreier) Every subgroup of a free group is again free.

3.3.2 Presentations of Groups by Generators and Relations

The question is raised naturally from the universal property of free groups.

Given a group G and a subset $S \subseteq G$. By the universal property of $F(S)$, there exists a unique group homomorphism

$$\begin{aligned} f : F(S) &\to G \\ f|_S &= \text{ the inclusion map} \end{aligned}$$

Since $\mathrm{Im}(f) = \langle S \rangle$ since $F(S)$ is generated by S, in particular, if S generates G, f is surjective.

The question is: **How to describe the kernel of it?** If we can describe its kernel, we can construct isomorphism through isomorphism theorem.

Definition 3.3.3. (Normal Closure) Given a group G and a subset A, the normal closure of A is the **smallest normal subgroup** of G containing A.

$$\bigcap_{A \subseteq H, H \leq G} H$$

Also one can show that the normal closure of A is

$$\langle \{ gag^{-1} \mid g \in G,\ a \in A \} \rangle$$

Given A, if N is the normal closure of A, may consider $G \,/\, N$ is the "largest" quotient of G in which the elements of A is **identity**.

Definition 3.3.4. (presentation) A presentation of a group G is a pair $(S, \mathfrak{R})$ where S is a set, $\mathfrak{R} \subseteq F(S)$, such that if N is the normal closure of $\mathfrak{R}$ in $F(S)$, then:

$$F(S) \Big/ N \cong G$$

Intuition. S as generator and $\mathfrak{R}$ as the relation, so there is no redundant relation by the normal closure, thus we have an isomorphism.

Example. If $n \geq 3$, then D_{2n} has a presentation with

$$S = \{\sigma, \tau\}$$
$$\mathfrak{R} = \{\sigma^n, \tau^2, \tau\sigma^{-(n-1)}\tau\sigma\}$$

usually written as:

$$D_{2n} = \{\sigma, \tau \mid \sigma^n = e,\ \tau^2 = e,\ \tau\sigma = \sigma^{n-1}\tau\}$$

Proof. Let N be the normal closure of $\mathfrak{R} \subseteq F(\{\tau, \sigma\})$, it is clear:

$$\begin{aligned} &\text{if } F(\{\tau,\sigma\}) \overset{\varphi}{\twoheadrightarrow} D_{2n} \\ &\quad \text{and } \mathfrak{R} \subseteq \ker(\varphi) \\ &\quad \Rightarrow N \subseteq \ker(\varphi) \end{aligned}$$

We get a group homomorphism which is also surjective:

$$F(\{\tau,\sigma\}) \Big/ N \overset{\overline{\varphi}}{\twoheadrightarrow} D_{2n}$$

By the relation $\tau\sigma^{-(n-1)}\tau\sigma$, every element in $F(\{\tau,\sigma\}) \,/\, N$ will be in the form $\sigma^i\tau^j$. By the relation $\sigma^n,\ \tau^2$, may assume $i \in [\![0, n-1]\!],\ j \in [\![0, 1]\!]$, then we have $\leq 2n$ elements in $F(\{\tau,\sigma\}) \,/\, N$, then it has to be injection and thus bijection, thus be an isomorphism. ■

Definition 3.3.5. A group G is finitely presented if there exists presentation $(S, \mathfrak{R})$ of G with both $\mathfrak{R}, S$ finite.

Note.

1. In general, finite generated $\not\Rightarrow$ finite presented.
2. Know that given $(S_1, \mathfrak{R}_1)$, $(S_2, \mathfrak{R}_2)$, figuring out whether:

$$F(S_1)\Big/_{N_1} \cong F(S_2)\Big/_{N_2}$$

is **undecidable**. (very hard, no algorithm to do)

Theorem 3.3.2. Every finite group is finitely presented.

Proof. Let G be finite group, take $S = G$ and $\mathfrak{R} = \{g_1 g_2 g_3^{-1} \in F(G) \mid g_3 = g_1 g_2,\ g_1, g_2, g_3 \in G\}$

Note. Note that $g_1 g_2 g_3^{-1}$ is in $F(G)$ not G, so there is really no inverse cancellation. The relation here is intended to **go through all multiplication combination**, and for each pair of (g_i, g_j), we have $g_k = g_i \cdot g_j$ in G, and thus we construct a word by such three **alphabet** as $g_i g_j g_k^{-1}$.

May consider the map:

$$\begin{aligned} \varphi : F(G) &\to G \\ \varphi|_G &= Id\ (g_i \mapsto g_i) \end{aligned}$$

such is clearly surjective, with the left hand side is the alphabet and the right hand side is the corresponding group element.

By construction, clear that $\mathfrak{R} \subseteq \ker(\varphi)$, let N be normal closure of $\mathfrak{R}$ in $F(G)$, then $N \subseteq \ker(\varphi)$, so

$$\exists!\ \overline{\varphi} :\ F(G)\Big/_{N} \to G$$

such that:

$$\begin{array}{ccc} F(S) & \xrightarrow{\pi} & F(S)/N \\ {\scriptstyle\varphi}\downarrow & \swarrow_{\overline{\varphi}} & \\ G & & \end{array}$$

by the universal property of quotient.

Now let $A = \{\pi(g) \mid g \in G\}$, see that:

$$\left.\begin{array}{l} \langle A \rangle = F(G)\,/\,N \text{ since } \langle g \mid g \in G \rangle = F(g) \\ \underbrace{A \text{ is } \textbf{closed} \text{ under multiplication and inverses}}_{A \text{ itself is a group, so it equals to its generator}} \end{array}\right\} \Rightarrow A = F(G)\Big/_{N}$$

thus:

$$\left.\begin{array}{l} |F(G)\,/\,N| \leq |G| \\ \overline{\varphi} \text{ surjective} \end{array}\right\} \Rightarrow \overline{\varphi} \text{ is isomorphism.}$$

■

Appendix