Jordan-Hölder theorem, simplicity of alternating group, and finitely generated abelian groups

Theorem (Jordan-Hölder)

Let G be a group. Suppose that we are given two composition series

$$\{e\} = A_0 \triangleleft A_1 \triangleleft \cdots \triangleleft A_m = G \text{ and } \{e\} = B_0 \triangleleft B_1 \triangleleft \cdots \triangleleft B_n = G$$

$$(\text{s.t. } A_i/A_{i-1} \text{ \& } B_j/B_{j-1} \text{ are simple})$$

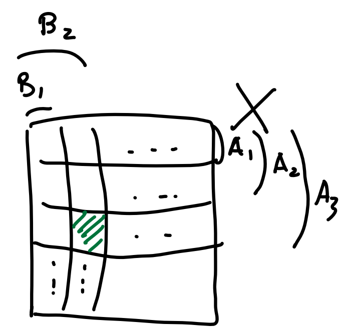
Then $m=n$, and there is a bijection $\sigma : \{1, \cdots, m\} \xrightarrow{\sim} \{1, \cdots, m=n\}$ s.t.

$$A_i/A_{i-1} \simeq B_{\sigma(i)}/B_{\sigma(i)-1}.$$

(Will prove a stronger version of J-H Theorem)

Toy model:

	Set theory	vs.	Group theory
	A		G
	$A \subseteq B$		$H \leq G$
	$B \setminus A$ complement set		G/H



Set theoretic version: Let X be a set with two filtrations

$$\phi = A_0 \subseteq A_1 \subseteq \cdots \subseteq A_m = X, \quad \phi = B_0 \subseteq B_1 \subseteq \cdots \subseteq B_n = X$$

then for any i, j, $\left(A_{i-1} \cup (A_i \cap B_j)\right) \setminus \left(A_{i-1} \cup (A_i \cap B_{j-1})\right)$

$$= \left(B_{j-1} \cup (A_i \cap B_j)\right) \setminus \left(B_{j-1} \cup (A_{i-1} \cap B_j)\right)$$

Group theoretic version: Let G be a group (not necessarily finite)

Suppose given two chains of subgroups: $\{e\} = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_m = G$

$$\{e\} = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_n = G$$

Then $A_{i-1}(A_i \cap B_{j-1})$ is a normal subgroup of the group $A_{i-1}(A_i \cap B_j)$

$B_{j-1}(A_{i-1} \cap B_j)$ is a normal subgroup of the group $B_{j-1}(A_i \cap B_j)$

Moreover, $$\frac{A_{i-1}(A_i \cap B_j)}{A_{i-1}(A_i \cap B_{j-1})} \simeq \frac{B_{j-1}(A_i \cap B_j)}{B_{j-1}(A_{i-1} \cap B_j)}.$$

• <u>Group version $\Rightarrow$ Jordan-Hölder theorem</u>:

Given the two composition series, the group version thm refines them into chains

$$\{e\} \trianglelefteq \underbrace{A_1 \cap B_1 \trianglelefteq A_1 \cap B_2 \trianglelefteq \cdots \trianglelefteq A_1 \cap B_n}_{\text{exactly one is nontriv, say } A_1 \cap B_{\sigma(1)}} = A_1 \trianglelefteq \underbrace{A_1(A_2 \cap B_1) \trianglelefteq A_1(A_2 \cap B_2) \trianglelefteq}_{\text{exactly one nontriv, say } A_2 \cap B_{\sigma(2)}} \cdots \trianglelefteq A_m \cap B_n = G$$

$$\{e\} \trianglelefteq \underbrace{A_1 \cap B_1 \trianglelefteq A_2 \cap B_1 \trianglelefteq \cdots \trianglelefteq A_m \cap B_1}_{\text{exactly one nontriv, must be } A_{\sigma^{-1}(1)} \cap B_1} = B_1 \trianglelefteq B_1(A_1 \cap B_2) \trianglelefteq \cdots\cdots \trianglelefteq A_m \cap B_n = G$$

This shows $m = n$ and $$\frac{A_i}{A_{i-1}} \cong \frac{A_{i-1}(A_i \cap B_{\sigma(i)})}{A_{i-1}(A_i \cap B_{\sigma(i)-1})} \cong \frac{B_{\sigma(i)-1}(A_i \cap B_{\sigma(i)})}{B_{\sigma(i)-1}(A_{i-1} \cap B_{\sigma(i)})} \cong \frac{B_{\sigma(i)}}{B_{\sigma(i)-1}} \quad \square$$

• <u>Proof of the group version</u>:

Inside A_i, A_{i-1} is normal and $A_i \cap B_{j-1}$ is a subgroup

$\Rightarrow A_{i-1}(A_i \cap B_{j-1})$ is a subgroup of A_i

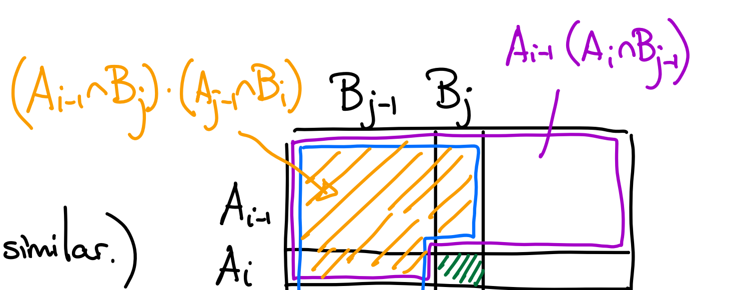
Moreover, $B_{j-1} \trianglelefteq B_j \Rightarrow A_i \cap B_{j-1} \trianglelefteq A_i \cap B_j$

<u>Claim</u>: $\underset{a}{A_{i-1}} \, \underset{b}{(A_i \cap B_{j-1})} \trianglelefteq \underset{\alpha}{A_{i-1}} \, \underset{\beta}{(A_i \cap B_j)}$

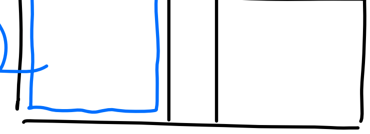
<u>Check</u>: $\alpha\beta \cdot ab \cdot (\alpha\beta)^{-1} = \alpha\beta a b \beta^{-1} \alpha^{-1} = \underbrace{\alpha}_{\text{in } A_{i-1}} \cdot \underbrace{(\beta a \beta^{-1})}_{\substack{\text{in } A_{i-1} \\ \text{b/c } \beta \in A_i \\ \text{normalizes } A_{i-1}}} \underbrace{(\beta b \beta^{-1})}_{\text{in } A_i \cap B_{j-1}} \underbrace{\alpha^{-1}}_{\text{in } A_{i-1}}$. ✓

<u>Key</u>. $$\frac{A_i \cap B_j}{(A_{i-1} \cap B_j)(A_i \cap B_{j-1})} \overset{?}{\cong} \frac{A_{i-1}(A_i \cap B_j)}{A_{i-1}(A_i \cap B_{j-1})}$$

(the other isom with $\frac{B_{j-1}(A_i \cap B_j)}{B_{j-1}(A_{i-1} \cap B_j)}$ is similar.)



<u>Note</u>: $\varphi : A_i \cap B_j \longrightarrow A_{i-1}(A_i \cap B_j) \longrightarrow \dfrac{A_{i-1}(A_i\cap B_j)}{A_{i-1}(A_i \cap B_{j-1})}$ $B_{j-1}(B_j \cap A_{i-1})$



is clearly a <u>surjective</u> homomorphism.

$$\ker\varphi = A_i \cap B_j \cap \big(\underset{\underset{a}{\cup}}{A_{i-1}}\,(\underset{\underset{b}{\cup}}{A_i \cap B_{j-1}})\big)$$

$\rightsquigarrow ab \in B_j \Rightarrow a \in B_j$ So $\ker\varphi \subseteq (A_{i-1}\cap B_j)\cdot(A_i \cap B_{j-1})$

The reversed inclusion is also clear.

By 1st isom theorem, we deduce $\dfrac{A_i \cap B_j}{(A_{i-1}\cap B_j)(A_i\cap B_{j-1})} \overset{\bar\varphi}{\cong} \dfrac{A_{i-1}(A_i\cap B_j)}{A_{i-1}(A_i\cap B_{j-1})}$

<u>Alternating Group</u>.

One example of composition series is $\{e\} \subseteq A_n \overset{2}{\subseteq} S_n$ for $n \geq 5$

<u>Recall</u>. Every cycle $(a_1 a_2 \cdots a_m)$ in S_n is a product of transpositions

$$(a_1 a_2 \cdots a_m) = (a_1, a_m)(a_1, a_{m-1}) \cdots (a_1, a_2)$$

So every elements of S_n is a product of transpositions

Consider $\Delta := \prod_{1\leq i<j\leq n} (x_i - x_j)$, $\sigma(\Delta) := \prod_{1\leq i<j\leq n} (x_{\sigma(i)} - x_{\sigma(j)}) = \pm\Delta$

For each $\sigma \in S_n$, define $\operatorname{sgn}\sigma \in \{\pm 1\}$ so that $\sigma(\Delta) = \operatorname{sgn}(\sigma)\cdot\Delta$

call $\operatorname{sgn}(\sigma)$ the <u>sign</u> of σ $\rightsquigarrow$ σ is called an <u>even permutation</u> (偶置換) if $\operatorname{sgn}(\sigma)=1$

<u>odd permutation</u> (奇置換) if $\operatorname{sgn}(\sigma) = -1$

<u>Proposition</u> $\operatorname{sgn}: S_n \longrightarrow \{\pm 1\}$ is a homomorphism.

Proof: $\operatorname{sgn}(\sigma\tau) = \dfrac{\prod_{1\leq i<j\leq n}(x_{\sigma\tau(i)} - x_{\sigma\tau(j)})}{\cdots}$

$$\operatorname{sgn}(\sigma\tau) = \frac{\cdots}{\prod_{1\le i<j\le n}(x_i - x_j)}$$

$$\operatorname{sgn}(\sigma)\cdot\operatorname{sgn}(\tau) = \frac{\prod_{1\le i'<j'\le n}(x_{\sigma(i')} - x_{\sigma(j')})}{\prod_{1\le i'<j'\le n}(x_{i'} - x_{j'})} \cdot \frac{\cancel{\prod_{1\le i<j\le n}(x_{\tau(i)} - x_{\tau(j)})}}{\prod_{1\le i<j\le n}(x_i - x_j)}$$

$$\| \; i' = \tau(i),\ j' = \tau(j)$$

$$\frac{\prod_{1\le i<j\le n}(x_{\sigma\tau(i)} - x_{\sigma\tau(j)})}{\cancel{\prod_{1\le i<j\le n}(x_{\tau(i)} - x_{\tau(j)})}}$$

Note: $\operatorname{sgn}(\text{transposition}) = -1$

So if $\sigma =$ product of r transpositions $\Rightarrow \operatorname{sgn}(\sigma) = (-1)^r$

Definition $A_n = \ker(\operatorname{sgn}: S_n \to \{\pm 1\})$ is called the alternating group (交错群)

- $A_n \triangleleft S_n$ and $S_n / A_n \cong \{\pm 1\}$

$\Rightarrow \# A_n = \# S_n / \# \{\pm 1\} = \frac{1}{2} n!$

Theorem When $n \geq 5$, A_n is a simple group.

Remark: $A_3 = \langle (123) \rangle$ is a cyclic group of order 3.

$A_4 \trianglerighteq \{1, (12)(34), (13)(24), (14)(23)\}$

It is known that a simple group of order 60 is isomorphic to A_5.

Proof: Call (ijk) a 3-cycle (for i, j, k distinct) $\qquad (ijk) \in A_n$

Frequently used observation: if $\sigma \in S_n$, then

$$\sigma (a_1 a_2 \cdots a_t) \sigma^{-1} = (\sigma(a_1)\sigma(a_2) \cdots \sigma(a_t))$$

b/c $\sigma(a_i) \xmapsto{\sigma^{-1}} a_i \longmapsto a_{i+1} \xmapsto{\sigma} \sigma(a_{i+1})$

Step 1: A_n is generated by 3-cycles

A_n is generated by elements of the form $(ab)(cd)$ and $(ab)(ac)$

Yet $(ab)(cd) = (acb)(acd)$ and $(ab)(ac) = (acb)$

Step 2: If $N \trianglelefteq A_n$ contains one 3-cycle, then N contains all 3-cycles

Will show: $\forall \sigma \in S_n$, $(\sigma(i)\,\sigma(j)\,\sigma(k)) \in N$.

- If $\sigma \in A_n$, then $\sigma(i\,j\,k)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k)) \in N$

If $\sigma \notin A_n$, then $\sigma\cdot(ij) \in A_n$

$$\Rightarrow \sigma(ij)(ijk)(ij)\sigma^{-1} \in N$$

$$\| $$

$$\sigma(jik)\sigma^{-1} = (\sigma(j)\sigma(i)\sigma(k))$$

$$\Rightarrow (\sigma(j)\,\sigma(i)\,\sigma(k))^2 = (\sigma(i)\sigma(j)\sigma(k)) \in N$$

Step 3. If $\{e\} \neq N \trianglelefteq A_n$, then N contains a 3-cycle.

Fix $e \neq \sigma \in N$.

(1) If σ is the product of disjoint cycles, at least one cycle has length ≥ 4.

i.e. $\sigma = \mu \cdot (a_1 a_2 \cdots a_r)$ with $r \geq 4$

$$\Rightarrow (a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} = \mu(a_2 a_3 a_1 a_4 \cdots a_r) \in N$$

So $\sigma^{-1} \circ (a_1 a_2 a_3)\sigma(a_1 a_2 a_3)^{-1} \in N$ is

$$\begin{array}{ccccccc} a_1 & a_2 & a_3 & a_4 & \cdots & a_r & \\ a_4 & a_3 & a_1 & a_5 & \cdots & a_1 & \big) \ (a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \\ a_3 & a_2 & a_r & a_4 & \cdots & a_r & \big) \ \sigma \end{array}$$

So $(a_1 a_3 a_r) \in N$.

(2) Suppose (1) doesn't hold $\Rightarrow \sigma$ is a product of disjoint cycles of length 2 and 3.

$$\Rightarrow \begin{cases} \sigma^3 \text{ is a product of disjoint transpositions} \\ \sigma^2 \text{ ———————— 3-cycles} \end{cases} \text{ and } \sigma^2, \sigma^3 \text{ can't be all trivial.}$$

(3) If σ is a product of disjoint transpositions

$\sigma = \mu(a_1 a_2)(a_3 a_4)$ (b/c we have at least 2 transpositions) then $(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1}\sigma^{-1} = (a_1a_3)(a_2a_4) =: \sigma' \in N$

Next, we use $n \geq 5$ to take $a_5 \in \{1, \cdots, n\}$ different from $a_1, \cdots, a_4$

then $(a_1a_2a_5)\sigma'(a_1a_2a_5)^{-1}\sigma'^{-1} = (a_1a_2a_5a_4a_3) \in N$ Back to (1)

(4) If σ is a product of disjoint 3-cycles, similar arguement to go back to (1).

Definition Let I be an index set and let G_i (for $i \in I$) be a group (with operator $\star_i$)

Define the direct product (直积) of $(G_i)_{i\in I}$, denoted by $\prod_{i\in I} G_i =: G$

(or $G_1 \times \cdots \times G_n$ if $I = \{1, \cdots, n\}$)

to be the group with operation $(g_i)_{i\in I} \star (h_i)_{i\in I} = (g_i \star_i h_i)_{i\in I}$

The identity is $(e_i)_{i\in I}$ and the inverse of $(g_i)_{i\in I}$ is $(g_i^{-1})_{i\in I}$

· For each $j \in I$, there is a nature embedding $G_j \hookrightarrow G$

"injective homomorphism" $g_j \longmapsto (1, \cdots, g_j, \cdots)$ (jth place)

realizing G_j as a normal subgroup of G

& $G/G_j \cong \prod_{i\in I\setminus\{j\}} G_i$

There's also a natural projection $\pi_j : G \to G_j$

"surjective homomorphism" $(g_i)_{i\in I} \mapsto g_j$

$\ker(\pi_j) \cong \prod_{i\in I\setminus\{j\}} G_i$

When all G_i's are isomorphic to H and $I = \{1, \ldots, n\}$, write H^n instead

Recall. A group G is finitely generated if there's a finite subset A of G s.t. $G = \langle A \rangle$

Theorem (Fundamental Theorem of finitely generated abelian groups)

Let G be a finitely generated abelian group.

divides

divides

Then $G = \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ for integers $r \geq 0$, $2 \leq n_1 \mid n_2 \mid \cdots \mid n_s$

Moreover, such $r, n_1, \ldots, n_s$ are unique

r called the rank (秩) of G

Proof: Abelian groups = $\mathbb{Z}$-modules

Follows from the classification of modules over PID (Later in semester)

Lemma. If $m, n \in \mathbb{N}_{\geq 2}$ satisfies $\gcd(m,n) = 1$, then $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$

Proof: Consider $\varphi: \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ homomorphism

$$a \bmod mn \longmapsto (a \bmod m,\ a \bmod n)$$

$$\ker\varphi = \left\{ a \bmod mn \;\middle|\; \begin{matrix} a \equiv 0 \bmod m \\ a \equiv 0 \bmod n \end{matrix} \right\} = \{0\}$$

$\Rightarrow \varphi$ is injective

But $\#\mathbb{Z}_{mn} = \#(\mathbb{Z}_m \times \mathbb{Z}_n)$ So φ is an isomorphism.

Cor. Every finitely generated abelian group is of the form

$$G = \mathbb{Z}^r \times (\mathbb{Z}_{p_1^{r_{11}}} \times \cdots \times \mathbb{Z}_{p_1^{r_{1s_1}}}) \times (\mathbb{Z}_{p_2^{r_{21}}} \times \cdots$$

r and p_i, r_{ij} are uniquely determined.

Example: $\mathbb{Z}_{30} \times \mathbb{Z}_{100} \overset{?}{\simeq} \mathbb{Z}_{60} \times \mathbb{Z}_{50}$

Proof: $\mathbb{Z}_{30} \times \mathbb{Z}_{100} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$

$\mathbb{Z}_{60} \times \mathbb{Z}_{50} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25} \times \mathbb{Z}_2$ They are isomorphic

Example: List all abelian groups of order $72 = 8 \times 9$

	$\mathbb{Z}_2^3$	$\mathbb{Z}_2 \times \mathbb{Z}_4$	$\mathbb{Z}_8$
$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_2^3 \times \mathbb{Z}_3^2$	...	...
$\mathbb{Z}_9$			