Lecture 14: Nilpotent groups, Simplicity of A_n for $n \geq 5$

Recall: Last time we defined nilpotent groups & characterize solvable gps

§1. Nilpotent groups:

- Lower central series

$$G = C^1(G) \triangleleft C^2(G) \triangleleft \cdots \triangleleft C^n(G) \triangleleft C^{n+1}(G) \triangleleft \cdots$$

where $C^1(G) = G$

$$C^{n+1}(G) = (G, C^n(G)) \quad \forall n \geq 1 \qquad (\triangleleft G \text{ if } C^n(G) \triangleleft G)$$

Definition: G is nilpotent if $\exists\, n \geq 1$ such that $C^n(G) = \{e\}$.

Equivalently, $\mathcal{C}$ is a composition series for G.

Examples (1) $G = \mathbb{Z}/6\mathbb{Z}$, $\quad C^2(G) = (G, G) = 1$ (G abelian)

(2) $G = D_n \qquad C^2(G) = \langle \rho^2 \rangle$

$$C^3(G) = (G, \langle \rho^2 \rangle) = \langle [s\rho^i, \rho^{2j}] : \begin{smallmatrix} i = 0, \ldots, n-1 \\ j = 0, \ldots, n-1 \end{smallmatrix} \rangle = \langle \rho^4 \rangle$$

$$s\rho^i \rho^{2j} (s\rho^i)^{-1} \rho^{-2j} = s\rho^{2j} s \rho^{-2j} = \rho^{-4j}$$

$$C^4(G) = (G, \langle \rho^4 \rangle) = \langle \rho^8 \rangle$$

By induction: $\quad C^{m+1}(G) = \langle \rho^{2^m} \rangle \quad \forall\, m \geq 1.$

Conclude: D_n is nilpotent if and only if n is a power of 2.

Remarks: $\mathcal{C}$ satisfies the following properties:

(1) $(G, C^n(G)) = C^{n+1}(G) \quad \forall n \qquad C^{n+1}(G) \triangleleft C^n(G)$

(2) $C^n(G) / C^{n+1}(G)$ is abelian $\forall n$

(because $(C^n(G), C^n(G)) \subseteq (G, C^n(G)) = C^{n+1}(G)$. ✓)

(3) $C^2(G) = (G,G) = D^1(G)$

(4) $(C^n(G), C^m(G)) \subset C^{n+m}(G)$ (Exercise HW5)

$\Rightarrow D^\ell(G) \subseteq C^{2^\ell}(G)$ for all $\ell \geq 0$.

Pf/ True for $\ell=0$ & $\ell=1$.

$$D^{\ell+1}(G) = (D^\ell(G), D^\ell(G)) \subseteq (C^{2^\ell}(G), C^{2^\ell}(G)) \subseteq \underset{\displaystyle \overset{\parallel}{C^{2^{\ell+1}}(G)}}{C^{2^\ell+2^\ell}(G)}$$

Corollary: Nilpotent $\Rightarrow$ Solvable

⚠ Solvable $\not\Rightarrow$ Nilpotent (eg D_3 is solvable but not nilpotent)

Nilpotent groups can be characterized by having composition series with special graded pieces, as we did with solvable. This is the content of the next theorem.

Theorem 1: G is nilpotent if and only if it has a composition series

$$\Sigma: G = G_0 \geq G_1 \geq \cdots\cdots \geq G_n = \{e\}$$

with (1) $gr_j^\Sigma(G) = G_j/G_{j+1}$ is abelian $\forall j=0,\ldots,n-1$

(2) $(G, G_j) \subset G_{j+1}$ $\forall j=0,\ldots,n-1$.

Remark: (2) $\Rightarrow$ (1) because $(G_j, G_j) \subset (G, G_j) \underset{(2)}{\subseteq} G_{j+1}$ forces G_j/G_{j+1} to be abelian.

Proof of Thm 1 ($\Rightarrow$) Take $G_j = C^{j-1}(G)$ from lower central series.

($\Leftarrow$) It's enough to check the following

Claim: $C^{j+1}(G) \subseteq G_j$ $\forall j=0,\ldots,n$ ($\Rightarrow C^{n+1}(G) \subseteq \{e\}$, so $C^{n+1}(G) = \{e\}$)

Pf/ By induction on j:

- <u>Base case</u>: $j=0$. $C^1(G) = G = G_0$.
- <u>Inductive step</u>: Fix $j>0$ & assume $C^j(G) \subseteq G_{j-1}$.

$$C^{j+1}(G) = (G, C^j(G)) \underset{IH}{\subseteq} (G, G_{j-1}) \underset{(2)}{\subseteq} G_j$$

□

Proposition:

① Subgroups and quotients of nilpotent groups are nilpotent

[Same proof as for solvable groups (see Lecture 13)]

② G is nilpotent if and only if there is a subgroup $A \subset Z(G)$ with G/A nilpotent.

<u>Proof</u>: We only need to show ($\Leftarrow$). Consider $\pi: G \twoheadrightarrow G/A$ ($A \triangleleft G$ because $A \subset Z(G)$) pick n with $C^n(G/A) = \{e\}$

<u>Claim</u>: $\pi(C^k(G)) = C^k(G/A)$ $\forall k$

<u>Proof</u>: By induction on k.

- <u>$k=1$</u>: $\pi(G:G) = (\pi(G):\pi(G))$
- <u>Inductive Step</u>: $C^{k+1}(G) = (G : C^k(G))$ so

$$\pi(C^{k+1}(G)) = (\pi(G) : \pi(C^n(G))) \underset{[IH]}{=} \left(\frac{G}{A} : C^n(G/A)\right) = C^{n+1}(G/A))$$

Then, $\pi(C^n(G)) \overset{(*)}{=} C^n(G/A) = \{e\} \underset{\ker\pi = A}{\Longrightarrow} C^n(G) \subset A$

By $A \subset Z(G)$ so $C^{n+1}(G) = (G:A) = \{e\}$.

□

⚠ The last statement fails if A is not included in $Z(G)$, ie $1 \to G_1 \to G_2 \to G_3 \to 1$ ses & G_1, G_3 nilpotent

$\not\Longrightarrow$ G_2 is nilpotent.

Example: $G_2 = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{C}^\times \; b \in \mathbb{C} \right\}$

$\cup$

$G_2 \underset{[HW3]}{\rhd} G_1 = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{C} \right\} \simeq \mathbb{C}$

$G_2/G_1 = \mathbb{C}^\times \times \mathbb{C}^\times$ (diagonal entries)

- G_1 & G_2/G_1 are nilpotent (see HW5)
- G_2 is solvable but not nilpotent

Corollary: Every p-group is nilpotent.

Proof By induction on $k \geq 1$ with $|G| = p^k$.

- Clear for $k=1$: $G \simeq \mathbb{Z}/p\mathbb{Z}$ so abelian, hence nilpotent
  $(C^2(G) = (G:G) = \{e\})$
- Induction Step:

We know $Z(G) \neq \{e\}$ so $Z(G) = p^s$ $1 \leq s \leq k$

CASE 1 If $G = Z(G)$, then G is abelian, hence nilpotent

CASE 2 If $s < k$, then by inductive hypothesis: $Z(G)$ is nilpotent & $|G/Z(G)| = p^{k-s}$ $k-s<k$, so also nilpotent.

By Proposition 2, G is nilpotent. $\square$

In fact, more is true: the only nilpotent groups are direct products of p-groups. The proof of this fact is a homework exercise, and depends on the following:

Lemma: Let G be a nilpotent group & $H \lneq G$. Then:

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

Proof: Since G is nilpotent, the lower central series satisfies,

$$G = G_0 \supseteq G_1 \supseteq \cdots\cdots \supseteq G_n = \{e\}$$

with $(G, G_j) \subset G_{j+1}$ & $G_j \triangleleft G$ $\forall j$.

[HW 5] If $N_1, N_2 \triangleleft G$ & $(G : N_1) \subset N_2 \subset N_1$ $\Rightarrow$ for all $H < G$ we have $N_2 H \triangleleft N_1 H$.

Since $(G; G_j) \subset G_{j+1} \subset G_j$ then $G_{j+1} H \triangleleft G_j H$ $\forall j$

We get $G = G_0 H \supseteq G_1 H \supseteq \cdots\cdots \supseteq G_n H = H$.

Fix k to be the largest index with $G_k H \supsetneq G_{k+1} H = H$

Then $H \trianglelefteq G_k H$ and hence $N_G H \supset G_k H \neq H$ as we wanted.

§2 Simplicity of A_n for $n \geq 5$

Recall A_n = group of even permutations.

It was defined as the kernel of the sign morphism $S_n \longrightarrow \{\pm 1\}$

$$\sigma \longmapsto (-1)^{\ell(\sigma)}$$

(This map was unique defined by $\operatorname{sign}((ab)) = -1$ $\forall a \neq b$.)

Examples $A_2 = \{e\}$, $A_3 \simeq \mathbb{Z}/3\mathbb{Z} = \langle (123) \rangle$

$A_4 = \langle (123), (12)(34) \rangle$

Lemma 1: For $n \geq 3$: A_n is generated by 3 cycles.

Obs: $(12)(34) = (12)(13)(13)(34) = (132)(341)$

Proof: Since $(abc) = (ab)(bc)$ is even, we have that

$$\langle \sigma : \sigma \text{ is a 3-cycle} \rangle \subseteq A_n.$$

To finish, we must show that every even permutation is a product of 3 cycles. We do so by arguing $\sigma \in A_n$ is a product of an even number of transpositions. We group them in parts & analyze the various options:

- $(ac)(ac) = e$
- $(ac)(ab) = (abc)$
- $(ab)(cd) = (abc)(bcd)$ $\square$

Lemma 2: For $n \geq 5$: all 3-cycles in S_n are conjugate to each other in A_n, ie if σ, σ' are 3-cycles, there exists $\tau \in A_n$ with $\tau\sigma\tau^{-1} = \sigma'$

Proof: Let $(a_1\, a_2\, a_3)$ & $(b_1\, b_2\, b_3)$ be two 3-cycles. We know that $\exists\, \gamma \in S_n$ st $\gamma(a_1\, a_2\, a_3)\gamma^{-1} = (b_1\, b_2\, b_3)$

(Pick $\gamma \in S_n$ with $\gamma(a_i) = b_i$ for $i = 1,2,3$)

If γ is even, there is nothing to prove. If γ is odd, pick $c, d \notin \{b_1, b_2, b_3\}$ with $c \neq d$ (they exist because $n \geq 5$)

Then: $\underbrace{(cd)\gamma}_{\in A_n} (a_1 a_2 a_3) \underbrace{\gamma^{-1}(cd)}_{=((cd)\gamma)^{-1} \in A_n} = (b_1 b_2 b_3)$ $\square$

Theorem 2: A_n is simple for $n \geq 5$.

Proof: Pick $K \triangleleft A_n$ with $K \neq \{id\}$. We will show that $K = A_n$ by finding a 3-cycle in it. Lemma 2 will then imply

$A_n \underset{\substack{\uparrow \\ \text{by Lemma 1}}}{=} \langle \sigma : \sigma \text{ is a 3-cycle} \rangle \subset K$ (because $K \triangleleft A_n$)

- Pick $\sigma \in K \setminus \{e\}$ with $\overset{X}{\overset{/\!/}{X^\sigma}} = \{x \in \{1, \dots n\} : \sigma(x) = x\}$ has maximum cardinality.

Claim: σ is a 3-cycle.

Pf/ Write σ as a product of disjoint cycles $\sigma = (a_1, a_2, a_3 \cdots) \cdots\cdots$

We analyze 2 cases

CASE 1 Assume σ has a cycle of length ≥ 3 in its decomposition.

If $\sigma = (a_1\, a_2\, a_3)$ we are done. Otherwise we can find a_4, a_5 with

$$\begin{cases} \cdot\ a_4 \neq a_5 \\ \cdot\ a_4, a_5 \notin \{a_1, a_2, a_3\} \\ \cdot\ \sigma(a_4) \neq a_4 \quad \& \quad \sigma(a_5) \neq a_5 \end{cases}$$

Let $\tau = (a_3, a_4, a_5)$ & $\sigma' = \underbrace{\tau\sigma\tau^{-1}}_{\in K}\sigma^{-1} \in K$. Then:

$$\left.\begin{array}{l} ① \ X^{\sigma'} \supset X^{\sigma} \\ ② \ a_2 \in X^{\sigma'}, \quad a_2 \notin X^{\sigma} \end{array}\right\} \Rightarrow |X^{\sigma'}| \gneq |X^{\sigma}| \text{ Contra!}$$

Check: $\sigma'(a_2) = \tau\sigma\tau^{-1}\sigma^{-1}(a_2) = \tau\sigma\tau^{-1}(a_1) = \tau\sigma(a_1) = \tau(a_2) = a_2$ ✓

$\sigma(a_2) = a_3 \neq a_2$. ✓

If $\sigma(x) = x$, then $x \notin \{a_1, a_2, a_3, a_4, a_5\}$ by construction, so

$\sigma'(x) = \tau\sigma\tau^{-1}\sigma^{-1}(x) = \tau\sigma\tau^{-1}(x) = \tau\sigma(x) = \tau(x) = x$ ✓

CASE 2: All cycles in σ have length ≤ 2.

Write $\sigma = (a b)(c d) \cdots\cdots$ (we have at least 2 transpositions because $K \subset A_n$ & $\sigma \neq id$.) Pick $k \notin \{a, b, c, d\}$ (ok because $n \geq 5$). Then $\tau := (c\ d\ k)$ & $\sigma' := \tau\sigma\tau^{-1}\sigma^{-1} \in K$ satisfies:

$$\left.\begin{array}{l} ① \ X^{\sigma'} \supset X^{\sigma} \setminus \{k\} \\ ② \ a, b \in X^{\sigma'}, \quad a, b \notin X^{\sigma} \end{array}\right\} \Rightarrow |X^{\sigma'}| \gneq |X^{\sigma}| \text{ Contra!}$$

Check: $\cdot\ \sigma'(a) = \tau\sigma\tau^{-1}\sigma^{-1}(a) = \tau\sigma\tau^{-1}(b) = \tau\sigma(b) = \tau(a) = a$ ✓

- $\sigma'(b) = b$ by symmetry
- $\sigma(a) = b \quad \sigma(b) = a \quad \Rightarrow \quad a, b \notin X^{\sigma}$
- Pick $x \neq k$ with $\sigma(x) = x$. Then, $x \notin \{a, b, c, d, k\}$ & so

$$\sigma'(x) = \tau\sigma\tau^{-1}\sigma^{-1}(x) = \tau\sigma\tau^{-1}(x) = \tau\sigma(x) = \tau(x) = x. \quad \square$$