Lecture 10: An application of alternating group

Monday, October 29, 2018 11:08 PM

<u>Proposition</u>. Suppose m is a positive odd integer, and G is a group of order $2m$. Then G has a characteristic subgroup of order m.

<u>Lemma</u>. Let $\phi: G \to S_G$ be the group homomorphism associated with $G \curvearrowright G$ by left translations; that means $\phi(g)(g') := gg'$. Suppose $|G| < \infty$. Then the cycle type of $\phi(g)$ is $o(g) \geq \cdots \geq o(g)$ ($|G|/_{o(g)}$ - many times); in particular for any $\theta \in \mathrm{Aut}(G)$ $\phi(g)$ and $\phi(\theta(g))$ have the same cycle type.

<u>Pf</u>. Any orbit of $\langle g \rangle$ has $o(g)$-many elements as $G \curvearrowright G$ freely; and claim follows. For the 2^{nd} part, notice that $o(g) = o(\theta(g))$ for any $\theta \in \mathrm{Aut}(G)$. ∎

<u>Pf of proposition</u>. By Cauchy's theorem $\exists g \in G$, $o(g) = 2$. Then the cycle type of $\phi(g)$ is $\underbrace{2 \geq \cdots \geq 2}_{m \text{ times}}$; and so $\phi(g)$ is odd.

Let $H := \{ g \in G \mid \phi(g) \text{ is even} \} = \phi^{-1}(A_n)$. Then by the above lemma, H is a characteristic subgp. (Since the

Lecture 10: An example

Monday, October 29, 2018 11:22 PM

cycle types of $\Phi(h)$ and $\Phi(\theta(h))$ are the same, $\Phi(h)$ and $\Phi(\theta(h))$ have the same parity.) And Φ induce an injective group homomorphism $\bar{\Phi}: G/H \hookrightarrow S_n/A_n \simeq \{\pm 1\}$; and since $\bar{\Phi}(gH) = \Phi(g)A_n \neq 1$, $\bar{\Phi}$ is onto. Therefore $|H| = m$. ∎

In your HW, you will see a generalization of this.

Next we see how we can treat simple finite groups as building blocks of finite groups.

<u>Def</u>- A <u>composition series</u> of a group G is

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_k = G$$

such that N_i/N_{i-1} is a simple group for any integer i. For any i, N_i/N_{i-1} is called a <u>composition factor</u> of G.

<u>Def</u>. We say $(S_1, \ldots, S_m) \sim (S_1', \ldots, S_m')$ if they are the same sequence after a rearranging and applying isomorphisms.

Lecture 10: Jordan-Holder theorem

Monday, October 29, 2018 11:36 PM

<u>Theorem</u> (Jordan-Hölder) Suppose G is a finite group, $|G|>1$.

(a) G has a composition series.

(b) If $\{1\}=N_0 \triangleleft \cdots \triangleleft N_k = G$ and $\{1\}=M_0 \triangleleft \cdots \triangleleft M_s = G$ are two composition series of G, then $k=s$ and

$$\left(N_1/N_0, N_2/N_1, \dots, N_k/N_{k-1}\right) \sim \left(M_1/M_0, \dots, M_s/M_{s-1}\right).$$

<u>Pf.</u> (a) Among all chains $\{1\} =: N_0 \underset{\neq}{\trianglelefteq} N_1 \underset{\neq}{\trianglelefteq} \cdots \underset{\neq}{\trianglelefteq} N_k = G$, take one of the longest choices. Notice that, since G is a non-trivial finite group, there is such a chain.

<u>Claim</u>. For any i, N_i/N_{i-1} is simple; and so it is a composition series.

<u>Pf of claim</u>. If not, $\exists\ \{1\} \neq \overline{K} \underset{\neq}{\trianglelefteq} N_i/N_{i-1}$; this implies $\exists\ N_{i-1} \underset{\neq}{\triangleleft} K \underset{\neq}{\trianglelefteq} N_i$ (and $\overline{K} = K/N_{i-1}$); but then

$$1 = N_0 \underset{\neq}{\trianglelefteq} \cdots \underset{\neq}{\trianglelefteq} N_{i-1} \underset{\neq}{\triangleleft} K \underset{\neq}{\trianglelefteq} N_i \underset{\neq}{\trianglelefteq} \cdots \underset{\neq}{\trianglelefteq} N_k = G$$

is a longer chain, which is a contradiction.

Lecture 10: Jordan-Holder; uniqueness

Monday, October 29, 2018 11:46 PM

(b) We proceed by strong induction on $|G|$. The base case $|G|=2$ is clear. Suppose $\{1\}=:N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_r := G$ and $\{1\}=:M_0 \triangleleft \cdots \triangleleft M_s := G$ are two composition series.

<u>Case 1.</u> If $\underbrace{N_{r-1}}_{H} = M_{s-1}$, then $N_0 \triangleleft \cdots \triangleleft N_{r-1}$ and $M_0 \triangleleft \cdots \triangleleft M_{s-1}$ are two composition series of H. And $|H| < |G|$; hence by the strong induction hypothesis, $r-1 = s-1$ ① and

$$\left(N_1/N_0, \ldots, N_{r-1}/N_{r-2}\right) \sim \left(M_1/M_0, \ldots, M_{s-1}/M_{s-2}\right). \quad ②$$

As $N_r/N_{r-1} = G/H = M_s/M_{s-1}$, by ① and ② claim follows.

<u>Case 2.</u> Suppose $N_{r-1} \neq M_{s-1}$ and let $N := N_{r-1}$ and $M := M_{s-1}$.

Hence G/M and G/N are simple and $M \underset{\neq}{\triangleleft} MN \trianglelefteq G$. Therefore $MN/M \trianglelefteq G/M$, which implies $MN = G$. Moreover

$$\boxed{G/M = MN/M \simeq N/M\cap N \quad \text{and} \quad G/N = MN/N \simeq M/M\cap N.} \quad ③$$

In particular, these are simple groups. Let $1 = K_0 \triangleleft \cdots \triangleleft K_\ell = M\cap N$ be a composition series of $M\cap N$. Then by ③ the following are composition series:

Lecture 10: Jordan-Holder; uniqueness

Tuesday, October 30, 2018 12:03 AM

$1 = K_0 \lhd \cdots \lhd K_\ell \lhd M$ and $1 = M_0 \lhd \cdots \lhd M_{s-1} = M$;

$1 = K_0 \lhd \cdots \lhd K_\ell \lhd N$ and $1 = N_0 \lhd \cdots \lhd N_{r-1} = N$.

As $|M|, |N| < |G|$, by the strong induction hypothesis,

$\ell + 1 = s-1$ and $\ell+1 = r-1$; and

$$(M_1/M_0, \ldots, M_{s-1}/M_{s-2}) \sim (K_1/K_0, \ldots, K_\ell/K_{\ell-1}, \underbrace{M/M\cap N}_{\simeq G/N}) \text{ and}$$

$$(N_1/N_0, \ldots, N_{r-1}/N_{r-2}) \sim (K_1/K_0, \ldots, K_\ell/K_{\ell-1}, \underbrace{N/M\cap N}_{\simeq G/M}) .$$

Hence $(M_1/M_0, \ldots, M_s/M_{s-1}) \sim (K_1/K_0, \ldots, K_\ell/K_{\ell-1}, G/N, G/M)$

$$\sim (N_1/N_0, \ldots, N_r/N_{r-1}) . \quad \blacksquare$$

<u>Observation 1</u> If $(G_1, \ldots, G_\ell)$ are composition factors of G (with multiplicity), then $|G| = \prod_{i=1}^{\ell} |G_i|$.

- $1 = N_0 \lhd N_1 \lhd \cdots \lhd N_\ell = G$ a composition series $\Rightarrow$

$$\prod_{i=1}^{\ell} |G_i| = \prod_{i=1}^{\ell} |N_i/N_{i-1}| = |G| .$$

<u>Observation 2</u>. Suppose A is an abelian group of order $\prod p_i^{k_i}$ where p_i's are distinct primes. Then the composition factors

Lecture 10: Composition factors of abelian groups

Tuesday, October 30, 2018 12:16 AM

of A are k_i-times $\mathbb{Z}/p_i\mathbb{Z}$.

Pf. Since A is abelian, its composition factors are abelian (and simple). So they are cyclic groups of prime order. On the other hand by Observation 1, $|A| = \prod |G_i|$; and so using unique factor. of integers, claim follows. ∎

$\boxed{Q}$ What can we say about a group if all of its composition factors are cyclic groups of prime order?

Def. $\forall\, h,k \in G$, $[h,k] := h^{-1}k^{-1}hk$.

- $H, K \leq G$, let $[H,K] := \langle \{[h,k] \mid h \in H, k \in K\} \rangle$ (subgroup generated by $[h,k]$'s).

Lemma. $H, K \trianglelefteq G \Rightarrow [H,K] \trianglelefteq G$ and $[H,K] \subseteq H \cap K$.

In particular, if $H \cap K = 1$, then $[H,K] = 1$ which means $\forall\, h \in H, k \in K$, $hk = kh$.

Pf. $\forall g \in G$, let $c_g : G \to G$ be the conjugation by g.

Then $\langle \{c_g([h,k]) \mid h \in H, k \in K\} \rangle = \langle \{[c_g(h), c_g(k)] \mid h \in H, k \in K\} \rangle$
$= \langle \{[h',k'] \mid h' \in H, k' \in K\} \rangle$;

and so $\Phi_g([H,K]) = [H,K]$, which implies $[H,K] \trianglelefteq G$.

$$\forall h \in H, k \in K, \quad h^{-1}k^{-1}hk = \underbrace{(h^{-1}kh)^{-1}}_{K} \cdot \underbrace{k}_{K} \in K$$

$$= \underbrace{h^{-1}}_{H} \underbrace{(k^{-1}hk)}_{H} \in H,$$

and claim follows. ∎

Def. • The derived subgroup of G is $[G,G]$; it is also denoted by $G^{(1)}$.

• The derived series of G is defined recursively:

$$G^{(0)} := G, \quad G^{(i+1)} := [G^{(i)}, G^{(i)}] \text{ for any } i \in \mathbb{Z}^{\geq 0}.$$

Lemma. Suppose $N \triangleleft G$. Then

$$G/N \text{ is abelian} \Leftrightarrow [G,G] \subseteq N.$$

(Exercise)

Theorem. Suppose G is a group. Then

$$G^{(k)} = 1 \Leftrightarrow \exists\, 1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_k = G \text{ s.t. } N_i/N_{i-1} \text{ is abelian for any } i.$$

Pf. ($\Rightarrow$) By the above lemma $G^{(i)}/[G^{(i)}, G^{(i)}]$ is abelian; and so $1 = G^{(k)} \triangleleft G^{(k-1)} \triangleleft \cdots \triangleleft G^{(0)} = G$ is such a chain.

Lecture 10: Solvable groups

Tuesday, October 30, 2018 8:43 AM

($\Leftarrow$) We proceed by induction on n. The previous lemma implies the base of induction. Suppose $1 = N_1 \triangleleft \cdots \triangleleft N_{k+1} = G$ and N_i/N_{i+1} is abelian. Then, by the induction hypothesis, $N_k^{(k)} = 1$. As G/N_k is abelian, $G^{(1)} \subseteq N_k$; and so $(G^{(1)})^{(k)} = G^{(k+1)} = 1$. ■

<u>Def.</u> A group G is called <u>solvable</u> if $\exists k \in \mathbb{Z}^{\geq 0}$, $G^{(k)} = 1$.

(Name is given because of a theorem by Galois on <u>solvability</u> of a polynomial by radicals.)