Lecture 12: Some properties of nilpotent groups

Tuesday, November 6, 2018 8:16 AM

<u>Proposition</u>. Suppose G is nilpotent. Then

(1) G is solvable, (2) If $1 \neq N \trianglelefteq G$, then $N \cap Z(G) \neq 1$,

(3) If $H \leq G$, $N \trianglelefteq G$, then H and $G/_N$ are nilpotent.

<u>Pf.</u> (1) $G = \gamma_1(G) \triangleright \gamma_2(G) \triangleright \cdots \triangleright \gamma_{c+1}(G)$ and $\gamma_i(G)/_{\gamma_{i+1}(G)}$ is abelian (in fact $\gamma_i(G)/_{\gamma_{i+1}(G)} \subseteq Z(G/_{\gamma_{i+1}(G)})$.)

And so G is solvable.

(2) Consider $N = N \cap \gamma_1(G) \triangleright N \cap \gamma_2(G) \triangleright \cdots \triangleright N \cap \gamma_{c+1}(G) = 1$.

Then $\exists i$ s.t. $N \cap \gamma_i(G) \neq 1$ and $N \cap \gamma_{i+1}(G) = 1$.

<u>Claim</u>. $N \cap \gamma_i(G) \subseteq Z(G)$.

<u>Pf.</u> Let $h \in N \cap \gamma_i(G)$ and $g \in G$. Then

$$[g,h] \in [G,N] \cap [G,\gamma_i(G)] \subseteq N \cap \gamma_{i+1}(G) = 1.$$

$\Rightarrow \forall g \in G,\ [g,h] = 1 \Rightarrow h \in Z(G)$.

(3) By induction on i, show $\gamma_i(H) \subseteq \gamma_i(G)$ and

$\gamma_i(G/_N) = \gamma_i(G)N/_N$. ∎

Lecture 12: Frattini subgroup

Tuesday, November 6, 2018 2:59 PM

Def. The <u>Frattini subgroup</u> $\Phi(G)$ of a group is the <u>intersection</u> of all of its <u>maximal</u> subgroups.

- Let $\mathrm{Max}(G) := \{M < G \mid M \text{ is a maximal subgroup of } G\}$.

Observe. $\forall\ \theta \in \mathrm{Aut}(G)$, $M \in \mathrm{Max}(G) \Rightarrow \theta(M) \in \mathrm{Max}(G)$

And so $\theta: \mathrm{Max}(G) \to \mathrm{Max}(G)$, $M \mapsto \theta(M)$ is a bijection.

$$\left.\begin{array}{l}\Phi(G) = \bigcap_{M \in \mathrm{Max}(G)} M \\ \theta \in \mathrm{Aut}(G)\end{array}\right\} \Rightarrow \theta(\Phi(G)) = \theta\Big(\bigcap_{M \in \mathrm{Max}\, G} M\Big) \underset{\boxed{\theta \text{ is a bij.}}}{=} \bigcap_{M \in \mathrm{Max}\, G} \theta(M) = \bigcap_{M \in \mathrm{Max}\, G} M = \Phi(G).$$

Lemma. $\mathrm{Max}(G/N) = \{M/N \mid M \in \mathrm{Max}\, G,\ N \subseteq M.\}$

Pf.
- $\overline{M} \in \mathrm{Max}\, G/N \Rightarrow \overline{M} = M/N$ for some $N \le M \le G$

If $M \le M' \le G$, then $M/N \le M'/N \le G$. Since $M/N \in \mathrm{Max}\, G/N$, either $M/N = M'/N$ (in which case $M = M'$) or $G/N = M'/N$ (in which case $M' = G$). Therefore $M \in \mathrm{Max}\, G$.

- Suppose $N \le M \le G$ and $M \in \mathrm{Max}\, G$. Let $\overline{M} := M/N$. If $\overline{M} \le \overline{M}' \le G/N$, then $\overline{M}' = M'/N$ for some $N \le M' \le G$. Since $M/N \subseteq M'/N$, $M \le M'$.

Since $M \in \operatorname{Max} G$, either $M' = M$ (in which case $\overline{M}' = \overline{M}$) or $M' = G$ (in which case $\overline{M}' = G/N$). Hence $\overline{M} \in \operatorname{Max} G/N$. ∎

<u>Cor.</u> $\Phi(G)N/N \subseteq \Phi(G/N)$.

<u>Pf.</u>
$$\Phi(G/N) = \bigcap_{\overline{M} \in \operatorname{Max} G/N} \overline{M} = \bigcap_{\substack{M \in \operatorname{Max} G \\ N \leq M}} M/N$$
$$= \Big(\bigcap_{\substack{M \in \operatorname{Max} G \\ N \leq M}} M\Big)/N \supseteq \Phi(G)N/N. \quad ∎$$

<u>Lemma</u>. Suppose $\theta: G \to H$ is an onto group homomorphism. Then $\theta(\Phi(G)) \subseteq \Phi(H)$.

<u>Pf.</u> By the 1^{st} isomorphism theorem, the following is a commutative diagram: $\quad \overline{\theta}(g \ker \theta) := \theta(g)$.

$$\begin{tikzcd} G \arrow[r, "\theta"] \arrow[dr, "\pi"'] & H \\ & G/\ker\theta \arrow[u, "\simeq\, \overline{\theta}"'] \end{tikzcd}$$

And so $\theta(\Phi(G)) = \overline{\theta}(\pi(\Phi(G))) \underset{\text{prev. Cor.}}{\subseteq} \overline{\theta}(\Phi(G/\ker\theta)) \underset{\overline{\theta} \text{ is an isomo.}}{=} \Phi(H)$. ∎

Let V be an abelian group; and suppose any non-trivial element

Lecture 12: Abelian groups with prime exponent

Tuesday, November 6, 2018 3:25 PM

$v \in V$ has order p. Then we can define a $\mathbb{Z}/p\mathbb{Z}$-scalar multiplication on V. Let's use $+$ for the group operation. We let $(n+p\mathbb{Z}) \circ v := nv = \underbrace{v + \cdots + v}_{n \text{ times}}$. Since $pv = 0$, it is well-defined. One can check that this scalar multipli. makes V a vector space over $\mathbb{Z}/p\mathbb{Z}$. In particular, if V is finite, then $\dim_{\mathbb{Z}/p\mathbb{Z}} V < \infty$; and so after choosing a basis we see $V \simeq \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$.

(By classification of finite abelian groups any abelian group is of the form $\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$. If all non-trivial elements have order p, then $n_1 = \cdots = n_k = p$. We will prove the classification theorem in 200B.)

Any subgroup of V can be viewed as a subspace of V. So maximal subgroups are precisely codimension 1 subspaces.

For $v \in V \setminus \{0\}$, there is a $\mathbb{Z}/p\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$ s.t. $v_1 = v$. So the $\mathbb{Z}/p\mathbb{Z}$-span of $v_2, \ldots, v_n$ is a maximal subgroup W of V

Lecture 12: Frattini subgroup of p-groups

Wednesday, November 7, 2018 8:59 AM

which does not contain v. Hence $v \notin \Phi(V)$; and so $\Phi(V) = \{0\}$.

<u>Summary</u>. If V is an abelian group and any non-trivial element has order p, then $\Phi(V) = 0$.

<u>Theorem</u>. Suppose G is a finite p-group. Then

$$\Phi(G) = G^p[G,G], \text{ where } G^p = \{g^p \mid g \in G\}.$$

(Notice that G^p is NOT necessarily a subgroup.)

<u>Pf.</u> • Suppose M is a maximal subgroup. Since G is nilpotent, $M \trianglelefteq G$.

Since M is maximal, G/M has no proper non-trivial subgroup.

Hence G/M is a cyclic group of prime order. As G is a finite p-group, we deduce $G/M \simeq \mathbb{Z}/p\mathbb{Z}$. Therefore

(1) G/M is abelian $\Rightarrow [G,G] \subseteq M$

(2) $\forall g \in G$, $(gM)^p = M \Rightarrow G^p \subseteq M$

$\Rightarrow G^p[G,G] \subseteq M$ and so $G^p[G,G] \subseteq \Phi(G)$. 1

• Since $G/[G,G]$ is abelian, $(G/[G,G])^p$ is a normal subgroup.

$(G/[G,G])^p = \{g^p[G,G] \mid g \in G\} = G^p[G,G]/[G,G]$. Therefore $G^p[G,G]$

is a normal subgroup of G. Let $V_0 := G/G^p[G,G]$. Then V_0 is a finite abelian group and any non-trivial element has order p. Hence $\Phi(V_0)=\{1\}$. Since $\pi: G \longrightarrow G/G^p[G,G] = V_0$ is onto, by a lemma we proved earlier $\pi(\Phi(G)) \subseteq \Phi(V_0)=\{1\}$. And so $\Phi(G) \subseteq \ker \pi = G^p[G,G]$. ②

①, ② imply the claim. ■

Def. A set M with a binary operation $\cdot$ is called a monoid if

(1) (Associativity) $\forall x,y,z \in M$, $(x\cdot y)\cdot z = x\cdot(y\cdot z)$

(2) (Neutral element) $\exists e\in M$, $\forall x\in M$, $e\cdot x = x = x\cdot e$.

Ex. Any group; $(\mathbb{Z}^{\geq 0}, +)$; $(\mathbb{Z}, \times)$.

• Suppose X is a non-empty set. Let $\mathcal{L}(X)$ be the language in the alphabet of X; that means elements of $\mathcal{L}(X)$ (we call them words) are finite sequences with terms in X:

$$\omega = x_1 x_2 \cdots x_n \quad \text{where } x_i \in X.$$

Lecture 12: Free monoid

Tuesday, November 6, 2018 8:30 AM

We include the empty word $\emptyset$ in $\mathcal{L}(X)$.

Concatination defines a binary operator on $\mathcal{L}(X)$; that is

$$(x_1 x_2 \cdots x_n) \cdot (y_1 y_2 \cdots y_m) := x_1 \cdots x_n y_1 \cdots y_m .$$

Clearly $\cdot$ is an associative operator; and the empty word is the neutral element of $(\mathcal{L}(X), \cdot)$. So $(\mathcal{L}(X), \cdot)$ is a monoid. In fact $\mathcal{L}(X)$ is the <u>free monoid</u> <u>generated</u> by X; that means $\mathcal{L}(X)$ satisfies the following universal property:

(Universal Proprety of free objects.)

Any function f from X to a monoid M has a unique extension to a monoid homomorphism $\hat{f} : \mathcal{L}(X) \to M$.

The Universal Property of a free object is often described using the following diagram:

$$\begin{tikzcd}
 & \mathcal{L}(X) \arrow[d, dashed, "\exists!\, \hat{f}"] \\
X \arrow[ur, hook] \arrow[r, "f"'] \arrow[ur, phantom, shift right=3ex, "\circlearrowright"] & M
\end{tikzcd}$$

Set $\qquad\qquad$ Monoid

Lecture 12: Free monoid

Wednesday, November 7, 2018 3:13 PM

Remark.

If monoid is changed to group, we get the definition of free group generated by X; if monoid is changed to k-algebra, we get the definition of free k-algebra; etc.

Pf of freeness of $\mathcal{L}(X)$.

Let $\hat{f}(x_1 \cdots x_n) := f(x_1) \cdot f(x_2) \cdot \cdots \cdot f(x_n)$ and $\hat{f}(\emptyset) = 1_M$; and check that $\hat{f}$ is a monoid homomorphism. Uniquess is clear! ∎

Suppose $\{G_i\}_{i \in I}$ is a family of groups. Let X be the disjoint union of G_i's. (Notice that we can consider the set $G_i \times \{i\}$ instead of G_i, and think about it as a copy of G_i. This way we can make sure that G_i's are disjoint.)

Let $\mathcal{L}(X)$ be the free monoid generated by X. For example Suppose $G_1 = \mathbb{Z}/2\mathbb{Z}$ and $G_2 = \mathbb{Z}/3\mathbb{Z}$. First we pick isomorphic copies of G_1 and G_2 that are disjoint, say $G_1 = \{e, a\}$ and $a^2 = e$; $G_2 = \{1, b, b^2\}$ and $b^3 = 1$.

Lecture 12: Free product of groups

Wednesday, November 7, 2018 3:30 PM

Then $e\, a\, 1\, 1\, b\, b\, b^2 \in \mathcal{L}(X)$ and this is different from the word ab. The first word has length 7 and the 2nd word has length 2. To get a group structure we have to define an equivalency relation on $\mathcal{L}(X)$; let $\sim$ be the equi. relation generated by the following:

- $\omega_1 e \omega_2 \sim \omega_1\omega_2$ if e is the neutral element of G_i for some $i \in I$.
- $\omega_1 x_1 x_2 \omega_2 \sim \omega_1 x_3 \omega_2$ if $x_1, x_2 \in G_i$ and $x_3 = x_1 \cdot x_2$.

Let $\mathcal{F}(X) := \mathcal{L}(X)/_\sim$.

<u>Claim.</u> $\omega_1 \sim \omega_1'$ and $\omega_2 \sim \omega_2' \Rightarrow \omega_1\omega_2 \sim \omega_1'\omega_2'$

(try to convince yourself that this is true.)

Let $[\omega_1]_\sim \cdot [\omega_2]_\sim := [\omega_1\omega_2]_\sim$. Then by the above claim

This is a well-defined operator.

<u>Claim.</u> $(\mathcal{F}(X), \cdot)$ is a group.

<u>Pf.</u> • (Associative) $\big([\omega_1]\cdot[\omega_2]\big)\cdot[\omega_3] = [\omega_1\omega_2]\cdot[\omega_3]$

$$= [\omega_1\omega_2\omega_3]$$

Lecture 12: Free product of groups

Wednesday, November 7, 2018 3:39 PM

$$[\omega_1]\cdot([\omega_2]\cdot[\omega_3]) = [\omega_1]\cdot[\omega_2\omega_3]$$
$$= [\omega_1\omega_2\omega_3]$$

- (Neutral element) $[\omega]\cdot[\emptyset] = [\omega] = [\emptyset]\cdot[\omega]$

- (Inverse) $[x_1x_2\cdots x_n]\cdot[x_n^{-1}\, x_{n-1}^{-1}\cdots x_1^{-1}]$
$$= [x_1x_2\cdots x_n x_n^{-1}\, x_{n-1}^{-1}\cdots x_1^{-1}].$$

$$x_1\cdots x_{n-1}\underbrace{x_n x_n^{-1}}\, x_{n-1}^{-1}\cdots x_1^{-1} \sim x_1\cdots x_{n-1}\, e\, x_{n-1}^{-1}\cdots x_1^{-1}$$
$$\sim x_1\cdots x_{n-1}x_{n-1}^{-1}\cdots x_1^{-1}$$

So by induction on n, we have
$$x_1\cdots x_n x_n^{-1}\cdots x_1^{-1} \sim \emptyset.$$

Similarly $[x_n^{-1}\cdots x_1^{-1}]\cdot[x_1\cdots x_n] = [\emptyset]$. ■

$\mathcal{F}(X)$ is called the free product of G_i's; and it is denoted

by $\mathop{*}\limits_{i\in I} G_i$.