Proposition. Suppose $G$ is nilpotent. Then

1. $G$ is solvable,
2. If $1 \neq N \triangleleft G$, then $N \cap Z(G) \neq 1$,
3. If $H \leq G$, $N \triangleleft G$, then $H$ and $G/N$ are nilpotent.

Proof. (1) $G = \gamma_1(G) \triangleright \gamma_2(G) \triangleright \cdots \triangleright \gamma_{i+1}(G)$ 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 $N = N \cap \gamma_1(G) \triangleright N \cap \gamma_2(G) \triangleright \cdots \triangleright N \cap \gamma_{i+1}(G) = 1$.

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

Claim. $N \cap \gamma_i(G) \subseteq Z(G)$.

Proof. Let $n \in N \cap \gamma_i(G)$ 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 $\gamma_i(G/N) = \gamma_i(G)N/N$. □
**Def.** The *Frattini subgroup* \( \Phi(G) \) of a group is the intersection of all of its *maximal* subgroups.

*Let* \( \text{Max}(G) := \{ M \leq G \mid M \text{ is a maximal subgroup of } G \} \).

**Observe.** \( \forall \Theta \in \text{Aut}(G), \ M \in \text{Max}(G) \implies \Theta(M) \in \text{Max}(G) \)

And so \( \Theta : \text{Max}(G) \to \text{Max}(G) \), is a bijection.

\[
\Phi(G) = \bigcap_{M \in \text{Max}(G)} M \implies \Theta(\Phi(G)) = \Theta\left( \bigcap_{M \in \text{Max}(G)} M \right) \]

\(
\Theta \in \text{Aut}(G) \)

\[
\text{is a bijection.}
\]

\[
= \bigcap_{M \in \text{Max}(G)} \Theta(M) = \bigcap_{M \in \text{Max}(G)} M = \Phi(G).
\]

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

**Pf.** \( \forall M \in \text{Max}(G/N) \implies \bar{M} = M/N \) for some \( N \leq M \leq G \).

If \( N \leq M, M \leq G \), then \( M/N \leq M'/N \leq G/N \).

Since \( M/N \in \text{Max}(G/N) \), either \( M/N = M'/N \) (in which case \( M = M' \)) or \( G/N = M'/N \) (in which case \( M = G \)). Therefore \( M \in \text{Max}(G) \).

*Suppose* \( N \leq M \leq G \) and \( M \in \text{Max}(G) \). Let \( \bar{M} = M/N \). If \( \bar{M} \leq M' \leq G/N \), then \( \bar{M}' = M'/N \) for some \( N \leq M' \leq G \). Since \( M/N \leq M'/N \), \( N \leq M' \).
Since $M \in \text{Max } G$, either $M' = M$ (in which case $\overline{M'} = M$) or $M' = G$ (in which case $\overline{M'} = G/N$). Hence $\overline{M} \in \text{Max } G/N$. 

**Cor.** $\Phi(G)N/N \subseteq \Phi(G/N)$.

**Pf.** $\Phi(G/N) = \bigcap_{M \in \text{Max } G/N} \overline{M} = \bigcap_{M \in \text{Max } G} M/N$

$= \left( \bigcap_{N \leq M} M \right) /N \supseteq \Phi(G)N/N$.

**Lemma.** Suppose $\theta : G \rightarrow H$ is an onto group homomorphism.

Then $\theta(\Phi(G)) \subseteq \Phi(H)$.

**Pf.** By the 1st isomorphism theorem, the following is a commutative diagram:

\[
\begin{array}{cccc}
G & \xrightarrow{\theta} & H \\
\downarrow{\pi} & & \uparrow{\overline{\theta}} \\
G/\ker{\theta} & \xrightarrow{2} & \overline{\theta}(G/\ker{\theta})
\end{array}
\]

And so $\theta(\Phi(G)) = \overline{\theta}(\pi(\Phi(G))) \subseteq \overline{\theta}(\Phi(G/\ker{\theta})) = \Phi(H)$.

Let $V$ be an abelian group; and suppose any non-trivial element
\(v \in V\) 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 \((n+p\mathbb{Z}v) = nV.\) Since \(pv = 0\), it is well-defined. One can check that this scalar multiplication 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 \(V \cong \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}\).

(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 2008.)

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 \(V\)
which does not contain \( v \). Hence \( v \notin \Phi(V) \); and so \( \Phi(V) = \mathbb{Z}_p \).

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

**Theorem.** 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.)

**Proof.** Suppose \( M \) is a maximal subgroup. Since \( G \) is nilpotent, \( M \triangleleft G \).

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 \( G/M \cong \mathbb{Z}/p\mathbb{Z} \). Therefore

1. \( G/M \) is abelian \( \Rightarrow \) \( [G,G] \subseteq M \rightarrow G^p[G,G] \subseteq M 

2. \( \forall g \in G, (g^p) = M \Rightarrow G^p \subseteq M \), and so \( G^p[G,G] \subseteq \Phi(G) \).

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 \( G^p[G,G] \)
Lecture 12: Frattini subgroup of finite p-groups

Tuesday, November 6, 2018  8:42 AM

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 $\Phi(V_0) = \mathfrak{I}_G$. Since $\pi : G \rightarrow G / G_{p_{[G,G]}} = V_0$ is onto, by a lemma we proved earlier $\pi(\Phi(G)) \subseteq \Phi(V_0) = \mathfrak{I}_G$. And so $\Phi(G) \subseteq \ker \pi = G_{p_{[G,G]}}$.

$\mathfrak{I}_G$ implies the claim. $\blacksquare$

---

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 $; (\mathbb{Z}, \geq, +); (\mathbb{Z}, \times)$.

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

$\omega = x_1 x_2 \ldots x_n$ where $x_i \in X$. 


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

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

$$(x_1x_2\cdots x_n) \cdot (y_1y_2\cdots y_m) := x_1\cdots x_ny_1\cdots y_m.$$  

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 free monoid generated by $X$; that means $\mathcal{L}(X)$ satisfies the following universal property:

**Universal Property of free objects:**

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

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

$$
\begin{array}{ccc}
X & \xrightarrow{f} & M \\
\downarrow \cong & & \downarrow \text{\hat{f}} \\
\mathcal{L}(X) & \xrightarrow{id} & \mathcal{L}(X) \\
\end{array}
$$

Set $\xrightarrow{\cong}$ Monoid
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.

Proof of freeness of \( L(X) \).

Let \( \hat{f}(x_1, \ldots, x_n) = f(x_1) \cdot f(x_2) \cdot \cdots \cdot f(x_n) \) and \( \hat{f}(\emptyset) = 1_M \); and check that \( \hat{f} \) is a monoid homomorphism. Uniqueness 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 one can consider the set \( G_i \times \emptyset \emptyset \) 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 \( L(X) \) 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 \( G_1 = \{ e, a, a^2 \} \) and \( a^2 = e \); \( G_2 = \{ 1, b, b^2 \} \) and \( b^3 = 1 \).
Then \( e \cdot 1 \cdot b \cdot b^2 \cdot e \in \mathbb{L}(X) \) 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 \( \mathbb{L}(X) \); let \( \sim \) be the equivalence relation generated by the following:

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

Let \( \mathbb{F}(X) := \mathbb{L}(X)/\sim \).

Claim. \( \omega_1 \sim \omega_1' \) 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 \( [\omega_1] \sim [\omega_2] := [\omega_1 \omega_2] \sim \). Then by the above claim this is a well-defined operator.

Claim. \( (\mathbb{F}(X), \cdot) \) is a group.

Proof. (Associative) \( ([\omega_1] \cdot [\omega_2]) \cdot [\omega_3] = [\omega_1 \omega_2] \cdot [\omega_3] = [\omega_1 \omega_2 \omega_3] \).
\[[\omega_1] \cdot ([\omega_2] \cdot [\omega_3]) = [\omega_1] \cdot [\omega_2 \omega_3] = [\omega_1 \omega_2 \omega_3]\]

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

- (Inverse) \[ [x_1 x_2 \ldots x_n]. [x_1^{-1} x_2^{-1} \ldots x_n^{-1}] = [x_1 x_2 \ldots x_n x_n^{-1} x_{n-1}^{-1} \ldots x_1^{-1}] \]

\[x_1 \ldots x_{n-1} x_n x_n^{-1} x_{n-1}^{-1} \ldots x_1^{-1} \sim x_1 \ldots x_{n-1} e x_{n-1}^{-1} \ldots x_1^{-1} \sim x_1 \ldots x_{n-1} x_{n-1}^{-1} \ldots x_1^{-1} \]

So, by induction on \( n \), we have \[x_1 \ldots x_n x_n^{-1} \ldots x_1^{-1} \sim \emptyset \].

Similarly \[ [x_n^{-1} \ldots x_1^{-1}] \cdot [x_1 \ldots x_n] = [\emptyset] \]. \[ \square \]

\( \mathcal{F}(x) \) is called the free product of \( G_i \)'s; and it is denoted by \( \ast_{i \in I} G_i \).