Lecture 09: Split extensions

Tuesday, October 17, 2017 9:37 PM

In the previous lecture we have seen how (in certain cases) Sylow's theorems can help us to find a normal subgroup N of G such that $\gcd(|N|, |G/N|) = 1$. How can this help?

<u>Def.</u> Suppose $G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_n} G_n$ is a sequence of groups and group homomorphisms. This is called an <u>exact sequence</u> if $\operatorname{Im} \phi_i = \ker \phi_{i+1}$ for $1 \le i \le n-1$.

- An exact sequence of the form $1 \to G_1 \to G_2 \to G_3 \to 1$ is called a short exact sequence.
- We say the SES $1 \to G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \to 1$ splits if $\exists\, \psi: G_3 \to G_2$ s.t. $\phi_2 \circ \psi = I_{G_3}$; we write

$$\begin{tikzcd} 1 \arrow[r] & G_1 \arrow[r, "\phi_1"] & G_2 \arrow[r, shift left, "\phi_2"] & G_3 \arrow[l, shift left, "\psi"] \arrow[r] & 1 \end{tikzcd}$$

is a commutative diagram.

<u>Observation</u>. Suppose $1 \xrightarrow{\phi_0} G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \xrightarrow{\phi_4} 1$ is a SES.

Then ① $\ker \phi_1 = 1$; and so ϕ_1 is injective

② $\operatorname{Im} \phi_1 = \ker \phi_2$; and so $\phi_1(G_1) \lhd G_2$.

③ $\operatorname{Im} \phi_2 = \ker \phi_4 = G_3$; and so ϕ_2 is surjective.

Lecture 09: Split extension

Tuesday, October 17, 2017 9:49 PM

By the 1^{st} isomorphism theorem we have

$$G_2/_{\ker \Phi_2} \simeq \operatorname{Im} \Phi_2 \quad ;$$

and so $\quad G_2/_{\operatorname{Im}\Phi_1} \simeq G_3 .$

Lemma. If a SES $1 \to N \xrightarrow{\Phi_1} G \xrightarrow{\Phi_2} H \to 1$ splits, then $\exists \psi : H \to G$ s.t.

① ψ is injective

② $\psi(H) \cap \Phi_1(N) = 1$.

Pf. $\exists \psi : H \to G$ s.t. $\Phi_2 \circ \psi = I_H$.

- $\psi(h_1) = \psi(h_2) \Rightarrow \Phi_2(\psi(h_1)) = \Phi_2(\psi(h_2))$
$\Rightarrow h_1 = h_2$. So ψ is injective.

- Suppose $\psi(h) = \Phi_1(n)$. Then
$\psi(h) \in \operatorname{Im}\Phi_1 = \ker \Phi_2$. So $1 = \Phi_2(\psi(h)) = h$. ∎

Suppose $N \trianglelefteq G$ and the SES $1 \to N \to G \to G/N \to 1$ splits.

Then by the previous lemma $\exists H \leq G$ and an isomorphism

$\psi: G/N \xrightarrow{\sim} H$ such that $\psi(gN)N = gN$ for any $g \in G$.

Equivalently $\forall g \in G$, $\psi(gN)^{-1} g \in N$. And so for any $g \in G$

there are $h=\Psi(gN)\in H$ and $n=\Psi(gN)^{-1}g\in N$ s.t.

$$g=hn \text{ ; and so } G=HN.$$

[An example of this kind we have seen before when we were studying groups of order pq where $p<q$ are primes. In that case we prove $\exists\, Q_0 \triangleleft G$ s.t. $|Q_0|=q$ and $G=P_0Q_0$ where P_0 is a Sylow p-subgroup. This is equivalent to say

$$1\to \mathbb{Z}/q\mathbb{Z}\to G\to \mathbb{Z}/p\mathbb{Z}\to 1$$

is a SES.]

Let's notice that

$$\begin{aligned} H\times N &\longrightarrow G \\ (h,n) &\longmapsto hn \end{aligned}$$

is a bijection:

We have already proved that it is onto.

<u>Injectivity</u>: $h_1n_1=h_2n_2 \Rightarrow h_2^{-1}h_1=n_2n_1^{-1}\in H\cap N=\{1\}$

$$\Rightarrow h_1=h_2 \text{ and } n_1=n_2.$$

So far we have identified G as a set with $H\times N$; next we will describe its multiplication: for any $h_1,h_2\in H$, $n_1,n_2\in N$

$$h_1n_1\cdot h_2n_2 = h_1h_2\,\underbrace{(h_2^{-1}n_1h_2)}_{\text{in } N}n_2 .$$

Lecture 09: Semidirect product and split extensions

Wednesday, October 18, 2017 8:13 AM

So, for any $h \in H$, we need to know

$$c_h : N \to N, \quad c_h(n) = h n h^{-1}.$$

Notice that $c_h \in \mathrm{Aut}(N)$ and $c: H \to \mathrm{Aut}(N)$,

$$h \mapsto c_h$$

is a group homomorphism. And

$$h_1 n_1 h_2 n_2 = h_1 h_2 \; c_{h_2^{-1}}(n_1)\, n_2 .$$

We can do this construction in the following generality:

<u>Prop./Def.</u> N, H : groups

$c: H \to \mathrm{Aut}(N)$ group hom.

On the set $H \times N$, define the following product:

$$(h_1, n_1) \cdot (h_2, n_2) := (h_1 h_2 \,,\, c(h_2^{-1})(n_1)\, n_2).$$

Then $(H \times N, \cdot)$ is a group; and it is denoted by $H \ltimes_c N$ or simply $H \ltimes N$; and it is called a semi-direct product of H and N.

Exercise check why $H \ltimes N$ is a group.

Lecture 09: Direct product and semi-direct product

Wednesday, October 18, 2017 8:26 AM

When $c: H \to \mathrm{Aut}(N)$ is the trivial group homomorphism,

$$(h_1, n_1)\cdot(h_2, n_2) = (h_1 h_2, c(h_2^{-1})(n_1)\, n_2)$$
$$= (h_1 h_2, n_1 n_2)$$

This group is called the direct product of H and N and it is denoted by $H \times N$.

So, if $\mathrm{Hom}(H, \mathrm{Aut}(N)) = \{1\}$, then $H \ltimes N = H \times N$.

We have seen an application of this before:

$|G| = pq$, $p < q \Rightarrow$

$$\exists P_0, Q_0 \leq G, \ |P_0| = p, \ |Q_0| = q, \ G = P_0 Q_0, \ Q_0 \trianglelefteq G$$

$\Rightarrow \quad 1 \to Q_0 \to G \rightleftarrows P_0 \to 1$ is a split SES

$\Rightarrow \quad G \simeq P_0 \ltimes Q_0 \simeq \mathbb{Z}/p\mathbb{Z} \ltimes \mathbb{Z}/q\mathbb{Z}$.

$\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^{\times} \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ (why?)

$\Rightarrow$ if $p \nmid q-1$, then $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})) = 1$

$\Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$.

Lecture 09: Schur-Zassenhaus theorem

Wednesday, October 18, 2017 8:33 AM

When can we be sure that a SES $1 \to N \to G \to G/N \to 1$ splits? The following theorem due to Schur and Zassenhaus is an extremely strong tool:

<u>Theorem</u> (Schur-Zassenhaus)

Suppose G is a finite group, $N \trianglelefteq G$, and $\gcd(|N|, |G/N|) = 1$. Then

$$1 \to N \to G \to G/N \to 1$$

splits; this implies $G \simeq G/N \ltimes N$.