Lecture 10

Objective: we continue studying semidirect product.

Book reference: Dummit & Foote section 5.5

Theorem (semidirect product as a direct product)

In a semidirect product $H \rtimes_\varphi K$, the subgroup $1 \times K$ is normal if and only if $\varphi: K \mapsto Aut(H)$ is trivial, which makes $H \rtimes_\varphi K = H \times K$

Pf: Since $H \rtimes_\varphi K$ is generated by $H \times 1$ and $1 \times K$, $1 \times K$ is normal in $H \rtimes_\varphi K$ iff for each $h \in H$, $k \in K$, $(h,1)(1,k)(h,1)^{-1} = (h\varphi_1(1), k)(h^{-1}, 1) = (h\varphi_k(h^{-1}), k) \in 1 \times K$, which is equivalent to $\varphi_k(h) = h$. Thus, $1 \times K \lhd H \rtimes_\varphi K$ iff $\varphi_k$ is the identity mapping for each $k$, namely, $\varphi$ is trivial. In this case, clearly $H \rtimes_\varphi K = H \times K$.

The followings are equivalent:

① $H \rtimes_\varphi K = H \times K$

② $1 \times K \lhd H \rtimes_\varphi K$

③ $\varphi: K \mapsto Aut(H)$ is trivial.

Example: Take $H = \mathbb{R}$, $K = \mathbb{R}^*$, and $\varphi: \mathbb{R}^* \to Aut(\mathbb{R})$, where $\varphi_x(y) = xy$.

The group $\mathbb{R} \rtimes_\varphi \mathbb{R}^*$ has the operation $(a,b)(a',b') = (a + \varphi_b(a'), bb')$
$= (a + ba', bb')$.

$Aff(\mathbb{R}) = \left\{ \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{R}, b \in \mathbb{R}^* \right\}$. (mapping a line to a line)

$\mathbb{R} \rtimes_\varphi \mathbb{R}^* \cong Aff(\mathbb{R})$ $(a, b) \to \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}$.

When is a group isomorphic to a semidirect product of two subgroups?

Theorem (semidirect product recognition theorem)

Let $G$ be a group with subgroups $H$ and $K$ such that

① $G = HK$ ② $H \cap K = \{1\}$ ③ $H \lhd G$

Let $\varphi: K \to Aut(H)$ be conjugation: $\varphi_k(h) = khk^{-1}$. Then $\varphi$ is a homomorphism and the map $f: H \rtimes_\varphi K \to G$ where $f(h,k) = hk$ is an isomorphism.

Pf: Check $\varphi$ is a homomorphism, namely, $\varphi_{xy} = \varphi_x \circ \varphi_y$ for all $x, y \in K$.

$f$ is surjective by ①

$f$ is injective by ②

$f$ is a homomorphism: $f((h,k)(h',k')) = f(h\varphi_k(h'), kk') = h\varphi_k(h')kk' = hkh'k^{-1}kk'$
$= hkh'k'$, $f(h,k)f(h',k') = hkh'k$. Hence $f((h,k)(h',k')) = f(h,k)f(h',k')$.

Example: In $G = S_n$, $n \geq 3$, let $H = A_n$ and $K = \langle (1,2) \rangle = \{(1), (1,2)\}$.

① $G = HK$

② $H \cap K = \{1_G\}$

③ $H \trianglelefteq G$

$G = H \rtimes_\varphi K$, where $\varphi_k(h) = khk^{-1}$ for each $h \in H$, $k \in K$.

Example. $Aff(\mathbb{R}) \cong \mathbb{R} \rtimes_\varphi \mathbb{R}^*$, $\varphi: \mathbb{R}^* \mapsto Aut(\mathbb{R})$. $\varphi(x) = \varphi_x$ for each $x \in \mathbb{R}^*$

$\varphi_x(y) = xy$ for $y \in \mathbb{R}$.

Write $\widetilde{\mathbb{R}} = \{(x,1) \mid x \in \mathbb{R}\}$, $\widehat{\mathbb{R}^*} = \{(0,y) \mid y \in \mathbb{R}^*\}$.

$(x_1, y_1)(x_2, y_2) = (x_1 + \varphi_{y_1}(x_2), y_1 y_2) = (x_1 + y_1 x_2, y_1 y_2)$

Define $\widetilde{\varphi}: \widehat{\mathbb{R}^*} \mapsto Aut(\widetilde{\mathbb{R}})$, $\widetilde{\varphi}_{(0,y)}(x,1) = (0,y)(x,1)(0,y)^{-1} = (0,y)(x,1)(0,y^{-1})$
$= (\varphi_y(x), y)(0, y^{-1}) = (yx, 1)$.

$(x_1, y_1)(x_2, y_2) = (x_1, 1)(0, y_1)(x_2, 1)(0, y_2) = (x_1, 1)(0, y_1)(x_2, 1)(0, y_1^{-1})(0, y_1)(0, y_2)$
$= (x_1, 1)\widehat{\varphi}_{(0,y_1)}(x_2, 1)(0, y_1 y_2) = (x_1, 1)(x_2 y_1, 1)(0, y_1 y_2) = (x_1 + x_2 y_1, 1)(0, y_1 y_2) = (x_1 + x_2 y_1, y_1 y_2)$

Example In $G = S_4$, let $H$ be a Sylow 2-subgroup and $K$ be a Sylow 3-subgroup. Then $H \cong D_4$ and $K \cong \mathbb{Z}_3$. Clearly, $G = HK$ and $H \cap K = \{1_G\}$. However, $H \ntriangleleft G$ and $K \ntriangleleft G$. Hence $G$ is not a semidirect product of $H$ and $K$.

Classification of groups with prescribed order

Example (Groups of order $pq$, $p$ and $q$ primes with $p < q$)

Let $G$ be a group of order $pq$. Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$. Since $Q \triangleleft G$, $PQ = G$, and $P \cap Q = \{1_G\}$, then $G = Q \rtimes_\varphi P$ for some group homomorphism $\varphi : P \longmapsto Aut(Q)$.

Note that $|Aut(Q)| = q-1$. If $p \nmid q-1$, then $\varphi$ must be the identity homomorphism.

Therefore $G = Q \times P \cong \mathbb{Z}_{pq}$.

If $p \mid q-1$, let $P = \langle y \rangle$ and $\langle r \rangle$ be the unique order $p$ subgroup of $Aut(Q)$.

Hence there exist $p$ group homomorphisms $\varphi_i$, $0 \le i \le p-1$, such that $\varphi_i(y) = r^i$.

If $i = 0$, then $\varphi_0$ is the identity homomorphism. $G = Q \rtimes_{\varphi_0} P = Q \times P \cong \mathbb{Z}_{pq}$

If $i \neq 0$, $G = Q \rtimes_{\varphi_i} P$. For distinct $i_1, i_2 \neq 0$, $\theta : Q \rtimes_{\varphi_{i_1}} P \cong Q \rtimes_{\varphi_{i_2}} P$

$\theta(g, y^i) = (g, y^{ij})$, where $j = i_2^{-1} i_1 \pmod p$, is a group isomorphism.

$$\theta(g_1, y^{l_1})\,\theta(g_2, y^{l_2}) = (g_1, y^{jl_1}) \cdot (g_2, y^{jl_2}) = (g_1\, r^{jl_1 i_2}(g_2),\ y^{j(l_1+l_2)}) = (g_1\, r^{l_1 i_1}(g_2),\ y^{j(l_1+l_2)})$$

$$\theta((g_1, y^{l_1})(g_2, y^{l_2})) = \theta(g_1\, r^{l_1 i_1}(g_2),\ y^{l_1+l_2}) = (g_1\, r^{l_1 i_1}(g_2),\ y^{j(l_1+l_2)})$$

Indeed, $\varphi_{i_2} = \varphi_{i_1} \circ f$, where $f : P \longmapsto P$ is a group isomorphism s.t. $f(y) = y^{i_1^{-1} i_2}$.

This is the reason that $Q \rtimes \varphi_{i_1} P \cong Q \rtimes \varphi_{i_2} P$.