Section 5.5 (Continued) Semidirect products

Definition Let H, K be groups, and let $\varphi : K \longrightarrow \mathrm{Aut}(H)$ be a homomorphism. Thus K acts on H as $k.h = \varphi(k)(h)$. The semidirect product of H and K (relative to φ) is

$$G = H \rtimes_{\varphi} K,$$

where $H \rtimes_{\varphi} K = \{(h, k) \mid h \in H,\ k \in K\}$ with operation

$$(h,k)(h',k') = (h\,k.h',\ kk')$$

This is a group. Check that operation is associative.

Identity $(1,1)$

Inverses $(h,k)^{-1} = (k^{-1}.h^{-1},\ k^{-1})$

In checking this, keep in mind the following action properties.

$$\left.\begin{aligned} 1.h &= h \\ k'.k.h &= (kk').h \end{aligned}\right\} \text{usual action properties}$$

$$\left.\begin{aligned} k.1 &= 1 \\ k.h\ k.h' &= k.(hh') \end{aligned}\right\} \text{properties specific to this situation}$$

$$\varphi(k)(h)\,\varphi(k)(h') = \varphi(k)(hh') \quad \text{because } \varphi(k) \text{ is a homomorphism.}$$

Note: If $\varphi(k)=1$ then $H \rtimes_{\varphi} K = H \times K$.
but this is not so for other φ.

$$G = \boxed{H \quad \varphi \quad K}$$

Example $D_{2n} \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$

$\mathbb{Z}_n = \langle r \rangle = \{1, r, r^2, \dots, r^{n-1}\}$

$\mathbb{Z}_2 = \langle s \rangle = \{1, s\}$

Select $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$

$\alpha(x) = x^{-1}$

> Note: α is an automorphism of order 2.
> homo: $\alpha(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \alpha(x)\varphi(y)$
> clearly bijective.
> order 2: $\alpha^2(x) = \alpha\alpha(x) = x$ i.e. $\alpha^2 = 1$.

$\langle \alpha \rangle = \{1, \alpha\} \leq \mathrm{Aut}(\mathbb{Z}_n)$

Let $\varphi : \mathbb{Z}_2 \xrightarrow{\sim} \langle \alpha \rangle \leq \mathrm{Aut}(\mathbb{Z}_n)$

Then $\left.\begin{array}{l} s.x = \varphi(s)(x) = \alpha(x) = x^{-1} \\ 1.x = x \end{array}\right\}$ $\mathbb{Z}_2$ action on $\mathbb{Z}_n$.

$\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2 = \{(1,1), (r,1), (r^2,1) \dots (r^{n-1},1), (1,s), (r,s), (r^2,s) \dots (r^{n-1},s)\}$

$D_{2n} = \{1 \quad r \quad r^2 \quad r^{n-1} \quad s \quad rs \quad r^2s \dots r^{n-1}s\}$

$(r,1)^2 = (r,1)(r,1) = (r1.r, 1) = (r^2,1)$

$(r,1)^k = (r^k,1)$

$(1,s)^2 = (1,s)(1,s) = (1s.1, s^2) = (1,1)$

> $(r^{-k},1)(r^k,1)$
> $= (1,1)$

Relations on $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$ same as those for D_{2n}.

$\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$	$(r,1)^n = (1,1)$	$(1,s)^2 = (1,1)$	$(1,s)(r^k,1) = (r^{-k},s) = (r^{-k},1)(1,s)$
D_{2n}	$r^n = 1$	$s^2 = 1$	$sr^k = r^{-k}s$

Conclusion: $D_{2n} \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$.

Notation $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n := \{0, 1, 2, \dots, n-1\}$

<u>Example</u> Find a non-abelian group of order 21.

Idea: $G = \mathbb{Z}_7 \rtimes_\varphi \mathbb{Z}_3$ has order $7 \cdot 3 = 21$

Need homomorphism $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_7)$

$$\varphi : \underset{\substack{\uparrow \\ \text{order } 3}}{\langle 1 \rangle} \longrightarrow \underset{\substack{\uparrow \\ \text{order } 3}}{\langle \alpha \rangle} \leq \mathrm{Aut}(\mathbb{Z}_7)$$

Let $\alpha : \mathbb{Z}_7 \to \mathbb{Z}_7$

$$\begin{aligned} \alpha(x) &= 2x \\ \alpha(x+y) &= 2(x+y) \\ &= 2x + 2y \\ &= \alpha(x) + \alpha(y) \end{aligned}$$

(homomorphism)

$$\begin{aligned} 0 &\to 0 \\ 1 &\to 2 \\ 2 &\to 4 \\ 3 &\to 6 \\ 4 &\to 1 \\ 5 &\to 3 \\ 6 &\to 5 \end{aligned}$$

(automorphism)

$$\begin{aligned} \alpha^3(x) &= \alpha\alpha\alpha(x) \\ &= \alpha\alpha(2x) \\ &= \alpha(4x) \\ &= 8x = 7x + x = x = 1(x) \end{aligned}$$

Thus $\alpha^3 = 1$.

(order 3)

Let $\varphi : \mathbb{Z}_3 \to \langle \alpha \rangle = \{1, \alpha, \alpha^2\}$ be $\varphi(p) = \alpha^p$

Homomorphism because $\varphi(p+q) = \alpha^{p+q} = \alpha^p \alpha^q = \varphi(p)\varphi(q)$

Operation on $G = \mathbb{Z}_7 \rtimes_\varphi \mathbb{Z}_3$

$$\begin{aligned} (k, l)(m, n) &= (k + l.m,\ l + n) \\ &= (k + \varphi(l)(m),\ l + n) \\ &= (k + \alpha^l(m),\ l + n) \\ &= (k + 2^l m,\ l + n) \end{aligned}$$

$$\boxed{(k, l)(m, n) = (k + 2^l m,\ l + n)}$$

$$\boxed{(m, n)(k, l) = (m + 2^n k,\ n + l)}$$

<u>Non-abelian</u>:

$$(1, 2)(0, 1) = (1 + 2^4 \cdot 0,\ 0) = (1, 0)$$
$$(0, 1)(1, 2) = (0 + 2^1 1,\ 0) = (2, 0)$$

Theorem 10 Consider $G = H \rtimes_\varphi K$

(1) G is a group under the stated operation.

(2) $H \cong \tilde{H} = \{ (h,1) \mid h \in H \} \leq G$

$K \cong \tilde{K} = \{ (1,k) \mid k \in K \} \leq G$

$\tilde{H} = H \quad (h,1) = h$

$\tilde{K} = K \quad (1,k) = k$

$(h,1)(1,k) = (h,k) = hk$

(3) $\tilde{H} \trianglelefteq G$

(4) $\tilde{H} \cap \tilde{K} = 1$.

(5) $(1,k)(h,1)(1,k)^{-1} = \cancel{(khk^{-1}, 1)} = (k.h, 1)$

$$khk^{-1} = \cancel{khk^{-1}} = k.h$$

Proposition 11 The following are equivalent

(1) $H \rtimes_\varphi K \cong H \times K$ (by identity map)

(2) $\varphi(K) = 1$

(3) $\tilde{K} \trianglelefteq H \rtimes_\varphi K$

Theorem 12 (Decomposition Theorem – Generalization of Theorem 9)

Suppose $H, K \leq G$, such that

(1) $H \trianglelefteq G$

(2) $H \cap K = 1$

(3) $\varphi : K \to \mathrm{Aut}(H)$, where $\varphi(k)(x) = kxk^{-1}$

Then $HK \cong H \rtimes_\varphi K$

If $G = HK$, then $G = H \rtimes_\varphi K$.