Semidirect Products

Let G be a group and $H, K \leq G$ such that $H \lhd G$, and $H \cap K = \{1_G\}$. From general theory, $HK \leq G$ and each element of HK can be written uniquely:

$$(h_1k_1)(h_2k_2) = h_1k_1h_2k_1^{-1}k_1k_2$$

is an element of HK because $k_1k_2 \in k$, $k_1h_2k_1^{-1} \in H$ by normality, and therefore $h_1k_1h_2k_1^{-1} \in H$ as well. The uniqueness argument is the usual one.

We move on to a general discussion. Let H and K be two abstract groups. Suppose that $\varphi : K \to \mathrm{Aut}(H)$ is a group homomorphism. We define

$$G := \{(h, k) \mid h \in H \text{ and } k \in K\}$$

with multiplication

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2).$$

We claim that $\langle G, \cdot_\varphi \rangle$ is a group.

- **Closure:** By Construction.
- **Associativity:** Multiplication in H and K is associative and the composition of functions is associative.
- **Identity:** $(1_H, 1_K)$.
- **Inverse:** $(\varphi(k)^{-1}(h^{-1}), k^{-1})$ inverts (h, k).

An Action of K on H. We note that there is an action of K on H given by

$$\begin{aligned} K \times H &\to H \\ (k,h) &\mapsto \varphi(k)(h) \end{aligned}$$

because

-
$$\begin{aligned} 1_K \cdot h &= \varphi(1_K)(h) \\ &= \mathrm{Id}_H(h) \\ &= h \end{aligned}$$

-
$$\begin{aligned} (k_1 \cdot k_2) \cdot h &= \varphi(k_1 k_2)(h) \\ &= (\varphi(k_1) \circ \varphi(k_2)(h) \\ &= k_1 \cdot (k_2 \cdot h) \end{aligned}$$

Remark 1. Suppose we have this setup and φ is the trivial homomorphism. That is, $\varphi(k) = \mathrm{Id}_H$ for every $k \in K$. Then

(1)
$$\begin{aligned} (h_1, k_1)(h_2, k_2) &= (h_1 \varphi(k_1)(h_2), k_1 \cdot k_2) \\ &= (h_1 \cdot h_2, k_1 \cdot k_2) \end{aligned}$$

(2)

$$
\begin{aligned}
(h,k)(1_H,k')(k^{-1}h^{-1},k^{-1}) &= (h\varphi(k)(1_H),kk')(k^{-1}h^{-1},k^{-1})\\
&= (h,kk')(k^{-1}h^{-1},k^{-1})\\
&= (h\cdot\varphi(kk)(\varphi(k)^{-1}(h^{-1})),kk'k^{-1})\\
&= (h\varphi(kk'k^{-1})(h^{-1}),kk'k^{-1})\\
&= (1_H,kk'k^{-1})
\end{aligned}
$$

This implies that $K \lhd G$. So, we've now witnessed that $G \cong H \times K$. In fact, $K \lhd G$ and $G \cong H \times K$ if and only if φ is the trivial homomorphism.

To get the forward implication, note that the commutator

$$hkh^{-1}k^{-1} \in K \text{ because } K \lhd G$$

and

$$hkh^{-1}k{-}1 \in H \text{ because } H \lhd G$$

and one sees that $[h,k] \in H \cap K$ for all $h \in H$ and $k \in K$. Hence,

$$k \cdot h = \varphi(k)(h) = h \cdot k \in H \text{ for every } k \in K$$

and instantly we have that φ is the trivial homomorphism.

Notation. Our setup is that H and K are two abstract groups with a group homomorphism $\varphi : K \to \mathrm{Aut}(H)$. Then the semidirect product of H and K with respect to φ is denoted

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

and often times the φ is suppressed in the literature. The symbolism is chose to remind us that $H \lhd G$.

Conjugation Action. We have one item left to mention. The action of K on H that we mentioned earlier is by conjugation. Since $H \lhd G$, $khk^{-1} \in H$ for every $k \in K$. We've identified H and K in G via the usual way. So,

$$\begin{aligned} khk^{-1} &= (1_H, k)(h, 1_k)(1_H, k^{-1}) \\ &= (1_H \cdot \varphi(k)(h), k)(1_H, k^{-1}) \\ &= (\varphi(k)(h) \cdot \varphi(k)(1_H), kk^{-1}) \\ &= (\varphi(k)(h), 1_K) \\ &= \varphi(k)(h) \end{aligned}$$

and therefore $k \cdot h = \varphi(k)(h) = khk^{-1}$.

Example 1. Suppose H is an abelian group, $K = \mathbb{Z}/2$, and $\varphi : K \to \mathrm{Aut}(H)$ a group homomorphism. We that have two choices for φ:

Case 1: φ is the trivial group homomorphism.

In this case, we know that $G = H \rtimes \mathbb{Z}/2 \cong H \times \mathbb{Z}/2$.

Case 2: φ sends the generator σ of $\mathbb{Z}/2$ to the inversion automorphism

$$\begin{aligned} i : H &\to H \\ h &\mapsto h^{-1} \end{aligned}$$

.

Observations:

- H is a subgroup of index 2 in $G = H \rtimes K$, so $H \lhd G$.
- $\sigma \cdot h = h^{-1}$ as given above. We've also seen that $\sigma \cdot h = \sigma h \sigma^{-1} = \sigma h \sigma$ and therefore $\sigma h \sigma = h^{-1}$. That is, σ is an involution.

Of particular interest, is when $H = \mathbb{Z}/n$ for $n \geq 2$. Then $H \rtimes \mathbb{Z}/2$ can be presented as

$$\langle h, \sigma \mid h^n = \sigma^2 = 1 \text{ and } \sigma h \sigma = h^{-1} \rangle \cong D_{2n}$$

and when $H = \mathbb{Z}$, we have that $H \rtimes \mathbb{Z}/2 \cong D_\infty$.