# 21 Semidirect products (11/10)

**Construction 21.1** (The normal action)**.** Let $G$ be a group and let $N$ be a normal subgroup, with automorphism group $\mathrm{Aut}(N)$. Then, conjugation induces a group homomorphism

$$G \to \mathrm{Aut}(N),$$

which we will also denote by $g \mapsto c_g$. The kernel of $c_g \colon G \to \mathrm{Aut}(N)$ is

$$C_G(N) = \{g \in G \mid gng^{-1} = n \text{ for all } n \in N\},$$

which is a subgroup of $N_G(N)$. The group $C_G(N)$ is called the centralizer of $N$ in $G$.

**Example 21.2** (Normal abelian subgroups)**.** A very important example of the previous construction is when the normal subgroup $N \subseteq G$ is abelian. In this case, $N$ is in the kernel of $G \to \mathrm{Aut}(N)$ and so there is an induced homomorphism $G/N \to \mathrm{Aut}(N)$.

**Example 21.3** (The center)**.** The center $Z(G) \subseteq G$ is always normal, but the homomorphism $G \to \mathrm{Aut}(Z(G))$ is trivial, so one does not learn much from this construction in this case.

**Example 21.4** (The dihedral reflection)**.** Consider the dihedral group $D_{2n}$ as an extension

$$1 \to \mathbf{Z}/n \to D_{2n} \to \mathbf{Z}/2 \to 1$$

of $\mathbf{Z}/2$ by $\mathbf{Z}/n$. As the normal subgroup $\mathbf{Z}/n$ is abelian, there is an induced group homomorphism $D_{2n}/(\mathbf{Z}/n) \cong \mathbf{Z}/2 \to \mathrm{Aut}(\mathbf{Z}/n)$. This homomorphism corresponds to multiplication by $-1$.

**Notation 21.5.** If $\sigma$ is an automorphism of $G$ and $g \in G$ we write $g^\sigma$ for $\sigma(g)$.

**Construction 21.6.** Let $\varphi \colon H \to \mathrm{Aut}(N)$ be a group homomorphism. We define a group structure, denoted by $N \rtimes_\varphi H$ or $N \rtimes H$, on the set $N \times H$ by decreeing that

$$(n_0, h_0) \cdot (n_1, h_1) = (n_0 n_1^{\varphi(h_0)}, h_0 h_1).$$

**Lemma 21.7.** *Given $\varphi \colon H \to \mathrm{Aut}(N)$, the binary operation on $N \rtimes_\varphi H$ makes it into a group.*

*Proof.* The operation has an identity element $(e_N, e_H)$. The inverse of $(n, h)$ is $((n^{-1})^{\varphi(h)^{-1}}, h^{-1})$ as

$$(n, h)((n^{-1})^{\varphi(h)^{-1}}, h^{-1}) = (n((n^{-1})^{\varphi(h)^{-1}})^{\varphi(h)}, hh^{-1}) = (nn^{-1}, hh^{-1}) = (e_N, e_H),$$

and the other order is the same. We leave associativity for the reader as Exercise 21.1. $\square$

**Lemma 21.8.** *Given a group homomorphism $\varphi \colon H \to \mathrm{Aut}(N)$, the semidirect product $N \rtimes_\varphi H$ fits into an exact sequence*

$$1 \to N \xrightarrow{i} N \rtimes_\varphi H \xrightarrow{q} H \to 1.$$

*In particular, $N \subseteq N \rtimes_\varphi H$ is normal.*

*Proof.* We define $i$ by $i(n) = (n, e_H)$. This defines a group homomorphism as

$$i(n_0)i(n_1) = (n_0, e_H)(n_1, e_H) = (n_0(n_1)^{\varphi(e_H)}, e_H^2) = (n_0 n_1, e_H) = i(n_0 n_1).$$

as $\varphi(e_H)$ is the identity automorphism. The group homomorphism $i$ is injective, by definition of $N \rtimes_\varphi H$. We identify $N$ with its image under $i$. This subgroup is normal. Rather than check this directly, we check that $i(N)$ is the kernel of a homomorphism $q$, which is defined by $q(n, h) = h$. That $q$ is a homomorphism follows from the definition of multiplication on $N \rtimes_\varphi H$. The kernel of $q$ consists of those elements $(n, h)$ of $N \rtimes_\varphi H$ where $h = e_H$. But, this is precisely $N$. In particular, $N$ is normal. Since $q$ is also surjective, the lemma is complete. $\square$

**Definition 21.9** (Split extensions)**.** An exact sequence

$$1 \to N \xrightarrow{i} G \xrightarrow{q} H \to 1$$

of groups is **split** if there is a group homomorphism $f\colon H \to G$ such that $q \circ f = \mathrm{id}_H$. We illustrate this as

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "i"'] & G \arrow[r, "q"'] & H \arrow[l, bend right, "f"'] \arrow[r] & 1 . \end{tikzcd}$$

Semidirect products are very special extensions: they are split.

**Lemma 21.10.** *If $\varphi\colon H \to \mathrm{Aut}(N)$, then the exact sequence*

$$1 \to N \to N \rtimes_\varphi H \to H \to 1$$

*is split.*

*Proof.* We define $f\colon H \to N \rtimes_\varphi H$ by $f(h) = (e_N, h)$. Evidently, $q \circ f = \mathrm{id}_H$ and $f$ is a group homomorphism. $\square$

**Example 21.11** (Not every extension is split)**.** Consider

$$1 \to \mathbf{Z}/2 \xrightarrow{i} \mathbf{Z}/8 \xrightarrow{q} \mathbf{Z}/4 \to 1.$$

This is extension is not split. Indeed, a group homomorphism $f\colon \mathbf{Z}/4 \to \mathbf{Z}/8$ must send $1 \in \mathbf{Z}/4$ to an element of order dividing 4 in $\mathbf{Z}/8$, i.e., one of $\{0, 2, 4, 6\} \subseteq \mathbf{Z}/8$. As $q(1) = 1$, it follows that $q(f(4))$ is in $\{0, 2\}$, so $q \circ f$ is not the identity. In particular, we see that $\mathbf{Z}/8$ is **not** the semidirect product of $\mathbf{Z}/2$ and $\mathbf{Z}/4$.

**Proposition 21.12.** (i) *An extension $G$ of $H$ by $N$ is isomorphic to $N \rtimes_\varphi H$ for some $\varphi\colon H \to \mathrm{Aut}(N)$ if and only if the extension*

$$1 \to N \xrightarrow{i} G \xrightarrow{q} H \to 1$$

*is split.*

(ii) *A group $G$ is isomorphic to a semidirect product $N \rtimes_\varphi H$ if and only if it contains $N$ and $H$ as subgroups with $N$ normal, $N \cap H = \{e\}$, and $NH = G$.*

*Proof.* We have already seen that if $G \cong N \rtimes_\varphi H$, then the corresponding exact sequence is split. Thus, assume that we have an extension as in (i), split by $f\colon H \to G$. Let $\varphi$ be the composition $H \xrightarrow{f} G \xrightarrow{c} \mathrm{Aut}(N)$ of $f$ with the normal action homomorphism and set $G' = N \rtimes_\varphi H$. Define a function $a\colon G' \to G$ by $a(n, h) = nf(h)$. This is a group homomorphism as

$$a(n_0(n_1)^{\varphi(h_0)}, h_0h_1) = n_0(n_1)^{\varphi(h_0)} f(h_0h_1) = n_0 f(h_0) n_1 f(h_0)^{-1} f(h_0) f(h_1) = n_0 f(h_0) n_1 f(h_1) = a(n_0, h_0)a(n_1, h_1).$$

It is injective as $a(n, h) = nf(h) = e_G$ implies $q(nf(h)) = q(n)q(f(h)) = h = e_H$, so $h = e_H$ and then $n = e_N$. It is surjective as any element of $G$ is isomorphic to $nf(h)$ for some $n$ and $h$. To see this, fix $g \in G$ and then note that $gf(q(g))^{-1}$ is in $N$. This completes the proof of (i). The proof of (ii) is left to the reader as Exercise 21.3. $\square$

## 21.1 Exercises

**Exercise 21.1.** Prove that if $\varphi\colon H \to \mathrm{Aut}(N)$ is a homomorphism, then the binary operation of Construction 21.6 is associative. This completes the proof of Lemma 21.7.

**Exercise 21.2.** Let $G$ be a group with subgroups $N$ and $H$. Find necessary and sufficient conditions for the function $f\colon N \times H \to G$ defined by $f(n, h) = nh$ to be a group isomorphism.

**Exercise 21.3.** Prove part (ii) of Proposition 21.12.