SEMIDIRECT PRODUCTS

Let G be a group and $N \triangleleft G$ a normal subgroup. We would like to understand the relation between G on one hand and the the two groups N and G/N on the other. A complete understanding still eludes us, so we will work under an additional assumption. We first need a definition.

Definition 1. Two subgroups N and H of G are called *complementary* if

(1) $N \cap H = \{1\}$, and
(2) $NH = G$, where $NH = \{nh \mid n \in N, h \in H\}$.

Proposition 2. *Suppose N and H are two complementary subgroups of G. Then every $g \in G$ can be written uniquely as $g = nh$ where $n \in N$ and $h \in H$.*

Proof. It follows from the definition that every g can be written this way. For the uniqueness, suppose $n_1h_1 = n_2h_2$. Then $n_2^{-1}n_1 = h_2h_1^{-1}$. But $n_2^{-1}n_1 \in N$, $h_2h_1^{-1} \in H$, and $N \cap H = \{1\}$. So $n_1 = n_2$ and $h_1 = h_2$. $\square$

The additional assumption we need is that the normal subgroup $N \triangleleft G$ admits a complementary subgroup $H \subset G$. Note that H need not be a normal subgroup.

Example 3. There are many examples where complementary subgroups exist.

(1) Let $G = S_n$ and $N = A_n$. Then $H = \{\mathrm{id}, \tau\}$ is a complementary subgroup, where τ is any transposition.
(2) Let $G = D_n$ and let N be the subgroup of rotations in D_n. Then $H = \{\mathrm{id}, r\}$ is a complementary subgroup, where r is any reflection in G.
(3) Let $G = M$ be the group of all isometries of the plane and let N be the subgroup of translations. Then $H \cong O_2$ consisting of isometries fixing the origin is a complementary subgroup.
(4) Let $G = G_1 \times G_2$ and $N = G_1 \times \{1\}$. Then $H = \{1\} \times G_2$ is a complementary subgroup.
(5) Let $G = O_2$ and $N = SO_2$. Then $H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ is a complementary subgroup.
(6) Let $G = O_3$ and $N = SO_3$. Then $H = \{I_3, -I_3\}$ is a complementary subgroup.

Example 4. There are also examples where a complementary subgroup does not exist.

(1) Let $G = \mathbf{Z}_4$ and $N = \{[0], [2]\}$. Then N does not have a complementary subgroup.
(2) Let $G = Q$ be the quaternion group and $N = \{\pm 1\}$. Then N does not have a complementary subgroup.

Proposition 5. *Let $N \triangleleft G$. Then a subgroup $H \subset G$ is complementary to N if and only if the quotient map $G \to G/N$ restricted to H gives an isomorphism $H \to G/N$.*

Thus, we can think of the complementary subgroup H as a copy of G/N in G.

Proof. Since the kernel of $G \to G/N$ is N, the kernel of $H \to G/N$ is $N \cap H$. Hence $H \to G/N$ is injective if and only if $N \cap H = \{1\}$.

Next, the right coset Ng is the image of h under the quotient map if and only if $Nh = Ng$. In turn, $Nh = Ng$ if and only if there is an $n \in N$ such that $g = nh$. Since elements of G/N are exactly the right cosets Ng, we conclude that $H \to G/N$ is surjective if and only if every $g \in G$ can be expressed as $g = nh$ for some $n \in N$ and $h \in H$.

Combining the two, we get that $N \cap H = \{1\}$ and $HN = G$ if and only if $H \to G/N$ is injective and surjective, that is, an isomorphism. □

Example 6. Suppose $N \cong \mathbf{Z}_3$ and $H \cong \mathbf{Z}_2$. We find that there is more than one G that has N as its normal subgroup and H as its complementary subgroup:

(1) $G = \mathbf{Z}_6$, with $N = \{[0], [2], [4]\}$ and $H = \{[0], [3]\}$.
(2) $G = S_3$, with $N = A_3$ and $H = \{\mathrm{id}, (12)\}$.

Example 6 shows that we need more information to identify G than just the information of N and H. What is this extra piece of information? I claim that this extra piece is a homomorphism

$$\phi \colon H \to \operatorname{Aut} N.$$

Where does this ϕ come from? Suppose we have a G with $N \triangleleft G$ and complementary H. Let $h \in H$ and $n \in N$. Since N is normal, we have $hnh^{-1} \in N$. Thus, the rule $n \mapsto hnh^{-1}$ defines a function $\phi_h \colon N \to N$. Observe that the function ϕ_h is an automorphism of the group N. Furthermore, we have $\phi_{h_1 h_2} = \phi_{h_1} \circ \phi_{h_2}$. Indeed, for $n \in N$, we have

$$\phi_{h_1 h_2}(n) = h_1 h_2 n (h_1 h_2)^{-1} = h_1 (h_2 n h_2^{-1}) h_1^{-1} = \phi_{h_1} \circ \phi_{h_2}(n).$$

Thus the rule $h \mapsto \phi_h$ defines a homomorphism (which we denote by ϕ) from H to $\operatorname{Aut} N$, the group of automorphisms of N.

Given N, H, and $\phi \colon H \to \operatorname{Aut} N$, we can recover the group structure of G. To do so, we must describe how to multiply and take inverses in G. By Proposition 2 we can write elements of G uniquely as nh, for $n \in N$ and $h \in H$. Then we have

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

We have thus recovered the multiplication rule for G from the multiplication rules in N, H, and the function ϕ. We can also recover the inverse

$$(nh)^{-1} = h^{-1} n^{-1} = h^{-1} n^{-1} h \cdot h^{-1} = \phi_h^{-1}(n^{-1}) \cdot h^{-1}.$$

So far, we saw that a group G with $N \triangleleft G$ and complementary H gives a homomorphism $\phi \colon H \to \operatorname{Aut} N$ and this homomorphism, along with N and H, allows us to recover G. Suppose we now start with a group N, a group H, and a homomorphism $\phi \colon H \to \operatorname{Aut} N$, can we construct a G which has $N \triangleleft G$ and a complementary H where conjugation on N by elements of H corresponds exatly to ϕ? The answer is yes! We build G as follows. Let the elements of G be (n, h), where $n \in N$ and $h \in H$. Let the multiplication rule be

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2). \tag{1}$$

Proposition 7. *The above rule is associative, there is an identity, and every element has an inverse.*

Proof. The proof is straightforward. You should not read it, but do it yourself. Let us check associativity:

$$\begin{aligned}((n_1,h_1)\cdot(n_2,h_2))\cdot(n_3,h_3) &= ((n_1\phi_{h_1}(n_2),h_1h_2))(n_3,h_3)\\ &= (n_1\phi_{h_1}(n_2)\phi_{h_1h_2}(n_3),h_1h_2h_3)\\ &= (n_1\phi_{h_1}(n_2)\phi_{h_1}\circ\phi_{h_2}(n_3),h_1h_2h_3)\\ &= (n_1\phi_{h_1}(n_2\phi_{h_2}(n_3)),h_1h_2h_3)\\ &= (n_1,h_1)\cdot(n_2\phi_{h_2}(n_3),h_2h_3)\\ &= (n_1,h_1)\cdot((n_2,h_2)\cdot(n_3,h_3)).\end{aligned}$$

The identity is $(1,1)$, because

$$\begin{aligned}(n,h)\cdot(1,1) &= (n\phi_h(1),h) = (n,h)\\ (1,1)\cdot(n,h) &= (\phi_1(n),h) = (n,h).\end{aligned}$$

The inverse of (n,h) is $(\phi_h^{-1}(n^{-1}),h^{-1})$ because

$$\begin{aligned}(n,h)\cdot(\phi_h^{-1}(n^{-1}),h^{-1}) &= (n\phi_h\circ\phi_h^{-1}(n^{-1}),hh^{-1}) = (1,1)\\ (\phi_h^{-1}(n^{-1}),h^{-1})\cdot(n,h) &= (\phi_h^{-1}(n^{-1})\phi_{h^{-1}}(n),h^{-1}h) = (1,1).\end{aligned}$$

□

Definition 8. The group defined by the multiplication rule in Equation 1 is called the *semidirect product* of N and H via ϕ, and denoted by $N \rtimes_\phi H$.

Remark 9. Suppose the homomorphism $\phi\colon H \to \operatorname{Aut} N$ is trivial. Then $N \rtimes_\phi H$ is isomorphic to the direct product $N \times H$. Indeed, in this case the multiplication rule (Equation 1) becomes

$$(n_1,h_1)\cdot(n_2,h_2) = (n_1n_2,h_1h_2).$$

Note that the map $N \rtimes_\phi H \to H$ defined by $(n,h) \mapsto h$ is a homomorphism. Its kernel is $\{(n,1) \mid n \in N\}$, which is isomorphic to N. The set $\{(1,h) \mid h \in H\}$ forms a complementary subgroup. Thus, $N \rtimes_\phi H$ has a copy of N as a normal subgroup and a copy of H as a complementary subgroup. Finally, we check that in $N \rtimes_\phi H$, the homomorphism $\phi\colon H \to \operatorname{Aut} N$ comes from conjugation:

$$(1,h)\cdot(n,1)\cdot(1,h)^{-1} = (1,h)\cdot(n,1)\cdot(1,h^{-1}) = (\phi_h(n),h)\cdot(1,h^{-1}) = (\phi_h(n),1).$$

We can summarize the whole discussion in the following theorem.

Theorem 10. *Let G be a group with a normal subgroup N and a complementary subgroup H. Conjugation by elements of H gives a homomorphism $\phi\colon H \to \operatorname{Aut} N$ and we have an isomorphism $N \rtimes_\phi H \cong G$ defined by $(n,h) \mapsto nh$.*

Conversely, given N, H, and a homomorphism $\phi\colon H \to \operatorname{Aut} N$, we can construct a group G with N as a normal subgroup and H as a complementary subgroup such that ϕ is given by conjugation by elements of H.

Example 11. Let us identify the ϕ in some of the examples from Example 3 and thus exhibit them as semidirect products.

(1) Let $G = D_n$, $N \cong C_n$, the subgroup of rotations, and $H = \{\mathrm{id}, r\} \cong C_2$ be the complementary subgroup generated by a reflection r. Observe that $\phi_{\mathrm{id}} = \mathrm{id}$ and $\phi_r(x) = rxr^{-1} = x^{-1}$. Thus $\phi\colon C_2 \to \operatorname{Aut} C_n$ is the homomorphism that sends the generator of C_2 to the automorphism $x \mapsto x^{-1}$ of C_n. Thus we have
$$D_n \cong C_n \rtimes_\phi C_2.$$
(2) Let $G = M$, the group of isometries of the plane, $N = T \cong \mathbf{R}^2$, the subgroup of translations and $H \cong O_2$ be the complementary subgroup of isometries fixing the origin. Then $\phi_A(t_v) = At_vA^{-1} = t_{Av}$. Thus, $\phi\colon O_2 \to \operatorname{Aut} \mathbf{R}^2$ is simply the homomorphism that sends the matrix A to the automorphism of $\mathbf{R}^2$ defined by left multiplication by A. Thus we have
$$M \cong \mathbf{R}^n \rtimes_\phi O_2.$$
(3) Let $G = O_3$, $N = SO_3$, and $H = \{I, -I\} \cong \mathbf{Z}_2$. Note that conjugation by either I or $-I$ is the identity operation, and thus the homomorphism $\phi\colon H \to \operatorname{Aut} N$ in this case is trivial. We thus get
$$O_3 \cong SO_3 \times \mathbf{Z}_2.$$

Example 12. Let us construct a group as a semidirect product. Let $N = \mathbf{Z}$, $H = \mathbf{Z}_2$ and let $\phi\colon H \to \operatorname{Aut} N$ be the homomorphism that sends $[0]$ to the identity automorphism of N and $[1]$ to the automorphism of N given by $n \mapsto -n$. We then get a group
$$G = \mathbf{Z} \rtimes_\phi \mathbf{Z}_2.$$
Note that G is not abelian. We have
$$(m, [0]) \cdot (n, [1]) = (m + \phi_{[0]}(n), [1]) = (m + n, [1]),$$
but
$$(n, [1]) \cdot (m, [0]) = (n + \phi_{[1]}(m), [1]) = (n - m, [1]).$$
In particular, G is not isomorphic to $\mathbf{Z} \times \mathbf{Z}_2$; it is something new!

We may wonder whether we have seen G before. Consider the group G' of isometries of the infinite pattern
$$\cdots \mathrm{T\,T\,T\,T\,T\,T\,T\,T} \cdots.$$
Let N' be the normal subgroup of G' consisting of translations. Then $N' \cong \mathbf{Z}$. Let r be the reflection in a vertical line. Then $H' = \{\mathrm{id}, r\}$ forms a subgroup complementary to N'. Denoting by t_n the translation by n, we see that
$$rt_nr^{-1} = t_{-n}.$$
Hence the homomorphism $H' \to \operatorname{Aut} N'$ given by conjugation corresponds exactly to the ϕ we had above. We thus realize that
$$G' \cong \mathbf{Z} \rtimes_\phi \mathbf{Z}_2.$$

References

[1] David Dummit and Richard Foote *Abstract Algebra, 3E* John Wiley & Sons 2004.
[2] Walter Neumann *Notes on Semidirect Products*, `www.math.columbia.edu/~bayer/S09/ModernAlgebra/semidirect.pdf`