Semidirect Products

Patrick J. Morandi

September 18, 1998

Let G be a group. Recall that G is a direct product of two groups iff G contains normal subgroups N_1, N_2 such that $N_1 \cap N_2 = \{e\}$ and $G = N_1 N_2$. We discuss here a generalization of this notion. Suppose instead that we have a group G that contains subgroups N and H such that N is normal in G, $N \cap H = \{e\}$, and that $G = NH$. Under these circumstances, we call G a *semidirect product* of N and H.

Suppose that $G = NH$ with N and H as above. Note that every element of G is uniquely expressible in the form nh; the uniqueness follows from $N \cap H = \{e\}$, since if $nh = n'h'$, then $(n')^{-1} n = h'h^{-1} \in N \cap H$. Since N is normal in G, for each $h \in H$ we have an automorphism of N given by $n \mapsto hnh^{-1}$. In other words, this automorphism is the inner automorphism of h restricted to N. Furthermore, the map $H \to \mathrm{Aut}(N)$ given by $h \mapsto (n \mapsto hnh^{-1})$ is a group homomorphism. To verify this, let us write φ_h for the inner automorphism of h restricted to N. We have for $g, h \in H$ and $n \in N$,

$$\begin{aligned} \varphi_{gh}(n) &= ghn(gh)^{-1} = ghnh^{-1}g^{-1} \\ &= g(hnh^{-1})g^{-1} = \varphi_g(hnh^{-1}) \\ &= \varphi_g(\varphi_h(n)) = (\varphi_g \circ \varphi_h)(n). \end{aligned}$$

So, $\varphi_{gh} = \varphi_g \circ \varphi_h$. Therefore, the map $\varphi : H \to \mathrm{Aut}(N)$ given by $\varphi(h) = \varphi_h$ is a homomorphism of groups, as claimed. Furthermore, given the subgroups N, H and the homomorphism φ, we can write down the multiplication on G. For, given $nh, n'h' \in G$, we have

$$\begin{aligned} (nh)(n'h') &= (nhn'h^{-1})(hh') \\ &= (n\varphi_h(n'))(hh'). \end{aligned}$$

We now show that we can reverse this process, thereby giving a notion of "external" semidirect product. Let N and H be groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homo-

morphism. Let $G = N \times H$ as sets, and define multiplication by

$$(n, h)(n', h') = (n\varphi_h(n'), hh').$$

Then it is an easy exercise to show that G is a group; the identity of G is (e_N, e_H), and the inverse of (n, h) is $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Furthermore, the subset $N' := N \times \{e_H\}$ is a normal subgroup of G isomorphic to N and $H' := \{e_N\} \times H$ is a subgroup of G isomorphic to H. Moreover, $N' \cap H' = \{e_G\}$. Thus, from this external construction we obtain G as an internal semidirect product of N' and H'. We denote this external semidirect product by $N \times_\varphi H$ (and sometimes by $N \rtimes H$).

We note some simple facts about this construction. First, we get the direct product $N \times H$ as the semidirect product $N \times_\varphi H$, where $\varphi : H \to \mathrm{Aut}(N)$ is the trivial group homomorphism (that sends every element of H to the identity), since for this φ, $(n, h)(n', h') = (n\varphi_h(n'), hh') = (nn', hh')$, the formula for multiplication in $N \times H$. Second, with $H' = \{e_N\} \times H$, we see that H' is normal in G iff φ is trivial. For, if there is an $h \in H$ and $n \in N$ such that $\varphi_h(n) \neq n$, then

$$\begin{aligned}(n, 1)(1, h)(n, 1)^{-1} &= (n, 1)(1, h)(n^{-1}, 1) \\ &= (n, h)(n^{-1}, 1) \\ &= (n\varphi_h(n)^{-1}, h) \notin H',\end{aligned}$$

so if φ is nontrivial, then H' is not normal in G. Conversely, if φ is trivial, then G is the direct product $N \times H$, in which case H' is normal in G. Finally, if φ is not the trivial map, then $N \times_\varphi H$ is non-Abelian, even if N and H are both Abelian. To show this, suppose that there are $h \in H$ and $n \in N$ such that $\varphi_h(n) \neq n$. We then have

$$\begin{aligned}(n, 1)(1, h) &= (n, h), \\ (1, h)(n, 1) &= (\varphi_h(n), h),\end{aligned}$$

so $(n, 1)(1, h) \neq (1, h)(n, 1)$. Using semidirect products is a nice way to construct non-Abelian groups.

We now give a number of examples of semidirect products.

Example 1 Let $N = \mathbb{Z}/n\mathbb{Z}$, let $H = \mathbb{Z}/2\mathbb{Z}$, and let $\varphi : H \to \mathrm{Aut}(N)$ be the homomorphism that sends e to e and the nontrivial element of H to the inverse map of N. In other words, the map $x \mapsto x^{-1}$ is a group automorphism of N since N is Abelian, and this automorphism has order 2. So, it generates a subgroup of $\mathrm{Aut}(N)$ isomorphic to H; we define the map φ to be the isomorphism of H onto this subgroup. Let $G = N \times_\varphi H$. We claim that $G \cong D_n$, the

Dihedral group of order $2n$. Recall that D_n is the group generated by elements a, b subject to the relations $a^n = b^2 = 1$ and $bab = a^{-1}$. Let $N = \langle x \rangle$ and $H = \langle y \rangle$. Then $(x, 1)$ has order n and $(1, y)$ has order 2. Note that φ_y is the inverse map on N. So,

$$\begin{aligned}(1,y)(x,1)(1,y) &= (\varphi_y(x), y)(1,y) = (\varphi_y(x), y^2) = (\varphi_y(x), 1) \\ &= (x^{-1}, 1) = (x,1)^{-1}.\end{aligned}$$

Therefore, in G we have elements $u = (x, 1)$ and $v = (1, y)$ satisfying $u^n = v^2 = 1$ and $vuv = u^{-1}$. So, there is a group homomorphism $D_n \to G$, and this map is surjective since G is clearly generated by u, v. However, $|G| = |N|\,|H| = 2n$, so $|G| = |D_n|$. This shows that D_n is isomorphic to G.

Example 2 Consider the alternating group A_4. The subgroup

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

is normal in A_4. The subgroup $H = \langle (123) \rangle$ is a subgroup of order 3 that is not normal in A_4. Since $|V|$ and $|H|$ are relatively prime, we have $V \cap H = \{1\}$. So, A_4 is the semidirect product of V and H. We can determine the appropriate homomorphism φ by determining $\varphi_{(123)}$. We have

$$\begin{aligned}(123)(12)(34)(123)^{-1} &= (23)(14), \\ (123)(13)(24)(123)^{-1} &= (21)(34), \\ (123)(14)(23)(123)^{-1} &= (24)(13).\end{aligned}$$

Since φ is a group homomorphism, $\varphi_{(123)^2} = \left(\varphi_{(123)}\right)^2$. This in effect determines φ. Let $a = (12)(34)$, $b = (13)(24)$, and $c = (123)$. Then V is generated by a, b and H is generated by c. We have the relations $a^2 = b^2 = 1$ and $ab = ba$ in V, and $c^3 = 1$ in H. Moreover, the relations above say that $cac^{-1} = ab$ and $cbc^{-1} = a$. Note that the third equation is a consequence of the previous two, since $(13)(24) = b = a(ab)$. So, if G is the group generated by x, y, z subject to the relations $x^2 = y^2 = z^3 = 1$, $xy = yx$, $zxz^{-1} = xy$, and $zyz^{-1} = x$, then there is a surjective group homomorphism $G \to A_4$. By playing with these relations, one can show that $|G| \leq 12 = |A_4|$. This forces $G \cong A_4$.

Example 3 The symmetric group S_4 can also be described as a semidirect product using V. Let $H = \{\sigma \in S_4 : \sigma(4) = 4\}$. Then H is a subgroup of S_4 isomorphic to S_3, and $|H| = 6$. Moreover, by inspection we see that $V \cap H = \{1\}$. So, S_4 is a semidirect product of V with H. In order to describe the corresponding map φ, we view these groups in other ways. First, $H \cong S_3$, as noted above. Second, V is a $\mathbb{F}_2$-vector space, and any element

of $\mathrm{Aut}(V)$ is actually an $\mathbb{F}_2$-vector space automorphism. Since $\dim_{\mathbb{F}_2}(V) = 2$, we see that $\mathrm{Aut}(V) \cong \mathrm{Gl}_2(\mathbb{F}_2)$. So, φ can be viewed as a group homomorphism $S_3 \to \mathrm{Gl}_2(\mathbb{F}_2)$. Moreover, $|\mathrm{Gl}_2(\mathbb{F}_2)| = 6$, and, in fact, the map φ is an isomorphism from S_3 to $\mathrm{Gl}_2(\mathbb{F}_2)$. To see this explicitly, we view V as an $\mathbb{F}_2$-vector space with basis $u = (12)(34)$, $v = (13)(24)$. Moreover, $H = \langle (123), (12) \rangle$. Conjugation by (123) sends u to uv and v to u (see the previous example). So, we may view this transformation as the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Also, conjugation by (12) sends u to u and v to uv, so this transformation corresponds to the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. This is enough information to explicitly write down the isomorphism φ. (Think about linear transformations correspond to matrices in order to see how we obtained these two matrices!)

Example 4 Let p, q be primes such that p divides $q-1$. Then $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ is a cyclic group of order $q-1$, so it has an element of order p. Explicitly, if r is an integer such that $r^p \equiv 1 \bmod q$ but $r \not\equiv 1 \bmod q$, then the automorphism f given by $f(a + q\mathbb{Z}) = a^r + q\mathbb{Z}$ has order p. If we send a generator of $\mathbb{Z}/p\mathbb{Z}$ to this element, we get a homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. Let G be the semidirect product of these groups. If $\mathbb{Z}/p\mathbb{Z} = \langle a \rangle$ and $\mathbb{Z}/q\mathbb{Z} = \langle b \rangle$, then with $\varphi(a) = f$, we have $a^p = b^q = 1$ and $aba^{-1} = \varphi_a(b) = f(b) = b^r$. So, this semidirect product is a group of order pq, and since $aba^{-1} = b^r \neq b$ (as $r \not\equiv 1 \bmod q$), we see that G is non-Abelian. It is an exercise to show that any non-Abelian group of order pq (with p dividing $q-1$) is isomorphic to this semidirect product.

Example 5 Let $N = \mathbb{Z}/3\mathbb{Z} = \langle a \rangle$ and $H = \mathbb{Z}/4\mathbb{Z} = \langle b \rangle$. We have a homomorphism $\varphi : H \to \mathrm{Aut}(N)$ that sends b to the automorphism $x \mapsto x^{-1}$. This is well defined since the inverse map has order 2. Consider $G = N \times_\varphi H$. Then $|G| = 12$. Moreover, N is a normal subgroup of G but H is not normal in G (since φ is nontrivial). Thus, G has a normal 3-Sylow subgroup but G does not have a normal 2-Sylow subgroup. So, this is a non-Abelian group of order 12 distinct from A_4. It is another exercise to show that any non-Abelian group of order 12 is isomorphic to either G or to A_4.

Example 6 Let $N = \mathbb{Z}/5\mathbb{Z} = \langle a \rangle$ and let $H = \mathbb{Z}/4\mathbb{Z} = \langle b \rangle$. The group $\mathrm{Aut}(N)$ is cyclic of order 4; a generator is f, where f is defined by $f(a^i) = a^{2i}$. By sending b to f, we get a group isomorphism $\varphi : H \to \mathrm{Aut}(N)$. Let $G = N \times_\varphi H$. Then $|G| = 20$. Moreover, G is generated by a, b, and the generators satisfy $a^5 = b^4 = 1$ and $bab^{-1} = a^2$. This group arises as a Galois group in the following way. Let $\alpha \in \mathbb{Q}$ be such that $x^5 - \alpha$ is irreducible over $\mathbb{Q}$ (e.g., take α to be any element that is not a 5-th power). If ω is a primitive 5-th root of unity and β is any root of $x^5 - \alpha$, then the splitting field over $\mathbb{Q}$ of $x^5 - \alpha$ is $\mathbb{Q}(\omega, \beta)$. Moreover, there are automorphisms of $\mathbb{Q}(\omega, \beta)$ satisfying $\sigma(\beta) = \omega\beta$ and $\sigma(\omega) = \omega$, and $\tau(\beta) = \beta$ and $\tau(\omega) = \omega^2$

(apply the isomorphism extension theorem to $\mathbb{Q}(\omega,\beta)/\mathbb{Q}(\omega)$ and $\mathbb{Q}(\omega,\beta)/\mathbb{Q}(\beta)$, respectively. You also need to know that $\min(\mathbb{Q}(\beta),\omega) = \min(\mathbb{Q},\omega)$). The group G is generated by σ,τ since the fixed field of $\{\sigma,\tau\}$ is $\mathbb{Q}$. Moreover, σ,τ satisfy $\sigma^5 = \tau^4 = \mathrm{id}$ and $\tau\sigma\tau^{-1} = \sigma^2$. By showing that the group generated by x, y subject to the relations $x^5 = y^4 = 1$ and $yxy^{-1} = x^2$ has order at most 20, we will have shown that it has order 20, and that it is isomorphic to both G and to $\mathrm{Gal}(\mathbb{Q}(\omega,\beta)/\mathbb{Q})$. Therefore, G is isomorphic to this Galois group.

Example 7 The group S_n is the semidirect product of A_n and $H = \langle(12)\rangle \cong \mathbb{Z}/2\mathbb{Z}$, since A_n is normal in S_n and $A_n \cap H = \{1\}$. However, We won't describe here what is the map φ.

Example 8 Let N be a group. We can form the semidirect product $G = N \times_\varphi \mathrm{Aut}(N)$, where $\varphi : \mathrm{Aut}(N) \to \mathrm{Aut}(N)$ is the identity map. So, multiplication in G is given by

$$(n,\sigma)(m,\tau) = (n\sigma(m),\sigma\tau),$$

where $n, m \in N$ and $\sigma,\tau \in \mathrm{Aut}(N)$.

Example 9 Not all groups can be described as semidirect products of smaller groups. If $G = Q_8$, the quaternion group, then $G = \{\pm 1, \pm i, \pm j, \pm k\}$, where multiplication is defined by using $i^2 = j^2 = k^2 = -1$ and $ij = k = -ji$. The only subgroups of G are $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, $\langle -1\rangle$, and each contains -1. So, there does not exist two nontrivial subgroups of G that have trivial intersection. So, G is not the semidirect product of two proper subgroups. Likewise, if $n \geq 5$, then the alternating group A_n is not a semidirect product of proper subgroups. This follows from the fact that A_n is simple; there are no nontrivial normal subgroups of A_n.