Semidirect products

Jack Schmidt

Semidirect products are a very useful rudiment of finite group theory, but the difficulties in working with them are often both under- and over-estimated. This document attempts to handle some of these issues.

A motivating example: describe the semi-direct products of S_3 by S_3. In this case we get 3 conjugacy classes of actions $f : S_3 \to \mathrm{Aut}(S_3)$, but when we look more closely at the result semi-direct products, they all turn out to be isomorphic to $S_3 \times S_3$. Why is this?

The first section tries to explain this, but first we fix notation and definitions.

Definition 1. If Q, N are groups and $f : Q \to \mathrm{Aut}(N)$ is a homomorphism, then the group $Q \ltimes_f N$, the **external semidirect product** of Q acting on N, is defined on the set $Q \times N$ using the rule $(q, n) \cdot (r, m) = (qr, n^{(r^f)}m)$ where $n^{(r^f)}$ is also written $f(r)(n)$. Note that $(1, 1)$ is the identity element, and $(q, k)^{-1} = (q^{-1}, x)$ where $x^q = k^{-1}$.

The subgroups $Q \ltimes 1 = \{(q, 1) : q \in Q\}$ and $1 \ltimes N = \{(1, n) : n \in N\}$ have the nice property that $1 \ltimes N$ is normal, $(Q \ltimes 1)(1 \ltimes N) = Q \ltimes N$ and $(Q \ltimes 1) \cap (1 \ltimes N) = 1$.

Definition 2. Suppose G is a group, with normal subgroup $N \trianglelefteq G$ and subgroup $Q \leq G$ with $G = QN$ and $Q \cap N = 1$. Then G is called the **internal semidirect product** of Q acting on N. The **action** is the homomorphism $f : Q \to \mathrm{Aut}(N) : q \mapsto (n \mapsto n^q)$. Here q^n is also written as $n^{-1}qn$.

The following calculation is routine and shows the difference between internal and external semidirect products is just a matter of omitting parentheses.

Proposition 3. If G is an internal semidirect product of Q and N with action f, then each element of G has a unique expression as qn for $q \in Q$ and $n \in N$ and there is an isomorphism from G to $Q \ltimes_f N$ given by $qn \mapsto (q, n)$. Conversely, the external semidirect product is an internal semidirect product of $(Q \ltimes 1)$ acting on $(1 \ltimes N)$ with action $\bar{f} : (Q \ltimes 1) \to \mathrm{Aut}(1 \ltimes N) : (q, 1) \mapsto ((1, n) \mapsto (1, n^{q^f})$, which upon identifying Q with $Q \ltimes 1$ and N with $1 \ltimes N$ just becomes f.

1 Complements to a normal subgroup

If G is an internal semidirect product of Q acting on N, can it also be an internal semidirect product of R acting on N? Can we find all the R? How do the actions of Q and R relate?

Definition 4. If $N \trianglelefteq G$ is a normal subgroup, then a subgroup $Q \leq G$ is called a **complement** to N in G iff $G = QN$ and $Q \cap N = 1$. A normal subgroup is called **complemented** if it has a complement.

We first observe that any conjugate of a complement is a complement.

Proposition 5. If Q is a complement to N in G, then Q^g is also a complement to N in G. The action of Q^g is $Q \times \mathrm{Inn}(N)$-conjugate to the action of Q.

Proof. This follows form the fact that conjugation is an automorphism fixing N: $G = G^g = (QN)^g = Q^g N^g = Q^g N$ and $1 = 1^g = (Q \cap N)^g = Q^g \cap N^g = Q^g \cap N$. Note that $g = qn$ and $Q = Q^q$ so up to Q-conjugacy, the action of Q and Q^q are the same. The action of Q^n is then $f(q^n)(x) = x^{n^{-1}qn} = ((x^{n^{-1}})^q)^n$, so $f(q^n)$ is the conjugate of $f(q)$ by the inner automorphis of N induced by n. □

What does Q^g look like? This is especially clear in the external case:

Proposition 6. $(Q \ltimes 1)^{(q,n)} = \{(r, [r, n]) : r \in Q\}$ where $[r, n] = (n^{-1})^r \cdot n$ externally and $[r, n] = r^{-1}n^{-1}rn$ internally.

Proof. Easy calculation. □

Notice how for each $q \in Q$, the conjugate of Q^n of Q has a unique element of the form (q, y), with $y = [q, n]$. In other words, there is a function $\delta_n : Q \to N : q \mapsto [q, n]$ and $Q^n = \{(q, \delta_n(q)) : q \in Q\}$ is the graph of that function.

Definition 7. The **graph** of a function $\delta : Q \to N$ is the set $\{(q, \delta(q))\} \subseteq Q \times N$.

In fact we can prove that every conjugate is the graph of a function!

Proposition 8. If R is a complement to $(1 \ltimes N)$ in $Q \ltimes N$, then R is the graph of a function $\delta : Q \to N$.

Proof. Since $(q, 1) \in Q \ltimes N = R(1 \ltimes N)$ there must be some $(q, n) \in R$ and $(1, n^{-1}) \in 1 \ltimes N$ such that $(q, 1) = (q, n) \cdot (1, n^{-1})$. If (q, n) and (q, m) are both in R, then

$$(q, n)^{-1}(q, m) = (q^{-1}, (n^{-1})^{(q^{-1})}) \cdot (q, m) = (1, n^{-1}m) \in R \cap (1 \ltimes N) = 1,$$

so $m = n$. This means that for every $q \in Q$, there is a uniquely defined $\delta(q) \in N$ such that $q\delta(q) \in R$. □

Does every function work? Well conjugates only come from functions of the form $q \mapsto [q, n]$. These functions have a special name and are part of a larger collection of functions called derivations (hence the name derived subgroup) or crossed homomorphisms, since they satisfy a twisted or crossed version of the defining property of homomorphisms.

Definition 9. An f-**crossed homomorphism** from Q to N, where $f : Q \to \mathrm{Aut}(N)$, is a function $\delta : Q \to N$ with the property

$$\delta(qr) = \delta(q)^{(r^f)}\delta(r).$$

A **principal** f-**crossed homomorphism** is an f-crossed homomorphism of the form $q \mapsto (n^{-1})^{(q^f)}n$.

A quick calculation confirms:

Proposition 10. A principal f-crossed homomorphism is an f-crossed homomorphism.

And we come to the main theoretical result of this section:

Proposition 11. The complements of $1 \ltimes N$ in $Q \ltimes_f N$ are exactly the graphs of the f-crossed homomorphisms from Q to N.

XXX: Include the action here?

Proof. The graph R a function from Q to N is always a sort of complement in that $R(1 \ltimes N) = Q \ltimes N$ and $R \cap (1 \ltimes N) = 1$, as the previous proof has shown. The main trouble is whether R is in fact a subgroup. In other words, which functions have graphs that are subgroups? Well we just need $(q, \delta(q)) \cdot (r, \delta(r)) = (qr, \delta(q)^{r^f}\delta(r))$ to be of the form $(s, \delta(s))$. Since $s = qr$, we get the needed equality $\delta(qr) = \delta(q)^{(r^f)}\delta(r)$, and δ must be a f-crossed homomorphism in order for its graph to be a subgroup. Conversely of course the same calculations show that the graph of an f-crossed homomorphism is a subgroup. $\square$

Now we use this to give a suprising family of examples.

Example 12. Suppose Q, N are groups and $\hat{f} : Q \to N$ is a homomorphism. Define $f : Q \to \mathrm{Aut}(N) : q \mapsto (n \mapsto n^{(q^{\hat{f}})})$, so that $f(q)$ is the inner automorphism of N defined by $\hat{f}(q)$. Then $Q \ltimes_f N \cong Q \times N$.

Proof. Let $G = Q \times N = Q \ltimes_t N$ where $t : Q \to \mathrm{Aut}(N) : q \mapsto (n \mapsto n)$ is the trivial action. A t-crossed homomorphism is just a homomorphism, so the graph of $\hat{f}$ is a complement to $1 \ltimes_t N$. But the graph of $\hat{f}$ is $(q, \hat{f}(q))$ and the action on $(1, x)$ is $(q, \hat{f}(q))^{-1}(1, x)(q, \hat{f}(q)) = \left(q^{-1}(\hat{f}(q)^{-1})^{q^{-1}}\right) \cdot (1, x) \cdot (q, \hat{f}(q)) = (q^{-1}q, \hat{f}(q)^{-1}x\hat{f}(q)) = (1, x^{q^f})$, so the action of the graph R of $\hat{f}$ on $1 \ltimes N$ is just f. By the internal-external equivalence, $Q \ltimes_t N = R(1 \ltimes_t N) \cong R \ltimes_f N \cong Q \ltimes_f N$. $\square$

In particular, if $Q = N = S_3$, then $\mathrm{Aut}(N) = \mathrm{Inn}(N) \cong N$ and every action f comes from some $\hat{f}$, so every semidirect product of S_3 by S_3 is isomorphic to the direct product.

Jack Schmidt

Contents