CHAPTER 16

Semidirect products are split short exact sequences

Chit-chat 16.1. Last time we talked about short exact sequences

$$G \to H \to K.$$

To make things easier to read, from now on we'll write

$$L \to H \to R.$$

The L is for left, the R is for right. Since $L \to H$ is injective, from now on we'll identify L with its image in H for simplicity of notation.

Note there is no way to think of R as a subgroup of H a priori. For instance, in the example

$$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$$

the second copy of $\mathbb{Z}/2\mathbb{Z}$ doesn't naturally "embed" back into $\mathbb{Z}/4\mathbb{Z}$.

Proposition 16.2. The above short exact sequence doesn't split.

PROOF. $\mathbb{Z}/2\mathbb{Z}$ only has elements of order 1 and 2, so no homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ can have an image containing elements of order ≥ 3. [1]

But let's observe that both [1] and [3] are elements of order 4 inside $\mathbb{Z}/4\mathbb{Z}$:

$$\langle [1] \rangle = \{[1], [2], [3], [0]\}, \qquad \langle [3] \rangle = \{[3], [6] = [2], [5] = [1], [0]\}.$$

Hence any homomorphism $j : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ must have image contained in $\{[0], [2]\} \subset \mathbb{Z}/4\mathbb{Z}$. But this is the kernel of the map from $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ above; so no j could factor the identity map of $R = \mathbb{Z}/2\mathbb{Z}$. □

Here's a more dramatic example:

Example 16.3. The short exact sequence

$$\mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

does not split for any $n \neq -1, 0, 1$. [2]

[1] After all, if $g^n = 1$, we must have that $j(g)^n = 1$ as well.

[2] Any homomorphism from $\mathbb{Z}/n\mathbb{Z}$ must send an element of order n to some element of finite order. But $\mathbb{Z}$ has no element of finite order except 0, so there is no injection from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}$.

Chit-chat 16.4. Since this is our first time trying to understand short exact sequences, let's try to analyze the case where we *are* allowed to think of R as a subgroup of H. If both L and R are inside H, maybe you'll buy the philosophy more that H is "built up" from L and R. So we come to the definition we ended with last time:

Definition 16.5. A short exact sequence *splits* if there is a group homomorphism $j : R \to H$ such that the composition $R \xrightarrow{j} H \to R$ is equal to id_R. We will call a choice of $j : R \to H$ a *splitting*.

Chit-chat 16.6. So if the short exact sequence is given by homomorphisms $\phi : L \to H, \psi : H \to R$, the definitions says that $\psi \circ j = \mathrm{id}_R$. In particular, j is an *injection*.

Chit-chat 16.7. In the above example, clearly there is no way to think about $\mathbb{Z}/n\mathbb{Z}$ as a subgroup of $\mathbb{Z}$.

Chit-chat 16.8. So we have a new idea. We'd like to be able to recognize semidirect products in nature, and we'd like to be able to produce examples! Let's analyze.

As before, let's identify R with $j(R)$ when we have a split short exact sequence. Well, every element of R defines an action on H itself by conjugation: $h \mapsto rhr^{-1}$. But since L is normal, $rLr^{-1} = L$, so this defines an action on L, via $C_r : l \mapsto rlr^{-1}$.

Moreover, this is a group isomorphism from L to itself. As you showed in your homework, this defines a group homomorphism $R \to \mathrm{Aut}(L)$ given by $r \mapsto C_r$. So any splitting gives rise to a homomorphism $R \to \mathrm{Aut}(L)$. [3]

Question 16.9. Fix two groups R and L. The natural question is: Does any homomorphism $R \to \mathrm{Aut}(L)$ give rise to a split exact sequence?

Chit-chat 16.10. Another observation is that, given a splitting, both R and L become subgroups of H. Moreover, their intersection consists only of 1_H—after all, if a non-identity element $l \in L \cap R$, then the map $R \to H \to R$ could not be injective (l would be in the image of R, hence in the kernel of $H \to L$). Finally, since the orbits of the L action span H itself, we see that $H = \bigcup_{r \in R} Lr$. That is, $H = LR$.[4]

[3] Here, $\mathrm{Aut}(L)$ refers to the group of *group automorphisms*; not of set automorphisms.

[4] See below.

Definition 16.11. Let L, R be subgroups of H. We let

$$LR = \{g \text{ such that } g = lr \text{ for some } l \in L, r \in R\}.$$

Question 16.12. Fix $L, R \subset H$. If $L \cap R = \{1\}$, $L \subset H$ is normal, and $LR = H$, is H a semidirect product of L and R?

What good questions we ask, when the answers are yes!

Theorem 16.13. Fix a normal subgroup $L \subset H$, and let $R \cong H/L$. The following are equivalent:

(1) A homomorphism $j : R \to H$ splitting a short exact sequence $L \to H \to R$.
(2) An isomorphism $R \to R'$ to a subgroup $R' \subset H$ such that $R' \cap L = \{1\}$ and the set map $L \times R' \to H$ is a surjection.
(3) A group homomorphism $\phi : R \to \mathrm{Aut}(L)$.

Proof. Another time. □

Chit-chat 16.14. Of these, my favorite interpretation is the last. It's because it has no reference to the group H—once you construct a group homomorphism $\phi : R \to \mathrm{Aut}(L)$, one can construct a short exact sequence $L \to H \to R$.

What is the group operation on H in terms of R and L?

Proposition 16.15. Fix a homomorphism

$$\phi : R \to \mathrm{Aut}(L), \qquad r \mapsto \phi_r.$$

Then

(1) the following defines a group structure on the set $L \times R$:

$$(l_1, r_1) \cdot (l_2, r_2) := (l_1 \cdot \phi_{r_1}(l_2), r_1 r_2).$$

Moreover,
(2) The set $\{(l, 1)\}$ is a normal subgroup isomorphic to L,
(3) The set $\{(1, r)\}$ is a subgroup isomorphic to R.

Definition 16.16. Given $\phi : R \to \mathrm{Aut}(L)$, we will write

$$L \rtimes_\phi R$$

to be the group defined in the above proposition. We call it the *semidirect product* of L by R. When ϕ is implicit, we will drop the subscript and simply write

$$L \rtimes R.$$

PROOF. Clearly, $(1,1)$ is the identity element, since $\phi_1 = \mathrm{id}_L$. Likewise, the inverse to (l,r) is the element $(\phi_r^{-1}(l^{-1}), r^{-1})$:

$$\begin{aligned}(\phi_r^{-1}(l^{-1}), r^{-1}) \cdot (l,r) &= (\phi_r^{-1}(l^{-1}) \cdot \phi_{r^{-1}}(l), r^{-1}r) \\ &= (\phi_r^{-1}(l^{-1}) \cdot \phi_r^{-1}(l), r^{-1}r) \\ &= (\phi_r^{-1}(l^{-1}l), r^{-1}r) \\ &= (1,1).\end{aligned}$$

and

$$\begin{aligned}(l,r) \cdot (\phi_r^{-1}(l^{-1}), r^{-1}) &= (l\phi_r(\phi_r^{-1}(l^{-1})), rr^{-1}) \\ &= (ll^{-1}, rr^{-1}) \\ &= (1,1).\end{aligned}$$

I'll leave it to you to check associativity. □

Chit-chat 16.17. Next time, we'll study the symmetries of the regular n-gon. This group can be written as a semi-direct product.

1. Some practice

Exercise 16.18. If L and R are finite groups, and if one has a short exact sequence $1 \to L \to H \to R \to 1$, verify that $|H| = |L| \cdot |R|$.

Exercise 16.19. If L is an abelian group, show that the "inversion" map $a \mapsto a^{-1}$ is a group automorphism. Show that this defines a group homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(L)$.

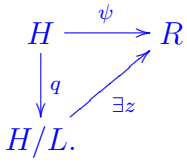
Exercise 16.20. Convince yourself that all the non-splitting short exact sequences from this lecture really don't split.

2. Proof that $H = LR$

By request, here is a more detailed proof that $H = LR$ when the SES splits.

Lemma 16.21. Let $L \to H \xrightarrow{\psi} R$ be a short exact sequence. Let $q : H \to H/L$ be the quotient homomorphism sending $h \mapsto Lh$. Then there exists an isomorphism $z : H/L \to R$ such that $z \circ q = \psi$. (That is, there exists a z so

that the diagram



is commutative.)

Once we have the lemma, we have

Corollary 16.22. If $j : R \to H$ is a splitting of the $L \to H \to R$, then

$$H = \bigcup_{r \in R} Lj(r).$$

Proof of corollary. By definition of splitting, we have that $\psi \circ j = \mathrm{id}_R$. On the other hand, we know that $\psi = z \circ q$ by the Lemma, so we have

$$z \circ q \circ j = \mathrm{id}_R .$$

Since z is a group isomorphism, its inverse is a homomorphism, and we have an equality of homomorphisms

$$q \circ j = z^{-1}.$$

Now we interpret the map $q \circ j$. The homomorphism q sends $h \mapsto Lh$. So the composite $q \circ j$ sends r to the coset $Lj(r) \in H/L$. Well, z^{-1} is a bijection onto H/L, so for any coset $Lh \in H/L$, we have a unique $r \in R$ for which $Lh = Lj(r)$. Since

$$\bigcup_{H/L} Lh = H,$$

this proves that

$$\bigcup_{r \in R} Lj(r) = H.$$

In the notes above, we identified elements $r \in R$ with their image in H using j, so we wrote this as

$$\bigcup_{r \in R} Lr = H.$$

□