Notes on Semidirect Products

Alex Provost

November 21, 2015

Contents

1 Introduction 1
2 Short exact sequences, group extensions 1
3 Split extensions 2
4 Semidirect products: existence and uniqueness 6
5 More examples 8

1 Introduction

Given two groups K and H, a semidirect product of K and H is a group G containing K and H as subgroups, with K normal inside G, and with a unique factorization $G = KH$. As we will see through many examples, semidirect products appear naturally in group theory and geometry. Our preferred approach of introducing semidirect products as split extensions is slightly more abstract than the standard, hands-on construction, but we believe that this method offers a clearer perspective of the big picture.

In these notes we work almost exclusively in the category of groups. Unless stated otherwise, every object is a group and every arrow is a group homomorphism. Depending on the context, the symbol 1 denotes the trivial group or the identity in a given group (except in some rings like $\mathbb{Z}$ or $\mathbb{Z}/n$). The symbol 1_G denotes the identity map on G.

2 Short exact sequences, group extensions

Definition. A **short exact sequence of groups** is a sequence of groups and group homomorphisms of the form

$$1 \to K \to G \to H \to 1 \tag{2.1}$$

which is exact. Exactness means that everywhere an arrow enters and leaves an object, the image of the entering arrow is equal to the kernel of the exiting arrow. Explicitly, this says that $K \to G$ is injective, $G \to H$ is surjective, and $\mathrm{im}(K \to G) = \ker(G \to H)$.

In practice, this allows one to identify K with its homomorphic image $\mathrm{im}(K \to G) = \ker(G \to H)$, which is a kernel and thus normal, and so by the first isomorphism theorem $H \cong G/K$.

Any homomorphism f from a group G to some other group induces a short exact sequence

$$1 \to \ker(G \to \mathrm{im}\, f) \to G \to \mathrm{im}\, f \to 1,$$

and of course every short exact sequence is of this form.

Example 1 (Two non-split extensions)**.** There are short exact sequences

$$1 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2 \to 1,$$

$$1 \to \mathbb{Z}/2 \xrightarrow{2} \mathbb{Z}/4 \to \mathbb{Z}/2 \to 1.$$

In both sequences, the monomorphism is multiplication by 2 and the epimorphism is reduction mod 2.

When one has a short exact sequence as in (2.1), we say that G is an **extension of H by K**. In general, given two groups K and H, it is a very hard problem to classify all the extensions of H by K.

3 Split extensions

The problem of classifying extensions of H by K becomes drastically simpler when we require H to sit inside G as a subgroup in such a way that the epimorphism $G \to H$ restricts to the identity on H. In this case, we say that the extension is split, and then G is what we call a semidirect product of K and H.

Definition. A homomorphism $f : G \to H$ is said to **split** if there exists a **section** or **splitting map** $s : H \to G$, that is, a homomorphism satisfying $f \circ s = 1_H$. Note that in this case f is necessarily surjective and the section s is necessarily injective. If the epimorphism $G \to H$ in (2.1) splits then G is called a **split extension** of H by K, or a **semidirect product** of K and H.

The existence of a section $s : H \to G$ is in fact a very strong property with many important consequences. First of all, we can (and will) identify H with the (not necessarily normal) subgroup $s(H) \subset G$. Given an extension as in (2.1), we may identify G/K with H, so the section lets us treat G/K as a subgroup of G. (See Figure 1.) Regarding s as a section $s : G/K \to G$ that splits the quotient map, we see that s is a choice of a representative for each coset in G/K. (One could be led to think that there is nothing special about the existence of a such a "choice function"; after all, any surjective map admits right inverses. The crucial point here is that s has to be a *homomorphism*.) An important consequence of this setup is that K and H, viewed as subgroups of G, intersect trivially: any $k \in K$ is mapped to the identity element in $G/K \cong H$. Moreover, we have a decomposition $G = KH$: given any $g \in G$, there exists a unique $h \in H$ such that $Kg = Kh$, so that $gh^{-1} \in K$; hence there exists a unique $k \in K$ such that $g = kh$. (Uniqueness of the decomposition also follows from the fact that $K \cap H = \{1\}$.) Hence we have a set-theoretic bijection between G and $K \times H$.

Conversely, if G is a group with a normal subgroup $K \triangleleft G$ and another subgroup $H < G$ such G factors uniquely as $G = KH$, then it is clear that G is a semidirect product of K and H.

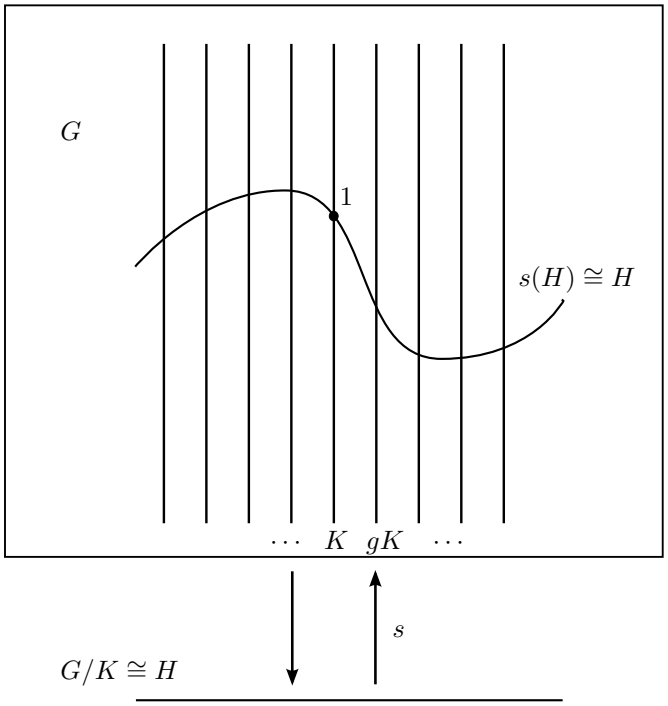


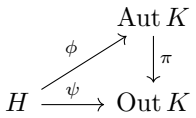
Figure 1: G as a semidirect product of K and H. The vertical bars represent the cosets in G/K, which partition G.

Another important feature of split extensions is that they induce actions of H on K which, as we will see later, let us turn the problem around and reconstruct G from K and H uniquely. This completely solves the classification problem for split extensions. First, note that a group action of H on K is the same thing as a homomorphism $\phi : H \to \operatorname{Aut} K$. Now, given a split extension, we let H act on K by conjugation. This means that $\phi(h) := \phi_h \in \operatorname{Aut} K$ is defined by $\phi_h(k) = hkh^{-1}$. (Again, it is very important to remember that *this is only possible because of the existence of a splitting map*, which lets us identify H with a subgroup of G. Also note that it may very well happen that different splitting maps induce different actions.) This is well-defined since K is normal in G, and so the image of ϕ_h cannot leave K.

Here is another way to think about this. Recall that an *inner automorphism* of K is an automorphism of the form $\phi_k(k') = kk'k^{-1}$ for some $k \in K$. Inner automorphisms form a normal subgroup $\operatorname{Inn} K \triangleleft \operatorname{Aut} K$, and the quotient $\operatorname{Out} K = \operatorname{Aut} K / \operatorname{Inn} K$ is called the group of *outer automorphisms* of K. Given that G is a (not necessarily split) extension of H by K, the normality of K implies that there always exists a conjugacy homomorphism $G \to \operatorname{Aut} K$. Since this homomorphism maps K inside $\operatorname{Inn} K$, it descends to a well-defined homomorphism

$$\psi : H \cong G/K \to \operatorname{Aut} K / \operatorname{Inn} K = \operatorname{Out} K.$$

We can think of the splitting map $s : H \to G$ as an object that lets us lift $\psi : H \to \operatorname{Out} K$ to $\phi : H \to \operatorname{Aut} K$, as in the following diagram:



If $\pi : \operatorname{Aut} K \to \operatorname{Out} K$ denotes the quotient map, and if $h \in H$, identified with $s(h) \in G$, belongs to the coset gK, then we have $g^{-1}h \in K$, which implies that $\phi_g^{-1}\phi_h = \phi_{g^{-1}h} \in \operatorname{Inn} K$, or $\phi_g \operatorname{Inn} K = \phi_h \operatorname{Inn} K$. But the left-hand side is precisely $\psi(h)$, and the right-hand side is precisely $(\pi \circ \phi)(h)$. Hence ϕ lifts ψ.

To sum things up, we should think of a semidirect product of K and H as made up of two components: a normal subgroup K, and a subgroup $H \cong G/K$ that lies transverse to the cosets in G/K and meets each exactly once. The homomorphism $H \to \operatorname{Aut} K$ gives us information about how H lies inside G. As we will see shortly, if this homomorphism is trivial then G is just a direct product of K and H.

This is all rather abstract, so let's look at some concrete examples. First of all, note that neither of the extensions in Example 1 split. For the first sequence, a splitting map would have to be an injective homomorphism from $\mathbb{Z}/2$ to $\mathbb{Z}$, but no such homomorphism exists. For the second sequence, we'd need a homomorphism $s : \mathbb{Z}/2 \to \mathbb{Z}/4$ such that $s(1)$ is odd and has order 2, but again no such homomorphism exists since every odd element has order 4 in $\mathbb{Z}/4$.

Now let's see examples of extensions that do split.

Example 2 (Direct product)**.** The most trivial split extension is given by the direct product. Let K, H be any two groups and let $G = K \times H$. The extension

$$1 \to K \to K \times H \to H \to 1$$

clearly admits the section $s : H \to K \times H$ given by $s(h) = (1, h)$. Moreover, the homomorphism $\phi : H \to \operatorname{Aut} K$ is trivial since

$$\phi_h(k, 1) = (1, h)(k, 1)(1, h)^{-1} = (k, hh^{-1}) = (k, 1).$$

Note that in this example H is actually normal in G; in fact, this is the only time this can happen: *G is a split extension of H by K with $H \lhd G$ if and only if G is isomorphic to $K \times H$.*

Indeed, first note that the normality of K and H and the condition $K \cap H = \{1\}$ together imply that every element of K commutes with every element of H: for any $k \in K$, $h \in H$, the commutator $[k, h] = khk^{-1}h^{-1}$ belongs to $K \cap H = \{1\}$. This in turn implies that we have a homomorphism $\xi : K \times H \to G$ defined by $\xi(k, h) = kh$, since

$$\xi((k, h)(k', h')) = \xi(kk', hh') = kk'hh' = khk'h' = \xi(k, h)\xi(k', h').$$

It is bijective because, as we noted at the beginning of the §, every element of the semidirect product G can be written uniquely as kh with $k \in K$ and $h \in H$.

Example 3 (Dihedral group)**.** The dihedral group $G = D_n$ is the group of symmetries of a regular n-sided polygon. (The degenerate cases $n = 1, 2$ have to be handled somewhat carefully; it is natural to define $D_1 = \mathbb{Z}/2$ and $D_2 = \mathbb{Z}/2 \times \mathbb{Z}/2$.) It has order $2n$ and consists of n rotations and n reflections. One only needs two elements to generate D_n, namely a rotation ρ of $2\pi/n$ and a reflection b with respect to a bisector of some vertex. These generators satisfy the relation

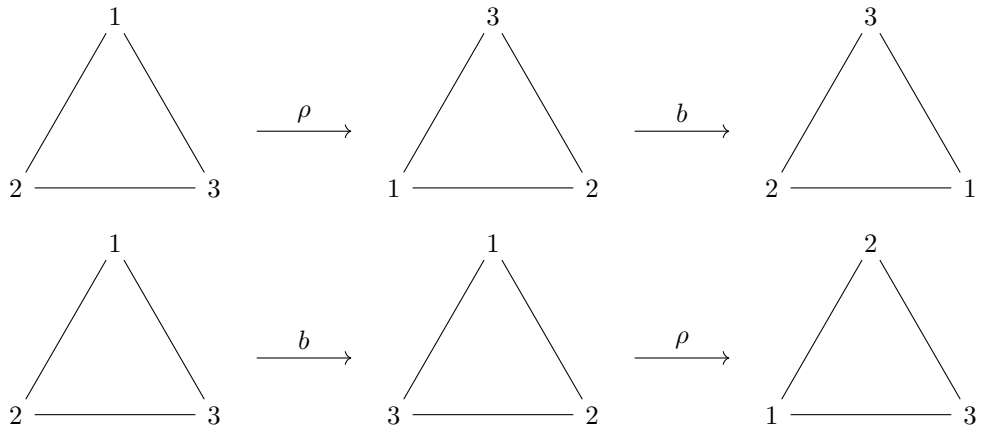


Figure 2: A rotation ρ of $2\pi/3$ and a reflection b through the line bisecting the top vertex, two generators of D_3, do not commute.

$b\rho b = \rho^{-1}$. Note that ρ and b do not commute as soon as $n \geq 3$, c.f. Figure 2. Interestingly, the dihedral group is also generated by the two reflections $a = \rho b$ and b; in fact, it is not hard to show that any finite (resp. infinite) nonabelian group with two generators of order 2 is isomorphic to some D_n (resp. to the infinite dihedral group, defined in the next example). One way to see this is to invoke the uniqueness of semidirect products, proved in Theorem 4.1.

Take $K = \mathbb{Z}/n$ and $H = \mathbb{Z}/2$. We have a split short exact sequence

$$1 \to \mathbb{Z}/n \to D_n \to \mathbb{Z}/2 \to 1,$$

where the generator $1 \in \mathbb{Z}/n$ is mapped to the rotation $\rho \in D_n$, and the epimorphism $D_n \to \mathbb{Z}/2$ is essentially just the determinant map, sending a symmetry in D_n to the generator of $\mathbb{Z}/2$ if and only if the symmetry is orientation-reversing. To split this sequence, we can simply take the section $s : \mathbb{Z}/2 \to D_n$ that maps the generator to the reflection $b \in D_n$.

The homomorphism $\phi : \mathbb{Z}/2 \to \operatorname{Aut} \mathbb{Z}/n$ is given by the inversion $\phi_1(k) = n - k$, since inside D_n we have

$$\phi_1(\rho) = b\rho b = \rho^{-1}.$$

Example 4 (Infinite dihedral group)**.** Let $G = (\mathbb{Z}/2)\langle a\rangle * (\mathbb{Z}/2)\langle b\rangle$ be the *free product* of two copies of $\mathbb{Z}/2$, with generators a and b respectively. This means that G consists of reduced words on the alphabet $\{a, b\}$ subject to the relations $a^2 = b^2 = 1$ (empty word). The group G is known as the *infinite dihedral group*. Since two adjacent generators of the same kind cancel each other out, sample elements of G look like a, ba, aba, $abab$... you get the picture. Note that any word of odd length has order 2 in G since it starts and ends with the same letter; for example, $(aba)^2 = abaaba = abba = aa = 1$.

Now, let $K = \mathbb{Z}$ and $H = \mathbb{Z}/2$. Define a monomorphism $\mathbb{Z} \to G$ by sending the positive generator to the word ab. So, for example, 2 is identified with $abab$ and -1 is identified with $(ab)^{-1} = ba$. Next define an epimorphism $G \to \mathbb{Z}/2$ by counting the length of the reduced words

mod 2. Since the image of the injection $\mathbb{Z} \to G$ consists exactly of words of even length, we have a short exact sequence

$$1 \to \mathbb{Z} \to (\mathbb{Z}/2)\langle a \rangle * (\mathbb{Z}/2)\langle b \rangle \to \mathbb{Z}/2 \to 1.$$

We claim that this extension of $\mathbb{Z}/2$ by $\mathbb{Z}$, as opposed to the one in Example 1, is split. Indeed, we can choose $s : \mathbb{Z}/2 \to G$ to map the generator to any word of odd length, say a. This is a homomorphism since, as noted earlier, any reduced word of odd length has order 2 in G.

What is the homomorphism $\phi : \mathbb{Z}/2 \to \operatorname{Aut} \mathbb{Z}$ in this case? It suffices to compute

$$\phi_1(ab) = a(ab)a^{-1} = ba,$$

and so we see that ϕ is the only nontrivial homomorphism from $\mathbb{Z}/2$ to $\operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}/2$.

Example 5 (Symmetric group)**.** Like the dihedral groups above, many groups are split extensions of $\mathbb{Z}/2$, since in this case normality of the complementary subgroup comes for free. The symmetric group S_n is no exception: as the reader can readily check, the sign homomorphism $S_n \to \mathbb{Z}/2$ splits, so that S_n is a semidirect product of the alternating group A_n and $\mathbb{Z}/2$.

Example 6 (Matrix groups)**.** Let $\mathbb{F}$ be a field. The determinant homomorphism on $\mathrm{GL}(n, \mathbb{F})$ and some of its subgroups yields examples of split extensions. For example, we have split short exact sequences

$$1 \to \mathrm{SL}(n, \mathbb{F}) \to \mathrm{GL}(n, \mathbb{F}) \xrightarrow{\det} \mathbb{F}^\times \to 1,$$

$$1 \to \mathrm{SO}(n, \mathbb{F}) \to O(n, \mathbb{F}) \xrightarrow{\det} \mathbb{Z}/2 \to 1,$$

$$1 \to \mathrm{SU}(n) \to U(n) \xrightarrow{\det} U(1) \to 1.$$

To split the determinant map in these sequences, one simply has to consider elements of $\mathbb{F}^\times$, $\mathbb{Z}/2$ and $U(1)$ as 1×1 matrices, embedded inside $n \times n$ matrices by padding the diagonal with 1's.

We will look at many more examples in §5.

4 Semidirect products: existence and uniqueness

Now let us reverse the process above. Given two groups K and H, how can we construct all the split extensions of H by K? For this we will need the extra piece of information afforded by the homomorphisms from H to $\operatorname{Aut} K$.

Definition. Let $1 \to K \to G \to H \to 1$ be a short exact sequence and let $\theta : H \to \operatorname{Aut} K$ be a homomorphism. We say that G is a semidirect product of K and H **realizing** θ if there exists a splitting map $s : H \to G$ such that the action by conjugation $\phi : H \to \operatorname{Aut} K$ with respect to s coincides with θ.

Theorem 4.1 (Existence and uniqueness of semidirect products)**.** *Given any groups K and H and any homomorphism $\theta : H \to \operatorname{Aut} K$, there exists a semidirect product of K and H realizing θ. It is denoted by $K \rtimes_\theta H$. Moreover any semidirect product G of K and H realizing θ is isomorphic to $K \rtimes_\theta H$.*

Proof. As a set underling $K \rtimes_\theta H$, we take the direct product $K \times H$. The group operation on $K \rtimes_\theta H$ is given as follows:

$$(k, h)(k', h') := (k\theta_h(k'), hh').$$

One easily checks that this makes $K \rtimes_\theta H$ into a group, with $(1, 1)$ as the identity and with the inversion formula

$$(k, h)^{-1} = (\theta_{h^{-1}}(k^{-1}), h^{-1}).$$

This group $K \rtimes_\theta H$ is a semidirect product of K and H for we have the following split short exact sequence:

$$1 \to K \to K \rtimes_\theta H \to H \to 1,$$

where $K \to K \rtimes_\theta H$ maps k to $(k, 1)$ and $K \rtimes_\theta H \to H$ maps (k, h) to h. The sequence is split by $s : H \to K \rtimes_\theta H$ which maps h to $(1, h)$. The conjugation homomorphism induced by s is given by

$$\phi_h(k, 1) = (1, h)(k, 1)(1, h)^{-1} = (\theta_h(k), h)(1, h^{-1}) = (\theta_h(k), 1),$$

so that as a map $\phi : H \to \operatorname{Aut} K$, ϕ coincides with θ; hence $K \rtimes_\theta H$ realizes θ.

For the uniqueness part, let G be any semidirect product of K and H realizing θ. By definition, there exists a section $H \to G$ such that, after identification of H as a subgroup of G, the action of θ corresponds to the conjugation action $\phi : H \to \operatorname{Aut} K$. Let $\xi : K \rtimes_\theta H \to G$ be given by $\xi(k, h) = kh$. Then ξ is a homomorphism since

$$\xi((k, h)(k', h')) = \xi(k\theta_h(k'), hh') = k\phi_h(k')hh' = k(hk'h^{-1})hh' = khk'h' = \xi(k, h)\xi(k', h').$$

Moreover ξ is a bijection because, as we noted in the paragraph following the definition of a semidirect product in §3, every element of G can be written uniquely as kh with $k \in K$ and $h \in H$. □

We can now restate the discussion about direct products in Example 2 in more elegant terms.

Corollary 4.2 (Characterization of direct products)**.** *Let*

$$1 \to K \xrightarrow{m} G \xrightarrow{f} H \to 1$$

be a short exact sequence of groups. Then the following are equivalent:

(1) $G \cong K \times H$;
(2) The sequence splits and H is normal in G with respect to the splitting;
(3) G is a semidirect product of K and H realizing the trivial homomorphism $H \to \operatorname{Aut} K$;
(4) There exists a ***retraction*** *$r : G \to K$, that is, a homomorphism such that $r \circ m = 1_K$.*

Proof. The equivalence of (1) and (2) was discussed in Example 2. The equivalence of (1) and (3) is a direct consequence of the uniqueness part of Theorem 4.1. The implication (1) $\implies$ (4) is obvious; all that remains to be proved is the implication (4) $\implies$ (1).

Let $r : G \to K$ be a retraction. We have a homomorphism $\xi : G \to K \times H$ that maps $g \in G$ to $\xi(g) = (r(g), f(g))$. We claim that ξ is an isomorphism.

To see that ξ is injective, let $g \in \ker \xi$. This means that $r(g) = f(g) = 1$. By exactness, $f(g) = 1$ implies that there exists $k \in K$ such that $g = m(k)$. Since r is a retraction, we get $k = r(m(k)) = r(g) = 1$, hence $g = m(1) = 1$.

To see that ξ is surjective, let (k, h) by any element in $K \times H$. Let $g \in G$ be any preimage of h by f (which is surjective). Then the element $m(kr(g)^{-1})g \in G$ is a preimage of (k, h) by ξ:

$$\begin{aligned}\xi(m(kr(g)^{-1})g) &= (r(m(kr(g)^{-1})g), f(m(kr(g)^{-1})g)) \\ &= (kr(g)^{-1}r(g), f(g)) \quad \text{since } r \circ m = 1_K \text{ and } f \circ m = 1 \\ &= (k, h).\end{aligned}$$

□

Note however that, despite (3), it is possible for a direct product to realize nontrivial homomorphisms! For example, let G be any nonabelian group and let $g \in G \setminus Z(G)$. Then the short exact sequence

$$1 \to G \to G \times \mathbb{Z} \to \mathbb{Z} \to 1$$

splits by mapping the positive generator $1 \in \mathbb{Z}$ to $(g, 1)$, and the corresponding homomorphism $\phi : \mathbb{Z} \to \operatorname{Aut} G$ is given by

$$\phi_1(g', 1) = (g, 1)(g', 1)(g, 1)^{-1} = (gg'g^{-1}, 1),$$

i.e., it is conjugation by g. Since g does not belong to the center of G, this action is nontrivial.

Note also that, as a consequence of Corollary 4.2, for short exact sequences of *abelian* groups, the only semidirect product is the direct product, and the existence of a section is equivalent to the existence of a retraction.

Example 7 (Vector spaces)**.** Consider any short exact sequence of vector spaces (or free modules), written additively:

$$0 \to U \xrightarrow{m} V \xrightarrow{f} W \to 0.$$

We claim that any such sequence splits, so that $V \cong U \oplus W$. (For finite-dimensional vector spaces, this yields the rank-nullity theorem.) This is a consequence of the fact that any vector space admits a basis, and that linear maps are determined by their action on a basis. To construct a retraction $r : V \to U$, one can extend a basis of U to all of V, then define r by mapping the basis of U to itself and the new basis vectors to 0. Alternatively, one can construct a section $s : W \to V$ by choosing a basis of W and letting s pick a preimage for each basis vector.

5 More examples

Example 8. Let $K = \mathbb{Z}$ and $H = \mathbb{Z}/2$. Since there are only two homomorphisms $\mathbb{Z}/2 \to \operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}/2$, there are at most two distinct semidirect products of K and H up to isomorphism. In fact, both homomorphisms yield distinct groups: the trivial homomorphism yields $\mathbb{Z} \times \mathbb{Z}/2$, and the nontrivial homomorphism yields the infinite dihedral group $\mathbb{Z}/2 * \mathbb{Z}/2$, as we saw in Example 4.

Example 9 (Fundamental group of the torus and Klein bottle)**.** Let $K = H = \mathbb{Z}$. Again there are precisely two homomorphisms $\mathbb{Z} \to \operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}/2$. The trivial one yields the direct product $\mathbb{Z}^2$. What about the nontrivial one? Let $\theta : \mathbb{Z} \to \operatorname{Aut} \mathbb{Z}$ be given by $\theta_1(x) = -x$. The construction in Theorem 4.1 gives us a group $\mathbb{Z} \rtimes_\theta \mathbb{Z}$ whose underlying set is $\mathbb{Z}^2$ and whose operation is given by

$$(a, b)(c, d) = (a + (-1)^b c, b + d).$$

Note that the elements $x = (1, 0)$ and $y = (1, 1)$ satisfy the relation $xyx = y$ in $\mathbb{Z} \rtimes_\theta \mathbb{Z}$. Inspired by this, let G be the group with presentation

$$G = \langle x, y \mid xyx = y \rangle.$$

Consider the following short exact sequence:

$$1 \to \mathbb{Z} \to G \xrightarrow{f} \mathbb{Z} \to 1,$$

where the monomorphism maps $1 \in \mathbb{Z}$ to $x \in G$ and the epimorphism f is defined by $f(x) = 0$, $f(y) = 1$. Note that f, a priori only defined on the free group generated by x and y, descends to a well-defined homomorphism on G since $f(xyx) = 1 = f(y)$. Exactness amount to showing that $\ker f$ consists exactly of the reduced words that can be written without the letters y, y^{-1}. Let $g \in G$ be any word such that $f(g) = 0$. This means that y appears exactly as many times as y^{-1} in g. If y appears at all then a little thought shows that at least one of the following four strings must appear in g:

$$yxy^{-1} \qquad yx^{-1}y^{-1} \qquad y^{-1}xy \qquad y^{-1}x^{-1}y.$$

But these are, respectively, x^{-1}, x, x^{-1} and x. Continuing this process, we can eventually eliminate all the letters y and y^{-1} in g.

Also note that f splits by $s : \mathbb{Z} \to G$, $s(1) = y$, and that the induced homomorphism $\phi : \mathbb{Z} \to \operatorname{Aut} \mathbb{Z}$ coincides with θ:

$$\phi_1(x) = yxy^{-1} = x^{-1}.$$

Hence G is a semidirect product of $\mathbb{Z}$ and $\mathbb{Z}$ realizing θ; by Theorem 4.1, it must be isomorphic to $\mathbb{Z} \rtimes_\theta \mathbb{Z}$.

From the above we can conclude that the trivial semidirect product of $\mathbb{Z}$ with itself admits the presentation $\langle x, y \mid xy = yx \rangle$, while the nontrivial semidirect product of $\mathbb{Z}$ with itself admits the presentation $\langle x, y \mid xyx = y \rangle$. It is interesting to note that both of these groups come up naturally in topology: they are the fundamental groups of the two closed surfaces that admit nowhere-vanishing vector fields, namely the torus (which is orientable) and the Klein bottle (which is not).

To get an idea of why the fundamental group of the Klein bottle admits that presentation, consider the following two affine homeomorphisms of $\mathbb{R}^2$:

$$g(x, y) = (x + 1, y) \text{ and } h(x, y) = (-x, y + 1).$$

Note that

$$(g \circ h \circ g)(x, y) = (g \circ h)(x + 1, y) = g(-x - 1, y + 1) = (-x, y + 1) = h(x, y),$$

that is to say $g \circ h \circ g = h$; in fact the group generated by g and h is isomorphic to G above, by interchanging instances of g and h by instances of x and y. That group acts on $\mathbb{R}^2$ by homeomorphisms, and the orbit space $\mathbb{R}^2/G$ is seen to be homeomorphic to the Klein bottle. (The fundamental polygon is the square $[-\frac{1}{2}, \frac{1}{2}] \times [0, 1]$.) In fact this exhibits $\mathbb{R}^2$ as the universal cover of the bottle, and G as its group of deck transformations; a fundamental theorem of covering space theory then asserts that the fundamental group of the bottle is isomorphic to G.

Example 10 (Affine group)**.** The affine group $A(n, \mathbb{R})$ of $\mathbb{R}^n$ is the group of all affine transformations $x \mapsto Ax + b$, where $A \in \mathrm{GL}(n, \mathbb{R})$ and $b \in \mathbb{R}^n$. We have the split short exact sequence

$$1 \to \mathbb{R}^n \to A(n, \mathbb{R}) \to \mathrm{GL}(n, \mathbb{R}) \to 1,$$

where the monomorphism maps $b \in \mathbb{R}^n$ to $(x \mapsto x + b) \in A(n, \mathbb{R})$ and the epimorphism maps $(x \mapsto Ax + b) \in A(n, \mathbb{R})$ to $A \in \mathrm{GL}(n, \mathbb{R})$. There is an obvious section sending $A \in \mathrm{GL}(n, \mathbb{R})$ to $(x \mapsto Ax) \in A(n, \mathbb{R})$. The induced action $\phi : \mathrm{GL}(n, \mathbb{R}) \to \mathrm{Aut}\,\mathbb{R}^n$ is given by matrix-vector multiplication:

$$\phi_A(x \mapsto x + b) = (x \mapsto Ax)(x \mapsto x + b)(x \mapsto A^{-1}x) = (x \mapsto Ax)(x \mapsto A^{-1}x + b) = x \mapsto x + Ab.$$

Hence $A(n, \mathbb{R}) \cong \mathbb{R}^n \rtimes_\phi \mathrm{GL}(n, \mathbb{R})$.

Example 11 (Infinite dihedral group as affine group)**.** We can recover the infinite dihedral group $\mathbb{Z} \rtimes \mathbb{Z}/2 \cong \mathbb{Z} * \mathbb{Z}$ of Example 4 as a special case of the example above. Indeed, the group $A(1, \mathbb{Z})$ consists of the affine transformations of the form $x \mapsto ax+b$, where $a \in \{\pm 1\} \cong \mathbb{Z}/2$ and $b \in \mathbb{Z}$. The same short exact sequence as in the example above shows that $A(1, \mathbb{Z})$ is a semidirect product of $\mathbb{Z}$ and $\mathbb{Z}/2$ realizing the nontrivial homomorphism $\mathbb{Z}/2 \to \mathrm{Aut}\,\mathbb{Z}$, so the result follows by Theorem 4.1.

Alternatively, one can use the fact that the infinite dihedral group is the unique infinite non-abelian group that is generated by two elements of order 2, and note that $A(1, \mathbb{Z})$ is generated by the two involutions $x \mapsto -x$ and $x \mapsto -x + 1$.

Example 12 (Hyperoctahedral group)**.** The group $O(n, \mathbb{Z})$ of orthogonal matrices with integer coefficients is the group of signed permutation matrices: matrices with a single nonzero entry per line and per column, and such that the nonzero entries are either 1 or -1. The reader can check that the determinant homomorphism $O(n, \mathbb{Z}) \to \mathbb{Z}/2$ and the "forget all the signs" homomorphism $O(n, \mathbb{Z}) \to S_n$ yield two semidirect product decompositions

$$O(n, \mathbb{Z}) \cong SO(n, \mathbb{Z}) \rtimes \mathbb{Z}/2 \quad \text{and} \quad O(n, \mathbb{Z}) \cong (\mathbb{Z}/2)^n \rtimes S_n.$$

Are there other interesting decompositions of $O(n, \mathbb{Z})$?