SEMIDIRECT PRODUCTS

KEITH CONRAD

1. Introduction

For two groups H and K, the most basic construction of a group that contains copies of H and K as subgroups is the direct product $H \times K$, where the group law is componentwise: $(h, k)(h', k') = (hh', kk')$. Since $(h, 1)(h', 1) = (hh', 1)$ and $(1, k)(1, k') = (1, kk')$, we can embed H and K into $H \times K$ "on the axes" by $h \mapsto (h, 1)$ and $k \mapsto (1, k)$ for $h \in H$ and $k \in K$. This lets us think of $H \times K$ as a group generated by subgroups isomorphic to H and K. The significance of direct products is that some groups not initially constructed as direct products might decompose into a direct product of smaller groups, so we get a kind of factorization of the group. For example, every finite abelian group is isomorphic to the direct product of its Sylow subgroups. Other groups are not isomorphic to a direct product of smaller groups, such as S_n for $n \geq 3$.

There is a group construction using two groups H and K that is more subtle (more cunning?) than $H \times K$, called a semidirect product. Interesting features include: (i) it may be nonabelian even if H and K are abelian (note $H \times K$ is abelian if and only if H and K are abelian) and (ii) there can be multiple nonisomorphic semidirect products using the same two groups.

2. Recognizing direct products

When H and K are embedded into $H \times K$ in the standard way, here are three properties of the images of H and K inside $H \times K$:

- they generate $H \times K$: $(h, k) = (h, 1)(1, k)$,
- they intersect trivially: $(h, 1) = (1, k) \Longrightarrow h = 1, k = 1$,
- they commute elementwise: $(h, 1)(1, k) = (1, k)(h, 1)$.

This can be turned into the following "recognition theorem" for a group G to look like a direct product of two subgroups H and K: we have $H \times K \cong G$ by the *specific* mapping $(h, k) \mapsto hk$ precisely when the above conditions hold.

Theorem 2.1. *Let G be a group with subgroups H and K where*

1. *$G = HK$; that is, every element of G has the form hk for some $h \in H$ and $k \in K$,*
2. *$H \cap K = \{1\}$ in G,*
3. *$hk = kh$ for all $h \in H$ and $k \in K$.*

Then the map $H \times K \to G$ by $(h, k) \mapsto hk$ is an isomorphism.

Proof. Let $f\colon H \times K \to G$ by $f(h, k) = hk$. This is a homomorphism:

$$f((h, k)(h', k')) = f(hh', kk') = hh'kk'$$

and

$$f(h, k)f(h', k') = (hk)(h'k') = h(kh')k' = h(h'k)k' = hh'kk',$$

where we use (3) to know that h' and k commute.

To show f is injective, we check its kernel is trivial: if $f(h,k) = 1$ then $hk = 1$ in G, so $h = k^{-1} \in H \cap K$. By (2), $H \cap K = \{1\}$, so $h = 1$ and $k = 1$.

The function f is surjective by (1). □

There are many groups that decompose into a product of two subgroups that fit the first and second conditions of Theorem 2.1 but not the third one.

Example 2.2. In $G = \mathrm{Aff}(\mathbf{R})$, let

$$H = \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} : y \in \mathbf{R} \right\} \cong \mathbf{R}, \qquad K = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x \in \mathbf{R}^\times \right\} \cong \mathbf{R}^\times.$$

Since

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}}_{\in H} \underbrace{\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}}_{\in K}$$

we have $G = HK$, and clearly $H \cap K$ is trivial, but matrices in H and in K often do not commute with each other. You can find your own such matrices (nearly any random choice will work), but also observe that if elements of H and of K always commute with one another then $G \cong H \times K$ by Theorem 2.1, but $G \ncong H \times K$ since $H \times K$ is abelian (H and K are abelian) while G is nonabelian.

Example 2.3. In $G = \mathrm{GL}_2(\mathbf{R})$, let $H = \mathrm{SL}_2(\mathbf{R})$ and $K = \{\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) : x \in \mathbf{R}^\times\}$. For each $g \in G$, the number $\Delta = \det g$ is nonzero and the matrix $\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}$ has determinant Δ, so

$$g = \underbrace{g \begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}^{-1}}_{\in H} \cdot \underbrace{\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}}_{\in K}.$$

Thus $\mathrm{GL}_2(\mathbf{R}) = HK$, and easily $H \cap K = \{I_2\}$. It turns out that $\mathrm{GL}_2(\mathbf{R}) \ncong \mathrm{SL}_2(\mathbf{R}) \times \mathbf{R}^\times$. For example, $\mathrm{GL}_2(\mathbf{R})$ has infinitely many elements of order 2, such as reflections across any line in $\mathbf{R}^2$ through the origin, but $\mathrm{SL}_2(\mathbf{R})$ has just one element of order 2 ($-I_2$; check it is the only one!) and $\mathbf{R}^\times$ obviously does as well, so $\mathrm{SL}_2(\mathbf{R}) \times \mathbf{R}^\times$ has 3 elements of order 2.

Example 2.4. In $G = S_n$, for $n \geq 3$, let $H = A_n$ and $K = \langle (12) \rangle = \{(1), (12)\}$. We have $G = HK$: for $\sigma \in S_n$, if $\sigma \in A_n$ then $\sigma = \sigma \cdot (1)$, while if $\sigma \notin A_n$ then $\sigma = \sigma(12) \cdot (12)$ and $\sigma(12) \in A_n$. Clearly $H \cap K = \{(1)\}$. However, $S_n \ncong H \times K \cong A_n \times \mathbf{Z}/(2)$ for $n \geqslant 3$ by computing the center: for $n \geq 3$, S_n has a trivial center while $A_n \times \mathbf{Z}/(2)$ has a nontrivial center since $\mathbf{Z}/(2)$ has a nontrivial center.

Example 2.5. In $G = S_4$, let H be a 2-Sylow subgroup subgroup and K be a 3-Sylow subgroup (so $H \cong D_4$ and K is cyclic of order 3). In the Sylow theorems for S_4, $n_2 = 3$ and $n_3 = 4$, so H and K are not normal in S_4. The set HK can be written as H-cosets Hk and as K-cosets hK, so $|HK|$ is divisible by $|H| = 8$ and by $|K| = 3$, so $|HK| = 24$. Therefore $S_4 = HK$. The subgroups H and K intersect trivially. We have $S_4 \ncong H \times K \cong D_4 \times \mathbf{Z}/(3)$ since $D_4 \times \mathbf{Z}/(3)$ has a nontrivial center (D_4 and $\mathbf{Z}/(3)$ both have nontrivial center) while S_4 has a trivial center.

A difference between the last example and the previous ones is that H and K are not normal in G. In the earlier examples, $H \lhd G$. Because of that difference, the semidirect product we define below will include Examples 2.2, 2.3, 2.4 as special cases, but will not include Example 2.5.

3. Semidirect products

When H and K are subgroups of a group G, the set-product HK might not be a subgroup. For example, in S_3 if $H = \langle(12)\rangle$ and $K = \langle(13)\rangle$ then $HK = \{(1), (12), (13), (132)\}$ has size 4 and is not a subgroup of S_3. However, if H or K is normal in G then HK is a subgroup. Taking $H \lhd G$, for instance,

$$\boxed{(hk)(h'k') = (hkh'k^{-1})(kk') \in HK, \quad (hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK} \tag{3.1}$$

since $kh'k^{-1} \in H$ and $k^{-1}hk \in H$. This includes Examples 2.2, 2.3, and 2.4. (Note that in $H \times K$, the standard copies of H and K are *both* normal subgroups of $H \times K$, *e.g.*, H and K are the kernels of the projection homomorphisms from $H \times K$ to K and H, respectively.)

The formulas in (3.1) are going to be the motivation for our definition of the group law in a semidirect product of two groups. Specifically, the product in (3.1) involves $kh'k^{-1}$, so K is acting on H by conjugation, which is an action by *automorphisms* of H.

Consider now two arbitrary groups H and K, *not* initially inside a common group, and suppose we have an action of K on H by automorphisms: this means we are given a homomorphism $\varphi\colon K \to \mathrm{Aut}(H)$. Write the automorphism on H associated to k as φ_k, so $\varphi_k\colon H \to H$ is a bijection and $\varphi_k(hh') = \varphi_k(h)\varphi_k(h')$ for all $h, h' \in H$. That φ is a homomorphism from K to $\mathrm{Aut}(H)$ means

$$\varphi_{k_1} \circ \varphi_{k_2} = \varphi_{k_1k_2} \qquad \text{and} \qquad \varphi_1 = \mathrm{id}_H$$

for all $k_1, k_2 \in K$. In particular, $\varphi_k \circ \varphi_{k^{-1}} = \varphi_1 = \mathrm{id}_H$, so

$$\varphi_k^{-1} = \varphi_{k^{-1}}. \tag{3.2}$$

That is, the inverse of $\varphi_k \in \mathrm{Aut}(H)$ is $\varphi_{k^{-1}}$. As an example, we could let K act trivially on H: $\varphi_k(h) = h$ for all $k \in K$ and $h \in H$. We're more interested in nontrivial actions of K on H by automorphisms, but sometimes the only choice is the trivial action, for instance if H and K are finite with $|K|$ and $|\mathrm{Aut}(H)|$ being relatively prime. In Examples 2.2, 2.3, and 2.4, K can act on H by conjugation since H is a normal subgroup of G.

Definition 3.1. For two groups H and K and an action $\varphi\colon K \to \mathrm{Aut}(H)$ of K on H by automorphisms, the corresponding *semidirect product* $H \rtimes_\varphi K$ is defined as follows: as a set it is $H \times K = \{(h, k) : h \in H,\ k \in K\}$. The group law on $H \rtimes_\varphi K$ is

$$(h, k)(h', k') = (h\varphi_k(h'), kk').$$

This group operation is inspired by the first formula in (3.1), with $\varphi_k(h')$ being an abstracted version of $kh'k^{-1}$, where the latter notation makes no sense when H and K are not initially inside a common group. The notation $\rtimes$ in $H \rtimes_\varphi K$ has a small $\lhd$: think of the slanted lines in the small $\lhd$ as "pointing" to the normal subgroup H: we'll see in Theorem 3.7 that $\{(h, 1) : h \in H\}$ in $H \rtimes_\varphi K$ is isomorphic to H and is a normal subgroup of the semidirect product. (Also $\{(1, k) : k \in K\}$ is a subgroup isomorphic to K, but this need not be normal in $H \rtimes_\varphi K$.) In our semidirect product notation, the group being acted on always goes first in $H \rtimes_\varphi K$, and the group doing the acting goes second. If we reversed this then the notation could be $K \ltimes_\varphi H$ so the arrow still points to the normal subgroup.

Of course one has to check Definition 3.1 is valid: $H \rtimes_\varphi K$ really is a group. The element $(1, 1)$ is the identity:

$$(h, k)(1, 1) = (h\varphi_k(1), k1) = (h, k), \quad (1, 1)(h, k) = (1\varphi_1(h), 1k) = (h, k)$$

where $\varphi_k(1) = 1$ and $\varphi_1 = \mathrm{id}_H$ since homomorphisms preserve the identity elements. To find an inverse for (h,k) in $H \rtimes_\varphi K$, we want to find a pair (h',k') that makes $(h,k)(h',k') = (1,1)$, or equivalently $(h\varphi_k(h'), kk') = (1,1)$. From the second coordinates being equal, $k' = k^{-1}$. Then in the first coordinates,

$$h\varphi_k(h') = 1 \Rightarrow \varphi_k(h') = h^{-1}.$$

Apply the inverse automorphsm $\varphi_k^{-1} = \varphi_{k^{-1}}$ (see (3.2)) and we get $h' = \varphi_k^{-1}(h^{-1}) = \varphi_{k^{-1}}(h^{-1}) = (\varphi_{k^{-1}}(h))^{-1}$. We have solved for both h' and k': if (h,k) has an inverse, it must be

$$(\varphi_{k^{-1}}(h^{-1}), k^{-1}) = ((\varphi_{k^{-1}}(h))^{-1}, k^{-1}). \tag{3.3}$$

The reader should check that this formula really is a 2-sided inverse for (h,k) in $H \rtimes_\varphi K$. Note the similarity of this formula for $(h,k)^{-1}$ to the second formula in (3.1) for an inverse of hk when H and K are subgroups of a group with H being a normal subgroup:

$$(hk)^{-1} = (k^{-1}h^{-1}k)k^{-1} = (k^{-1}hk)^{-1}k^{-1}.$$

This is the (conjugation) action of k^{-1} on h^{-1} that is then multiplied by k^{-1}.

Associativity of the operation on $H \rtimes_\varphi K$ is left as an exercise.

Example 3.2. If $\varphi\colon K \to \mathrm{Aut}(H)$ is the trivial homomorphism, so $\varphi_k = \mathrm{id}_H$ for all $k \in K$, then the group law on $H \rtimes_\varphi K$ is the direct product: $(h,k)(h',k') = (h\varphi_k(h'), kk') = (hh', kk')$. We'll see in Theorem 3.7 that a semidirect product is a direct product (in a natural way) only when φ is the trivial action of K on H.

Example 3.3. In $H \rtimes_\varphi K$, $(h,k)^2 = (h,k)(h,k) = (h\varphi_k(h), k^2)$, so $(h,k)^2 = (1,1)$ if and only if $\varphi_k(h) = h^{-1}$ and $k^2 = 1$.

Example 3.4. Take $H = \mathbf{R}$, $K = \mathbf{R}^\times$, and $\varphi\colon \mathbf{R}^\times \to \mathrm{Aut}(\mathbf{R})$ where $\varphi_x\colon \mathbf{R} \to \mathbf{R}$ by $\varphi_x(y) = xy$. Note φ_x is an automorphism of $\mathbf{R}$ as an additive group and $\varphi_x \circ \varphi_{x'} = \varphi_{xx'}$ since $x(x'y) = (xx')y$ for all $y \in \mathbf{R}$.

The group $\mathbf{R} \rtimes_\varphi \mathbf{R}^\times$ has the operation

$$(a,b)(a',b') = (a + \varphi_b(a'), bb') = (a + ba', bb'). \tag{3.4}$$

This resembles the multiplication in $\mathrm{Aff}(\mathbf{R})$, where $\left(\begin{smallmatrix} b & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} b' & a' \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} bb' & ba'+a \\ 0 & 1 \end{smallmatrix}\right)$. In the affine matrices we multiply in the upper left, while in $\mathbf{R} \rtimes_\varphi \mathbf{R}^\times$, components multiply in the second coordinate. That suggests turning $(a,b) \in \mathbf{R} \times_\varphi \mathbf{R}^\times$ into $\left(\begin{smallmatrix} b & a \\ 0 & 1 \end{smallmatrix}\right)$: $\mathbf{R} \times_\varphi \mathbf{R}^\times \cong \mathrm{Aff}(\mathbf{R})$ by $(a,b) \mapsto \left(\begin{smallmatrix} b & a \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} b & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

In the group $\mathrm{Aff}(\mathbf{R})$ you have to be careful about how you decompose a matrix:

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \quad \text{for } x \neq 1, y \neq 0.$$

The nice decomposition puts the matrix associated to y *first*, before that associated to x.

Example 3.5. In the previous example, replace $\mathbf{R}$ with $\mathbf{Z}/(m)$ and $\mathbf{R}^\times$ with $(\mathbf{Z}/(m))^\times$. We have $\mathrm{Aut}(\mathbf{Z}/(m)) \cong (\mathbf{Z}/(m))^\times$ since automorphisms of the additive group $\mathbf{Z}/(m)$ are the mappings $\varphi_a\colon x \bmod m \mapsto ax \bmod m$ for $a \in (\mathbf{Z}/(m))^\times$. Let $\varphi\colon (\mathbf{Z}/(m))^\times \to \mathrm{Aut}(\mathbf{Z}/(m))$ by making $\varphi_a\colon \mathbf{Z}/(m) \to \mathbf{Z}/(m)$ for each a be multiplication by a. The semidirect product $\mathbf{Z}/(m) \rtimes_\varphi (\mathbf{Z}/(m))^\times$ has operation

$$(a,b)(a',b') = (a + ba', b + b').$$

and is isomorphic to $\mathrm{Aff}(\mathbf{Z}/(m))$ by $(a,b) \bmod m \mapsto \left(\begin{smallmatrix} b & a \\ 0 & 1 \end{smallmatrix}\right) \bmod m$.

Example 3.6. Since ± 1 acts as additive automorphisms on $\mathbf{Z}$, we have a semidirect product $\mathbf{Z} \rtimes \{\pm 1\}$ where $(a, \varepsilon)(a', \varepsilon') = (a + \varepsilon a', \varepsilon\varepsilon')$. The homomorphism $\mathbf{Z} \to \{\pm 1\}$ given by $n \mapsto (-1)^n$ leads to a semidirect product $\mathbf{Z} \rtimes \mathbf{Z}$ by $(m, n)(m', n') = (m + (-1)^n m', n + n')$.

The next theorem says how H and K fit in $H \rtimes_\varphi K$. It is similar to the direct product, except elements of H and of K may not commute with each other, and they do all commute with each other only if $\varphi\colon K \to \mathrm{Aut}(H)$ is trivial (each φ_k is the identity mapping on H).

Theorem 3.7. *Inside $H \rtimes_\varphi K$, we have*

$$H \cong \{(h, 1) : h \in H\} \text{ by } h \mapsto (h, 1), \quad K \cong \{(1, k) : k \in K\} \text{ by } k \mapsto (1, k),$$

and $(h, k) = (h, 1)(1, k) = (1, k)(\varphi_k^{-1}(h), 1)$. The copy of H in $H \rtimes_\varphi K$ is a normal subgroup with conjugation by k being described with φ_k:

$$(1, k)(h, 1)(1, k)^{-1} = (\varphi_k(h), 1). \tag{3.5}$$

In particular, $(1, k)$ commutes with each $(h, 1)$ if and only if $k \in \ker \varphi$, and every $(1, k)$ and $(h, 1)$ commute if and only if $\varphi\colon K \to \mathrm{Aut}(H)$ is trivial on K: $\varphi_k = \mathrm{id}_H$ for all $k \in K$.

The formula $(h, k) = (1, k)(\varphi_k^{-1}(h), 1)$ in the theorem looks less strange if H and K are in a common group, where we could write $hk = k(k^{-1}hk)$. The term $k^{-1}hk$ in parentheses is the (conjugation) action of k^{-1} on h and corresponds to $(\varphi_{k^{-1}}(h), 1) = (\varphi_k^{-1}(h), 1)$.

Proof. In $H \rtimes_\varphi K$, the mappings $h \mapsto (h, 1)$ and $k \mapsto (1, k)$ are obviously injective from H and K into $H \rtimes_\varphi K$. These multiply together like elements of H and K do:

$$\begin{aligned} (h, 1)(h', 1) &= (h\varphi_1(h'), 1 \cdot 1) = (hh', 1) \qquad \text{since } \varphi_1 = \mathrm{id}_H, \\ (1, k)(1, k') &= (1\varphi_k(1), kk') = (1, kk') \qquad \text{since } \varphi_k(1) = 1, \end{aligned}$$

Therefore we have copies of H and K inside $H \rtimes_\varphi K$ in a natural way. For instance, $(h, 1)^{-1} = (h^{-1}, 1)$ and $(1, k)^{-1} = (1, k^{-1})$. We will call write subgroups as $H \times 1$ and $1 \times K$. The use a direct product symbol is okay since elements of $H \times 1$ multiply just like a direct product of H with the trivial subgroup, and similarly for $1 \times K$.

For a single pair (h, k) in $H \rtimes_\varphi K$,

$$(h, 1)(1, k) = (h\varphi_1(1), 1 \cdot k) = (h, k)$$

and

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

To show $H \times 1$ is a normal subgroup of $H \rtimes_\varphi K$, it suffices to show $1 \times K$ in $H \rtimes_\varphi K$ conjugates $H \times 1$ back to itself, since $H \times 1$ does and each element of $H \rtimes_\varphi K$ is built from $H \times 1$ and $1 \times K$ (that is, $(h, k) = (h, 1)(1, k)$):

$$\begin{aligned} (1, k)(h, 1)(1, k)^{-1} &= (1, k)(h, 1)(1, k^{-1}) \\ &= (1 \cdot \varphi_k(h), k \cdot 1)(1, k^{-1}) \\ &= (\varphi_k(h), k)(1, k^{-1}) \\ &= (\varphi_k(h) \cdot \varphi_k(1), kk^{-1}) \\ &= (\varphi_k(h), 1). \end{aligned}$$

This tells us that $H \times 1$ is normal in $H \rtimes_\varphi K$, and *also* shows the action $\varphi\colon K \to \mathrm{Aut}(H)$ of K on H looks like conjugation of $1 \times K$ on $H \times 1$ inside $H \rtimes_\varphi K$.

For $h \in H$ and $k \in K$,

$$(h,1)(1,k) = (1,k)(h,1) \Longleftrightarrow (h,k) = (1 \cdot \varphi_k(h), k \cdot 1) \Longleftrightarrow (h,k) = (\varphi_k(h), k).$$

Therefore $(1,k)$ commutes with all $(h,1)$ if and only if $\varphi_k(h) = h$ for all $h \in H$, which means $k \in \ker\varphi$. That all $(1,k)$ and $(h,1)$ commute means $\ker\varphi = K$, which is another way of saying the action $\varphi\colon H \to \mathrm{Aut}(K)$ is trivial. □

Thus $H \rtimes_\varphi K$ is nonabelian whenever φ is not trivial. Even if H and K are both abelian, if $\varphi\colon K \to \mathrm{Aut}(H)$ is nontrivial then $H \rtimes_\varphi K$ is a nonabelian group.

Example 3.8. Let $H = \mathbf{R}$, $K = \mathbf{R}^\times$, and $\varphi\colon \mathbf{R}^\times \to \mathbf{R}$ by $\varphi_x(y) = xy$. We saw in Example 3.4 that $\mathrm{Aff}(\mathbf{R}) \cong \mathbf{R} \times_\varphi \mathbf{R}^\times$ by $\left(\begin{smallmatrix} x & y \\ 0 & 1 \end{smallmatrix}\right) \mapsto (y, x)$.

Equation (3.5) says the effect of φ_x on $\mathbf{R}$ looks like conjugation in $\mathbf{R} \rtimes_\varphi \mathbf{R}^\times$, and this is related to the affine group conjugation formula:

$$\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & xy \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \varphi_x(y) \\ 0 & 1 \end{pmatrix}.$$

Example 3.9. In Example 3.6 we met the nontrivial semidirect product $\mathbf{Z} \rtimes \mathbf{Z}$ where $(m,n)(m',n') = (m + (-1)^n m', n + n')$. In this group,

$$(m,n) = (m,0)(0,n) = (1,0)^m(0,1)^n,$$

so $\mathbf{Z} \rtimes \mathbf{Z}$ is generated by $(1,0)$ and $(0,1)$ where

$$(0,1)(1,0)(0,1)^{-1} = (-1,0) = (1,0)^{-1}.$$

Setting $x = (1,0)$ and $y = (0,1)$, the group $\mathbf{Z} \rtimes \mathbf{Z}$ is generated by x and y subject to the relation $yxy^{-1} = x^{-1}$. (Check as an exercise that when a group contains two elements x and y such that $yxy^{-1} = x^{-1}$, then $yx^my^{-1} = x^{-m}$ for all $m \in \mathbf{Z}$ and then $y^nx^my^{-n} = x^{(-1)^n m}$ for all $n \in \mathbf{Z}$.)

Example 3.10. Let H be an abelian group written *additively*, so negation $\mathrm{neg}\colon h \mapsto -h$ is an automorphism of order 2. Let $\varphi\colon \mathbf{Z}/(2) \to \mathrm{Aut}(H)$ by $\varphi_0 = \mathrm{id}_H$ and $\varphi_1 = [h \mapsto -h]$. Then φ is a homomorphism (tip: when a group G contains an element g of order m, we always get a homomorphism $\mathbf{Z}/(m) \to G$ by $a \bmod m \mapsto g^a$, and here we're using the special case $G = \mathrm{Aut}(H)$ and g is inversion on H). The group $H \rtimes_\varphi \mathbf{Z}/(2)$ has operation

$$(h, a \bmod 2)(h', a' \bmod 2) = (h + \mathrm{neg}^a(h'), a + a' \bmod 2) = (h + (-1)^a h', a + a' \bmod 2). \tag{3.6}$$

Then

$$(h,0)(0,1) = (h,1) \quad \text{and} \quad (0,1)(h,0) = (0 + \mathrm{neg}(h), 1 + 0) = (-h, 1).$$

Thus $(h,0)$ and $(0,1)$ commute in $H \rtimes_\varphi \mathbf{Z}/(2)$ if and only if $h = -h$. If all nonzero elements of H have order 2 (so negation on H is the identity) then $H \rtimes_\varphi \mathbf{Z}/(2) = H \times \mathbf{Z}/(2)$. If some nonzero element of H does not have order 2 then $H \rtimes_\varphi \mathbf{Z}/(2)$ is nonabelian.

Consider the case $H = \mathbf{Z}/(n)$ where $n \geq 3$. The group $\mathbf{Z}/(n) \rtimes_\varphi \mathbf{Z}/(2)$ has order $2n$ and the group law (3.6) in this special case is

$$(j,k)(j',k') = (j + (-1)^k j', k + k'). \tag{3.7}$$

This may look like a weird group of order $2n$, but in fact it is isomorphic to D_n. If we identify $(1,0)$ with r and $(0,1)$ with s in D_n then $\mathbf{Z}/(n) \rtimes_\varphi \mathbf{Z}/(2) \cong D_n$ by $(1,0) \mapsto r$ and $(0,1) \mapsto s$. For example, (3.7) says $(0,1)(1,0) = (-1,1) = (-1,0)(0,1)$, which matches the familiar dihedral relation $sr = r^{-1}s$. (The general multiplication rule in D_n is $(r^j s^k)(r^{j'} s^{k'}) = r^{j + (-1)^k j'} s^{k+k'}$, where the exponents on r and s look like (3.7).)

Theorem 3.11. *In a semidirect product $H \rtimes_\varphi K$, the subgroup $1 \times K$ is normal if and only if $\varphi\colon K \to \mathrm{Aut}(H)$ is trivial, which makes $H \rtimes_\varphi K = H \times K$.*

Proof. Since $H \times_\varphi K$ is generated by the subgroups $H \times 1$ and $1 \times K$, $1 \times K$ is a normal subgroup if and only if $(h,1)(1,k)(h,1)^{-1} \in 1 \times K$ for all $h \in H$ and $k \in K$. We have

$$(h,1)(1,k)(h,1)^{-1} = (h,k)(h^{-1},1) = (h\varphi_k(h^{-1}), k \cdot 1) = (h\varphi_k(h)^{-1}, k),$$

which is in $1 \times K$ if and only if $\varphi_k(h) = h$. Therefore $1 \times K$ is normal in $H \rtimes_\varphi K$ if and only if every φ_k is the identity mapping on H, which means φ is trivial. □

4. Recognizing semidirect products

Theorem 2.1 tells us when a group is isomorphic to the direct product of two subgroups. When is a group isomorphic to a semidirect product of two subgroups?

In $H \rtimes_\varphi K$, the subgroups $H \times 1$ and $1 \times K$ have the following properties:

- they generate $H \rtimes_\varphi K$: $(h,k) = (h,1)(1,k)$,
- they intersect trivially: $(h,1) = (1,k) \Longrightarrow h = 1, k = 1$,
- elements of $1 \times K$ conjugate $H \times 1$ by φ: $(1,k)(h,1)(1,k)^{-1} = (\varphi_k(h), 1)$.

These properties can be abstracted to a "recognition theorem" for semidirect products.

Theorem 4.1. *Let G be a group with subgroups H and K such that*

(1) $G = HK$,
(2) $H \cap K = \{1\}$,
(3) $H \lhd G$.

Let $\varphi\colon K \to \mathrm{Aut}(H)$ be conjugation: $\varphi_k(h) = khk^{-1}$. Then φ is a homomorphism and the map $f\colon H \rtimes_\varphi K \to G$ where $f(h,k) = hk$ is an isomorphism.

Proof. That φ makes sense at all is due to (3). That it is a homomorphism means $\varphi_k \circ \varphi_{k'} = \varphi_{kk'}$, and this is left to the reader to check. The function

$$f\colon H \rtimes_\varphi K \to G$$

where $f(h,k) = hk$ is surjective by (1), and f is injective by (2) using the same argument for injectivity as in the proof of Theorem 2.1. To show f is a homomorphism, calculate

$$\begin{aligned} f((h,k)(h',k')) &= f(h\varphi_k(h'), kk') \\ &= h\varphi_k(h')kk' \\ &= hkh'k^{-1}kk' \\ &= hkh'k' \\ &= f(h,k)f(h',k'). \end{aligned}$$

Hence f is an isomorphism. □

Example 4.2. For a transposition τ in S_n, Theorem 4.1 implies $S_n \cong A_n \rtimes \{1, \tau\}$ where the semidirect product of subgroups of S_n is a conjugation action. We also have $D_n \cong \langle r \rangle \rtimes \{1, s\}$ and $\mathrm{SL}_2(\mathbf{Z}/(3)) \cong P \rtimes \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ where P is the (normal) 2-Sylow subgroup. Lastly, $\mathrm{GL}_2(\mathbf{R}) \cong \mathrm{SL}_2(\mathbf{R}) \rtimes K$ where K is the set of diagonal matrices, $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for $a \in \mathbf{R}^\times$. We met this decomposition for $\mathrm{GL}_2(\mathbf{R})$ earlier in Example 2.3.

Internally within a semidirect product group $H \rtimes K$, the action of K on H is always a conjugation: $(\varphi_k(h), 1) = (1,k)(h,1)(1,k)^{-1}$. Externally, if we create a semi-direct product from scratch using two groups H and K where K acts by automorphisms on H then only *after* we have built $H \rtimes K$ can we interpret the action of K on H (really, the action of the $(1,k)$'s on the $(h,1)$'s, being the standard copies of K and H inside $H \rtimes K$) as a conjugation action.

A group G can have $G = HK = HK'$ where K and K' are different isomorphic subgroups that both intersect the normal subgroup H trivially. If K and K' conjugate H in genuinely different ways then we get isomorphic semidirect products using different φ's for the same two abstract groups.

Example 4.3. We will show for odd $n > 1$ that the direct product $\mathrm{SL}_n(\mathbf{R}) \times \mathbf{R}^\times$ is isomorphic to a nontrivial semidirect product $\mathrm{SL}_n(\mathbf{R}) \rtimes \mathbf{R}^\times$.

Inside the group $G = \mathrm{GL}_n(\mathbf{R})$, let $H = \mathrm{SL}_n(\mathbf{R})$ and K be the subgroup of diagonal matrices $\mathrm{diag}(a, 1, 1, \ldots, 1)$ for $a \in \mathbf{R}^\times$, so $K \cong \mathbf{R}^\times$. Then $G = HK$ with $H \lhd G$ and $H \cap K = \{I_n\}$ (Example 2.3 is the special case $n = 2$). When $n > 1$, the conjugation action of K on H is nontrivial, so $\mathrm{GL}_n(\mathbf{R})$ is isomorphic to a nontrivial semidirect product $\mathrm{SL}_n(\mathbf{R}) \times H \cong \mathrm{SL}_n(\mathbf{R}) \rtimes \mathbf{R}^\times$.

The center of G is $Z = \{cI_n : c \in \mathbf{R}^\times\}$, which is isomorphic to $\mathbf{R}^\times$ and $H \cap Z = \{I_n\}$ if n is odd (for even n, $H \cap Z = \{\pm I_n\}$). For odd n we have $G = HZ$: if $g \in G$ and $\Delta = \det g$, then $g = hz$ where $h = g(\sqrt[n]{\Delta} I_n)^{-1}$ and $z = \sqrt[n]{\Delta} I_n$ The conjugation action of Z on H is trivial, so $\mathrm{GL}_n(\mathbf{R})$ is isomorphic to the direct product $\mathrm{SL}_n(\mathbf{R}) \times Z \cong \mathrm{SL}_n(\mathbf{R}) \times \mathbf{R}^\times$.

We have met several examples of groups that are isomorphic to a semidirect product of two groups:

(1) $\mathrm{Aff}(\mathbf{R}) \cong \mathbf{R} \rtimes \mathbf{R}^\times$
(2) $S_n \cong A_n \rtimes \mathbf{Z}/(2)$;
(3) $D_n \cong \mathbf{Z}/(n) \rtimes \mathbf{Z}/(2)$;
(4) $\mathrm{GL}_2(\mathbf{R}) \cong \mathrm{SL}_2(\mathbf{R}) \rtimes \mathbf{R}^\times$;

In these respective groups,

(1) $\mathbf{R}^\times$ acts on $\mathbf{R}$ by multiplication maps $\varphi_x : y \mapsto xy$ for $x \in \mathbf{R}^\times$;
(2) $\mathbf{Z}/(2)$ is identified with $\{1, \tau\}$ for any transposition τ in S_n;
(3) $\mathbf{Z}/(n)$ is identified with $\langle r \rangle$ and $\mathbf{Z}/(2)$ is identified with $\{1, s\}$ in D_n;
(4) $\mathbf{R}^\times$ is identified with the group of matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (*not* with the matrices $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$);

The way to "understand" semidirect products is to see in all these examples how a group breaks up into a set-product HK of two subgroups H and K with trivial intersection and K acts by conjugation on H. If you can see how all these examples work (even just $\mathrm{Aff}(\mathbf{R})$, as something concrete but nontrivial to keep in mind) then you can get an idea of what a semidirect product "is". In the case of $S_n \cong A_n \rtimes \mathbf{Z}/(2)$ and $D_n \cong \mathbf{Z}/(n) \rtimes_\varphi \mathbf{Z}/(2)$, the $\mathbf{Z}/(2)$ factor in the semidirect product corresponds to a special type of element of order 2, either a transposition in S_n or reflection in D_n. Not all elements of order 2 in S_n (for $n \geq 4$) are transpositions and not all elements of order 2 in D_n are reflections: consider $(12)(34) \in S_4$ or $r^2 \in D_4$.

Part of the point of the semidirect product construction is to abstract the idea that a group G can have the form HK where H and K are subgroups that intersect trivially with one of them (say H) being a normal subgroup. Since the elements of H and the elements of K don't commute in general, a semidirect product is a kind of "twisted" product, whose

simplest manifestation is the multiplication in the affine group $\mathrm{Aff}(\mathbf{R})$, where the upper-right entry in a product isn't the sum of the two upper right entries in the factors but has a twist: scale one factor by the upper-left entry of the other. This aspect of affine group multiplication is the computational idea behind semi-direct products.

5. Building semidirect products

So far we have not used semidirect products to create new groups we didn't already know in another way. To build new groups, starting with two groups H and K, we want to find some homomorphisms $\varphi\colon K \to \mathrm{Aut}(H)$ and then we can construct $H \rtimes_\varphi K$. The interesting cases are nontrivial φ, since trivial φ always lead to a direct product.

The case when H and K are finite with $(|K|, |\mathrm{Aut}(H)|) = 1$ is boring, since φ has a trivial image and thus the only semidirect product $H \rtimes K$ is the direct product $H \times K$.

Example 5.1. A semidirect product $\mathbf{Z}/(5) \rtimes \mathbf{Z}/(3)$ has order 15 and it must be a direct product: $\mathrm{Aut}(\mathbf{Z}/(5)) = (\mathbf{Z}/(5))^\times$ has order 4 and that is relatively prime to 3. In fact, all groups of order 15 are cyclic; groups of order pq will be studied below.

Example 5.2. Is there a nontrivial $\mathbf{Z}/(25) \rtimes \mathbf{Z}/(15)$? Since $\mathrm{Aut}(\mathbf{Z}/(25)) = (\mathbf{Z}/(25))^\times$ has size 20 and $(20, 15) \neq 1$, there might be nontrivial examples. We seek a nontrivial homomorphism

$$\varphi\colon \mathbf{Z}/(15) \to (\mathbf{Z}/(25))^\times.$$

It is necessary that $\varphi(1)$ goes[1] to a g such that $g^{15} = 1$. If $g^{15} \equiv 1 \bmod 25$, then $g^{15} \equiv 1 \bmod 5$, so (by testing mod 5) $g \equiv 1 \bmod 5$. Then

$$g \in \{1, 6, 11, 16, 21\}.$$

Choose $g = 6$. Check $6^{15} \equiv 1 \bmod 25$ (in fact, if $a \equiv 1 \bmod 5$ then $a^5 \equiv 1 \bmod 25$, so $a^{15} \equiv 1 \bmod 25$). Let $\varphi\colon \mathbf{Z}/(15) \to (\mathbf{Z}/(25))^\times$ by $\varphi(1) = 6$, so $\varphi(k \bmod 15) = 6^k \bmod 25$ (*e.g.*, $\varphi(2) = \varphi(1+1) = \varphi(1)\varphi(1) = 6^2$). We get a nontrivial semidirect product $\mathbf{Z}/(25) \rtimes_\varphi \mathbf{Z}/(15)$ with the group law

$$(a, b)(c, d) = (a + \varphi_b(c), b + d) = (a + 6^b c, b + d).$$

This is a nonabelian group of order $15 \cdot 25 = 375$ built from two cyclic groups of order 15 and 25.

Example 5.3. Is there a nontrivial $\mathbf{Z}/(4) \rtimes_\varphi \mathbf{Z}/(2)$? Since

$$\mathrm{Aut}(\mathbf{Z}/(4)) = \{x \mapsto x,\ x \mapsto -x\} \cong \{\pm 1 \bmod 4\} = (\mathbf{Z}/(4))^\times,$$

there is one nontrivial $\varphi\colon \mathbf{Z}/(2) \to \mathrm{Aut}(\mathbf{Z}/(4))$, namely the one where $\varphi(k \bmod 2) = \{x \mapsto (-1)^k x\}$. In $\mathbf{Z}/(4) \rtimes_\varphi \mathbf{Z}/(2)$,

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

This is a group of order 8 built from two subgroups $H \cong \mathbf{Z}/(4)$ and $K \cong \mathbf{Z}/(2)$. It is isomorphic to D_4, with an isomorphism

$$f\colon \mathbf{Z}/(4) \rtimes_\varphi \mathbf{Z}/(2) \longrightarrow D_4 = \langle r, s \rangle$$

being given by $f(a, b) = r^a s^b$. This is a special case of Example 3.10.

[1]To choose a group homomorphism $\varphi\colon \mathbf{Z}/(n) \to G$ is tantamount to finding $g \in G$ such that $g^n = 1$. Then $\varphi(a \bmod n) = g^a$ is the unique homomorphism where $\varphi(1) = g$. Different g's give different φ's.

Example 5.4. For a group H (written multiplicatively) that has an automorphism f of order 2, we get the group $H \rtimes_\varphi \mathbf{Z}/(2)$ where

$$(h,k)(h',k') = (h \cdot f^k(h'), k+k').$$

Here $\varphi\colon \mathbf{Z}/(2) \to \mathrm{Aut}(H)$ by $\varphi_k = f^k$, *i.e.*,

$$\varphi_k(h) = \underbrace{f(f(\cdots(f(h))))}_{k \text{ times}}, \qquad k > 0.$$

The case where H is abelian and $f\colon H \to H$ is inversion on H is in Example 3.10. An example with nonabelian H is $H = \mathrm{GL}_2(\mathbf{R})$ and $f(A) = (A^\top)^{-1}$ (the inverse transpose mapping).

If a group H has an automorphism f such that $f^n = \mathrm{id}_H$, then we get a semidirect product $H \rtimes_\varphi \mathbf{Z}/(n)$ with group law

$$(h,k)(h',k') = (h \cdot f^k(h'), k+k').$$

Example 5.5. A semidirect product $\mathbf{Z}/(8) \rtimes_\varphi \mathbf{Z}/(2)$ has order 16 and comes from a homomorphism $\varphi\colon \mathbf{Z}/(2) \to \mathrm{Aut}(\mathbf{Z}/(8))$. There are four automorphisms of $\mathbf{Z}/(8)$: $x \mapsto x$, $x \mapsto 3x$, $x \mapsto 5x$, and $x \mapsto 7x$. This gives us four semidirect products $\mathbf{Z}/(8) \rtimes_\varphi \mathbf{Z}/(2)$, with the following different group laws:

$$(a,b)(c,d) = (a+c, b+d),$$

$$(a,b)(c,d) = (a+3^b c, b+d), \tag{5.1}$$

$$(a,b)(c,d) = (a+5^b c, b+d), \tag{5.2}$$

$$(a,b)(c,d) = (a+7^b c, b+d). \tag{5.3}$$

Just because formulas for two group laws look different does not mean the groups are nonisomorphic, although it turns out all of these groups of order 16 are nonisomorhic. The first one is abelian and the rest are nonabelian (nontrivial semidirect products). One way to distinguish the nonabelian examples is that they have different numbers of elements that square to the identity (this counts the identity and all elements of order 2).

Case 1: The group (5.1). Here $(a,b)^2 = (a(1+3^b), 0)$, so we want to count all (a,b) with $a \in \mathbf{Z}/(8)$ and $b \in \mathbf{Z}/(2)$ such that $a(1+3^b) \equiv 0 \bmod 8$. If $b = 0$ in $\mathbf{Z}/(2)$ then $(2a,0) = (0,0)$, so $a = 0, 4$ in $\mathbf{Z}/(8)$. If instead $b = 1$ in $\mathbf{Z}/(2)$ then $4a \equiv 0 \bmod 8$, so a is even. There are 4 such values of a, so the number of solutions of $(a,b)^2 = (0,0)$ is $2+4 = 6$.

Case 2: The group (5.2). Here $(a,b)^2 = (a(1+5^b), 0)$, so we will determine all (a,b) where $a(1+5^b) \equiv 0 \bmod 8$. If $b = 0$ then $(2a,0) = (0,0)$, so $a = 0, 4$ in $\mathbf{Z}/(8)$ (this is the same as in the previous case). If $b = 1$ then $6a \equiv 0 \bmod 8$, so $2a \equiv 0 \bmod 8$. There are 2 values of a, so the number of solutions of $(a,b)^2 = (0,0)$ is $2+2 = 4$.

Case 3: The group (5.3). Here $(a,b)^2 = (a(1+7^b), 0)$. When $b = 0$ there are 2 values of a (as in the other cases), while when $b = 1$ we have $a(1+7^b) = 0$ in $\mathbf{Z}/(8)$ for all a, so there are 8 values of a. Therefore the number of solutions of $(a,b)^2 = (0,0)$ is $2+8 = 10$.

6. Groups of order pq

Let p and q be primes such that $p < q$. We'll use the Sylow theorems and semidirect products to find all groups of order pq up to isomorphism. The point of this application is to see how different semidirect products can be isomorphic to each other. We'll see that there are two different cases, depending on whether or not $q \equiv 1 \bmod p$.

Theorem 6.1. *If primes $p < q$ satisfy $q \not\equiv 1 \bmod p$ then all groups of order pq are cyclic.*

Proof. Let $|G| = pq$, P be a subgroup of order p and Q be a subgroup of order q (by the Sylow theorems or by Cauchy's theorem). Let n_p and n_q be the number of p-Sylow and q-Sylow subgroups of G. From the third Sylow theorem $n_p \equiv 1 \bmod p$ with $n_p \mid q$, and $n_q \equiv 1 \bmod q$ with $n_q \mid p$. For the q-Sylow subgroups, $n_q = 1$ or $n_q = p$, but $n_q = p$ is impossible since $p < q$, so we can't have $p \equiv 1 \bmod q$. Thus $n_q = 1$, so $Q \lhd G$. For the p-Sylow subgroups, $n_p = 1$ or q.

Since $q \not\equiv 1 \bmod p$, we must have $n_p = 1$, so $P \lhd G$. Thus $xy = yx$ for all $x \in P$ and $y \in Q$, since $xyx^{-1}y^{-1} \in P \cap Q = \{1\}$. Letting x be nontrivial in P and y be nontrivial in Q, x has order p and y has order q, and x and y commute, so xy has order pq. Thus $\langle xy \rangle = G$, so G is cyclic. □

Lemma 6.2. *A semidirect product $H \rtimes_\varphi K$ is unchanged up to isomorphism if the action $\varphi\colon K \to \mathrm{Aut}(H)$ is composed with an automorphism of K: for automorphisms $f\colon K \to K$, $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$.*

$$K \xrightarrow{f} K \xrightarrow{\varphi} \mathrm{Aut}(H), \qquad K \xrightarrow{\varphi \circ f} \mathrm{Aut}(H)$$

Proof. Exercise. □

Theorem 6.3. *If primes $p < q$ satisfy $q \equiv 1 \bmod p$ then there are two groups of order pq up to isomorphism: one is cyclic and one is nonabelian.*

Proof. Using the notation from the previous proof, the argument there that $n_q = 1$ still works since it made no use of knowledge of $q \bmod p$. Thus $Q \lhd G$.

For the p-Sylow count, $n_p \equiv 1 \bmod p$ and $n_p \mid q$, so $n_p = 1$ or $n_p = q$. Both choices are consistent with the congruence condition $n_p \equiv 1 \bmod p$, so we consider each one.

Case 1: $n_p = 1$. Here the group G is cyclic by the same argument as in the proof of the previous theorem.

Case 2: $n_p = q$. Now G can't be cyclic, since cyclic groups have all Sylow counts equal to 1 (all Sylow subgroups are nornal). Since $Q \lhd G$ and $Q \cap P = \{1\}$, QP is a subgroup of G with order $qp = |G|$, so $G = QP = PQ$. The recognition theorem for semidirect products (Theorem 4.1) tells us that $G \cong Q \rtimes_\varphi P$ where $\varphi\colon P \to \mathrm{Aut}(Q)$ is the conjugation action of P on Q.

Semidirect product constructions are unchanged up to isomorphism if we replace the groups involved with isomorphic groups (see Theorem 10.2 below), so we may suppose $P = \mathbf{Z}/(p)$ and $Q = \mathbf{Z}/(q)$. Then every noncyclic group of order pq when $q \equiv 1 \bmod p$ is $\mathbf{Z}/(q) \rtimes_\varphi \mathbf{Z}/(p)$ for a nontrivial homomorphism

$$\varphi\colon \mathbf{Z}/(p) \longrightarrow \mathrm{Aut}(\mathbf{Z}/(q)) \cong (\mathbf{Z}/(q))^\times.$$

We will show there are $p-1$ such homomorphisms and they all lead to isomorphic semidirect products. (Contrast this with Example 5.5, where the three nontrivial semidirect products $\mathbf{Z}/(8) \rtimes_\varphi \mathbf{Z}/(2)$ are mutually nonisomorphic.)

The different homomorphisms $\varphi\colon \mathbf{Z}/(p) \to \mathrm{Aut}(\mathbf{Z}/(q)) \cong (\mathbf{Z}/(q))^\times$ are determined by where they send the generator 1, which has to go to a solution in $(\mathbf{Z}/(q))^\times$ to $z^p \equiv 1 \bmod q$, with $z = 1$ being the trivial homomorphism that does not interest us. Since $(\mathbf{Z}/(q))^\times$ has order $q-1$ and $p \mid (q-1)$ by hypothesis (that is, $q \equiv 1 \bmod p$), there are elements of order

p in $(\mathbf{Z}/(q))^\times$ by Cauchy's theorem. For each solution of $z^p \equiv 1 \bmod q$ with $z \not\equiv 1 \bmod p$, we get a semidirect product

$$\mathbf{Z}/(q) \rtimes_\varphi \mathbf{Z}/(p)$$

by

$$(a,b)(c,d) = (a + \varphi_b(c), b+d) = (a + z^b c, b+d). \tag{6.1}$$

(Note if $z = 1$ this is the direct product.)

The set $\{z \in (\mathbf{Z}/(q))^\times : z^p \equiv 1 \bmod q\}$ is a nontrivial subgroup of $(\mathbf{Z}/(q))^\times$. Each $z \neq 1$ in here generates a subgroup $\langle z \rangle$ of order p, all of whose elements have pth power 1. For all prime q, the group $(\mathbf{Z}/(q))^\times$ is cyclic, so it has only *one* subgroup of order p. Thus $\{z \in (\mathbf{Z}/(q))^\times : z^p \equiv 1 \bmod p\}$ has order p, so the number of φ's is p and the number of nontrivial φ's is $p-1$.

Two nontrivial φ's are associated (by (6.1)) to two elements z of order p in $(\mathbf{Z}/(q))^\times$, call them z_1 and z_2. They generate the same subgroup, so $z_2 = z_1^r$ for some $r \in \mathbf{Z}$ (necessarily $(r,p) = 1$). We will show from the relation $z_2 = z_1^r$ that the semidirect products in (6.1) using z_1 and z_2 are isomorphic groups.

Let $\varphi_1, \varphi_2 \colon \mathbf{Z}/(p) \to (\mathbf{Z}/(q))^\times$ be the homomorphisms associated to z_1 and z_2: $\varphi_1(b) = z_1^b$ and $\varphi_2(b) = z_2^b = z_1^{br}$. The group laws (6.1) using $z = z_1$ and $z = z_2$ are

$$(a,b)(c,d) = (a + z_1^b c, b+d) \quad \text{and} \quad (a,b)(c,d) = (a + z_2^b c, b+d) = (a + z_1^{rb} c, b+d).$$

The formula for φ_2 shows it is a composition: $\varphi_2 = \varphi_1 \circ f$ where $f \colon \mathbf{Z}/(p) \to \mathbf{Z}/(p)$ by $f(x) = rx$. This f is an automorphism of $\mathbf{Z}/(p)$, so $\mathbf{Z}/(q) \rtimes_{\varphi_2} \mathbf{Z}/(p) \cong \mathbf{Z}/(q) \rtimes_{\varphi_1} \mathbf{Z}/(p)$ by Lemma 6.2. So when $p < q$ and $q \equiv 1 \bmod p$, there are (up to isomorphism) two groups of order pq. □

Explicitly, for $q \equiv 1 \bmod p$, a nonabelian matrix group of order pq is

$$\left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in (\mathbf{Z}/(q))^\times, y \in \mathbf{Z}/(q), x^p \equiv 1 \bmod q \right\} \subset \mathrm{Aff}(\mathbf{Z}/(q)).$$

Remark 6.4. The classification of groups of order pq up to isomorphism (one group when $q \not\equiv 1 \bmod p$ and two groups when $q \equiv 1 \bmod p$) can be done using only Cauchy's theorem; there is no logical need for the Sylow theorems or semidirect products.[2] Some people prefer proofs using more mathematical machinery rather than less.

7. Groups of order 1881

The number 1881 factors as $3^2 \cdot 11 \cdot 19 = 9 \cdot 209$. We will use semidirect products to describe all groups of this order.

Theorem 7.1. *Up to isomorphism there are five groups of order* 1881*: three semidirect products* $\mathbf{Z}/(209) \rtimes \mathbf{Z}/(9)$ *and two semidirect products* $\mathbf{Z}/(209) \rtimes (\mathbf{Z}/(3))^2$.

Proof. Let G be a group of order 1881.

Step 1: $G \cong \mathbf{Z}/(209) \rtimes K$ where K is a group of order 9.

[2]See Section 3 of https://kconrad.math.uconn.edu/blurbs/grouptheory/cauchyapp.pdf.

For a prime p, let n_p the number of p-Sylow subgroups of G of order 1881. By the third Sylow theorem,

$$\begin{aligned} n_3 \equiv 1 \bmod 3, \quad n_3 \mid 11 \cdot 19 &\implies n_3 = 1 \text{ or } 19, \\ n_{11} \equiv 1 \bmod 11, \quad n_{11} \mid 3^2 \cdot 19 &\implies n_{11} = 1, \\ n_{19} \equiv 1 \bmod 19, \quad n_{19} \mid 3^2 \cdot 11 &\implies n_{19} = 1. \end{aligned}$$

Therefore G has normal subgroups P of order 11 and Q of order 19, so the set PQ is a normal subgroup of order $11 \cdot 19 = 209$. This in fact is the *only* subgroup of G with order 209: a subgroup of that order has subgroups of order 11 and 19, which can only be P and Q, so the subgroup must contain PQ, which has order 209.

Since $(|P|, |Q|) = 1$, elements of P commute with elements of Q (a commutator of such elements is in $P \cap Q = \{1\}$). Both P and Q are cyclic since they have prime order. Letting x generate P and y generate Q, their orders are relatively prime and they commute, so xy has order $11 \cdot 19 = 209$ and thus $PQ = \langle xy \rangle$: PQ is a cyclic normal subgroup of G with order 209.

Set $H = PQ$ and let K be a 3-Sylow subgroup of G. Since $H \lhd G$ and $|K| = 9$, HK is a subgroup of G of order $|H||K|/|H \cap K| = 1881$, so $G = HK$ and the recognition theorem for semidirect products (Theorem 4.1) tells us G is isomorphic to a semidirect product $H \rtimes_\varphi K$. The group K is isomorphic to $\mathbf{Z}/(9)$ or $(\mathbf{Z}/(3))^2$, so by Theorem 10.2 we can take $H = \mathbf{Z}/(209)$ and $K = \mathbf{Z}/(9)$ or $(\mathbf{Z}/(3))^2$. Isomorphic groups have isomorphic 3-Sylow subgroups, so semidirect products where $K = \mathbf{Z}/(9)$ are not isomorphic to semidirect products where $K = (\mathbf{Z}/(3))^2$.

Step 2: Classify all semidirect products $\mathbf{Z}/(209) \rtimes \mathbf{Z}/(9)$.

Let $\varphi\colon \mathbf{Z}/(9) \to (\mathbf{Z}/(209))^\times$ be a homomorphism. It is determined by $\varphi(1)$, which is a solution of $a^9 \equiv 1 \bmod 209$. Since $209 = 11 \cdot 19$,

$$(\mathbf{Z}/(209))^\times \cong (\mathbf{Z}/(11))^\times \times (\mathbf{Z}/(19))^\times \cong C_{10} \times C_{18} \cong C_{10} \times C_2 \times C_9.$$

Therefore $(\mathbf{Z}/(209))^\times$ has one subgroup of order 9 and it is cyclic.

To find an element of order 9 in $(\mathbf{Z}/(209))^\times$, in $(\mathbf{Z}/(11))^\times \times (\mathbf{Z}/(19))^\times$ an element of order 9 is $(1, 4)$. The solution of $x \equiv 1 \bmod 11$ and $x \equiv 4 \bmod 19$ is $23 \bmod 209$. Thus $23 \bmod 209$ generates the subgroup of $(\mathbf{Z}/(209))^\times$ with order 9, so $\varphi(1) = 23^r \bmod 209$ for some $r \in \{0, 1, \ldots, 8\}$. To be explicit, when $\varphi(1) = 23^r \bmod 209$ the group law on $\mathbf{Z}/(209) \rtimes_\varphi \mathbf{Z}/(9)$ is

$$(a, b)(c, d) = (a + \varphi_b(c), b + d) = (a + 23^{rb}c, b + d). \tag{7.1}$$

Depending on $\gcd(r, 9)$, we'll see the group law (7.1) can be rescaled to three cases: $r = 1$, $r = 3$, and $r = 0$.

Case 1: $\gcd(r, 9) = 1$, so $r = 1, 2, 4, 5, 7$, or 8.

In $\mathbf{Z}/(9)$, r generates the (additive) group. Let $rr' \equiv 1 \bmod 9$ and $f\colon \mathbf{Z}/(9) \to \mathbf{Z}/(9)$ by $f(x) = r'x$. This is an automorphism of $\mathbf{Z}/(9)$ and $\varphi \circ f\colon \mathbf{Z}/(9) \to (\mathbf{Z}/(209))^\times$ is a homomorphism where $(\varphi \circ f)(1 \bmod 9) = 23^{rr'} \equiv 23 \bmod 209$, so in $\mathbf{Z}/(209) \rtimes_{\varphi\circ f} \mathbf{Z}/(9)$,

$$(a, b)(c, d) = (a + 23^b c, b + d). \tag{7.2}$$

By Lemma 6.2, $\mathbf{Z}/(209) \rtimes_{\varphi\circ f} \mathbf{Z}/(9) \cong \mathbf{Z}/(209) \rtimes_\varphi \mathbf{Z}/(9)$, so the group given by (7.1) is isomorphic to the group given by (7.2).

Case 2: $\gcd(r, 9) = 3$, so $r = 3$ or 6.

If $r = 3$ then the group law in $\mathbf{Z}/(209) \rtimes_\varphi \mathbf{Z}/(9)$ is

$$(a,b)(c,d) = (a + \varphi_b(c), b + d) = (a + 23^{3b}c, b + d). \tag{7.3}$$

If $r = 6$ then $r \equiv -3 \bmod 9$, so composing $\varphi\colon \mathbf{Z}/(9) \to (\mathbf{Z}/(209))^\times$ with multiplication by -1 on $\mathbf{Z}/(9)$ turns the group law (7.1) with $r = 6$ into the one with $r = 3$ in (7.3), and the two groups are isomorphic by Lemma 6.2.

Case 3: $r = 0$. Here (7.1) is the direct product $\mathbf{Z}/(209) \times \mathbf{Z}/(9)$, which is cyclic of order 1881.

The group in Case 3 is not isomorphic to those in Cases 1 or 2 since the first two cases are nonabelian (a nontrivial semidirect product of two abelian groups is nonabelian). To show the groups (7.2) and (7.3) are not isomorphic, consider the conjugation action in both cases of G on its unique (normal) subgroup H of order 209. In (7.2), $(a,b)(c,0)(a,b)^{-1} = (23^b c, 0)$, while in (7.3), $(a,b)(c,0)(a,b)^{-1} = (23^{3b}c, 0)$. Since 23 mod 209 has order 9 and 23^3 mod 209 has order 3, conjugation by $(0,1)$ on H in (7.2) is an automorphism of H with order 9, while in (7.3) conjugation by *every* element of G on H is an automorphism with order 1 or 3.

Put differently, groups in the three different cases above are not isomorphic since the conjugation action of G on its unique subgroup H of order 209 is a homomorphism $G \to \mathrm{Aut}(H)$ whose image has order 9 in Case 1, order 3 in Case 2, and order 1 in Case 3.

Summing up, there are three nonisomorphic semidirect products $\mathbf{Z}/(209) \rtimes \mathbf{Z}/(9)$.

Step 3: Classify all semidirect products $\mathbf{Z}/(209) \rtimes (\mathbf{Z}/(3))^2$.

The trivial semidirect product is the direct product, which is abelian, and every nontrivial semidirect product is nonabelian, so those cases behave differently. We will show the nontrivial semidirect products are all isomorphic, so there are two semidirect products $\mathbf{Z}/(209) \rtimes (\mathbf{Z}/(3))^2$ up to isomorphism: one is trivial and one is nontrivial. The automorphism group of $(\mathbf{Z}/(3))^2$ is $\mathrm{GL}_2(\mathbf{Z}/(3))$, so $\mathrm{GL}_2(\mathbf{Z}/(3))$ will play a role in this step that $(\mathbf{Z}/(9))^\times = \mathrm{Aut}(\mathbf{Z}/(9))$ did in the previous step.

The unique subgroup of $(\mathbf{Z}/(209))^\times$ of order 3 is $\langle 23^3 \rangle = \langle 45 \rangle = \{1, 45, 144 \bmod 209\}$. Let $\varphi\colon (\mathbf{Z}/(3))^2 \to (\mathbf{Z}/(209))^\times$ be the homomorphism determined by $\varphi\binom{1}{0} = 45 \bmod 209$ and $\varphi\binom{0}{1} = 1 \bmod 209$, *i.e.*, $\varphi\binom{x}{y} = 45^x \bmod 209$. The group law in $\mathbf{Z}/(209) \rtimes_\varphi (\mathbf{Z}/(3))^2$ is

$$\left(a, \binom{x}{y}\right)\left(a', \binom{x'}{y'}\right) = \left(a + 45^x a', \binom{x+x'}{y+y'}\right). \tag{7.4}$$

We'll show all nontrivial semidirect products $\mathbf{Z}/(209) \rtimes (\mathbf{Z}/(3))^2$ are isomorphic to the group (7.4) by using matrices in $\mathrm{GL}_2(\mathbf{Z}/(3))$ to convert other semidirect product group structures into the one in (7.4)

The nonzero elements of $(\mathbf{Z}/(3))^2$ all have order 3 and $\langle 45 \bmod 209 \rangle$ is the only subgroup of $(\mathbf{Z}/(209))^\times$ with order 3, so each *nontrivial* homomorphism $\varphi\colon (\mathbf{Z}/(3))^2 \to (\mathbf{Z}/(209))^\times$ has image $\langle 45 \bmod 209 \rangle$. Thus for some $v \in (\mathbf{Z}/(3))^2$, $\varphi(v) = 45 \bmod 209$. The kernel of φ is nontrivial, so $\varphi(w) = 1 \bmod 209$ for some nonzero $w \in (\mathbf{Z}/(3))^2$. Clearly v is not a multiple of w in $(\mathbf{Z}/(3))^2$, so $\{v, w\}$ is a basis of $(\mathbf{Z}/(3))^2$ and $\varphi(xv + yw) = \varphi(v)^x \varphi(w)^y = 45^x \bmod 209$ for $x, y \in \mathbf{Z}/(3)$.

The matrix $A = [v \;\; w]$ with columns v and w in $(\mathbf{Z}/(3))^2$ is invertible (it has linearly independent columns) and it sends $\binom{1}{0}$ to v and $\binom{0}{1}$ to w. Therefore the composite homomorphism $\varphi \circ A\colon (\mathbf{Z}/(3))^2 \to (\mathbf{Z}/(209))^\times$ has the effect $\binom{1}{0} \mapsto v \mapsto 45 \bmod 209$ and $\binom{0}{1} \mapsto w \mapsto 1 \bmod 209$, which makes the semidirect product $\mathbf{Z}/(209) \rtimes_{\varphi \circ A} (\mathbf{Z}/(3))^2$ have the group structure in (7.4). By Lemma 6.2, $\mathbf{Z}/(209) \rtimes_{\varphi \circ A} (\mathbf{Z}/(3))^2 \cong \mathbf{Z}/(209) \rtimes_\varphi (\mathbf{Z}/(3))^2$,

so every nontrivial semidirect product $\mathbf{Z}/(209) \rtimes_{\varphi\circ A} (\mathbf{Z}/(3))^2$ is isomorphic to the group given by (7.4). □

8. Groups of order p^3

When p is an odd prime, we will show the nonabelian groups of order p^3 are semidirect products. First we'll describe these groups concretely and then show the examples we found are the only ones possible up to isomorphism.[3]

Two nonabelian groups of order p^3 are the mod p Heisenberg group

$$\mathrm{Heis}(\mathbf{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{Z}/(p) \right\}$$

and a mod p^2 matrix group with no standard name:

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbf{Z}/(p^2), a \equiv 1 \bmod p \right\} = \left\{ \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} : m, b \in \mathbf{Z}/(p^2) \right\},$$

In $\mathrm{Heis}(\mathbf{Z}/(p))$,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \tag{8.1}$$

and in G_p

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+pm' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(m+m') & b+b'+pmb' \\ 0 & 1 \end{pmatrix}. \tag{8.2}$$

It is left to you to show $\mathrm{Heis}(\mathbf{Z}/(p))$ and G_p are nonabelian. To see they're nonisomorphic,

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

for $n \in \mathbf{Z}$, so the right side is the identity matrix mod p when $n = p$ (here we use $p(p-1)/2 \equiv 0 \bmod p$ when $p \neq 2$), so all non-identity elements of $\mathrm{Heis}(\mathbf{Z}/(p))$ have order p. In G_p the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ mod p^2 has order p^2, so $\mathrm{Heis}(\mathbf{Z}/(p)) \ncong G_p$.[4]

Now let's see $\mathrm{Heis}(\mathbf{Z}/(p))$ and G_p are semidirect products. In $\mathrm{Heis}(\mathbf{Z}/(p))$ are subgroups

$$H = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : b, c \in \mathbf{Z}/(p) \right\} \quad \text{and} \quad K = \left\{ \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a \in \mathbf{Z}/(p) \right\},$$

with $H \cong (\mathbf{Z}/(p))^2$, $K \cong \mathbf{Z}/(p)$, and $H \lhd \mathrm{Heis}(\mathbf{Z}/(p))$ since $H = \ker f$ for the homomorphism $f\colon \mathrm{Heis}(\mathbf{Z}/(p)) \to \mathbf{Z}/(p))$ defined by

$$f \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = a.$$

[3]For $p = 2$, the two groups of order 8 up to isomorphism are D_4 and Q_8, and we'll see Q_8 is not a semidirect product in Example 9.2.

[4]It turns out that $\mathrm{Heis}(\mathbf{Z}/(2)) \cong G_2 \cong D_4$.

Since $H \cap K$ is trivial we have $\mathrm{Heis}(\mathbf{Z}/(p)) = HK$. The conjugation action of K on H is based on the mod p matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$:

$$K = \left\{ \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^a : a \in \mathbf{Z}/(p) \right\}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & b+c \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix},$$

and $\left(\begin{smallmatrix} b+c \\ c \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} b \\ c \end{smallmatrix}\right)$. Thus

$$\boxed{\mathrm{Heis}(\mathbf{Z}/(p)) \cong (\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)}$$

where $\varphi\colon \mathbf{Z}/(p) \to \mathrm{Aut}((\mathbf{Z}/(p))^2) = \mathrm{GL}_2(\mathbf{Z}/(p))$ is defined by $\varphi(1 \bmod p) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The center of $\mathrm{Heis}(\mathbf{Z}/(p))$ is

$$\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/(p) \right\} = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \bmod p \right\rangle,$$

so H contains the center of $\mathrm{Heis}(\mathbf{Z}/(p))$.

Turning next to the group G_p, it has subgroups

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/(p^2) \right\} \quad \text{and} \quad K = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in \mathbf{Z}/(p^2), a \equiv 1 \bmod p \right\},$$

with $H = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \bmod p^2 \rangle \cong \mathbf{Z}/(p^2)$, $K = \langle \left(\begin{smallmatrix} 1+p & 1 \\ 0 & 1 \end{smallmatrix}\right) \bmod p^2 \rangle \cong \mathbf{Z}/(p)$, and $H \lhd G_p$ since $H = \ker f$ for the homomorphism $f\colon G_p \to \mathrm{Aut}(\mathbf{Z}/(p^2)) = (\mathbf{Z}/(p^2))^\times$ defined by

$$f \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = a.$$

Since $H \cap K$ is trivial, $G_p = HK$. The conjugation action of K on H is described by

$$\begin{pmatrix} 1+pm & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+pm & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & (1+pm)b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{1+pm}.$$

Thus

$$\boxed{G_p \cong \mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)}$$

where $\psi\colon \mathbf{Z}/(p) \to \mathrm{Aut}(\mathbf{Z}/(p^2)) = (\mathbf{Z}/(p^2))^\times$ is defined by $\psi(1 \bmod p) = 1 + p$.

The center of G_p is

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/(p^2), b \equiv 0 \bmod p \right\} = \left\langle \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \bmod p^2 \right\rangle,$$

so H contains the center of G_p.

Now we'll start over and show a nonabelian group of order p^3 for odd prime p is isomorphic to one of the semidirect products we just constructed.[5]

Theorem 8.1. *For prime $p > 2$, a nonabelian group of order p^3 is isomorphic to one of the semidirect products $(\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)$ or $\mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)$ for the homomorphisms $\varphi\colon \mathbf{Z}/(p) \to \mathrm{GL}_2(\mathbf{Z}/(p))$ where $\varphi(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\psi\colon \mathbf{Z}/(p) \to (\mathbf{Z}/(p^2))^\times$ where $\psi(1) = 1 + p \bmod p^2$, and these two semidirect products are not isomorphic.*

[5] That such a group is isomorphic to $\mathrm{Heis}(\mathbf{Z}/(p))$ or G_p, without using semidirect products, is in https://kconrad.math.uconn.edu/blurbs/grouptheory/groupsp3.pdf.

Proof. Step 1: If G is nonabelian of order p^3 then its center Z has order p.

Since G is a nontrivial group of p-power order, its center is nontrivial. Therefore $|Z| = p, p^2$, or p^3. Since G is nonabelian, $|Z| \neq p^3$. For a group G, if G/Z is cyclic then G is abelian. So G being nonabelian forces G/Z to be noncyclic. Therefore $|G/Z| \neq p$, so $|Z| \neq p^2$. Thus $|Z| = p$.

Step 2: For each subgroup H of G with order p^2, $Z \subset H$.

The subgroup H is abelian since it has order p^2. If $Z \not\subset H$ then $H \cap Z$ is trivial by Step 1, so $G = HZ$, which is abelian, and that's a contradiction. (This step confirms abstractly what we observed above in $\mathrm{Heis}(\mathbf{Z}/(p))$ and G_p: the subgroup H we defined in each of them with order p^2 contains the center of the group.)

Step 3: If each non-identity element of G has order p, then $G \cong (\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)$ where $\varphi\colon \mathbf{Z}/(p) \to \mathrm{GL}_2(\mathbf{Z}/(p))$ is the homomorphism such that $\varphi(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$

Pick $z \in Z - \{1\}$ and $x \in G - Z$. Then $Z = \langle z \rangle$ by Step 1, $xz = zx$, and $z \notin \langle x \rangle$, so $H := \langle z, x \rangle \cong (\mathbf{Z}/(p))^2$ because x and z have order p.[6] In a p-group, every subgroup of index p is normal,[7] so $H \lhd G$.

Pick $y \in G - H$ and set $K = \langle y \rangle$, so K has order p and $H \cap K$ is trivial. Thus $|HK| = |H||K|/|H \cap K| = p^3$, so $G = HK$. Thus $G = H \rtimes K$ where K acts on H by conjugation.

Claim: $yxy^{-1} = z^i x$ for some $i \not\equiv 0 \bmod p$.

To prove the claim, since $H \lhd G$ we have

$$yxy^{-1} = z^i x^j \tag{8.3}$$

for some $i, j \in \mathbf{Z}/(p)$. Conjugating both sides by y,

$$y^2xy^{-2} = y(z^ix^j)y^{-1} = z^iyx^jy^{-1} = z^i(yxy^{-1})^j = z^i(z^ix^j)^j = z^{i+ij}x^{j^2} = z^{i(1+j)}z^{j^2}.$$

By induction,

$$y^m x y^{-m} = z^{i(1+j+j^2+\cdots+j^{m-1})}x^{j^m} \tag{8.4}$$

for all $m \geq 1$. Since $y^p = 1$, setting $m = p$ turns (8.4) into

$$x = z^{i(1+j+j^2+\cdots+j^{p-1})}x^{j^p} = z^{i(1+j+j^2+\cdots+j^{p-1})}x^j \tag{8.5}$$

since x has order p and $j^p \equiv j \bmod p$.

Assume $j \not\equiv 1 \bmod p$. Then in the exponent of z in (8.5) we have $1 + j + j^2 + \cdots + j^{p-1} = (j^p - 1)/(j - 1) \equiv (j-1)/(j-1) \equiv 1 \bmod p$, so (8.5) turns into $x = z^i x^j$. Thus $x^{1-j} = z^i$. The intersection $\langle x \rangle \cap \langle z \rangle$ is trivial, so $x^{1-j} = 1$, which implies $j \equiv 1 \bmod p$. That's a contradiction, so $j \equiv 1 \bmod p$. Now (8.3) says $yxy^{-1} = z^i x$. If $i \equiv 0 \bmod p$ then $yxy^{-1} = x$, so y commutes with x. Then since $H = \langle z, x \rangle$ and $z \in Z$, y commutes with all of H, which implies $G = HK$ is abelian: contradiction! Thus $i \not\equiv 0 \bmod p$, which proves the claim.

Since $H = \langle z, x \rangle = \langle z^i, x \rangle$, *rename* z^i *as* z. Then $K = \langle y \rangle$,

$$yzy^{-1} = z, \quad \text{and} \quad yxy^{-1} = zx \tag{8.6}$$

by the claim (and the new meaning of z). Using the isomorphisms $H \to (\mathbf{Z}/(p))^2$ where $z^b x^c \mapsto \binom{b}{c}$ and $K \to \mathbf{Z}/(p)$ where $y^a \mapsto a$ together with the formulas in (8.6), the conjugation action $K \to \mathrm{Aut}(H)$ turns into the homomorphism $\varphi\colon \mathbf{Z}/(p) \to \mathrm{GL}_2(\mathbf{Z}/(p))$ where $\varphi(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, so $G \cong (\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)$.

[6] Step 2 explains why it is reasonable to define H to contain a generator of Z.

[7] See Corollary 6.4 in https://kconrad.math.uconn.edu/blurbs/grouptheory/gpaction.pdf.

Step 4: If some non-identity element of G has order p^2, then $G \cong \mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)$ where $\psi\colon \mathbf{Z}/(p) \to (\mathbf{Z}/(p^2))^\times$ is the homomorphism such that $\psi(1) = 1 + p$.

Let x be an element of G with order p^2 and set $H = \langle x\rangle$. We have $Z \subset H$ by Step 2. Since H is cyclic of order p^2 and $|Z| = p$ by Step 1, $Z = \langle x^p\rangle$.

Claim: There is an element of $G - H$ with order p.

Pick $y \in G - H$. Its order is p or p^2. If its order is p then we're done. Assume y has order p^2. We will find an element of the coset $Hy = \{x^m y : m \in \mathbf{Z}/(p^2)\}$ with order p.

As in Step 3, $H \lhd G$ and G/H has order p, so $\overline{y}^p = \overline{1}$ in G/H. Since y has order p^2, y^p has order p in $H = \langle x\rangle$, so $y^p = (x^p)^r = x^{pr}$ for some $r \in (\mathbf{Z}/(p))^\times$. Since $[G : H] = p$ and $y \notin H$, $G = \langle x, y\rangle$. Summarizing,

$$G = \langle x, y\rangle, \quad H = \langle x\rangle, \quad Z = \langle x^p\rangle, \quad \boxed{y^p = (x^r)^p}.$$

The group G/Z has order p^2, so it is abelian. Thus $\overline{y}\,\overline{x}\,\overline{y}^{-1} = \overline{x}$ in G/Z, which means $yxy^{-1} = xx^{pk} = x^{1+pk}$ in G for some $k \in \mathbf{Z}$. Write this as $yxy^{-1} = x^j$ where $j = 1 + pk$. Check $G = \langle x, y\rangle$, so G being nonabelian means x and y don't commute. Thus $k \not\equiv 0 \bmod p$.

For $m \in \mathbf{Z}$, raise both sides of $yxy^{-1} = x^j$ to the mth power: $yx^m y^{-1} = x^{mj}$. Then

$$(x^m y)^2 = (x^m y)(x^m y) = x^m (yx^m)y = x^m x^{mj} yy = x^{m(1+j)} y^2,$$

and by induction

$$(x^m y)^n = x^{m(1+j+\cdots+j^{n-1})} y^n$$

for all $n \geq 1$. Setting $n = p$, $(x^m y)^p = x^{m(1+j+\cdots+j^{p-1})} y^p$. Since $j = 1 + pk$,

$$1 + j + \cdots + j^{p-1} = \sum_{\ell=0}^{p-1} (1 + pk)^\ell \equiv \sum_{\ell=0}^{p-1} (1 + \ell pk) \equiv p + \frac{p(p+1)}{2} pk \equiv p \bmod p^2,$$

so

$$(x^m y)^p = x^{mp} y^p = x^{mp} x^{rp}.$$

Use $m = -r$: $(x^{-r}y)^p = 1$ and $x^{-r}y \neq 1$ since $y \notin H$, so $x^{-r}y$ has order p in $G - H$. That proves the claim.

Now *rename* y, if needed, so it is an element of order p in $G - H$. Reasoning as above, $G = \langle x, y\rangle$. Since G is nonabelian, x and y don't commute.

Since G/Z is abelian with $Z = \langle x^p\rangle$, as before we can write $yxy^{-1} = x^j$ where $j = 1 + pk$ for some $k \not\equiv 0 \bmod p$. Conjugating by y again,

$$y^2 x y^{-2} = y(yxy^{-1})y^{-1} = yx^j y^{-1} = (yxy^{-1})^j = (x^j)^j = x^{j^2}.$$

Similarly, $y^n x y^{-n} = x^{j^n}$ for all $n \geq 1$. Then $j^n = (1 + pk)^n \equiv 1 + npk \bmod p^2$, so

$$y^n x y^{-n} = x^{1+npk}.$$

Because $k \not\equiv 0 \bmod p$, we can choose $n \geq 1$ so that $nk \equiv 1 \bmod p$. For this n we have $y^n x y^{-n} = x^{1+p}$.

Since $p \nmid n$, $G = \langle x, y\rangle = \langle x, y^n\rangle$. Now *rename* y^n *as* y, so $G = \langle x, y\rangle$ where x has order p^2, y has order p, and $yxy^{-1} = x^{1+p}$. By isomorphisms $H \to (\mathbf{Z}/(p^2))$ where $x^b \mapsto b \bmod p^2$ and $K \to \mathbf{Z}/(p)$ where $y^a \mapsto a \bmod p$, the conjugation action $K \to \mathrm{Aut}(H)$ turns into the homomorphism $\psi\colon \mathbf{Z}/(p) \to (\mathbf{Z}/(p^2))^\times$ where $\psi(1) = 1 + p$, so $G \cong \mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)$.

Step 5: The semidirect products $(\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)$ and $\mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)$ from Steps 3 and 4 are nonisomorphic.

The second semidirect product $\mathbf{Z}/(p^2) \rtimes_\psi \mathbf{Z}/(p)$ has elements with order p^2. Check a converse to Step 3: in $(\mathbf{Z}/(p))^2 \rtimes_\varphi \mathbf{Z}/(p)$ all nonidentity elements have order p. $\square$

9. Complementary subgroups

If a group G contains subgroups H and K such that $G = HK$ and $H \cap K = \{1\}$, then H and K are called *complementary* subgroups.[8] For a normal subgroup $H \lhd G$, is there always a complementary subgroup $K \subset G$? If so, we'd then have $G \cong H \rtimes_\varphi K$

The answer is no!

Example 9.1. Suppose G is a cyclic p-group with $|G| > p$. Every subgroup of G is normal. Pick a subgroup $H \subset G$ with $1 < |H| < |G|$. Suppose $G = HK$, so $|K| > 1$. Then H and K have subgroups of order p by Cauchy's theorem (or check this directly in cyclic p-groups). The cyclic group G has at most one subgroup per size, so the subgroups of order p in H and K are the same, and thus $H \cap K \neq \{1\}$. This contradiction shows G is not a semidirect product of two proper subgroups.

Example 9.2. Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. There is only one subgroup of order 2, namely $\{\pm 1\}$. All subgroups of Q_8 are normal. Pick $H \lhd Q_8$ with $1 < |H| < 8$. If $Q_8 = HK$, then $K \neq \{1\}$ and by the same argument as in the previous example we have $H \cap K \neq \{1\}$. In particular, Q_8 is not a semidirect product of two proper subgroups.

When $G = HK$ with $H \lhd G$ and $H \cap K = \{1\}$ such subgroups K can be far from unique.

Example 9.3. For $n \geq 3$, $S_n = A_n \cdot \{1, \tau\}$ for every transposition τ.

Example 9.4. For $n \geq 3$, $D_n = \langle r \rangle \cdot \{1, r^i s\}$ for every reflection $r^i s$ where $0 \leq i \leq n-1$.

When does a normal subgroup have a complement? We state without proof a sufficient (but far from necessary!) condition for the existence of a complementary subgroup to a normal subgroup of a finite group. We will not be using it here.

Theorem 9.5 (Schur–Zassenhaus)**.** *If $H \lhd G$ and $(|H|, |G/H|) = 1$, then H has a complementary subgroup in G and all complementary subgroups to H in G are conjugate.*

When $(|H|, |G/H|) > 1$, a complementary subgroup to H in G might not exist (*e.g.*, G is a cyclic p-group and $1 < |H| < |G|$) or more than one might exist but they may not be conjugate (*e.g.*, $G = \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ and $H = \langle 3 \rangle$, with complements $\langle 5 \rangle$ or $\langle 7 \rangle$).

If $G = HK$ with $H \lhd G$ and $H \cap K = \{1\}$, then the mapping $G \to K$ given by $hk \mapsto k$ is well-defined and a homomorphism (check!) with image K and kernel H, so $K \cong G/H$: every complementary subgroup to H in G is a subgroup of G that is *isomorphic* to G/H. So as abstract groups, all complementary subgroups of H in G (if there are any complements to H in G at all) have a structure determined by H as a normal subgroup of G.

Example 9.6. Let $G = \mathbf{Z}/(4) = \{0, 1, 2, 3\}$ and $H = \{0, 2\}$. Then H is the unique subgroup of order 2 in G, and $|G/H| = 2$, so there is no complementary subgroup to H in G.

Note when $G = HK$, $H \lhd G$, and $H \cap K = \{1\}$ that K is a group of representatives in G for G/H. The composite $K \hookrightarrow G \to G/H$ fills up the cosets. For $G = \mathbf{Z}/(4)$ and $H = \{0, 2\}$, some representatives in G for G/H are $\{0, 1\}$, $\{2, 1\}$, and $\{0, 3\}$, but there is no *group* of representatives in G for G/H.

For a normal subgroup $H \lhd G$, we will formulate the property of H having a complementary subgroup in G using the notion of a special type of map called a section.

[8] Note that complementary subgroups are *not* complementary as subsets, e.g., in $\mathbf{R}^2$ the subgroups $\mathbf{R} \times \{0\}$ and $\{0\} \times \mathbf{R}$ are complementary but they certainly are not complementary subsets of $\mathbf{R}^2$.

Definition 9.7. For a surjective function $\varphi\colon X \to Y$, a *section* of φ is a choice for each $y \in Y$ of an element $x \in X$ such that $\varphi(x) = y$. Equivalently, it is a function $\psi\colon Y \to X$ such that $\varphi(\psi(y)) = y$ for all $y \in Y$, *i.e.*, $\psi(y)$ is an inverse image of y.

(Do *not* confuse $\varphi(\psi(y)) = y$ for all $y \in Y$ with $\psi(\varphi(x)) = x$ for all $x \in X$; in the second condition, the existence of such ψ forces φ to be injective, but this is not desirable.)

Example 9.8. Let $f\colon \mathbf{R}^\times \to \mathbf{R}_{>0}$ by $f(x) = x^2$. A section of f is a choice for each $y > 0$ of a solution x to $x^2 = y$, *i.e.* it is a square root function. There are two standard sections, $g(y) = \sqrt{y}$ for all $y > 0$ and $g(y) = -\sqrt{y}$ for all $y > 0$. These are the only *continuous* sections of f.

Example 9.9. Let $f\colon \mathbf{C}^\times \to \mathbf{C}^\times$ by $f(z) = z^2$. One section of f is $g(re^{i\theta}) = \sqrt{r}e^{i\theta/2}$, $0 \leqslant \theta < 2\pi$, but g is not continuous on $(0, \infty)$. (Consider $\theta \to 0^+$ and $\theta \to 2\pi^-$ for fixed $r > 0$.) It is a theorem that *no* continuous section exists: there is no choice of square roots in $\mathbf{C}^\times$ that is continuous everywhere. This creates problems in complex analysis.

Example 9.10. Consider the 2-sphere S^2. Let T_p be the tangent plane at the point $p \in S^2$. Then there is a natural map

$$\bigcup_{p \in S^2} T_p \longrightarrow S^2$$

defined by $\mathbf{v} \mapsto p$, where p is the point at which $\mathbf{v}$ is tangent to S^2. A section to this map is a *vector field* on S^2. In practice, we care about vector fields that vary nicely from point to point (continuously or smoothly, say) which can be reformulated as saying the section to $\bigcup_{p \in S^2} T_p \to S^2$ is nice (continuous or smooth) when we give $\bigcup T_p$ a suitable topology. This shows that sections occur naturally in geometry.

Theorem 9.11. *If $H \lhd G$, then the following are equivalent:*

1. *H has a complement in G; i.e., for a subgroup K of G, $G = HK$ and $H \cap K = \{1\}$.*
2. *G/H has coset representatives in G that form a subgroup of G.*
3. *The reduction homomorphism $\pi\colon G \to G/H$, where $\pi(g) = \overline{g}$, has a section that is a homomorphism.*

Proof. (1) $\Rightarrow$ (2). The set K is a group of coset representatives for G/H: $hk \equiv k \bmod H$, and $k_1 \equiv k_2 \bmod H$ implies that $k_1 = k_2$ since $H \cap K = \{1\}$.

(2) $\Rightarrow$ (1). Let K be a group of coset representatives for G/H in G. For each $g \in G$, $\overline{g} = \overline{k}$ in G/H for some $k \in K$. Then $g = h \cdot k$ for some $h \in H$. This implies that $G = HK$. To show $H \cap K = \{1\}$, suppose that in G, $hk = 1$ for an $h \in H$ and $k \in K$. Then in G/H, $\overline{k} = \overline{1}$, and $1 \in K$, so $k = 1$ by the definition of coset representatives, which implies that $h = 1$ too.

(1) $\Rightarrow$ (3). By (1), $G = HK$. We seek a homomorphism $s\colon G/H \to G$ such that $\pi(s(\overline{g})) = \overline{g}$ for each $g \in G$. Write $g = hk$, so $\overline{g} = \overline{k}$. Define $s(\overline{g}) = k$. This is well-defined since the representation of g as hk is unique, and by definition $\pi(s(\overline{g})) = \overline{k} = \overline{g}$, so s is a section to π. For $k \in K$, $s(\overline{k}) = k$. Then $s(\overline{k_1}\overline{k_2}) = s(\overline{k_1 k_2}) = k_1 k_2 = s(\overline{k_1})s(\overline{k_2})$, so s is a group homomorphism.

(3) $\Rightarrow$ (1) We're given a homomorphism $s\colon G/H \to G$ such that $\pi(s(\overline{g})) = \overline{g}$ for all $\overline{g} \in G/H$. If (1) were true then each $\overline{g} \in G/H$ would have a unique representative from K because (1) $\Rightarrow$ (2). So one section $G/H \to G$ to π would be $\overline{g} \mapsto k \in K$ where $\overline{k} = \overline{g}$. With this in mind, define $K = s(G/H)$, which is a subgroup of G. For each $g \in G$, in G/H

$$\overline{g} = \pi(s(\overline{g})).$$

Set $k = s(\overline{g})$, so $\overline{g} = \pi(k) = \overline{k}$ in G/H. Hence $g = hk$ for some $h \in H$, so $G = HK$.

To show $H \cap K = \{1\}$, suppose $k \in K \cap H$. Since $k \in K$, $k = s(\overline{g})$ for some $g \in G$. Since $k \in H$, $\pi(k) = \overline{e}$. Also

$$\pi(k) = \pi(s(\overline{g})) = \overline{g},$$

so $\overline{g} = \overline{e}$. Thus

$$k = s(\overline{g}) = s(\overline{e}) = e$$

since $s\colon G/H \to G$ is a homomorphism. □

Example 9.12. Let $G = \mathrm{GL}_2(\mathbf{R})$ and $H = \mathrm{SL}_2(\mathbf{R})$. Note that

$$H = \ker(\mathrm{GL}_2(\mathbf{R}) \xrightarrow{\det} \mathbf{R}^\times),$$

so $G/H \cong \mathbf{R}^\times$. Is there a section to $G \xrightarrow{\pi} G/H$?

$$\mathrm{GL}_2(\mathbf{R}) \longrightarrow \mathrm{GL}_2(\mathbf{R})/\mathrm{SL}_2(\mathbf{R}) \cong \mathbf{R}^\times \quad (s \text{ over the arrow})$$

That is, can we find a homomorphism $s\colon \mathbf{R}^\times \to \mathrm{GL}_2(\mathbf{R})$ such that $\det(s(c)) = c$ for all $c \in \mathbf{R}^\times$? Yes, let $s(c) = \left(\begin{smallmatrix} c & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (or let $s(c) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & c \end{smallmatrix}\right)$). This is related to the fact that

$$\mathrm{GL}_2(\mathbf{R}) = \mathrm{SL}_2(\mathbf{R}) \cdot \left\{ \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

by

$$A = \left(A \cdot \begin{pmatrix} 1/d & 0 \\ 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix},$$

where $d = \det A$.

For a group G, let $H = Z(G) = Z$. Does the center Z have a complementary subgroup? That is, does $G = ZK$ where $Z \cap K = \{1\}$? If so, then $K \cong G/Z$ and since elements of Z commute with all elements of G, we get

$$G = ZK \cong Z \times K \cong Z \times (G/Z).$$

Conversely, if $G \cong Z \times G/Z$ (any isomorphism at all) then Z has a complementary subgroup in G. So the center Z of G has a complementary subgroup in G if and only if $G \cong Z \times (G/Z)$.

Example 9.13. Let $G = Q_8$ so $Z = \{\pm 1\}$ and $G/Z \cong (\mathbf{Z}/(2))^2$. Then $Z \times (G/Z)$ is abelian, but Q_8 is not, so Z has no complementary subgroup in Q_8. This is consistent with what we saw in Example 9.2: Q_8 is not a semidirect product of nontrivial groups.

Example 9.14. Let $G = \mathrm{GL}_2(\mathbf{R})$, so

$$Z = \left\{ \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} : c \in \mathbf{R}^\times \right\} = \mathbf{R}^\times I_2.$$

The center $\mathbf{R}^\times I_2$ has a complementary subgroup in $\mathrm{GL}_2(\mathbf{R})$ if and only if

$$\mathrm{GL}_2(\mathbf{R}) \cong (\mathbf{R}^\times I_2) \times \mathrm{PGL}_2(\mathbf{R}). \tag{9.1}$$

If the groups in both sides of (9.1) were isomorphic then their commutator subgroups would be isomorphic, but it can be shown that the commutator subgroups are not isomorphic. Therefore the center of $\mathrm{GL}_2(\mathbf{R})$ does not have a complementary subgroup in $\mathrm{GL}_2(\mathbf{R})$.

Example 9.15. Let $G = D_n = \langle r, s\rangle$ for even $n \geq 6$. Then $Z = \{1, r^{n/2}\}$. When $n/2$ is odd, the subgroup $K = \langle r^2, s\rangle$ of D_n has order n and trivial intersection with Z, so $D_n = ZK \cong Z \times K \cong \mathbf{Z}/(2) \times D_{n/2}$. When $n/2$ is even, $D_n \ncong \mathbf{Z}/(2) \times D_{n/2}$ since D_n has a center of order 2 and $\mathbf{Z}/(2) \times D_{n/2}$ has a center of order 4.

For all even $n \geq 6$, $\langle r^2, s\rangle$ and $\langle rs\rangle$ are complementary subgroups, so $D_n = \langle r^2, s\rangle\langle rs\rangle \cong D_{n/2} \rtimes \mathbf{Z}/(2)$.

10. Semidirect products of isomorphic groups

The construction of a direct product, and more generally a semidirect product, behaves as well as could be hoped under isomorphisms.

Theorem 10.1. *Let $f\colon H_1 \to H_2$ and $f'\colon K_1 \to K_2$ be group isomorphisms. Then the mapping $F\colon H_1 \times K_1 \cong H_2 \times K_2$ given by $F(h,k) = (f(h), f'(k))$ is a group isomorphism.*

Proof. Since f and f' are bijections, so is F. To check F is a homomorphism,

$$\begin{aligned} F((h,k)(h',k')) &= F(hh', kk') \\ &= (f(hh'), f'(kk')) \\ &= (f(h)f(h'), f'(k)f'(k')) \\ &= (f(h), f(k))(f'(h'), f'(k')) \\ &= F(h,k)F(h',k'). \end{aligned}$$

□

Theorem 10.2. *Let $f\colon H_1 \to H_2$ and $f'\colon K_1 \to K_2$ be isomorphisms. For each homomorphism $\varphi\colon K_1 \to \mathrm{Aut}(H_1)$ there is a corresponding homomorphism $\varphi'\colon K_2 \to \mathrm{Aut}(H_2)$ such that $H_1 \rtimes_\varphi K_1 \cong H_2 \rtimes_{\varphi'} K_2$.*

Proof. The isomorphism $f\colon H_1 \to H_2$ can turn each automorphism ψ of H_1 into an automorphism of H_2 by filling in the right arrow of the diagram below so that it commutes.

$$\begin{array}{ccc} H_1 & \xrightarrow{f} & H_2 \\ {\scriptstyle\psi}\downarrow & & \vdots\,{\scriptstyle ?} \\ H_1 & \xrightarrow{f} & H_2 \end{array}$$

The long way around from H_2 to H_2 is the mapping $f \circ \psi \circ f^{-1}$, which we can put on the right side. Define $c_f\colon \mathrm{Aut}(H_1) \to \mathrm{Aut}(H_2)$ by $c_f(\psi) = f \circ \psi \circ f^{-1}$ and check this is a group isomorphism (its inverse is the same type of formula with f replaced by f^{-1}). Using c_f and the given isomorphism $f'\colon K_1 \to K_2$, each action $\varphi\colon K_1 \to \mathrm{Aut}(H_1)$ becomes an action $\varphi'\colon K_2 \to \mathrm{Aut}(H_2)$ by making the diagram below commute: set $\varphi' := c_f \circ \varphi \circ (f')^{-1}$.

$$\begin{array}{ccc} K_1 & \xrightarrow{\varphi} & \mathrm{Aut}(H_1) \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle c_f} \\ K_2 & \xrightarrow{\varphi'} & \mathrm{Aut}(H_2) \end{array}$$

The mapping φ' is a homomorphism since $(f')^{-1}$, φ, and c_f all are. (If φ is trivial then φ' is trivial and we are in the case of Theorem 10.1.) For each $k \in K_2$, $\varphi'_k = c_f(\varphi_{(f')^{-1}(k)})$.

Let $F\colon H_1 \rtimes_\varphi K_1 \to H_2 \rtimes_{\varphi'} K_2$ by $F(h,k) = (f(h), f'(k))$. This is a bijection since f and f' are bijections. To show F is a homomorphism,

$$\begin{aligned} F((h,k)(h',k')) &= F(h\varphi_k(h'), kk') \\ &= (f(h\varphi_k(h')), f'(kk')) \\ &= (f(h)f(\varphi_k(h')), f'(k)f'(k')) \end{aligned}$$

and

$$\begin{aligned} F(h,k)F(h',k') &= (f(h), f'(k))(f(h'), f'(k')) \\ &= (f(h)\varphi'_{f'(k)}(f(h')), f'(k)f'(k')), \end{aligned}$$

so we need to show $f(\varphi_k(h')) = \varphi'_{f'(k)}(f(h'))$. Using the definition of φ',

$$\varphi'_{f'(k)} = c_f(\varphi_{(f')^{-1}(f'(k))}) = c_f(\varphi_k) = f \circ \varphi_k \circ f^{-1},$$

so

$$\varphi'_{f'(k)}(f(h')) = (f \circ \varphi_k \circ f^{-1})(f(h')) = f(\varphi_k(h')). \qquad \square$$