

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 . 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.

There is a construction using groups H and K that is more subtle 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: $(h, 1) = (1, k) \implies h = 1, k = 1$,
- 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 $H \times K \rightarrow G$ by $(h, k) \mapsto hk$ is an isomorphism. Also $G/H \cong K$ and $G/K \cong H$.

Proof. Let $f: H \times K \rightarrow G$ 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, 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 $k = 1$. By (1), f is surjective

The homomorphisms $G \rightarrow H \times K \rightarrow H$ and $G \rightarrow H \times K \rightarrow K$, where $hk \mapsto (h, k) \mapsto h$ and $hk \mapsto (h, k) \mapsto k$, have respective kernels K and H , so H and K are normal in G with $G/K \cong H$ and $G/H \cong K$. \square

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 $G = \text{Aff}(\mathbf{R})$, let

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

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 $G \not\cong H \times K$ since $H \times K$ is abelian (H and K are abelian) while G is nonabelian.

Example 2.3. In $G = \text{GL}_2(\mathbf{R})$, let $H = \text{SL}_2(\mathbf{R})$ and $K = \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x \in \mathbf{R}^\times \right\}$. 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 $\text{GL}_2(\mathbf{R}) = HK$, and easily $H \cap K = \{I_2\}$. It turns out that $\text{GL}_2(\mathbf{R}) \not\cong \text{SL}_2(\mathbf{R}) \times \mathbf{R}^\times$. For example, $\text{GL}_2(\mathbf{R})$ has infinitely many elements of order 2, such as reflections across any line in \mathbf{R}^2 through the origin, but $\text{SL}_2(\mathbf{R})$ has just one element of order 2 ($-I_2$; check it is the only one!) and \mathbf{R}^\times obviously does as well, so $\text{SL}_2(\mathbf{R}) \times \mathbf{R}^\times$ 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, $S_n \not\cong H \times K \cong A_n \times \mathbf{Z}/(2)$ for $n \geq 3$ 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 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 $S_4 \not\cong H \times K \cong D_4 \times \mathbf{Z}/(3)$ 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, $H \triangleleft G$. 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 $H \triangleleft G$, for instance,

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

since $kh'h'k^{-1} \in H$ 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 $kh'h'k^{-1}$, 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 $\varphi: K \rightarrow \text{Aut}(H)$. Write the automorphism on H associated to k as φ_k , so $\varphi_k: H \rightarrow H$ 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 $\text{Aut}(H)$ means

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

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

$$(3.2) \quad \varphi_k^{-1} = \varphi_{k^{-1}}.$$

That is, the inverse of $\varphi_k \in \text{Aut}(H)$ 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 $|\text{Aut}(H)|$ 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 $\varphi: K \rightarrow \text{Aut}(H)$ 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 $kh'h'k^{-1}$, 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 \triangleleft : think of the slanted lines in the small \triangleleft 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 $K \rtimes_{\varphi} H$ 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 $\varphi_1 = \text{id}_H$ 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 automorphism $\varphi_k^{-1} = \varphi_{k^{-1}}$ (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

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

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 $\varphi: K \rightarrow \text{Aut}(H)$ is the trivial homomorphism, so $\varphi_k = \text{id}_H$ 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 $\varphi: \mathbf{R}^{\times} \rightarrow \text{Aut}(\mathbf{R})$ where $\varphi_x: \mathbf{R} \rightarrow \mathbf{R}$ 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

$$(3.4) \quad (a, b)(a', b') = (a + \varphi_b(a'), bb') = (a + ba', bb').$$

This resembles the multiplication in $\text{Aff}(\mathbf{R})$, where $\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} bb' & ba'+a \\ 0 & 1 \end{pmatrix}$. 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 $(a, b) \in \mathbf{R} \rtimes_{\varphi} \mathbf{R}^{\times}$ into $\begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}: \mathbf{R} \rtimes_{\varphi} \mathbf{R}^{\times} \cong \text{Aff}(\mathbf{R})$ by $(a, b) \mapsto \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}$.

In the group $\text{Aff}(\mathbf{R})$ 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 $\text{Aut}(\mathbf{Z}/(m)) \cong (\mathbf{Z}/(m))^{\times}$ since automorphisms of the additive group $\mathbf{Z}/(m)$ are the mappings $\varphi_a: x \bmod m \mapsto ax \bmod m$ for $a \in (\mathbf{Z}/(m))^{\times}$. Let $\varphi: (\mathbf{Z}/(m))^{\times} \rightarrow \text{Aut}(\mathbf{Z}/(m))$ by making $\varphi_a: \mathbf{Z}/(m) \rightarrow \mathbf{Z}/(m)$ 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 $\text{Aff}(\mathbf{Z}/(m))$ by $(a, b) \bmod m \mapsto \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} \bmod m$.

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 $\mathbf{Z} \rightarrow \{\pm 1\}$ 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 $\varphi: K \rightarrow \text{Aut}(H)$ 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 :

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

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 $\varphi: K \rightarrow \text{Aut}(H)$ is trivial on K : $\varphi_k = \text{id}_H$ 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:

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

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 $\varphi: K \rightarrow \text{Aut}(H)$ 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 $k \in K$,

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

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 $\varphi: H \rightarrow \text{Aut}(K)$ is trivial. \square

Thus $H \rtimes_{\varphi} K$ is nonabelian whenever φ is not trivial. Even if H and K are both abelian, if $\varphi: K \rightarrow \text{Aut}(H)$ is nontrivial then the group $H \rtimes_{\varphi} K$ is nonabelian!

Example 3.8. Let $H = \mathbf{R}$, $K = \mathbf{R}^{\times}$, and $\varphi: \mathbf{R}^{\times} \rightarrow \mathbf{R}$ by $\varphi_x(y) = xy$. We saw in Example 3.4 that $\text{Aff}(\mathbf{R}) \cong \mathbf{R} \rtimes_{\varphi} \mathbf{R}^{\times}$ by $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \mapsto (y, x)$.

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 $xyx^{-1} = x^{-1}$. (Check as an exercise that if a group contains elements x and y such that $xyx^{-1} = x^{-1}$, then $yx^m y^{-1} = x^{-m}$ for all $m \in \mathbf{Z}$, so $y^n x^m y^{-n} = x^{(-1)^n m}$ for all $n \in \mathbf{Z}$.)

Example 3.10. Let H be an abelian group written *additively*, so negation $\text{neg}: h \mapsto -h$ is an automorphism of order 2. Let $\varphi: \mathbf{Z}/(2) \rightarrow \text{Aut}(H)$ by $\varphi_0 = \text{id}_H$ 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 $\mathbf{Z}/(m) \rightarrow G$ by $a \bmod m \mapsto g^a$, and here we're using the special case $G = \text{Aut}(H)$ and g is inversion on H). The group $H \rtimes_{\varphi} \mathbf{Z}/(2)$ has operation

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

Then

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

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

$$(3.7) \quad (j, k)(j', k') = (j + (-1)^k j', k + k').$$

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 $(j, k) \mapsto r^j s^k$. In particular, $(1, 0) \mapsto r$ and $(0, 1) \mapsto s$. For example, (3.7) says $(0, 1)(1, 0) = (-1, 1) = (-1, 0)(0, 1)$, which matches the dihedral relation $sr = r^{-1}s$. (The general multiplication 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 $\varphi: K \rightarrow \text{Aut}(H)$ is trivial, which makes $H \rtimes_{\varphi} K = H \times K$.*

Proof. Since $H \rtimes_{\varphi} K$ 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. \square

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: $(h, 1) = (1, k) \implies h = 1, k = 1$,
- 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) $H \triangleleft G$.

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

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 $f: H \rtimes_{\varphi} K \rightarrow G$ 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, we calculate

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

The map $G \rightarrow H \rtimes_{\varphi} K \rightarrow K$ where $hk \mapsto (h, k) \mapsto k$ is a homomorphism with kernel H , so $G/H \cong K$. \square

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 $D_n \cong \langle \tau \rangle \rtimes \{1, s\}$ and $\text{SL}_2(\mathbf{Z}/(3)) \cong P \rtimes \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$ where P is the (normal) 2-Sylow subgroup. Lastly, $\text{GL}_2(\mathbf{R}) \cong \text{SL}_2(\mathbf{R}) \rtimes K$ where K is the set of diagonal matrices, $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ for $a \in \mathbf{R}^{\times}$. We met this decomposition for $\text{GL}_2(\mathbf{R})$ earlier in Example 2.3.

Internally within a semidirect product group $H \rtimes K$, K always acts on H by conjugations: $(\varphi_k(h), 1) = (1, k)(h, 1)(1, k)^{-1}$. Externally, if we create a semi-direct product from scratch using 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 $\mathrm{diag}(a, 1, 1, \dots, 1)$ for $a \in \mathbf{R}^\times$, so $K \cong \mathbf{R}^\times$. Then $G = HK$ with $H \triangleleft G$ 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 $\mathrm{SL}_n(\mathbf{R}) \rtimes H \cong \mathrm{SL}_n(\mathbf{R}) \rtimes \mathbf{R}^\times$.

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 semidirect products:

- (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 $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ (not with the matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$);

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 $\varphi: K \rightarrow \text{Aut}(H)$ 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 $(|K|, |\text{Aut}(H)|) = 1$ 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: $\text{Aut}(\mathbf{Z}/(5)) = (\mathbf{Z}/(5))^{\times}$ 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 $\text{Aut}(\mathbf{Z}/(25)) = (\mathbf{Z}/(25))^{\times}$ has size 20 and $(20, 15) \neq 1$, there might be examples. We seek a homomorphism

$$\varphi: \mathbf{Z}/(15) \rightarrow (\mathbf{Z}/(25))^{\times}$$

that is nontrivial. It is necessary that $\varphi(1)$ goes¹ to a g such that $g^{15} = 1$. If $g^{15} \equiv 1 \pmod{25}$, then $g^{15} \equiv 1 \pmod{5}$, so (by testing mod 5) $g \equiv 1 \pmod{5}$. Then

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

Choose $g = 6$. Check $6^{15} \equiv 1 \pmod{25}$ (in fact, if $a \equiv 1 \pmod{5}$ then $a^5 \equiv 1 \pmod{25}$, so $a^{15} \equiv 1 \pmod{25}$). Let $\varphi: \mathbf{Z}/(15) \rightarrow (\mathbf{Z}/(25))^{\times}$ by $\varphi(1) = 6$, so $\varphi(k \pmod{15}) = 6^k \pmod{25}$ (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 nonabelian group of order $15 \cdot 25 = 375$ is built from cyclic groups of order 15 and 25.

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

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

there is one nontrivial $\varphi: \mathbf{Z}/(2) \rightarrow \text{Aut}(\mathbf{Z}/(4))$, namely the one where $\varphi(k \pmod{2}) = \{x \mapsto (-1)^k x\}$. 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

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

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

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 $\varphi: \mathbf{Z}/(2) \rightarrow \text{Aut}(H)$ by $\varphi_k = f^k$, i.e.,

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

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

The case where H is abelian and $f: H \rightarrow H$ is inversion on H is in Example 3.10. A nonabelian example 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 $\varphi: \mathbf{Z}/(2) \rightarrow \mathrm{Aut}(\mathbf{Z}/(8))$. 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:

$$(5.1) \quad (a, b)(c, d) = (a + c, b + d),$$

$$(5.2) \quad (a, b)(c, d) = (a + 3^b c, b + d),$$

$$(5.3) \quad (a, b)(c, d) = (a + 5^b c, b + d),$$

$$(5.3) \quad (a, b)(c, d) = (a + 7^b c, b + d).$$

Just because formulas for two group laws look different does not mean the groups are nonisomorphic, although it turns out these four groups of order 16 are nonisomorphic. 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 $a(1 + 3^b) \equiv 0 \pmod{8}$. 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 $4a \equiv 0 \pmod{8}$, 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 $a(1 + 5^b) \equiv 0 \pmod{8}$. 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 $6a \equiv 0 \pmod{8}$, so $2a \equiv 0 \pmod{8}$. 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 $2 + 8 = 10$.

A description of all groups of order 16 up to isomorphism can be read at <https://kconrad.math.uconn.edu/blurbs/grouptheory/group16.pdf>.

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 $q \equiv 1 \pmod{p}$.

Theorem 6.1. *If primes $p < q$ satisfy $q \not\equiv 1 \pmod{p}$ 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 $n_p \equiv 1 \pmod{p}$ with $n_p \mid q$, and $n_q \equiv 1 \pmod{q}$ 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 $p \equiv 1 \pmod q$. Thus $n_q = 1$, so $Q \triangleleft G$. For the p -Sylow subgroups, $n_p = 1$ or q .

Since $q \not\equiv 1 \pmod p$, we must have $n_p = 1$, so $P \triangleleft G$. 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. \square

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

$$\begin{array}{ccc} K & \xrightarrow{f} & K & \xrightarrow{\varphi} & \text{Aut}(H) \\ & & \searrow & \nearrow & \\ & & & \varphi \circ f & \end{array}$$

Proof. Exercise. \square

Theorem 6.3. *If primes $p < q$ satisfy $q \equiv 1 \pmod p$ 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 $q \pmod p$. Thus $Q \triangleleft G$.

For the p -Sylow count, $n_p \equiv 1 \pmod p$ and $n_p \mid q$, so $n_p = 1$ or $n_p = q$. Both choices are consistent with the congruence condition $n_p \equiv 1 \pmod p$, 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 normal). Since $Q \triangleleft G$ 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 $\varphi: P \rightarrow \text{Aut}(Q)$ 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 12.2 below), so we may suppose $P = \mathbf{Z}/(p)$ and $Q = \mathbf{Z}/(q)$. Then every noncyclic group of order pq when $q \equiv 1 \pmod p$ is $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(p)$ for a nontrivial homomorphism

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

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 $\varphi: \mathbf{Z}/(p) \rightarrow \text{Aut}(\mathbf{Z}/(q)) \cong (\mathbf{Z}/(q))^{\times}$ are determined by where they send the generator 1, which has to go to a solution in $(\mathbf{Z}/(q))^{\times}$ to $z^p \equiv 1 \pmod q$, 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, $q \equiv 1 \pmod p$), there are elements of order p in $(\mathbf{Z}/(q))^{\times}$ by Cauchy's theorem. For each solution of $z^p \equiv 1 \pmod q$ with $z \not\equiv 1 \pmod p$, we get a semidirect product

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

by

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

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

The set $\{z \in (\mathbf{Z}/(q))^\times : z^p \equiv 1 \pmod{q}\}$ 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 p th power 1. For all prime q , the group $(\mathbf{Z}/(q))^\times$ is cyclic, so it has only *one* subgroup of order p . Thus $\{z \in (\mathbf{Z}/(q))^\times : z^p \equiv 1 \pmod{q}\}$ 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 $\varphi_1, \varphi_2: \mathbf{Z}/(p) \rightarrow (\mathbf{Z}/(q))^\times$ 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 $f: \mathbf{Z}/(p) \rightarrow \mathbf{Z}/(p)$ 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 $q \equiv 1 \pmod{p}$, there are (up to isomorphism) two groups of order pq . \square

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

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

Example 6.4. Taking $p = 2$, primes $q > 2$ satisfy $q \equiv 1 \pmod{p}$, so there are two groups of order $2q$ up to isomorphism, one being cyclic and the other nonabelian. We can directly write down a nonabelian example: the dihedral group D_q . The proof above produces the nonabelian group as $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(2)$ where $\varphi: \mathbf{Z}/(2) \rightarrow \text{Aut}(\mathbf{Z}/(q)) = (\mathbf{Z}/(q))^\times$ by $\varphi(1 \pmod{2}) = -1$ in $(\mathbf{Z}/(q))^\times$, which gives $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(2)$ the group structure $(a, b)(c, d) = (a + (-1)^b c, b + d)$. An isomorphism $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(2) \rightarrow D_q$ is $(a, b) \mapsto r^a s^b$ where r and s are the usual generators of D_q with orders q and 2 , which we saw more generally in Example 3.10 with D_n .

Remark 6.5. The classification of groups of order pq up to isomorphism (one group when $q \not\equiv 1 \pmod{p}$ and two groups when $q \equiv 1 \pmod{p}$) 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 $4q$

When p and q are distinct primes, all groups of order p^2q can be classified using semidirect products. The general case is complicated, so we will focus here on order $4q$ where $q > 2$.

Theorem 7.1. *Let q be an odd prime.*

- (1) *If $q \equiv 1 \pmod{4}$, then there are five groups of order $4q$ up to isomorphism: two are abelian and three are nonabelian.*
- (2) *If $q \equiv 3 \pmod{4}$ and $q > 3$, then there are four groups of order $4q$ up to isomorphism: two are abelian and two are nonabelian.*

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

Proof. Let G be a group of order $4q$. Call a 2-Sylow subgroup K and a q -Sylow subgroup N . We will show $N \triangleleft G$ and then deduce that $G \cong N \rtimes_{\varphi} K$, where $\varphi : K \rightarrow \text{Aut}(N)$ is the conjugation action of K on N .

Let n_q be the number of q -Sylow subgroups in G . By the Sylow theorems, $n_q \mid 4$ and $n_q \equiv 1 \pmod{q}$. If $n_q > 1$ then $n_q = 2$ or $n_q = 4$. If $n_q = 2$ then $2 \equiv 1 \pmod{q}$, which is impossible. If $n_q = 4$ then $4 \equiv 1 \pmod{q}$, so $q = 3$. When $q \neq 3$, we get $n_q = 1$, so $N \triangleleft G$.

Let K be a 2-Sylow subgroup. Since $N \triangleleft G$, NK is a subgroup of G and $|NK| = |N||K| = 4q$ since $|N|$ and $|K|$ are relatively prime. Thus $G = NK$, so by Theorem 4.1 $G \cong N \rtimes_{\varphi} K$ where the homomorphism $\varphi : K \rightarrow \text{Aut}(N)$ is the conjugation action of K on N .

Since $|N| = q$, $N \cong \mathbf{Z}/(q)$ and $\text{Aut}(N) \cong (\mathbf{Z}/(q))^{\times}$. Since $|K| = 4$, K is isomorphic to $\mathbf{Z}/(4)$ or $(\mathbf{Z}/(2))^2$. To describe each φ we will determine all homomorphisms $\varphi : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ and $\varphi : (\mathbf{Z}/(2))^2 \rightarrow (\mathbf{Z}/(q))^{\times}$ and decide how many nonisomorphic groups

$$(7.1) \quad \mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(4) \quad \text{and} \quad \mathbf{Z}/(q) \rtimes_{\varphi} (\mathbf{Z}/(2))^2$$

are obtained in these ways.

Case 1: $K \cong \mathbf{Z}/(4)$.

A homomorphism $\varphi : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ is determined by where 1 mod 4 goes, which has to be an element of $(\mathbf{Z}/(q))^{\times}$ with order 1, 2, or 4. The only element of order 2 in $(\mathbf{Z}/(q))^{\times}$ is -1 , and there is an element of order 4 only when $4 \mid (q-1)$, so $q \equiv 1 \pmod{4}$. Thus when $q \equiv 3 \pmod{4}$ (and $q > 3$) this last option does not occur. When $q \equiv 1 \pmod{4}$, the congruence $x^2 \equiv -1 \pmod{q}$ has two solutions, which are the two elements of order 4 in $(\mathbf{Z}/(q))^{\times}$ and they are inverses (compare with $-i = 1/i$ in \mathbf{C}).

When $\varphi(1) = 1$, φ is trivial and the first semidirect product in (7.1) is $\mathbf{Z}/(q) \times \mathbf{Z}/(4)$, which is abelian and in fact cyclic.

When $\varphi(1) = -1$, $\varphi(b \pmod{4}) = (-1)^b$, so the first semidirect product in (7.1) is

$$(7.2) \quad (a, b)(c, d) = (a + (-1)^b c, b + d),$$

which is nonabelian since $(1, 0)(0, 1) = (1, 1)$ and $(0, 1)(1, 0) = (-1, 1) = (3, 1) \neq (1, 1)$.

When $\varphi(1)$ has order 4 in $(\mathbf{Z}/(q))^{\times}$, which occurs only when $q \equiv 1 \pmod{4}$, set $z := \varphi(1)$. Then $\varphi(b \pmod{4}) = z^b$ and the first semidirect product in (7.1) is

$$(7.3) \quad (a, b)(c, d) = (a + z^b c, b + d).$$

The only other element of order 4 in $(\mathbf{Z}/(q))^{\times}$ is $w = z^{-1}$. Since $w^b = z^{-b}$, the homomorphism $\psi : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ where $\psi(b \pmod{4}) = w^b$ is the composition of $b \mapsto z^b$ with inversion on $\mathbf{Z}/(4)$, which makes $\mathbf{Z}/(q) \rtimes_{\psi} \mathbf{Z}/(4) \cong \mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(4)$ by Lemma 6.2. So up to isomorphism there is only one semidirect product $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(4)$ where $\varphi : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ has an image of order 4 and this occurs if and only if $q \equiv 1 \pmod{4}$.

Check $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(4)$ where $\varphi(1)$ has order 2 has only one element of order 2 (the element $(0, 2)$), while $\mathbf{Z}/(q) \rtimes_{\varphi} \mathbf{Z}/(4)$ where $\varphi(1)$ has order 4 has q elements of order 2 (all $(a, 2)$). That makes these groups non-isomorphic when they both occur.

Thus the number of groups of order $4q$ up to isomorphism in Case 1 is 2 when $q \equiv 3 \pmod{4}$ (1 abelian and 1 non-abelian, as given by (7.2)) and is 3 when $q \equiv 1 \pmod{4}$ (1 abelian and 2 non-abelian, as given by (7.2) and (7.3)).

Case 2: $K \cong (\mathbf{Z}/(2))^2$.

A homomorphism $\varphi : (\mathbf{Z}/(2))^2 \rightarrow (\mathbf{Z}/(q))^{\times}$ is determined by where $(1, 0)$ and $(0, 1)$ are sent, which have to be to elements of $(\mathbf{Z}/(q))^{\times}$ with order 1 or 2, namely $\pm 1 \pmod{q}$.

When $\varphi(1, 0) = 1$ and $\varphi(0, 1) = 1$, φ is trivial and the second semidirect product in (7.1) is $\mathbf{Z}/(q) \times (\mathbf{Z}/(2))^2$, which is abelian and not cyclic.

When $\varphi(1,0) = -1$ and $\varphi(0,1) = -1$, the second semidirect product in (7.1) is

$$(7.4) \quad (a, (b, b'))(c, (d, d')) = (a + (-1)^{b+b'}c, (b + d, b' + d')),$$

which is nonabelian.

When $\varphi(1,0) = -1$ and $\varphi(0,1) = 1$, $\varphi(1,1) = \varphi(1,0)\varphi(0,1) = -1$. There is an automorphism f of $(\mathbf{Z}/(2))^2$ that fixes $(1,0)$ and exchanges $(0,1)$ and $(1,1)$, namely the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/(2))$. That makes $\mathbf{Z}/(q) \times_{\varphi} (\mathbf{Z}/(2))^2 \cong \mathbf{Z}/(q) \rtimes_{\varphi \circ f} (\mathbf{Z}/(2))^2$ by Lemma 6.2, and the semi-direct product on the right is (7.4).

When $\varphi(1,0) = 1$ and $\varphi(0,1) = -1$, $\varphi(1,1) = \varphi(1,0)\varphi(0,1) = -1$. The automorphism $g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ of $(\mathbf{Z}/(2))^2$ fixes $(0,1)$ and exchanges $(1,0)$ and $(1,1)$, which makes $\mathbf{Z}/(q) \times_{\varphi} (\mathbf{Z}/(2))^2 \cong \mathbf{Z}/(q) \rtimes_{\varphi \circ g} (\mathbf{Z}/(2))^2$ and the semi-direct product on the right is (7.4).

Therefore the number of groups of order $4q$ up to isomorphism in Case 2 is 2 (1 abelian and 1 non-abelian, as given by (7.4)).

Combining the cases, the number of groups of order $4q$ up to isomorphism when $q \neq 3$ is 4 when $q \equiv 3 \pmod{4}$ (2 abelian and 2 non-abelian) and 5 when $q \equiv 1 \pmod{4}$ (2 abelian and 3 non-abelian). Explicitly, there are 4 non-isomorphic constructions for all primes $q > 3$ and one extra construction when $q \equiv 1 \pmod{4}$. The constructions that work in all cases are the two abelian groups $\mathbf{Z}/(q) \times \mathbf{Z}/(4)$ and $\mathbf{Z}/(q) \times (\mathbf{Z}/(2))^2$ and the two nonabelian groups $\mathbf{Z}/(q) \rtimes_{\varphi_1} \mathbf{Z}/(4)$ and $\mathbf{Z}/(q) \rtimes_{\varphi_2} (\mathbf{Z}/(2))^2$ where $\varphi_1 : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ by $\varphi_1(b \pmod{4}) = (-1)^b$ (the group in (7.2)) and $\varphi_2 : (\mathbf{Z}/(2))^2 \rightarrow (\mathbf{Z}/(q))^{\times}$ by $\varphi_2(b, b') = (-1)^{b+b'}$ (the group in (7.4)). When $q \equiv 1 \pmod{4}$ there is an extra nonabelian group $\mathbf{Z}/(q) \rtimes_{\varphi_3} \mathbf{Z}/(4)$ where $\varphi_3 : \mathbf{Z}/(4) \rightarrow (\mathbf{Z}/(q))^{\times}$ by $\varphi_3(b \pmod{4}) = z^b$ with $z \pmod{q}$ being either solution to $z^2 \equiv -1 \pmod{q}$ (the group in (7.3)). \square

The omitted case $q = 3$ is different from order $4q$ when $q \equiv 3 \pmod{4}$ and $q > 3$: there are 5 groups of order 12, not 4 groups. In the extra one (A_4) the 3-Sylow subgroup is not normal. See <https://kconrad.math.uconn.edu/blurbs/grouptheory/group12.pdf>.

Example 7.2. The group D_{2q} has order $4q$. Which group is it in our list of such groups up to isomorphism? Writing $D_{2q} = \langle r, s \rangle$ where r has order $2q$, s has order 2, and $sr s^{-1} = r^{-1}$, a 2-Sylow subgroup is $\langle r^q, s \rangle \cong (\mathbf{Z}/(2))^2$ and D_{2q} is nonabelian, so D_{2q} must be isomorphic to (7.4), which is the only nonabelian group of order $4q$ with 2-Sylow subgroup $(\mathbf{Z}/(2))^2$. There is a unique isomorphism $f : D_{2q} \rightarrow \mathbf{Z}/(q) \rtimes_{\varphi_2} (\mathbf{Z}/(2))^2$ where $f(r) = (1, (1, 1))$ and $f(s) = (0, (1, 0))$: $f(r)^n = (1, (1, 1))^n = (n, (n, n))$ for all n , so $(1, (1, 1))$ has order $2q$, and $f(s) = (0, (1, 0))$ has order 2 and $f(s)f(r)f(s)^{-1} = (-1, (1, 1)) = f(r)^{-1}$. Then we get f by Remark 1.2 in <https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral2.pdf>.

Example 7.3. Let $G = \left\{ \begin{pmatrix} (-1)^b & a \\ 0 & (-1)^c \end{pmatrix} \pmod{q} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/(q))$ where $b, c \in \mathbf{Z}/(2)$. This group has order $4q$, is nonabelian since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ in G do not commute, and a 2-Sylow subgroup is $\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \cong (\mathbf{Z}/(2))^2$, so G must be isomorphic to (7.4). It is left to the reader to find an isomorphism between G and $\mathbf{Z}/(q) \rtimes_{\varphi_2} (\mathbf{Z}/(2))^2$. (It is *not* $\begin{pmatrix} (-1)^b & a \\ 0 & (-1)^c \end{pmatrix} \pmod{q} \mapsto (a, (b, c))$ since that is not a homomorphism.)

Example 7.4. Let $G = \left\{ \begin{pmatrix} \pm 1 & y \\ 0 & 1 \end{pmatrix} \pmod{2q} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/(2q))$. This group has order $4q$, is nonabelian since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ in G do not commute, and a 2-Sylow subgroup is $\left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \right\rangle \cong (\mathbf{Z}/(2))^2$, so G must be isomorphic to (7.4). It is left to the reader to find an isomorphism between G and $\mathbf{Z}/(q) \rtimes_{\varphi_2} (\mathbf{Z}/(2))^2$.

Example 7.5. When $q \equiv 1 \pmod{4}$, $(\mathbf{Z}/(q))^\times$ has an element of order 4. Let

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \pmod{q} : x^4 \equiv 1 \pmod{q} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/(q)).$$

This group has order $4q$, is nonabelian since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ in G do not commute, and a 2-Sylow subgroup is $\left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x^4 \equiv 1 \pmod{4} \right\} \cong \mathbf{Z}/(4)$. The group G is isomorphic to (7.3) and an isomorphism $f : \mathbf{Z}/(q) \rtimes_{\varphi_3} \mathbf{Z}/(4) \rightarrow G$ is $f(a, b) = \begin{pmatrix} z^b & a \\ 0 & 1 \end{pmatrix}$, where z has order 4 in $(\mathbf{Z}/(q))^\times$.

Example 7.6. When $q \equiv 1 \pmod{4}$, $(\mathbf{Z}/(q))^\times$ has an element of order 4. Let

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1/x \end{pmatrix} \pmod{q} : x^4 \equiv 1 \pmod{q} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/(q)).$$

This group has order $4q$, is nonabelian since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} z & 0 \\ 0 & 1/z \end{pmatrix}$ in G do not commute where z has order 4, and a 2-Sylow subgroup is $\left\{ \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} : x^4 \equiv 1 \pmod{4} \right\} \cong \mathbf{Z}/(4)$. The group G is isomorphic to (7.2) and an isomorphism $f : \mathbf{Z}/(q) \rtimes_{\varphi_1} \mathbf{Z}/(4) \rightarrow G$ is $f(a, b) = \begin{pmatrix} z^b & az^{-b} \\ 0 & z^{-b} \end{pmatrix}$ (this needs $z^2 = -1$).

When $q \equiv 3 \pmod{4}$, there is a field \mathbf{F} containing $\mathbf{Z}/(q)$ in which there is an element z with order 4. Let G be the matrices $\begin{pmatrix} z^b & az^{-b} \\ 0 & z^{-b} \end{pmatrix}$ where $a \in \mathbf{Z}/(q) \subset \mathbf{F}$ and $b \in \mathbf{Z}/(4)$. Check G is a group under matrix multiplication and that the mapping $f : \mathbf{Z}/(q) \rtimes_{\varphi_1} \mathbf{Z}/(4) \rightarrow G$ where $f(a, b) = \begin{pmatrix} z^b & az^{-b} \\ 0 & z^{-b} \end{pmatrix}$ is an isomorphism

Remark 7.7. The group $\mathbf{Z}/(q) \rtimes_{\varphi_1} \mathbf{Z}/(4)$ in (7.2) is generated by $x = (1, 0)$ with order q , $y = (0, 1)$ with order 4, and $yx y^{-1} = x^{-1}$. Check x commutes with $y^2 = (0, 2)$, so $\langle x, y \rangle = \langle xy^2, y \rangle$, where $w := xy^2$ has order $2q$, $w^q = y^{2q} = y^2$, and $ywy^{-1} = w^{-1}$. This group is called a generalized quaternion group Q_{4q} and also a dicyclic group of order $4q$.

What about the group

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \pmod{q} : x^4 \equiv 1 \pmod{q} \right\} \subset \mathrm{GL}_2(\mathbf{Z}/(q))$$

when $\mathbf{Z}/(q)$ has an element with multiplicative order 4? Perhaps surprisingly, G is abelian (check!) and in fact is cyclic.

8. GROUPS OF ORDER 1881

The number 1881 is $3^2 \cdot 11 \cdot 19 = 9 \cdot 209$. Let's describe all groups of this order.

Theorem 8.1. *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.

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

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

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 and elements of Q commute (a commutator of such elements is in $P \cap Q = \{1\}$). Both P and Q are cyclic (they have prime order). Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. The orders of x and y are relatively prime and $xy = yx$, 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 $H \triangleleft G$ 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 12.2 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 $\varphi: \mathbf{Z}/(9) \rightarrow (\mathbf{Z}/(209))^{\times}$ be a homomorphism. It is determined by $\varphi(1)$, which is a solution of $a^9 \equiv 1 \pmod{209}$. 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 $x \equiv 1 \pmod{11}$ and $x \equiv 4 \pmod{19}$ is $23 \pmod{209}$. Thus $23 \pmod{209}$ generates the subgroup of $(\mathbf{Z}/(209))^{\times}$ with order 9, so $\varphi(1) = 23^r \pmod{209}$ for some $r \in \{0, 1, \dots, 8\}$. To be explicit, when $\varphi(1) = 23^r \pmod{209}$ the group law on $\mathbf{Z}/(209) \rtimes_{\varphi} \mathbf{Z}/(9)$ is

$$(8.1) \quad (a, b)(c, d) = (a + \varphi_b(c), b + d) = (a + 23^{rb}c, b + d).$$

Depending on $\gcd(r, 9)$, we'll see the group law (8.1) 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 $rr' \equiv 1 \pmod{9}$ and $f: \mathbf{Z}/(9) \rightarrow \mathbf{Z}/(9)$ by $f(x) = r'x$. This is an automorphism of $\mathbf{Z}/(9)$ and $\varphi \circ f: \mathbf{Z}/(9) \rightarrow (\mathbf{Z}/(209))^{\times}$ is a homomorphism where $(\varphi \circ f)(1 \pmod{9}) = 23^{rr'} \equiv 23 \pmod{209}$, so in $\mathbf{Z}/(209) \rtimes_{\varphi \circ f} \mathbf{Z}/(9)$,

$$(8.2) \quad (a, b)(c, d) = (a + 23^b c, b + d).$$

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 (8.1) is isomorphic to the group given by (8.2).

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

$$(8.3) \quad (a, b)(c, d) = (a + \varphi_b(c), b + d) = (a + 23^{3b}c, b + d).$$

If $r = 6$ then $r \equiv -3 \pmod{9}$, so composing $\varphi: \mathbf{Z}/(9) \rightarrow (\mathbf{Z}/(209))^{\times}$ with multiplication by -1 on $\mathbf{Z}/(9)$ turns the group law (8.1) with $r = 6$ into the one with $r = 3$ in (8.3), and the two groups are isomorphic by Lemma 6.2.

Case 3: $r = 0$. Here (8.1) 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 (8.2) and (8.3) are not isomorphic, consider the conjugation action in both cases of G on its unique (normal) subgroup H of order 209. In (8.2), $(a, b)(c, 0)(a, b)^{-1} = (23^b c, 0)$, while in (8.3), $(a, b)(c, 0)(a, b)^{-1} = (23^{3b} c, 0)$. Since $23 \bmod 209$ has order 9 and $23^3 \bmod 209$ has order 3, conjugation by $(0, 1)$ on H in (8.2) is an automorphism of H with order 9, while in (8.3) 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 $G \rightarrow \text{Aut}(H)$ 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 $\text{GL}_2(\mathbf{Z}/(3))$, so $\text{GL}_2(\mathbf{Z}/(3))$ will play a role in this step that $(\mathbf{Z}/(9))^\times = \text{Aut}(\mathbf{Z}/(9))$ 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 $\varphi: (\mathbf{Z}/(3))^2 \rightarrow (\mathbf{Z}/(209))^\times$ be the homomorphism determined by $\varphi\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 45 \bmod 209$ and $\varphi\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1 \bmod 209$, *i.e.*, $\varphi\begin{pmatrix} x \\ y \end{pmatrix} = 45^x \bmod 209$. The group law in $\mathbf{Z}/(209) \rtimes_\varphi (\mathbf{Z}/(3))^2$ is

$$(8.4) \quad \left(a, \begin{pmatrix} x \\ y \end{pmatrix} \right) \left(a', \begin{pmatrix} x' \\ y' \end{pmatrix} \right) = \left(a + 45^x a', \begin{pmatrix} x + x' \\ y + y' \end{pmatrix} \right).$$

We'll show all nontrivial semidirect products $\mathbf{Z}/(209) \rtimes (\mathbf{Z}/(3))^2$ are isomorphic to the group (8.4) by using matrices in $\text{GL}_2(\mathbf{Z}/(3))$ to convert other semidirect product group structures into the one in (8.4)

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 $\varphi: (\mathbf{Z}/(3))^2 \rightarrow (\mathbf{Z}/(209))^\times$ 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 $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ to v and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ to w . Therefore the composite homomorphism $\varphi \circ A: (\mathbf{Z}/(3))^2 \rightarrow (\mathbf{Z}/(209))^\times$ has the effect $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto v \mapsto 45 \bmod 209$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto w \mapsto 1 \bmod 209$, which makes the semidirect product $\mathbf{Z}/(209) \rtimes_{\varphi \circ A} (\mathbf{Z}/(3))^2$ have the group structure in (8.4). 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 (8.4). \square

9. 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

³For $p = 2$, 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 11.2.

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

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

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

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

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

$$(9.1) \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

and in G_p

$$(9.2) \quad \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+pm' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(m+m') & b+b'+pmb' \\ 0 & 1 \end{pmatrix}.$$

It is left to you to show $\text{Heis}(\mathbf{Z}/(p))$ 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 $p(p-1)/2 \equiv 0 \pmod{p}$ when $p \neq 2$), so all non-identity elements of $\text{Heis}(\mathbf{Z}/(p))$ have order p . In G_p the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{p^2}$ has order p^2 , so $\text{Heis}(\mathbf{Z}/(p)) \not\cong G_p$.⁴

Now let's see $\text{Heis}(\mathbf{Z}/(p))$ and G_p are semidirect products. In $\text{Heis}(\mathbf{Z}/(p))$ 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 $H \triangleleft \text{Heis}(\mathbf{Z}/(p))$ since $H = \ker f$ for the homomorphism $f: \text{Heis}(\mathbf{Z}/(p)) \rightarrow \mathbf{Z}/(p)$ defined by

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

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

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

and $\begin{pmatrix} b+c \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b \\ c \end{pmatrix}$. Thus

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

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

where $\varphi: \mathbf{Z}/(p) \rightarrow \text{Aut}((\mathbf{Z}/(p))^2) = \text{GL}_2(\mathbf{Z}/(p))$ is defined by $\varphi(1 \bmod p) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The center of $\text{Heis}(\mathbf{Z}/(p))$ 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 $\text{Heis}(\mathbf{Z}/(p))$.

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 $H = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod p^2 \rangle \cong \mathbf{Z}/(p^2)$, $K = \langle \begin{pmatrix} 1+p & 1 \\ 0 & 1 \end{pmatrix} \bmod p^2 \rangle \cong \mathbf{Z}/(p)$, and $H \triangleleft G_p$ since $H = \ker f$ for the homomorphism $f: G_p \rightarrow \text{Aut}(\mathbf{Z}/(p^2)) = (\mathbf{Z}/(p^2))^\times$ 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 $\psi: \mathbf{Z}/(p) \rightarrow \text{Aut}(\mathbf{Z}/(p^2)) = (\mathbf{Z}/(p^2))^\times$ 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 9.1. *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 $\varphi: \mathbf{Z}/(p) \rightarrow \text{GL}_2(\mathbf{Z}/(p))$ where $\varphi(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\psi: \mathbf{Z}/(p) \rightarrow (\mathbf{Z}/(p^2))^\times$ where $\psi(1) = 1 + p \bmod p^2$, and these two semidirect products are not isomorphic.*

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 $\text{Heis}(\mathbf{Z}/(p))$ and G_p : the subgroup H we defined in each of them with order p^2 contains the center of the group.)

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

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 $\varphi: \mathbf{Z}/(p) \rightarrow \mathrm{GL}_2(\mathbf{Z}/(p))$ is the homomorphism such that $\varphi(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

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 $H \triangleleft G$.

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: $yxxy^{-1} = z^i x$ for some $i \not\equiv 0 \pmod{p}$.

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

$$(9.3) \quad yxy^{-1} = z^i x^j$$

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

$$y^2xy^{-2} = y(z^i x^j)y^{-1} = z^i yx^j y^{-1} = z^i (yxxy^{-1})^j = z^i (z^i x^j)^j = z^{i+i^2} x^{j^2} = z^{i(1+i)} z^{j^2}.$$

By induction,

$$(9.4) \quad y^m x y^{-m} = z^{i(1+j+j^2+\dots+j^{m-1})} x^{j^m}$$

for all $m \geq 1$. Since $y^p = 1$, setting $m = p$ turns (9.4) into

$$(9.5) \quad x = z^{i(1+j+j^2+\dots+j^{p-1})} x^{j^p} = z^{i(1+j+j^2+\dots+j^{p-1})} x^j$$

since x has order p and $j^p \equiv j \pmod{p}$.

Assume $j \not\equiv 1 \pmod{p}$. Then in the exponent of z in (9.5) we have $1 + j + j^2 + \dots + j^{p-1} = (j^p - 1)/(j - 1) \equiv (j - 1)/(j - 1) \equiv 1 \pmod{p}$, so (9.5) 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 $j \equiv 1 \pmod{p}$. That's a contradiction, so $j \equiv 1 \pmod{p}$. Now (9.3) says $yxy^{-1} = z^i x$. If $i \equiv 0 \pmod{p}$ 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 $i \not\equiv 0 \pmod{p}$, which proves the claim.

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

$$(9.6) \quad yzy^{-1} = z, \quad \text{and} \quad yxy^{-1} = zx$$

by the claim (and the new meaning of z). Using the isomorphisms $H \rightarrow (\mathbf{Z}/(p))^2$ where $z^b x^c \mapsto \begin{pmatrix} b \\ c \end{pmatrix}$ and $K \rightarrow \mathbf{Z}/(p)$ where $y^a \mapsto a$ together with the formulas in (9.6), the conjugation action $K \rightarrow \mathrm{Aut}(H)$ turns into the homomorphism $\varphi: \mathbf{Z}/(p) \rightarrow \mathrm{GL}_2(\mathbf{Z}/(p))$ where $\varphi(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so $G \cong (\mathbf{Z}/(p))^2 \rtimes_{\varphi} \mathbf{Z}/(p)$.

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 $\psi: \mathbf{Z}/(p) \rightarrow (\mathbf{Z}/(p^2))^{\times}$ 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, $H \triangleleft G$ and G/H has order p , so $\bar{y}^p = \bar{1}$ 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

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

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

$y \notin H$, $G = \langle x, y \rangle$. 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 $yxxy^{-1} = xx^{pk} = x^{1+pk}$ in G for some $k \in \mathbf{Z}$. Write this as $yxxy^{-1} = x^j$ where $j = 1 + pk$. Check $G = \langle x, y \rangle$, so G being nonabelian means x and y don't commute. Thus $k \not\equiv 0 \pmod{p}$.

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

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

and by induction

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

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

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

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 $yxxy^{-1} = x^j$ where $j = 1 + pk$ for some $k \not\equiv 0 \pmod{p}$. Conjugating by y again,

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

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

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

Because $k \not\equiv 0 \pmod{p}$, we can choose $n \geq 1$ so that $nk \equiv 1 \pmod{p}$. 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 $yxxy^{-1} = x^{1+p}$. By isomorphisms $H \rightarrow (\mathbf{Z}/(p^2))$ where $x^b \mapsto b \pmod{p^2}$ and $K \rightarrow \mathbf{Z}/(p)$ where $y^a \mapsto a \pmod{p}$, the conjugation action $K \rightarrow \text{Aut}(H)$ turns into the homomorphism $\psi: \mathbf{Z}/(p) \rightarrow (\mathbf{Z}/(p^2))^\times$ 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

10. GROUPS WITH SQUAREFREE ORDER

A positive integer is *squarefree* when it has no square factor greater than 1. Such a number is 1 or a product of distinct primes. In Section 6 we determined the groups with order pq for primes $p < q$, and pq is squarefree: such a group is cyclic or a semidirect product $\mathbf{Z}/(q) \rtimes \mathbf{Z}/(p)$. Since a cyclic group is a semidirect product of a cyclic group and a trivial group, all groups of order pq are semidirect products of two cyclic groups. We will now show, after a lemma, that this pattern holds for all groups with squarefree order.

Lemma 10.1. *If M is a finite group containing a normal subgroup N in the center of M such that M/N is cyclic, then M is abelian.*

Proof. Since M/N is cyclic, we can write $M/N = \langle \bar{m} \rangle$. Thus every element of M has the form $m^i n$ where $i \in \mathbf{Z}$ and $n \in N$. Since N is in the center of M , m commutes with each n in N , so all $m^i n$ and $m^j n'$ commute. Thus M is abelian. \square

Theorem 10.2. *Every group G with squarefree order is a semidirect product of two cyclic groups. More precisely, $G \cong G' \rtimes (G/G')$ where the commutator subgroup G' and the quotient group G/G' are both cyclic with relatively prime squarefree orders.*

Proof. The result is obvious if G is trivial, so we may suppose $|G| > 1$

Step 1: G/G' is cyclic.

If $G' = G$ the result is obvious, so we can assume $G' \neq G$. (We'll see in Step 2 that G' is actually not equal to G when $|G| > 1$.) The order of G/G' is squarefree, say $|G/G'| = q_1 \cdots q_k$ for distinct primes q_i . By Cauchy's theorem G/G' has an \bar{x}_i with order q_i . Since G/G' is abelian, the \bar{x}_i 's commute, so $\bar{x}_1 \cdots \bar{x}_k$ has order $q_1 \cdots q_k$. Thus G/G' is cyclic.

Step 2: $G' \neq G$.

Let p_0 be the smallest prime factor of $|G|$. Some g_0 in G has order p_0 by Cauchy's theorem. Set $H = \langle g_0 \rangle$. By a construction called the transfer map, there is a homomorphism $T : G \rightarrow H$ such that $T(h) = h^{[G:H]}$ for all $h \in H$, although $T(g)$ for general $g \in G$ is more complicated; this step uses minimality of p_0 among prime factors of $|G|$. The definition of T is a technical detour, so it has been placed in the appendix. (The homomorphism T is usually written as V because the German term for transfer is *Verlagerung*.)

Since $|H|$ and $[G : H]$ are relatively prime, $h \mapsto h^{[G:H]}$ is an automorphism of H , so $T(H) = H$. Thus $T(G) = H$. Since $T : G \rightarrow H$ has values in an abelian group, $G' \subset \ker T$. Also $T(G) = H$ and $|H| > 1$, so $G' \neq G$.⁸

Step 3: G' is cyclic.

Since $|G'|$ divides $|G|$, $|G'|$ is squarefree. Also $|G'| < |G|$ by Step 2, so by induction on squarefree orders of groups, $G'' = (G')'$ is cyclic. Since $G'' \triangleleft G$, G acts on G'' by conjugation, which gives us a homomorphism $f : G \rightarrow \text{Aut}(G'')$, and G'' being cyclic implies $\text{Aut}(G'')$ is abelian: $\text{Aut}(\mathbf{Z}/(m)) \cong (\mathbf{Z}/(m))^\times$. Commutativity of $\text{Aut}(G'')$ implies $G' \subset \ker f$. Since

$$\ker f = \{g \in G : gxg^{-1} = x \text{ for all } x \in G''\} = \{g \in G : gx = xg \text{ for all } x \in G''\},$$

all elements of G' commute with all elements of G'' . That means G'' is contained in the center of G' . By Step 1 with G' in place of G , G'/G'' is cyclic. Now Lemma 10.1 with $M = G'$ and $N = G''$ tells us G' is abelian. Since $|G'|$ is squarefree, G' being abelian implies G' is cyclic by the reasoning used in Step 1 to show G/G' is cyclic.

Step 4: $G \cong G' \rtimes (G/G')$.

Let $a = |G'|$ and $b = |G/G'|$, so $|G| = ab$ and $(a, b) = 1$. Since G/G' is cyclic by Step 1, $G/G' = \langle \bar{g} \rangle$ for some $g \in G$. Thus \bar{g} has order b in G/G' . Since $(a, b) = 1$, \bar{g}^a also has order b in G/G' . Perhaps surprisingly, g^a has order b in G : the order is at most b since $(g^a)^b = g^{ab} = g^{|G|} = 1$, and the order is at least b since if $(g^a)^k = 1$ with $k \geq 1$ then in G/G' we have $(\bar{g}^a)^k = \bar{1}$, so $b \mid k$ and thus $k \geq b$.

⁸Another approach to Step 2 is to show by induction on $|G|$ that G is solvable, so $G' \neq G$ since that's a property of nontrivial solvable groups. However, this is not a very different approach since proving G is solvable involves ideas just like our Step 2: see [1, Cor. 5.15].

In G we have cyclic subgroups G' of order a and $\langle g^a \rangle$ of order b . Since $(a, b) = 1$, $G' \cap \langle g^a \rangle = \{1\}$. Also $ab = |G|$, so $G = G'\langle g^a \rangle$. Then by Theorem 4.1, $G \cong G' \rtimes \langle g^a \rangle$ and $\langle g^a \rangle \cong G/G'$, so $G \cong G' \rtimes (G/G')$. \square

Remark 10.3. Theorem 10.2 can be generalized to an equivalence: a finite group G has all Sylow subgroups being cyclic if and only if $G \cong G' \rtimes (G/G')$ where G' and G/G' are both cyclic with relatively prime orders: see [1, Theorem 5.13, Corollary 5.14, Corollary 5.15, Theorem 5.16]. Saying $|G|$ is squarefree is the special case where the nontrivial Sylow subgroups of G have prime order.

11. 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.⁹ For a normal subgroup $H \triangleleft G$, 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 11.1. 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 11.2. 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 $H \triangleleft Q_8$ 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 $H \triangleleft G$ and $H \cap K = \{1\}$ such subgroups K can be far from unique.

Example 11.3. For $n \geq 3$, $S_n = A_n \cdot \{1, \tau\}$ for every transposition τ .

Example 11.4. 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 11.5 (Schur–Zassenhaus). *If $H \triangleleft G$ 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., $G = (\mathbf{Z}/(8))^\times$ and $H = \langle 3 \rangle$, with complements $\langle 5 \rangle$ or $\langle 7 \rangle$).

By Theorem 4.1, if $G = HK$ with $H \triangleleft G$ and $H \cap K = \{1\}$, then $K \cong G/H$, so every complementary subgroup to H is *isomorphic* to G/H . Thus all complementary subgroups of H in G (if there are any complements to H in G at all) are isomorphic, with a structure determined by H as a subgroup of G .

⁹Note 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 .

Example 11.6. 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 H has no complementary subgroup in G .

Note when $G = HK$, $H \triangleleft G$, and $H \cap K = \{1\}$ that K is a group of representatives in G for G/H . The composite $K \hookrightarrow G \rightarrow G/H$ 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 $H \triangleleft G$, 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.

Definition 11.7. For a surjective function $\varphi: X \rightarrow Y$, 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 $\psi: Y \rightarrow X$ 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 11.8. Let $f: \mathbf{R}^\times \rightarrow \mathbf{R}_{>0}$ 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 11.9. Let $f: \mathbf{C}^\times \rightarrow \mathbf{C}^\times$ by $f(z) = z^2$. One section of f is $g(re^{i\theta}) = \sqrt{r}e^{i\theta/2}$, $0 \leq \theta < 2\pi$, but g is not continuous on $(0, \infty)$. (Consider $\theta \rightarrow 0^+$ and $\theta \rightarrow 2\pi^-$ 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 11.10. 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 $\bigcup_{p \in S^2} T_p \rightarrow S^2$ is nice (continuous or smooth) when we give $\bigcup T_p$ a suitable topology. This shows that sections occur naturally in geometry.

Theorem 11.11. *If $H \triangleleft G$, 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 $\pi: G \rightarrow G/H$, where $\pi(g) = \bar{g}$, has a section that is a homomorphism.

Proof. (1) \Rightarrow (2). The set K is a group of coset representatives for G/H : $hk \equiv k \pmod{H}$, and $k_1 \equiv k_2 \pmod{H}$ 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 $g \in G$, $\bar{g} = \bar{k}$ 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 , $\bar{k} = \bar{1}$, 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 $s: G/H \rightarrow G$ such that $\pi(s(\bar{g})) = \bar{g}$ for each $g \in G$. Write $g = hk$, so $\bar{g} = \bar{k}$. Define $s(\bar{g}) = k$. This is well-defined since the representation of g as hk is unique, and by definition $\pi(s(\bar{g})) = \bar{k} = \bar{g}$, so s is a section to π . For $k \in K$, $s(\bar{k}) = k$. Then $s(\overline{k_1 k_2}) = s(\overline{k_1} \overline{k_2}) = k_1 k_2 = s(\overline{k_1}) s(\overline{k_2})$, so s is a group homomorphism.

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

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

Set $k = s(\bar{g})$, so $\bar{g} = \pi(k) = \bar{k}$ 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 $k \in K$, $k = s(\bar{g})$ for some $g \in G$. Since $k \in H$, $\pi(k) = \bar{e}$. Also

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

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

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

since $s: G/H \rightarrow G$ is a homomorphism. □

Example 11.12. 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 $G \xrightarrow{\pi} G/H$?

$$\begin{array}{ccc} & \xleftarrow{s} & \\ \mathrm{GL}_2(\mathbf{R}) & \longrightarrow & \mathrm{GL}_2(\mathbf{R})/\mathrm{SL}_2(\mathbf{R}) \cong \mathbf{R}^\times \end{array}$$

That is, can we find a homomorphism $s: \mathbf{R}^\times \rightarrow \mathrm{GL}_2(\mathbf{R})$ such that $\det(s(c)) = c$ for all $c \in \mathbf{R}^\times$? Yes, let $s(c) = \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$ (or let $s(c) = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$). 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 11.13. 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 11.2: Q_8 is not a semidirect product of nontrivial groups.

Example 11.14. 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

$$(11.1) \quad \mathrm{GL}_2(\mathbf{R}) \cong (\mathbf{R}^\times I_2) \times \mathrm{PGL}_2(\mathbf{R}).$$

If the groups in both sides of (11.1) 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 11.15. 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, $D_n \not\cong \mathbf{Z}/(2) \times D_{n/2}$ 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 $D_n = \langle r^2, s \rangle \langle rs \rangle \cong D_{n/2} \rtimes \mathbf{Z}/(2)$.

12. 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 12.1. *Let $f: H_1 \rightarrow H_2$ and $f': K_1 \rightarrow K_2$ be group isomorphisms. Then the mapping $F: H_1 \times K_1 \cong H_2 \times K_2$ 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,

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

Theorem 12.2. *Let $f: H_1 \rightarrow H_2$ and $f': K_1 \rightarrow K_2$ be isomorphisms. For each homomorphism $\varphi: K_1 \rightarrow \mathrm{Aut}(H_1)$ there is a corresponding homomorphism $\varphi': K_2 \rightarrow \mathrm{Aut}(H_2)$ such that $H_1 \rtimes_\varphi K_1 \cong H_2 \rtimes_{\varphi'} K_2$.*

Proof. The isomorphism $f: H_1 \rightarrow H_2$ 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.

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

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 $c_f: \mathrm{Aut}(H_1) \rightarrow \mathrm{Aut}(H_2)$ 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 $f': K_1 \rightarrow K_2$, each action $\varphi: K_1 \rightarrow \text{Aut}(H_1)$ becomes an action $\varphi': K_2 \rightarrow \text{Aut}(H_2)$ by making the diagram below commute: set $\varphi' := c_f \circ \varphi \circ (f')^{-1}$.

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

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 12.1.) For each $k \in K_2$, $\varphi'_k = c_f(\varphi_{(f')^{-1}(k)})$.

Let $F: H_1 \rtimes_{\varphi} K_1 \rightarrow H_2 \rtimes_{\varphi'} K_2$ 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

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

APPENDIX A. CONSTRUCTING A TRANSFER HOMOMORPHISM

Let G be a finite group and H be an *abelian* subgroup. We will show there is a homomorphism $T: G \rightarrow H$ such that, when $|H|$ is the smallest prime factor of $|G|$, $T(h) = h^{|G:H|}$ for all $h \in H$ while $T(g)$ for general $g \in G$ has a more complicated formula. This homomorphism is used in Step 2 of the proof of Theorem 10.2.

Let $m = [G:H]$ and x_1, \dots, x_m be left coset representatives for H in G : $G = \coprod_{i=1}^m x_i H$. For each $g \in G$, left multiplication by g on the left cosets of H can be viewed as a permutation ℓ_g of $\text{Sym}(G/H) \cong S_m$: $g(x_i H) = x_{\ell_g(i)} H$ for $i = 1, \dots, m$. Equivalently,

$$(A.1) \quad gx_i = x_{\ell_g(i)} h_i,$$

where $h_i \in H$.

Definition A.1. When H is an abelian subgroup of the finite group G , the *transfer* map $T: G \rightarrow H$ is defined by $T(g) = \prod_{i=1}^m h_i$, where h_i is defined by (A.1): $h_i = x_{\ell_g(i)}^{-1} g x_i$.

In the definition of $T(g)$, the order of multiplication in $\prod_{i=1}^m h_i$ doesn't matter since each h_i is in H and H is abelian.

To show $T(g)$ is well-defined, we check it does not change when the left coset representatives of H change. Writing $G = \coprod_{i=1}^m y_i H$, where $y_i H = x_i H$, we have $y_i = x_i k_i$ with $k_i \in H$. Since $x_i = y_i k_i^{-1}$

$$(A.2) \quad g y_i = g x_i k_i = (x_{\ell_g(i)} h_i) k_i = x_{\ell_g(i)} (h_i k_i) = y_{\ell_g(i)} k_{\ell_g(i)}^{-1} (h_i k_i) = y_{\ell_g(i)} (k_{\ell_g(i)}^{-1} h_i k_i).$$

Thus in (A.1), changing each x_i to y_i changes h_i to $k_{\ell_g(i)}^{-1}h_ik_i$, which changes the definition of $T(g)$ to

$$\prod_{i=1}^m (k_{\ell_g(i)}^{-1}h_ik_i)$$

and this product equals $\prod_{i=1}^m h_i$ since all h_i and k_i are in H and H is abelian. Thus $T(g)$ is well-defined.

To show $T : G \rightarrow H$ is a homomorphism, let g and g' be in G . Set $gx_i = x_{\ell_g(i)}h_i$ and $g'x_i = x_{\ell_{g'}(i)}h'_i$ for all i , where $h_i, h'_i \in H$. Then

$$(gg')x_i = g(g'x_i) = gx_{\ell_{g'}(i)}h'_i = x_{\ell_g(\ell_{g'}(i))}h_{\ell_{g'}(i)}h'_i = x_{\ell_{gg'}(i)}h_{\ell_{g'}(i)}h'_i,$$

so $T(gg') = \prod_{i=1}^m (h_{\ell_{g'}(i)}h'_i) = \prod_{i=1}^m h_{\ell_{g'}(i)} \prod_{i=1}^m h'_i = \prod_{i=1}^m h_i \prod_{i=1}^m h'_i = T(g)T(g')$.

Remark A.2. What is the analogue of $T : G \rightarrow H$ using *right* coset representatives of H in G and right multiplication of G on those right cosets? When the x_i 's are left coset representatives of H in G , the x_i^{-1} 's are right coset representatives of H in G . Check that in S_m the disjoint cycle decompositions of ℓ_g acting on the x_i 's is the same as r_g acting on the x_i^{-1} 's. Then (A.1) with g replaced by g^{-1} says $g^{-1}x_i = x_{\ell_{g^{-1}}(i)}h_i = x_{r_g(i)}h_i$, so $x_i^{-1}g = h_i^{-1}x_{r_g(i)}^{-1}$, which implies the right coset analogue of $T : G \rightarrow H$ is $g \mapsto \prod_{i=1}^m h_i^{-1} = T(g)^{-1}$.

Remark A.3. When H is nonabelian, the definition of $T(g)$ above no longer makes sense since we used commutativity of H several times to check that $T(g)$ is well-defined and T is a homomorphism. Those difficulties go away when we change the target group from H to H/H' , which is always abelian. So for a general subgroup H of G , the associated transfer map is $T : G \rightarrow H/H'$ where $T(g) = \prod_{i=1}^m h_iH'$. This is well-defined and a homomorphism by the same arguments used above.

The defining formula for $T(g)$ in general is quite technical. One case when there is a much simpler formula for $T(g)$ than its definition is when $H \subset Z(G)$, where it turns out that $T(g) = g^{[G:H]}$ for all $g \in G$: see <https://math.stackexchange.com/questions/842500>. (If $H \subset Z(G)$ then it is obvious that $g^{[G:H]} \in H$ since G/H is a group of order $[G : H]$, but it is *not* obvious that $g \mapsto g^{[G:H]}$ is a homomorphism!) When H is possibly nonabelian and we define the transfer as a map $G \rightarrow H/H'$ as in Remark A.3, a second case where $T(g)$ has a very simple formula for all $g \in G$ is $H = G'$: the transfer map $G \rightarrow G'/(G')'$ is trivial. This purely group-theoretic result, conjectured by Artin in 1927, was motivated by the goal of proving a conjecture of Hilbert in algebraic number theory that is now called the principal ideal theorem¹⁰. A proof of the triviality of the transfer map $G \rightarrow G'/(G')'$ was published by Furtwängler two years later.

Here is another case where there is a simple formula for $T(g)$, but this time just when $g \in H$. We need this in the proof of Theorem 10.2.

Theorem A.4. *If H is an abelian subgroup of the finite group G and $|H|$ is the smallest prime factor of $|G|$, then $T(h) = h^{[G:H]}$ for all $h \in H$.*

Proof. Two subgroups of G that contain H are its normalizer and centralizer:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}, \quad Z_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Clearly $Z_G(H) \subset N_G(H)$.

¹⁰This is not the same as Krull's principal ideal theorem in commutative algebra.

Step 1: $N_G(H) = Z_G(H)$.

The normalizer of H acts by conjugation on H . This action defines a homomorphism $N_G(H) \rightarrow \text{Aut}(H)$ with kernel $Z_G(H)$, so we get an embedding $N_G(H)/Z_G(H) \hookrightarrow \text{Aut}(H)$. Let $p_0 = |H|$, which is the smallest prime factor of $|G|$. Then $\text{Aut}(H) \cong (\mathbf{Z}/p_0\mathbf{Z})^\times$, so $|N_G(H)/Z_G(H)|$ divides $p_0 - 1$. At the same time, $|N_G(H)/Z_G(H)|$ divides $|G|$, which has no prime factor less than p_0 . Thus $|N_G(H)/Z_G(H)| = 1$, so $N_G(H) = Z_G(H)$.

Step 2: If two elements of H are conjugate in G , then they are equal.

Suppose $h, k \in H$ and $k = ghg^{-1}$ for some $g \in G$. To prove $k = h$, we can assume h and k are nontrivial in H , so $H = \langle h \rangle = \langle k \rangle$ since H has prime order. The equation $k = ghg^{-1}$ implies $k^r = gh^r g^{-1}$ for all integers r , so $H = \langle k \rangle = g\langle h \rangle g^{-1} = gHg^{-1}$. Thus $g \in N_G(H) = Z_G(H)$ by Step 1, so $ghg^{-1} = h$, which implies $k = h$.

Step 3: For $h \in H$, $T(h) = h^{[G:H]}$.

This is obvious when $h = 1$, so we can assume $h \neq 1$. Let $m = [G : H]$, $G = \coprod_{i=1}^m x_i H$ and $hx_i = x_{\ell_h(i)} h_i$ for $i = 1, \dots, m$. Since $h \in H$ we have $h^{p_0} = 1$, so $\ell_h^{p_0} = (1)$ in S_m . A permutation whose p_0 -power is (1) is a product of disjoint p_0 -cycles and 1-cycles.

If (i) is a 1-cycle in the cycle decomposition of ℓ_h , then for this i we have $hx_i = x_i h_i$, so $h = x_i h_i x_i^{-1}$. That says h and h_i are conjugate in G , so $\boxed{h_i = h}$ by Step 2.

If (j_1, \dots, j_{p_0}) is a p_0 -cycle in the cycle decomposition of ℓ_h , then

$$hx_{j_1} = x_{j_2} h_{j_1}, \quad hx_{j_2} = x_{j_3} h_{j_2}, \quad \dots, \quad hx_{j_{p_0-1}} = x_{j_{p_0}} h_{j_{p_0-1}}, \quad hx_{j_{p_0}} = x_{j_1} h_{j_{p_0}}.$$

Multiplying on the left repeatedly by h , these equations tell us that

$$h^2 x_{j_1} = hx_{j_2} h_{j_1} = x_{j_3} h_{j_2} h_{j_1},$$

$$h^3 x_{j_1} = hx_{j_3} h_{j_2} h_{j_1} = x_{j_4} h_{j_3} h_{j_2} h_{j_1},$$

$$\vdots$$

$$h^{p_0} x_{j_1} = hx_{j_{p_0}} h_{j_{p_0-1}} \cdots h_{j_2} h_{j_1} = x_{j_1} h_{j_{p_0}} \cdots h_{j_2} h_{j_1}.$$

Since $h^{p_0} = 1$, the last equation says $x_{j_1} = x_{j_1} h_{j_{p_0}} \cdots h_{j_2} h_{j_1}$, so $\boxed{h_{j_{p_0}} \cdots h_{j_2} h_{j_1} = 1}$.

Putting together the boxed relations due to 1-cycles and p_0 -cycles in ℓ_h , the definition $T(h) = \prod_{i=1}^m h_i$ simplifies to $T(h) = h^{|\{i: \ell_h(i)=i\}|}$. Let ℓ_h have a 1-cycles and b p_0 -cycles, so $a = |\{i: \ell_h(i) = i\}|$ and $m = a + p_0 b$. Thus $T(h) = h^a = h^{a+p_0 b} = h^m = h^{[G:H]}$. \square

Remark A.5. If $|H| = 2$ and $[G : H]$ is odd, then there is a simpler way than the transfer map to build a homomorphism $f : G \rightarrow H$ such that $f(h) = h^{[G:H]}$ for all $h \in H$, which is the same as $f(h) = h$ in this case: see the proof of Theorem 6.8 with $n = 1$ in <https://kconrad.math.uconn.edu/blurbs/grouptheory/sylowapp.pdf>, keeping in mind that $H \cong \{\pm 1\}$.

REFERENCES

- [1] I. M. Isaacs, "Finite Group Theory," Amer. Math. Society, Providence, RI, 2008.