

SOME PROPERTIES OF SEMIDIRECT PRODUCTS

In class, we classified groups of order pq , where p and q are distinct primes, as follows:

Proposition 1. *Suppose $p < q$.*

- (1) *If $q \not\equiv 1 \pmod{p}$, then the unique group of order pq is the cyclic group $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*
- (2) *If $q \equiv 1 \pmod{p}$, then in addition to the cyclic group $\mathbb{Z}/pq\mathbb{Z}$ there is a unique non-abelian group of order pq , given as the semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ for any nontrivial map $\mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$.*

However, we waved our hands over the uniqueness statement in part (2) of Proposition 1: why do the $p-1$ different nontrivial maps $\mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/(q-1)\mathbb{Z}$ all give isomorphic semidirect products? Similarly, we claimed that there is a unique non-abelian semidirect product $\mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^2$, namely D_{12} . The following lemma leads to a proof of these uniqueness claims.

Lemma 2. *Suppose $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$, and suppose there are automorphisms $\alpha \in \text{Aut}(K), \beta \in \text{Aut}(H)$ such that*

$$\phi_2 = \gamma_\beta \circ \phi_1 \circ \alpha,$$

where γ_β denotes conjugation by β in $\text{Aut}(H)$. Then $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$.

Proof. Define $\psi : H \rtimes_{\phi_1} K \rightarrow H \rtimes_{\phi_2} K$ by $(h, k) \mapsto (\beta(h), \alpha^{-1}(k))$. First we check that ψ is a homomorphism:

$$\begin{aligned} \psi(h_1, k_1)\psi(h_2, k_2) &= (\beta(h_1), \alpha^{-1}(k_1))(\beta(h_2), \alpha^{-1}(k_2)) \\ &= (\beta(h_1)\phi_2(\alpha^{-1}(k_1))(\beta(h_2)), \alpha^{-1}(k_1)\alpha^{-1}(k_2)) \\ &= (\beta(h_1)\gamma_\beta(\phi_1(k_1))(\beta(h_2)), \alpha^{-1}(k_1k_2)) \\ &= (\beta(h_1)(\beta \circ \phi_1(k_1) \circ \beta^{-1})(\beta(h_2)), \alpha^{-1}(k_1k_2)) \\ &= (\beta(h_1)\beta(\phi_1(k_1)(h_2)), \alpha^{-1}(k_1k_2)) \\ &= (\beta(h_1\phi_1(k_1)(h_2)), \alpha^{-1}(k_1k_2)) \\ &= \psi(h_1\phi_1(k_1)(h_2), k_1k_2) \\ &= \psi((h_1, k_1)(h_2, k_2)). \end{aligned}$$

But ψ is bijective with inverse map $(h, k) \mapsto (\beta^{-1}(h), \alpha(k))$. Therefore ψ is an isomorphism and the lemma follows. \square

As our first application, note that although there are three nontrivial homomorphisms $(\mathbb{Z}/2\mathbb{Z})^2 \rightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})$, they can all be obtained from one another by (pre-)composing with automorphisms of $(\mathbb{Z}/2\mathbb{Z})^2$. Therefore the resulting semidirect products are all isomorphic.

Corollary 3. *If K is cyclic and $\phi_1(K)$ and $\phi_2(K)$ are conjugate subgroups of $\text{Aut}(H)$, then $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$.*

Proof. Let $K = \langle k \rangle$, and note that by hypothesis there exists $\beta \in \text{Aut}(H)$ with $\beta\phi_1(K)\beta^{-1} = \phi_2(K)$; that is, $(\gamma_\beta \circ \phi_1)(k) = \beta\phi_1(k)\beta^{-1} = \phi_2(k)^a$ for some generator $\phi_2(k)^a$ of $\phi_2(K)$. The generator condition implies that $\gcd(a, |\phi_2(K)|) = 1$. Note that a can be replaced by $a + x|\phi_2(K)|$ for any integer x . By Lemma 4 (which follows this proof), we may assume that $\gcd(a, |K|) = 1$. Let a^{-1} denote the multiplicative inverse of $a \pmod{|K|}$. Then $\alpha : k^i \mapsto k^{a^{-1}i}$ is an automorphism of K and $\phi_2 = \gamma_\beta \circ \phi_1 \circ \alpha$, so the result follows from Lemma 2. \square

Lemma 4. *If $(a, m) = 1$ and $m \mid n$, then $(a + xm, n) = 1$ for some integer x . This may be restated algebraically as follows: if $m \mid n$, then the reduction mod m map $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ is surjective.*

Proof. Factor $n = NM$, where M contains the powers of primes dividing m , and N contains the powers of other primes. Then $(a + xm, M) = 1$ for all x , so it suffices to choose x such that $(a + xm, N) = 1$. But this is easy: since $(m, N) = 1$, the congruence $a + xm \equiv 1 \pmod{N}$ has a solution. \square

Any two nontrivial maps $\phi_1, \phi_2 : \mathbb{Z}/p\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/q\mathbb{Z})$ have the same image, namely the unique subgroup of order p in $\text{Aut}(\mathbb{Z}/q\mathbb{Z})$, so the uniqueness statement in part (2) of Proposition 1 follows from Corollary 3.

We will apply Corollary 3 again in the classification of groups of order p^3 , combined with the following proposition.

Proposition 5. *Any two subgroups of order p in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are conjugate.*

Proof using Sylow theorems. A subgroup of order p in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is a Sylow p -subgroup, and all Sylow p -subgroups are conjugate. \square

Proof using linear algebra. Suppose $A \in \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has order p . Then $A^p = I$, i.e., $(A - I)^p = 0$ (since $p = 0$ in $\mathbb{Z}/p\mathbb{Z}$). Since A is not the identity, it follows that the minimal polynomial of A is $(A - I)^2$, and so the rational canonical form for A is

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}.$$

It follows that every subgroup of order p is conjugate to $\langle B \rangle$; hence any two subgroups of order p are conjugate to one another. \square

Note that one example of a subgroup of order p in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is $\left\{ \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix} \right\}$; by the proposition, every subgroup of order p is conjugate to this one.

Sometimes it is useful to have a criterion which shows that two semidirect products are *not* isomorphic. The following proposition leads to one example of such a criterion.

Proposition 6. *Let $\phi : K \rightarrow \text{Aut}(H)$, and suppose H is abelian. Let $G = H \rtimes_\phi K$. Then $C_G(H) = \ker(\phi)H$.*

Proof. Since $H \triangleleft G$, we have $G = KH = \cup_{k \in K} kH$. Since H is abelian we have $C_G(H) \supset H$, so $C_G(H)$ is a union of cosets of H . The coset kH lies in $C_G(H)$ if and only if k does, and therefore $C_G(H) = \cup_{k \in C_G(H) \cap K} kH = (C_G(H) \cap K)H$. But by #1 on Homework 7 we have $\ker(\phi) = C_G(H) \cap K$. \square

Corollary 7. *Suppose $(\#H, \#K) = 1$ and H is abelian. If $\phi_1, \phi_2 : K \rightarrow \text{Aut}(H)$ and $\ker(\phi_1) \not\cong \ker(\phi_2)$, then $H \rtimes_{\phi_1} K$ and $H \rtimes_{\phi_2} K$ are not isomorphic.*

Proof. Let G be any semidirect product $H \rtimes K$. I claim that H is the unique subgroup of order $\#H$ in G . Indeed, let $\pi : G \rightarrow G/H \cong K$ be the natural map. If $x \in G \setminus H$ then $\text{ord}(\pi(x))$ is divisible by a prime dividing $\#K$. Since $\text{ord}(x)$ is also divisible by this prime, we have $\text{ord}(x) \nmid \#H$, and therefore x cannot be an element in a subgroup of G of order $\#H$. The claim follows.

Now let $G_i = H \rtimes_{\phi_i} K$ for $i = 1, 2$, and let H_i denote the copy of H inside G_i . If $\lambda : G_1 \rightarrow G_2$ is an isomorphism, then by the previous paragraph $\lambda(H_1) = H_2$. So $\lambda(C_{G_1}(H_1)) = C_{G_2}(H_2)$, and therefore λ induces an isomorphism $C_{G_1}(H_1)/H_1 \rightarrow C_{G_2}(H_2)/H_2$. By Proposition 6 this implies $\ker(\phi_1) \cong \ker(\phi_2)$, a contradiction. \square

As an application, we show:

Proposition 8. *There are exactly 15 different groups of order 24, up to isomorphism.*

Proof. Let G be a group of order 24. We factor $24 = 2^3 \cdot 3$, so that $n_2 = 1, 3$ and $n_3 = 1, 4$.

Suppose first that $n_3 = 4$. Since G acts transitively by conjugation on $\text{Syl}_3(G)$, we obtain a map $\varphi : G \rightarrow S_4$ whose kernel has order dividing 6. If the normal subgroup $\ker(\varphi)$ were to contain one Sylow 3-subgroup of G it would have to contain them all; this rules out $\#\ker(\varphi) = 3, 6$. If $\#\ker(\varphi) = 2$, then the normal subgroup $\ker(\varphi)$ is contained in all the Sylow 2-subgroups of G . But $G/\ker(\varphi)$ is isomorphic to a subgroup of order 12 in S_4 , and A_4 is the unique such subgroup. Since A_4 has just one Sylow 2-subgroup, this implies $n_2 = 1$.

If $\#\ker(\varphi) = 1$, then φ is an isomorphism $G \cong S_4$. Checking that S_4 does have four Sylow 3-subgroups and three Sylow 2-subgroups, this case actually does occur. We may therefore identify four cases: (a) $G \cong S_4$; (b) $n_3 = 1$; (c) $n_2 = 1$.

If $n_3 = 1$, then $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} P_2$, where P_2 is a group of order 8 and $\phi : P_2 \rightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. We exhaust the possibilities for P_2 :

- (i) $P_2 \cong Q$. Any nontrivial map $\phi : Q \rightarrow \mathbb{Z}/2\mathbb{Z}$ has kernel $\langle i \rangle$, $\langle j \rangle$, or $\langle k \rangle$, and for each kernel there is one map. These subgroups can be interchanged by automorphisms of Q , so by Lemma 2 there is exactly one nontrivial semidirect product, up to isomorphism. We obtain two groups: $\mathbb{Z}/3\mathbb{Z} \times Q$ and $\mathbb{Z}/3\mathbb{Z} \rtimes Q$.
- (ii) $P_2 \cong D_8$. The kernel of any nontrivial map $D_8 \rightarrow \mathbb{Z}/2\mathbb{Z}$ is a subgroup of order 4, so is one of $\langle r \rangle$, $\langle s, r^2 \rangle$, $\langle sr, r^2 \rangle$, and for each kernel there is one map. The latter two subgroups can be interchanged by automorphisms of D_8 , so by Lemma 2 they give isomorphic semidirect products. Since $\langle r \rangle \not\cong \langle s, r^2 \rangle$, by Corollary 7 we obtain three groups: $\mathbb{Z}/3\mathbb{Z} \times D_8$, $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} D_8$ where $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} D_8$ where $\ker(\phi) \cong V$.
- (iii) $P_2 \cong \mathbb{Z}/8\mathbb{Z}$. There is a unique nontrivial homomorphism $\mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$, so we obtain two groups: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/8\mathbb{Z}$.
- (iv) $P_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The kernel of a nontrivial map $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or V . There is a unique subgroup isomorphic to V . The two subgroups isomorphic to $\mathbb{Z}/4\mathbb{Z}$ can be interchanged by automorphisms of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so by Lemma 2 they give isomorphic semidirect products. By Corollary 7 we obtain three groups: $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ where $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ where $\ker(\phi) \cong V$.

- (v) $P_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. A nontrivial map $(\mathbb{Z}/2\mathbb{Z})^3 \rightarrow \mathbb{Z}/2\mathbb{Z}$ has kernel isomorphic to V . The subgroups of $(\mathbb{Z}/2\mathbb{Z})^3$ that are isomorphic to V can be interchanged by automorphisms of $(\mathbb{Z}/2\mathbb{Z})^3$, so by Lemma 2 we obtain two groups: $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^3$ and $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} (\mathbb{Z}/2\mathbb{Z})^3$.

Finally, suppose $n_2 = 1$, so that $G \cong P_2 \rtimes_{\phi} \mathbb{Z}/3\mathbb{Z}$ where $\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(P_2)$. If ϕ is trivial then we re-obtain one of the direct products that we have already listed, so we may assume that ϕ is nontrivial. But $\#\text{Aut}(\mathbb{Z}/8\mathbb{Z}) = 7$, $\#\text{Aut}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = 8$, and $\#\text{Aut}(D_8) = 8$, so ϕ cannot be nontrivial for these possibilities for P_2 .

- (vi) $P_2 \cong Q$. We have $\text{Aut}(Q) \cong S_4$, and any two subgroups of order 3 in S_4 are conjugate. By Corollary 3 there is a unique nontrivial semidirect product $Q \rtimes_{\phi} \mathbb{Z}/3\mathbb{Z}$.
- (vii) $P_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. In this case $\text{Aut}((\mathbb{Z}/2\mathbb{Z})^3) \cong \text{GL}_3(\mathbb{Z}/2\mathbb{Z})$ has order $7 \cdot 6 \cdot 4 = 168$. Since $3 \nmid 168$, any two subgroups of order 3 in $\text{GL}_3(\mathbb{Z}/2\mathbb{Z})$ are conjugate, and by Corollary 3 there is a unique nontrivial semidirect product $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes_{\phi} \mathbb{Z}/3\mathbb{Z}$.

One checks that we have found a total of 15 groups. □

Corollary 9. *The groups of order 24 are as follows:*

- (1) $\mathbb{Z}/24\mathbb{Z}$;
- (2) $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- (3) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- (4) $S_4 \cong \text{PGL}_2(\mathbb{Z}/3\mathbb{Z})$;
- (5) $SL_2(\mathbb{Z}/3\mathbb{Z}) \cong Q \rtimes \mathbb{Z}/3\mathbb{Z}$;
- (6) $D_{24} \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} D_8$ with $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$;
- (7) $\mathbb{Z}/2\mathbb{Z} \times A_4 \cong (\mathbb{Z}/2\mathbb{Z})^3 \rtimes \mathbb{Z}/3\mathbb{Z}$;
- (8) $\mathbb{Z}/2\mathbb{Z} \times D_{12} \cong S_3 \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/2\mathbb{Z})^3$;
- (9) $\mathbb{Z}/2\mathbb{Z} \times T \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ with $\ker(\phi) \cong V$;
- (10) $\mathbb{Z}/3\mathbb{Z} \times D_8$;
- (11) $\mathbb{Z}/3\mathbb{Z} \times Q_8$;
- (12) $\mathbb{Z}/4\mathbb{Z} \times S_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ with $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$;
- (13) $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/8\mathbb{Z}$;
- (14) $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} D_8$ with $\ker(\phi) \cong V$;
- (15) $\mathbb{Z}/3\mathbb{Z} \rtimes Q_8$;

Proof. Note that each group from Proposition 8 is on a separate line in this list, so it suffices to verify the isomorphisms with more familiar groups. Each group in Proposition 8 is determined uniquely by the number of Sylow 2- and 3-subgroups, the structure of the Sylow 2-subgroup, and the structure of the kernel of the map ϕ defining the semidirect product; so this is all we must check to verify the above isomorphisms. We give an interesting example and leave the rest of the details to the reader.

The group $D_{24} = \langle r, s \mid r^{12} = s^2 = 1, srs = r^{-1} \rangle$ has a unique subgroup of order 3, namely $\langle r^4 \rangle$, and three subgroups isomorphic to D_8 , namely $\langle sr^i, r^3 \rangle$ for $i = 0, 1, 2$. So $D_{24} \cong \mathbb{Z}/3\mathbb{Z} \rtimes_{\phi} D_8$ for some ϕ . Since $C_{D_{24}}(\langle r^4 \rangle) = \langle r \rangle$ and $\langle r \rangle / \langle r^4 \rangle \cong \mathbb{Z}/4\mathbb{Z}$, it follows by Proposition 6 that $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$. □

Proposition 10. *There are exactly 15 different groups of order 136, up to isomorphism.*

Proof. We factor $136 = 2^3 \cdot 17$, and note that $n_17 = 1$. Therefore every group G of order 136 is isomorphic to $\mathbb{Z}/17\mathbb{Z} \rtimes_{\phi} P_2$ for some group P_2 of order 8 and map $\phi : P_2 \rightarrow \text{Aut}(\mathbb{Z}/17\mathbb{Z}) \cong \mathbb{Z}/16\mathbb{Z}$. Note that since P_2 is a Sylow 2-subgroup, the group G uniquely determines the isomorphism type of P_2 . We exhaust the possibilities for P_2 .

- (a) $P_2 \cong Q$. Any map $Q \rightarrow \mathbb{Z}/16\mathbb{Z}$ factors through $Q/\langle -1 \rangle \cong V$, and so has kernel Q , $\langle i \rangle$, $\langle j \rangle$, or $\langle k \rangle$. For each nontrivial kernel there is exactly one map; these subgroups can be interchanged by automorphisms of Q , so by Lemma 2 there is exactly one nontrivial semidirect product, up to isomorphism. We obtain two groups: $\mathbb{Z}/17\mathbb{Z} \times Q$ and $\mathbb{Z}/17\mathbb{Z} \rtimes Q$.
- (b) $P_2 \cong D_8$. Any nontrivial map $D_8 \rightarrow \mathbb{Z}/17\mathbb{Z}$ factors through $D_8/\langle r^2 \rangle \cong V$, so has kernel D_8 , $\langle r \rangle$, $\langle s, r^2 \rangle$, $\langle sr, r^2 \rangle$. For each nontrivial kernel there is exactly one map. The latter two subgroups can be interchanged by automorphisms of D_8 , so by Lemma 2 they give isomorphic semidirect products. Since $\langle r \rangle \not\cong \langle s, r^2 \rangle$, by Corollary 7 we obtain three groups: $\mathbb{Z}/17\mathbb{Z} \times D_8$, $\mathbb{Z}/17\mathbb{Z} \rtimes_{\phi} D_8$ where $\ker(\phi) \cong \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/17\mathbb{Z} \rtimes_{\phi} D_8$ where $\ker(\phi) \cong V$.
- (c) $P_2 \cong \mathbb{Z}/8\mathbb{Z}$. There are four nontrivial maps $\mathbb{Z}/8\mathbb{Z} \rightarrow \mathbb{Z}/16\mathbb{Z}$, with kernel isomorphic to 1, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/8\mathbb{Z}$ respectively. By Corollary 7 we obtain four groups in this case.
- (d) $P_2 \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- (e) $P_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. Any nontrivial map has kernel isomorphic to V . Every subgroup of $(\mathbb{Z}/2\mathbb{Z})^3$ isomorphic to V gives rise to a unique such map, and these subgroups are all interchanged by automorphisms of $(\mathbb{Z}/2\mathbb{Z})^3$. By Lemma 2 we obtain two groups in this case.

□