Investigation 37

Groups of Order 8 and 12: Semidirect Products of Groups

Focus Questions

By the end of this investigation, you should be able to give precise and thorough answers to the questions listed below. You may want to keep these questions in mind to focus your thoughts as you complete the investigation.

- What is a semidirect product of groups? In what ways are semidirect products of groups useful?
- Up to isomorphism, how many groups are there of order 8?
- Up to isomorphism, how many groups are there of order 12?

Preview Activity 37.1. Summarize our previous work in classifying groups, and list all of the isomorphism classes of groups of orders from 1 to 7, 9 to 11, and 13 to 15. Provide whatever information you can about groups of orders 8 and 12.

Introduction

As Preview Activity 37.1 demonstrates, we have classified all groups of order 1 through 15, with the exception of groups of order 8 and 12. We have also determined all groups of prime order (see Activity 23.17 on page 326 and Theorem 26.18 on page 383), all groups of order $2p$, where p is prime (see Corollary 24.13 on page 341 and Theorem 26.16 on page 381), all groups of order pq where p and q are distinct primes and p does not divide $q - 1$ (see Activity 29.32 on page 431), and all groups of order p^2, where p is prime (see Activity 29.15 on page 425). In this investigation, we will fill in the gaps and classify all groups of order 8 and 12, which will complete our classification of groups of order less than 16. (Since there are 14 groups of order 16, this seems like a reasonable place to stop.) In the process of classifying the groups of order 8 and 12, we will introduce and use the idea of the semidirect product of two groups. We will also see that when classifying groups of a given order, it is not the order itself that determines the difficulty of the classification, but rather how large the powers of the prime divisors of the order are.

Groups of Order 8

In this section, we will determine the distinct isomorphism classes of groups of order 8. Since the Fundamental Theorem of Finite Abelian Groups tells us about the Abelian groups of order 8, we will concentrate on non-Abelian groups. Recall that we already know two non-Abelian groups of order 8—namely, D_4 and the quaternions $\mathbf{Q}$. We will now determine if there are, up to isomorphism, any other non-Abelian groups of order 8, and we will classify all such groups.

Activity 37.2. Let G be a non-Abelian group of order 8 with identity e.

(a) Use Exercise (2) of Investigation 18 (see page 274) to explain why G must contain an element b of order 4.

(b) Let $N = \langle b \rangle$. Explain why N is normal in G.

(c) Let $a \in G$ with $a \notin N$. Then $G = N \cup aN = \{e, b, b^2, b^3, a, ab, ab^2, ab^3\}$. The operation table for G will be determined once we know how to represent the elements ba and a^2 in the form $a^i b^j$, with $0 \leq i \leq 1$ and $0 \leq j \leq 3$. Given that $N \triangleleft G$, we know that $aba^{-1} \in N$, so $aba^{-1} = b^t$ for some t with $0 \leq t \leq 3$

(i) Explain why t cannot be 0 or 1.

(ii) Now explain why t cannot be equal to 2. (Hint: What is $|aba^{-1}|$?)

(iii) Assume $aba^{-1} = b^3 = b^{-1}$. Since $a \in G$ and $a \neq e$, we must have $|a| = 2$ or $|a| = 4$. What can we say about G if $|a| = 2$?

(iv) What can we say about G if $aba^{-1} = b^{-1}$ and $|a| = 4$?

(d) How many groups are there of order 8?

Activity 37.2 tells us about the groups of order 8, so we will now turn our attention to groups of order 12. It is possible (and not that difficult) to classify the groups of order 12 directly, but in the next section we will introduce a new tool, the semidirect product, that is very helpful in the general context of classifying groups of a given order. We will then use semidirect products to classify groups of order 12 and of order p^3, where p is an odd prime.

Semi-direct Products of Groups

Preview Activity 37.3. Let G be the set of ordered pairs

$$\{([a]_3, [b]_2) : [a]_3 \in \mathbb{Z}_3, [b]_2 \in \mathbb{Z}_2\}.$$

Define an operation $\cdot$ on G by

$$([a]_3, [b]_2) \cdot ([c]_3, [d]_2) = ([a + (-1)^b c]_3, [b + d]_2)$$

(a) Explain why this operation is well-defined on G.

(b) Construct the operation table for the set G with the operation defined above.

(c) Is G a group under this operation? If no, why not? If yes, to what familiar group is G isomorphic? Explain.

While we can decompose some groups into an internal direct product of normal subgroups, we cannot do this for every group. For example, if we try to write the group D_3 as an internal direct product of two proper subgroups, we run into a problem. Recall that the group $H = \langle R \rangle$ is a normal subgroup of D_3 of order 3, so we would need a normal subgroup K of order 2 to be able to write D_3 as the product $H \times K$. However, D_3 has no normal subgroup of order 2. So we cannot decompose D_3 into an internal direct product of nontrivial normal subgroups. It turns out, however, that we can decompose D_3 into what is called a semidirect product of subgroups. Activity 37.3 gives an example of such a decomposition. (Don't worry if the construction there does not seem obvious or natural to you at the moment.)

Up to this point, we have seen several different products of groups:

- The direct product $H \oplus K$ of two groups is again a group, external to both H and K.
- If H and K are subgroups of a group G with $H \triangleleft G$, then the product

  $$HK = \{hk : h \in H, K \in K\}$$

  is a subgroup of G. (See Activity 24.22 on page 346.) Moreover, if $H \cap K = \{e\}$, where e is the identity in G, then $|HK| = |H||K|$. To see this, suppose $h_1k_1 = h_2k_2$ in HK. Then $h_2^{-1}h_1 = k_2k_1^{-1} \in (H \cap K)$, so $h_2^{-1}h_1 = k_2k_1^{-1} = e$. Thus, $h_1 = h_2$, and $k_1 = k_2$. It follows that if $H \cap K = \{e\}$ and $|H||K| = |G|$, then $G = HK$.
- If H and K are normal subgroups of a group G with $H \cap K = \{e\}$, then $HK = H \times K$ is the internal direct product of H and K.

In this section, we will construct another type of product called a *semidirect product*. To understand how semidirect products work, recall that the construction of the internal product HK requires that H and K be subgroups of some group G that is already known. The question we want to answer now is if we can generalize this construction. In other words, given any two arbitrary groups H and K, can we find a group G so that G contains copies of both H and K—that is, subgroups H' and K' that are isomorphic to H and K, respectively—with $H' \triangleleft G$ and $H' \cap K' = \{e\}$, where e is the identity in G? If so, then $G = H'K'$, and we will denote this special decomposition as $H \rtimes K$. (We will say more about this notation later.)

To explore this construction more, let H and K be groups with identities e_H and e_K, respectively. We want to find a group G that contains isomorphic copies of H and K satisfying the conditions described above. A natural place to start is to let $G = \{(h, k) : h \in H, k \in K\}$. Certainly, G will contain a copy $H' = \{(h, e_K) : h \in H\}$ of H and a copy $K' = \{(e_H, k) : k \in K\}$ of K. The key to constructing the group G is to define an appropriate operation. We want to make $G = H'K'$ with $H' \triangleleft G$. This will mean that if $k \in K'$ and $h \in H'$, then $khk^{-1} \in H'$. If $a = h_1k_1$ and $b = h_2k_2$ are elements of $H'K'$, then it will follow that

$$ab = (h_1k_1)(h_2k_2) = h_1\left(k_1h_2k_1^{-1}\right)(k_1k_2) \tag{37.1}$$

is also an element of $H'K'$. So the operation we define in G will need to mimic the product in (37.1).

What makes the product in (37.1) work is that $k_1 h_2 k_1^{-1}$ is in H. In fact, conjugation by the element k_1 is an automorphism of H (an inner automorphism to be specific). We also saw this idea in Activity 37.3, where left multiplication by $(-1)^b$ for $b = 0$ or $b = 1$ is an automorphism on $\mathbb{Z}_3$. In other words, we had a mapping φ with domain $\mathbb{Z}_2$ that assigned to each $[b] \in \mathbb{Z}_2$ an automorphism on $\mathbb{Z}_3$. More specifically, we had $\varphi([0]_2)$ as the identity automorphism and $\varphi([1]_2)$ as the automorphism that sends $[a]_3$ to $[2a]_3$ for all $[a]_3 \in \mathbb{Z}_3$. Expressed another way, $\varphi : \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_3)$ is the mapping for which $\varphi([0]_2)([a]_3) = [a]_3$ (for all $[a]_3 \in \mathbb{Z}_3$) and $\varphi([1]_2)([a]_3) = [2a_3]$ (for all $[a]_3 \in \mathbb{Z}_3$). (It turns out that φ is a homomorphism as well, and you should verify that for yourself.)

Before we proceed, a word of caution is in order: the above notation can be very confusing since we are dealing with functions whose images are functions as well. As you work through this section, it is vitally important to distinguish between the elements of a given group and the functions that act on these elements. In the next activity, we will explore these ideas in a more general context.

Activity 37.4. Let H and K be groups with identities e_H and e_K, respectively, let $\varphi : K \to \text{Aut}(H)$ be a homomorphism, and let $G = H \times K$ be the Cartesian product of H and K. Then we can define a product on G as follows:

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2). \tag{37.2}$$

Note that this product has the same form as the products in (37.1) and Activity 37.3. In Activity 37.3, our example turned out to be a group, so it seems reasonable to ask if G will always be a group with the product defined by (37.2).

(a) Is G closed under the operation from (37.2)?

(b) Does G contain an identity element? If so, what is it? Explain.

(c) Is the operation defined by (37.2) associative? Prove your answer.

(d) Does G contain an inverse for each of its elements? If so, what is the form of an inverse of an element in G?

Activity 37.4 tells us that G, as defined above, is a group under the operation from (37.2). We can actually say more about the group G, as stated in the following theorem.

Theorem 37.5. *Let H and K be groups with identities e_H and e_K, respectively, and let $\varphi : K \to Aut(H)$ be a homomorphism. Then $G = \{(h, k) : h \in H, k \in K\}$ with the operation*

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2)$$

is a group. Moreover,

(i) *$H' = \{(h, e_K) : h \in H\}$ is a normal subgroup of G isomorphic to H;*

(ii) *$K' = \{(e_H, k) : k \in K\}$ is a subgroup of G isomorphic to K; and*

(iii) *$H' \cap K' = \{(e_H, e_K)\}$.*

Proof. Since Activity 37.4 shows that G is a group, we will focus here on parts (i) – (iii). In particular, we will prove part (i) and leave the remaining parts for the reader in Exercise (4).

We will show that $H' = \{(h, e_K) : h \in H\}$ is a normal subgroup of G isomorphic to H. The

element (e_H, e_K) is in H', so H' contains the identity element in G. Let (h_1, e_K) and (h_2, e_K) be in H'. Then

$$(h_1, e_K)(h_2, e_K) = (h_1, \varphi(e_K)(h_2), e_K) = (h_1 h_2, e_K) \in H',$$

and so H' is closed under the operation in G.

Also,

$$(h_1, e_K)^{-1} = \left(\varphi\left(e_K^{-1}\right)\left(h_1^{-1}\right), e_K^{-1}\right) = \left(h_1^{-1}, e_K\right) \in H',$$

and so H' is a subgroup of G by the Subgroup Test. (See page 279.)

To show that H' is a normal subgroup of G, let $(h, e_K) \in H'$ and let $g = (a, b) \in G$. Then

$$\begin{aligned}(a,b)^{-1}(h,e_K)(a,b) &= \left(\varphi\left(b^{-1}\right)\left(a^{-1}\right), b^{-1}\right)(h\varphi(e_K)(a), b) \\ &= \left(\varphi\left(b^{-1}\right)\left(a^{-1}\right)\varphi\left(b^{-1}\right)(ha), b^{-1}b\right) \\ &= \left(\varphi\left(b^{-1}\right)\left(a^{-1}\right)\varphi\left(b^{-1}\right)(ha), e_K\right)\end{aligned}$$

and $(a, b)^{-1}(h, e_K)(a, b) \in H'$. Therefore, $g^{-1}H'g = H'$ and $H' \triangleleft G$.

That H' is isomorphic to H can be shown by considering the mapping $\alpha : H \to H'$ defined by $\alpha(h) = (h, e_K)$. Let $h_1, h_2 \in H$. Then

$$\alpha(h_1 h_2) = (h_1 h_2, e_K) = (h_1, e_K)(h_2, e_K) = \alpha(h_1)\alpha(h_2),$$

and α is a homomorphism. If $\alpha(h_1) = \alpha(h_2)$, then $(h_1, e_K) = (h_2, e_K)$ and $h_1 = h_2$. Thus, α is a monomorphism. If $(x, e_K) \in H'$, then $\alpha(x) = (x, e_K)$, and so α is an epimorphism. We have therefore shown that α is an isomorphism and $H \cong H'$.

■

The group G described in Theorem 37.5 is called the **semidirect product** of H and K and is denoted $H \rtimes_\varphi K$ to indicate its dependence on the particular homomorphism $\varphi : K \to \text{Aut}(H)$. When the homomorphism φ is clear from the context, we will simply write $H \rtimes K$.

Definition 37.6. Let H and K be groups, and let $\varphi : K \to \text{Aut}(H)$ be a homomorphism. The **semidirect product** of H and K with respect to φ is the group

$$H \rtimes_\varphi K = \{(h, k) : h \in H, k \in K\}$$

with the operation

$$(h_1, k_1)(h_2, k_2) = (h_1 \varphi(k_1)(h_2), k_1 k_2).$$

Why are semidirect products important? First, the direct product $H \oplus K$ is an example of a semidirect product (see Exercise (3)), so we can think of the semidirect product as an extension of the direct product. (This is also the main motivation for the notation $\rtimes$ for the semidirect product, as it is more general than the internal direct product.) Second, if φ is a nontrivial homomorphism, then the semidirect product $H \rtimes_\varphi K$ is a non-Abelian group (see Exercise (6)), so semidirect products provide a method for constructing non-Abelian groups. Semidirect products are also useful in classifying groups. For example, if H and K are subgroups of a group G so that H is normal in G, $H \cap K$ is trivial, and $|HK| = |G|$, then G will be isomorphic to a semidirect product $H \rtimes_\varphi K$ for some φ. The next activity makes this last point clear.

Activity 37.7. Let G be a group with identity e and subgroups H and K such that

(i) $H \triangleleft G$ and

(ii) $H \cap K = \{e\}$.

Let $\varphi : K \to \text{Aut}(H)$ be the mapping that sends each element $k \in K$ to the inner automorphism defined by conjugation by k. That is, let $\varphi(k) = \pi_k$, where $\pi_k(h) = khk^{-1}$. There is a natural function $\Phi : HK \to (H \rtimes_\varphi K)$. Define this function Φ and show that it is an isomorphism. Then explain how we have proved the following theorem:

Theorem 37.8. *Let G be a group with identity e and subgroups H and K with*

(i) $H \triangleleft G$ *and*

(ii) $H \cap K = \{e\}$.

Then $HK \cong (H \rtimes_\varphi K)$ for some homomorphism $\varphi : K \to Aut(H)$.

In the next section, we will use Theorem 37.8 to classify all groups of order 12 and all groups of order p^3, where p is a prime.

Groups of Order 12 and p^3

We will begin this section with groups of order 12. The Fundamental Theorem of Finite Abelian Groups tells us that the groups $\mathbb{Z}_{12}$ and $\mathbb{Z}_6 \oplus \mathbb{Z}_2$ are the distinct Abelian groups of order 12. We already know at least three non-Abelian groups of order 12—namely, D_6, A_4, and T, where T is described in Exercise (18) of Investigation 22 (see page 318) as having presentations $\langle s, t \mid s^6 = 1, s^3 = t^2, sts = t\rangle$ and $\langle x, y \mid x^4 = y^3 = 1, yxy = x\rangle$. We will now show that these three groups are, up to isomorphism, the only non-Abelian groups of order 12.

Let G be a non-Abelian group of order 12 with identity e. Since $12 = 2^2 \times 3$, G has a Sylow 3-subgroup H of order 3 and a Sylow 2-subgroup K of order 4. Since H is cyclic, $H = \langle h\rangle$ for some $h \in G$.

Define $\varphi : G \to P(G/H)$ by $\varphi(a) = \pi_a$ where $\pi_a(gH) = (ag)H$. Recall that G/H denotes the collection of left cosets of H in G (even if H is not normal in G) and $P(G/H)$ denotes the group of permutations of G/H. In Exercise (7) of Investigation 30 (see page 442), we showed that φ is a homomorphism. Now $[G : H] = 4$, and so $P(G/H) \cong S_4$. If φ is a monomorphism, then G is isomorphic to a subgroup of order 12 in S_4. The only such subgroup is A_4, and so $G \cong A_4$ in this case.

Now assume that $|\text{Ker}(\varphi)| > 1$. We will next show that $\text{Ker}(\varphi) \subseteq H$. Let $a \in \text{Ker}(\varphi)$. Then $\varphi(a) = \pi_a$ is the identity permutation in $P(G/H)$, so $H = \pi_a(H) = aH$ and $a \in H$. Thus, $\text{Ker}(\varphi) \subseteq H$. Because $|H| = 3$ and $|\text{Ker}(\varphi)| > 1$, it follows that $\text{Ker}(\varphi) = H$, and so $H \triangleleft G$.

We know that $H \cap K = \{e\}$ and that $|G| = |H||K|$, so $G = HK$. Theorem 37.8 shows us that $G \cong (H \rtimes_\varphi K)$ for some φ. Next we will determine the different groups of this form.

Since $|H| = 3$, we know that $H \cong \mathbb{Z}_3$. Recall from Exercise (34) of Investigation 26 (see page 390) that $\text{Aut}(\mathbb{Z}_3) \cong U_3$, so $|\text{Aut}(H)| = 2$. The two automorphisms of H are the identity automorphism π_0 and the automorphism π_1 defined by $\pi_1(h) = h^{-1} = h^2$. Since $|K| = 4$, there are two possibilities for K: $K \cong \mathbb{Z}_4$ and $K \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.

Case 1: $K \cong \mathbb{Z}_4$**.** In this case, we can identify K with $\mathbb{Z}_4$, and so any homomorphism φ from K to

Aut(H) is determined by its action on $[1]$. Thus, there are two possibilities: $\varphi([1]) = \pi_0$ and $\varphi([1]) = \pi_1$. In the first case, G will be Abelian and isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_4$. In the second case, the product in HK will have the form

$$(h_1k_1)(h_2k_2) = (h_1h_2^{-1})(k_1k_2).$$

In particular, we will have

$$(h^ik^j)(h^uk^v) = h^{i-j}k^{u+v}$$

for all i, j, u, and v. More specifically, $hkh = k$. So G has the presentation

$$\langle h, k \mid h^3 = k^4 = 1, hkh = k\rangle,$$

and $G \cong T$.

Case 2: $K \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$**.** In this case, we will identify K with $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and so any homomorphism from K to Aut(H) will be determined by its actions on the generators $([1], [0])$ and $([0], [1])$.

- Let $\varphi_0 : K \to \text{Aut}(H)$ be defined by

  $$\varphi_0(([1], [0])) = \pi_0 \text{ and } \varphi_0(([0], [1])) = \pi_0.$$

  Then G is Abelian and isomorphic to $\mathbb{Z}_3 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)$.
- Let $\varphi_1 : K \to \text{Aut}(H)$ be defined by

  $$\varphi_1(([1], [0])) = \pi_0 \text{ and } \varphi_1(([0], [1])) = \pi_1.$$

  Then

  $$\varphi_1(([a], [b])) = \varphi_1(a([1], [0]) + b([0], [1])) = \pi_0^a\pi_1^b = \pi_1^b.$$

  Note that $\pi_1^b(t) = t^{2^b}$. In this case, the product on HK is

  $$\begin{aligned}(h^i([a], [b]))(h^u([c], [d])) &= (h^i\pi_1^b(h^u))([a + c], [b + d])\\ &= h^{i+u2^b}([a + c], [b + d]).\end{aligned}$$

  Let $x = ([1], [0])$ in K. Then $(hx)^2 = (hx)(hx) = h^2$, $(hx)^3 = x$, $(hx)^4 = h$, $(hx)^5 = h^2x$, and $(hx)^6 = e$. So $|hx| = 6$, and $N = \langle hx\rangle$ is a subgroup of G of order 6. Since $[G : N] = 2$, it follows that $N \triangleleft G$. (See Exercise (19) on page 349.) Let $y = ([0], [1]) \in K$. Then $y^2 = e$, and so $G = N\langle y\rangle$. Note that

  $$y(hx)y^{-1} = y(hx)y = h^2([1], [1])y = h^2x = (hx)^{-1}.$$

  So G has presentation $\langle hx, y \mid (hx)^6 = y^2 = 1, y(hx)y^{-1} = (hx)^{-1}\rangle$. But this is exactly the presentation for D_6, and so $G \cong D_6$ in this case.
- Let $\varphi_2 : K \to \text{Aut}(H)$ be defined by

  $$\varphi_2(([1], [0])) = \pi_1 \text{ and } \varphi_2(([0], [1])) = \pi_0.$$

  In this case, we also have $G \cong D_6$, which is left as an exercise for you to verify. (See Exercise (5).)
- Let $\varphi_3 : K \to \text{Aut}(H)$ be defined by

  $$\varphi_3(([1], [0])) = \pi_1 \text{ and } \varphi_3(([0], [1])) = \pi_1.$$

  In this case, we again have $G \cong D_6$, which is left as an exercise for you to verify. (See Exercise (5).)

We can therefore conclude that the only non-Abelian groups of order 12 are D_6, A_4, and T.

Our classification of groups of order 12 demonstrates that two groups $H \rtimes_\alpha K$ and $H \rtimes_\beta K$ can be isomorphic even if $\alpha \neq \beta$. In general, it can be difficult to determine if two semidirect products with the same underlying groups are isomorphic or not. One tool is given in the next lemma (which we will use in our classification of groups of order p^3), and others are presented in Activity 37.10.

Lemma 37.9. *Let K be a finite cyclic group, and let H be any group. Let $\varphi_1 : K \to Aut(H)$ and $\varphi_2 : K \to Aut(H)$ be homomorphisms so that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $Aut(H)$. Then $(H \rtimes_{\varphi_1} K) \cong (H \rtimes_{\varphi_2} K)$.*

Proof. Since K is cyclic, there is an element k so that $K = \langle k \rangle$. The fact that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$ means that there exists $\delta \in \mathrm{Aut}(H)$ so that $\delta^{-1}\varphi_2(K)\delta = \varphi_1(K)$. So

$$\varphi_1(k) = \delta^{-1}\varphi_2(k^t)\delta$$

for some integer t. Then

$$\varphi_1(k)^i = \left(\delta^{-1}\varphi_2(k^t)\delta\right)^i,$$

and so

$$\begin{aligned}\varphi_1(k^i) &= \delta^{-1}\varphi_2(k^t)^i\delta \\ &= \delta^{-1}\varphi_2(k^i)^t\delta\end{aligned}$$

for any integer i. Thus,

$$\varphi_1(x) = \delta\varphi_2(x^t)\delta^{-1} \tag{37.3}$$

for all $x \in K$.

Since $K = \langle k \rangle$, it follows that $\mathrm{Im}(\varphi_1) = \langle \varphi_1(k) \rangle$ and $\mathrm{Im}(\varphi_2) = \langle \varphi_2(k) \rangle$. Since $\varphi_1(k)$ and $\varphi_2(k)$ are conjugate, it also follows that $|\mathrm{Im}(\varphi_1)| = |\mathrm{Im}(\varphi_2)|$. Thus, $|\varphi_1(k)| = |\varphi_2(k)|$. Equation (37.3) shows that $\varphi_1(k) = \delta^{-1}\varphi_2(k)^t\delta$, and so $|\varphi_2(k)| = |\varphi_1(k)| = |\varphi_2(k)^t|$. Thus, $\gcd(|\varphi_1(K)|, t) = 1$. Since $|\varphi_1(K)|$ divides $|K|$, Exercise (12) shows that there is an integer t' with $t' \equiv t \pmod{|\varphi_1(K)|}$ and $\gcd(t', |K|) = 1$. Since $\varphi_2(x^t) = \varphi_2(x)^t = \varphi_2(x)^{t'} = \varphi_2(x^{t'})$ for all $x \in K$, we can replace t with t' in (37.3). This allows us to assume without loss of generality that $\gcd(t, |K|) = 1$, and so there exist integers x and y with $x|K| + yt = 1$.

Define $\Psi : (H \rtimes_{\varphi_1} K) \to (H \rtimes_{\varphi_2} K)$ by $\Psi((a, b)) = (\delta(a), b^t)$. To show that Ψ is a homomorphism, let (a_1, b_1) and (a_2, b_2) be in $H \times K$. Let $\cdot_1$ denote the operation in $H \rtimes_{\varphi_1} K$, and let $\cdot_2$ denote the operation in $H \rtimes_{\varphi_2} K$. Then

$$\begin{aligned}\Psi((a_1, b_1) \cdot_1 (a_2, b_2)) &= \Psi((a_1\varphi_1(b_1)(a_2), b_1b_2)) \\ &= (\delta(a_1\varphi_1(b_1)(a_2)), (b_1b_2)^t) \\ &= (\delta(a_1(\delta^{-1}\varphi_2(b_1^t)\delta)(a_2)), b_1^tb_2^t) \\ &= (\delta(a_1)\delta((\delta^{-1}\varphi_2(b_1^t)\delta)(a_2)), b_1^tb_2^t) \\ &= (\delta(a_1)\varphi_2(b_1^t)(\delta(a_2)), b_1^tb_2^t) \\ &= (\delta(a_1), b_1^t) \cdot_2 (\delta(a_2), b_2^t) \\ &= \Psi((a_1, b_1)) \cdot_2 \Psi((a_2, b_2)),\end{aligned}$$

and Ψ is a homomorphism.

To show that Ψ is a monomorphism, suppose $(a, k^r) \in \mathrm{Ker}(\Psi)$. Let e_H be the identity in H, and let e_K be the identity in K. Then

$$(e_H, e_K) = \Psi((a, k^r)) = (\delta(a), k^{rt}),$$

and so $\delta(a) = e_H$ and $k^{rt} = e_K$. Since $\delta \in \text{Aut}(H)$, we can conclude that $a = e_H$. That $k^{rt} = e_K$ means $|K|$ divides rt. But $\gcd(t, |K|) = 1$ implies that $|K|$ divides r. Thus, $k^r = e_K$, and so (a, k^r) is the identity in $H \rtimes_{\varphi_1} K$. Therefore, $\text{Ker}(\Psi)$ is trivial and Ψ is a monomorphism.

Finally, we will demonstrate that Ψ is an epimorphism. Let $(w, z) \in (H \rtimes_{\varphi_2} K)$. Since δ^{-1} is a surjection, there exists $a \in H$ such that $\delta^{-1}(a) = w$. Recall that $x|K| + yt = 1$, so

$$z = z^{x|K|+yt} = \left(z^{|K|}\right)^x (z^y)^t = (z^y)^t .$$

Then

$$\Psi\left((\delta^{-1}(a), z^y)\right) = (w, z),$$

and we have shown that Ψ is an epimorphism. Therefore, Ψ is an isomorphism, and $(H \rtimes_{\varphi_1} K) \cong (H \rtimes_{\varphi_2} K)$.

■

We will end this investigation by classifying all groups of order p^3, where p is a prime. Doing so will illustrate the fact that it is not necessarily the size of a group that makes classification difficult, but rather how large the powers of the prime divisors of the order are. In working out the classification, we will leave a number of details for you to complete in the exercises. Since we have already classified the groups of order 8, we will restrict ourselves to odd primes.

Let G be a group of order p^3, where p is an odd prime. We know the Abelian groups of order p^3 by the Fundamental Theorem of Finite Abelian Groups: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$, and $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Therefore, we will now focus on the non-Abelian groups of order p^3.

Let G be a non-Abelian group of order p^3. Since G is a p-group, we know that $Z = Z(G)$ is nontrivial. Since G is non-Abelian, there are two possibilities for $|Z|$: $|Z| = p$ or $|Z| = p^2$. If $|Z| = p^2$, then $|G/Z| = p$ and so G/Z is cyclic. It follows then that G is Abelian (see Theorem 24.10 on page 338), a contradiction. We can therefore conclude that $|Z| = p$. Thus, $|G/Z| = p^2$, and so $G/Z \cong \mathbb{Z}_{p^2}$ or $G/Z \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p)$. Since G/Z is not cyclic, it must be that $G/Z \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p)$.

Recall from Exercise (9) of Investigation 21 (see page 306) that the commutator of elements $x, y \in G$ is the element $[x, y] = x^{-1}y^{-1}xy$. Since G is non-Abelian, the subgroup G' generated by the commutators of pairs of elements is nontrivial. Let $x, y \in G$. Then $xZ, yZ \in G/Z \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p)$ (an Abelian group), and so

$$Z = (xZ)^{-1}(yZ)^{-1}(xZ)(yZ) = (x^{-1}y^{-1}xy)Z.$$

This, however, implies that $x^{-1}y^{-1}xy \in Z$. Thus, $G' \subseteq Z$, and so $G' = Z$.

Define $\psi : G \to G$ by $\psi(g) = g^p$. That ψ is a homomorphism can be demonstrated as follows. Let $a, b \in G$. Since $G' = Z$, the commutators commute with every element in G. Exercise (8) and the fact that every nonidentity element in Z has order p show that

$$\begin{aligned}
\psi(a)\psi(b) &= a^p b^p \\
&= (ab)^p [a, b]^{p(p-1)/2} \\
&= (ab)^p \left([a, b]^{(p-1)/2}\right)^p \\
&= (ab)^p \\
&= \psi(ab),
\end{aligned}$$

and ψ is a homomorphism. Moreover, we can again use the fact that every nonidentity element in G/Z has order p to see that

$$Z = (aZ)^p = a^p Z,$$

and so $a^p \in Z$ for every $a \in G$. Thus, $\text{Im}(\psi) \subseteq Z$.

Now consider $\text{Ker}(\psi)$. If every nonidentity element in G has order p, then $\text{Ker}(\psi) = G$. Otherwise, G contains an element of order p^2. We will consider each of these cases. Let e be the identity in G.

Case 1: There is an element h of order p^2 in G. Let $H = \langle h \rangle$. It follows that $H \cap Z = \langle h^p \rangle$. By Exercise (7), we have that H is normal in G. If we can find a subgroup K of G so that $G = HK$, then we will have $G \cong (H \rtimes_\varphi K$ for some φ.

Since $h^p \neq e$, we have $\text{Ker}(\psi) \neq G$. So $|\text{Im}(\psi)| > 1$, and it follows that $\text{Im}(\psi) = Z$. Thus, $|\text{Ker}(\psi)| = p^2$. Since $h \notin \text{Ker}(\psi)$, we have that $\text{Ker}(\psi) \neq H$. Let k be any element of $\text{Ker}(\psi)$ such that $k \notin H$, and let $K = \langle k \rangle$. Note that $e = \psi(k) = k^p$, so $|k| = p$. Since every nonidentity element in K generates K, it follows that $H \cap K = \{e\}$, and so $G = HK$. Thus, $G \cong (\mathbb{Z}_{p^2} \rtimes_\varphi \mathbb{Z}_p)$ for some nontrivial $\varphi : \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_{p^2})$. Now

$$\text{Aut}(\mathbb{Z}_{p^2}) \cong U_{p^2} \cong \mathbb{Z}_{p^2-p}$$

by Theorem 31.9 (see page 452), so $\text{Aut}(\mathbb{Z}_{p^2})$ contains a unique subgroup of order p. (In fact, $\text{Aut}(\mathbb{Z}_{p^2}) = \langle \gamma \rangle$, where $\gamma([x]) = (1+p)[x]$.) Lemma 37.9 then shows that the mappings $\varphi : \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_{p^2})$ will all produce isomorphic groups, and so there is just one non-Abelian group G of order p^3 if G contains an element of order p^2.

Case 2: Every nonidentity element in G has order p. Every p-group contains normal subgroups of any order dividing the order of the group (see Exercise (25) on page 433 of Investigation 29), so let H be a normal subgroup of G of order p^2. Since no element in G has order p^2, it must be the case that $H \cong (\mathbb{Z}_p \oplus \mathbb{Z}_p)$. Let a and b be generators for H so that $|a| = |b| = p$ and $H = \langle a \rangle \langle b \rangle$. Let $k \in G$ with $k \notin H$, and let $K = \langle k \rangle$. Again, $H \cap K = \{e\}$ and so $G = HK$. Thus, $G \cong (H \rtimes_\varphi K)$ for some nontrivial $\varphi : K \to \text{Aut}(H)$. (Note that $|k| = p$.) Now $\text{Aut}(H) \cong \text{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p) \cong \text{GL}_2(\mathbb{Z}_p)$, and $|\text{Aut}(H)| = p^4 - p^3 - p^2 + p = p(p^3 - p^2 - p + 1)$. (See Exercise (10).) The Sylow p-subgroups of $\text{Aut}(H)$ all have order p, so any two subgroups of $\text{Aut}(H)$ of order p are conjugate.

Define $\gamma \in \text{Aut}(H) = \langle a \rangle \langle b \rangle$ by $\gamma(a) = ab$ and $\gamma(b) = b$. Since every non-identity element in H has order p, it follows that $|\gamma| = p$, and so any Sylow p-subgroup of $\text{Aut}(H)$ is conjugate to $\gamma(K)$. (We can also represent γ as an element in $\text{GL}_2(\mathbb{Z}_p)$ as $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.) Lemma 37.9 again shows that there is exactly one non-Abelian group of order p^3 of this type. This group is the Heisenberg group we introduced in Exercise (9) of Investigation 26. (See page 387.)

So the groups of order p^3, for p an odd prime, are:

- $\mathbb{Z}_{p^3}$;
- $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$;
- $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$;
- $\mathbb{Z}_{p^2} \rtimes_\varphi \mathbb{Z}_p$, where $\varphi([1]) = \gamma$ with $\gamma([x]) = (1+p)[x]$; and
- $(\mathbb{Z}_p \oplus \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_p$, where $\varphi([1]) = \gamma$ with γ represented by the matrix transformation $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Concluding Activities

Activity 37.10. Let H and K be finite groups, and let φ_1 and φ_2 be homomorphisms from K to Aut(H). It can be a difficult task to determine if $H \rtimes_{\varphi_1} K$ is isomorphic to $H \rtimes_{\varphi_2} K$.

(a) If φ_1 and φ_2 act in a similar way on elements of K, then we might expect the corresponding semidirect products to be isomorphic. Show that if $\varphi_1 = \varphi_2\theta$ for some $\theta \in$ Aut(K), then $(H \rtimes_{\varphi_1} K) \cong (H \rtimes_{\varphi_2} K)$.

(b) If φ_1 and φ_2 are significantly different in some way, we should expect that $H \rtimes_{\varphi_1} K$ is not isomorphic to $H \rtimes_{\varphi_2} K$. In this part we will show that if $\gcd(|H|, |K|) = 1$ and Ker$(\varphi_1) \ncong$ Ker(φ_2), then $H \rtimes_{\varphi_1} K$ is not isomorphic to $H \rtimes_{\varphi_2} K$. Let e_H be the identity in H, and let e_K be the identity in K. Then let $H' = \{(h, e_K) : h \in H\}$ and $K' = \{(e_H, k) : k \in K\}$ be subgroups of $H \rtimes_{\varphi_1} K$ that are copies of H and K. For $h \in H$, let $h' = (h, e_K)$ and for $k \in K$, let $k' = (e_H, k)$.

(i) Show that Ker$(\varphi_1) = \{x \in K : x'h'(x')^{-1} = h' \text{ for all } h' \in H'\}$. In other words, Ker$(\varphi_1) \cong C_{K'}(H')$.

(ii) Assume that $\gcd(|H|, |K|) = 1$ throughout the remainder of this exercise. Show that H' is the only subgroup of order $|H|$ in $G_1 = H \rtimes_{\varphi_1} K$.

(iii) Prove that if $H \rtimes_{\varphi_1} K$ is isomorphic to $H \rtimes_{\varphi_2} K$, then Ker$(\varphi_1) \cong$ Ker(φ_2). This will show that if Ker$(\varphi_1) \ncong$ Ker(φ_2), then $(H \rtimes_{\varphi_1} K) \ncong (H \rtimes_{\varphi_2} K)$.

Exercises

(1) Let $H = \mathbb{Z}_n$ and $K = \mathbb{Z}_2$. Let $\varphi : K \to$ Aut(H) be defined by $\varphi([1]_2) = \pi$, where $\pi([x]) = -[x]$ for all $x \in H$. Show that $(H \rtimes_\varphi K) \cong D_n$.

(2) Can the group $\mathbf{Q} = \{\pm 1, \pm i, \pm j, \pm k\}$ of quaternions be written as a semidirect product of proper subgroups? Explain.

⋆ (3) **Direct sums and semidirect products.** The direct sum of two groups is a special case of the semidirect product, as this exercise illustrates. Let H and K be groups with identities e_H and e_K, respectively, and let $\varphi : K \to$ Aut(H) be a homomorphism. Show that the following are equivalent.

(a) The map $\Phi : (H \rtimes_\varphi K) \to (H \oplus K)$ defined by $\Phi((h, k)) = hk$ is an isomorphism.

(b) The homomorphism φ is the trivial homomorphism.

(c) The subgroup $K' = \{(e_H, k) : k \in K\}$ is normal in $H \rtimes_\varphi K$.

⋆ (4) Prove the remaining items from Theorem 37.5. That is, prove that

(ii) $K' = \{(e_H, k) : k \in K\}$ is a subgroup of G isomorphic to K and

(iii) $H' \cap K' = \{(e_H, e_K)\}$.

⋆ (5) Complete the classification of groups of order 12 by showing that $(\mathbb{Z}_3 \rtimes_{\varphi_2} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)) \cong D_3$ and that $(\mathbb{Z}_3 \rtimes_{\varphi_3} (\mathbb{Z}_2 \oplus \mathbb{Z}_2)) \cong D_3$, where φ_2 and φ_3 are as described in that section.

⋆ (6) When is $H \rtimes_\varphi K$ an Abelian group? Prove your answer. (Hint: Exercise (3) might be helpful.)

⋆ (7) Let G be a finite group of order n, and let p be the smallest prime divisor of n. Prove that any subgroup of index p in G is normal in G. (Hint: Consider the homomorphism $\pi : G \to P(G/N)$ defined by $\pi(a)(gN) = (ag)N$, where N is a subgroup of G of index p.)

⋆ (8) Let G be any group, and let $x, y \in G$ so that x and y commute with $[x, y] = x^{-1}y^{-1}xy$. Prove that

$$x^n y^n = (xy)^n [x, y]^{n(n-1)/2}$$

for every nonnegative integer n.

(9) **Groups of order pq.** We have previously shown that any group of order pq is cyclic if p and q are distinct primes and p does not divide $q - 1$. We will now classify the rest of the groups of order pq. Let p and q be primes with $p < q$ so that p divides $q - 1$, and let G be a group of order pq. Determine all of the groups to which G could be isomorphic.

⋆ (10) Let p be a prime. Explain why $\mathrm{Aut}(\mathbb{Z}_p \oplus \mathbb{Z}_p) \cong \mathrm{GL}_2(\mathbb{Z}_p)$. Then show that the order of $\mathrm{GL}_2(\mathbb{Z}_p)$ is $p^4 - p^3 - p^2 + p$. (Hint: Use the result from linear algebra that a 2×2 matrix is invertible if and only if no row is a multiple of the other.)

(11) Our definition of a semidirect product requires two groups. In this exercise, we will introduce a useful construction of a semidirect product that uses only one group. Let H be any group, and let $K = \mathrm{Aut}(H)$. Define $\varphi : K \to \mathrm{Aut}(H)$ by $\varphi(\pi) = \pi$. The resulting semidirect product $H \rtimes_\varphi K$ is called the **holomorph** of H and is denoted $\mathrm{Hol}(H)$. Holomorphs provide a context in which to study elements of a group and their automorphisms together.

(a) Let $n \geq 2$ be an integer. Find $|\mathrm{Hol}(\mathbb{Z}_n)|$ in terms of the prime factors of n. (Hint: See Exercise (13) on page 461 of Investigation 31.)

(b) Create the operation table for $\mathrm{Hol}(\mathbb{Z}_3)$. To which familiar group is $\mathrm{Hol}(\mathbb{Z}_3)$ isomorphic?

(c) Let $H = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $K = \mathrm{Aut}(H)$, and $G = \mathrm{Hol}(H)$. Show that $G \cong S_4$ using the following steps.

(i) Determine the order of $\mathrm{Hol}(\mathbb{Z}_2 \oplus \mathbb{Z}_2)$

(ii) For ease of notation, we will identify K with the subgroup of G that is isomorphic to K. Note that $[G : K] = 4$, so the permutation group $P(G/K)$ of the left cosets of K in G is isomorphic to S_4. Now define $\theta : G \to P(G/K)$ by $\theta(g)(aK) = (ga)K$. We have shown that θ is a homomorphism, so if we can show that θ is a bijection, then we will have that $G \cong S_4$. Prove that θ is a monomorphism. How can we conclude that $G \cong S_4$?

⋆ (12) Let t, m, and n be integers such that m divides n and $\gcd(t, m) = 1$. Prove that there exists an integer t' such that $t' \equiv t \pmod{m}$ and $\gcd(t', n) = 1$.

(13) (a) There are two distinct semidirect products of the form $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$. What are they? Construct the operation table for the non-Abelian one. To which familiar group is this non-Abelian semidirect product isomorphic?

(b) Let $n \geq 3$ be an integer. Show that $D_n \cong (\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2)$ for some appropriate choice of φ.

(14) **Groups of order pq^2.**

(a) Construct a non-Abelian group of order 75.

(b) Determine all non-Abelian groups of order 75.

(c) Determine all groups of order pq^2, where p and q are primes with $p < q$ such that p does not divide $q - 1$.

(15) Classify all groups of order 20.

(16) **Groups of order $2p^2$.** Let p be an odd prime. In this exercise, we work on the general problem of classifying all groups of order $2p^2$.

(a) Use the steps suggested below to determine the conjugacy classes of the elements of order 2 in $\mathrm{GL}_2(\mathbb{F}_p)$.

(i) Show that every element of order 2 or less in $\mathrm{GL}_2(\mathbb{F}_p)$ is conjugate to a diagonal matrix with 1's and/or -1's along the diagonal.

(ii) If A is an element of order 2 in $\mathrm{GL}_2(\mathbb{F}_p)$, show that A is conjugate to either $-I$ or the matrix $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

(b) Classify all groups of order $2p^2$. Note that there are three non-Abelian groups, and you may not be able to easily distinguish them. You might try to show that they have different centers. Part (a) of this exercise and Activity 37.10 should be useful.

Connections

This investigation continued our classification of groups of various orders that we began in Investigation 26. The tools we used in this investigation were mostly familiar, with the exception of the new construction of the semidirect product, an extension of the direct product first discussed in Investigation 25.