Extensions of Groups

1 Introduction

To better understand groups it is often useful to see how a group can be built from smaller groups. For example, given two groups $G$ and $H$, we can form the direct product $G \times H$. This new group can be studied in terms of the two pieces from which it is built. However, the direct product construction is too special to understand most groups. In other words, most groups are not expressible as the direct product of two nontrivial groups. In this note we will consider the general problem of how to build a group from two other groups. To motivate what we do, if $E = G \times H$, then we can view $H$ as a subgroup of $E$. In fact, $H$, or more precisely $\{e\} \times H$, is the kernel of the projection homomorphism $\pi : E \to G$. Therefore, $G \cong E/H$. We can write this in terms of short exact sequences; we have a short exact sequence $1 \to H \to E \xrightarrow{\pi} G \to 1$.

Definition 1.1. Let $K$ and $G$ be groups. An extension of $K$ by $G$ is a short exact sequence $1 \to K \to E \to G \to 1$.

We will be somewhat loose in our terminology at times, referring to $E$ as an extension instead of the short exact sequence. If $E$ is an extension of $K$ by $G$, then $K$ is isomorphic to a normal subgroup of $E$, and by identifying $K$ with this subgroup, we have $E/K \cong G$.

Example 1.2. The group $\mathbb{Z}_6$ is an extension of $\mathbb{Z}_3$ by $\mathbb{Z}_2$ since we have the exact sequence $1 \to \mathbb{Z}_3 \xrightarrow{i} \mathbb{Z}_6 \xrightarrow{\pi} \mathbb{Z}_2 \to 1$, where $i$ is defined by $i(\bar{a}) = 2\bar{a}$ and $\pi$ is defined by $\pi(\bar{a}) = \bar{a}$. Note that we are writing bars for equivalence classes modulo three different integers. The group $S_3$ is also an extension of $\mathbb{Z}_3$ by $\mathbb{Z}_2$; by defining $i : \mathbb{Z}_3 \to S_3$ by $i(\bar{a}) = (123)^a$ and $\pi : S_3 \to \mathbb{Z}_2$ by $\pi(\sigma) = \text{sgn}(\sigma) \mod 2$, we have an exact sequence $1 \to \mathbb{Z}_3 \xrightarrow{i} S_3 \xrightarrow{\pi} \mathbb{Z}_2 \to 1$.

Similarly, $\mathbb{Z}_4$ is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$, since the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_2$, and the quotient of $\mathbb{Z}_4$ by this group is isomorphic to $\mathbb{Z}_2$. Furthermore, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is also an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$. These examples indicate that, for fixed groups $K$ and $G$, there can be several extensions of $K$ by $G$.

Example 1.3. For any integer $n$, the group $S_n$ is an extension of $A_n$ by $\mathbb{Z}_2$, since $S_n/A_n \cong \mathbb{Z}_2$. The Dihedral group $D_n$ is an extension of $\mathbb{Z}_n$ by $\mathbb{Z}_2$ since if $D_n = \langle r, f \rangle$ with $r^n = f^2 = 1$ and $frf = r^{-1}$, then $R = \langle r \rangle$ is a normal subgroup of $D_n$ isomorphic to $\mathbb{Z}_n$, and $D_n/R \cong \mathbb{Z}_2$. 


Example 1.4. Let \( Q \) be the quaternion group. Then \( Q = \{ \pm 1, \pm i, \pm j, \pm k \} \). If \( K = \langle i \rangle \), then \( K \cong \mathbb{Z}_4 \) is a subgroup of order 4, so \( [Q : K] = 2 \). Thus, \( K \) is normal in \( Q \). Since \( Q/K \cong \mathbb{Z}_2 \), the quaternion group is an extension of \( \mathbb{Z}_4 \) by \( \mathbb{Z}_2 \). The groups \( \mathbb{Z}_4 \times \mathbb{Z}_2 \) and \( \mathbb{Z}_8 \) are also extensions of \( \mathbb{Z}_4 \) by \( \mathbb{Z}_2 \).

Example 1.5. Let \( K \) and \( G \) be groups, and let \( \varphi : G \to \text{Aut}(K) \) be a group homomorphism. If \( E = K \rtimes \varphi G \) is the semidirect product obtained from this data, then \( E \) is an extension of \( K \) by \( G \); to see this, define \( i : K \to E \) by \( i(k) = (k, 1) \). Then \( i \) is a group homomorphism, since \( i(k_1k_2) = (k_1k_2, 1) = (k_1, 1)(k_2, 1) \). Also, there is a group homomorphism \( \pi : E \to G \) given by \( \pi(k, g) = g \). Since \( \ker(\pi) = \{(k, 1) : k \in K \} = \text{im}(i) \), the sequence \( 1 \to K \xrightarrow{i} E \xrightarrow{\pi} G \to 1 \) is exact, so \( E \) is indeed an extension of \( K \) by \( G \).

Example 1.6. Let \( \text{GL}_n(\mathbb{R}) \) be the group of all \( n \times n \) invertible matrices. The determinant map \( \text{det} : \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\ast \) is a surjective homomorphism, and its kernel is the group \( \text{SL}_n(\mathbb{R}) \) of all \( n \times n \) matrices of determinant 1. Thus, we have an extension \( 1 \to \text{SL}_n(\mathbb{R}) \to \text{GL}_n(\mathbb{R}) \to \mathbb{R}^\ast \to 1 \). In fact, \( \text{GL}_n(\mathbb{R}) \) is the semidirect product of \( \text{SL}_n(\mathbb{R}) \) by \( \mathbb{R} \) if \( n \) is odd; we view \( \mathbb{R}^\ast \) as a subgroup of \( \text{GL}_n(\mathbb{R}) \) as the group of all scalar matrices. This subgroup has trivial intersection with \( \text{SL}_n(\mathbb{R}) \) since the scalar matrix \( aI_n \) has determinant \( a^n \), which is 1 only if \( a = 1 \), when \( n \) is odd. The intersection is \( \{ \pm 1 \} \) if \( n \) is even, so \( \text{GL}_n(\mathbb{R}) \) is not the semidirect product of these two groups when \( n \) is even.

Many of the extensions above are semidirect products. For example, \( S_n \) is the semidirect product of \( A_n \) and \( \langle (12) \rangle \cong \mathbb{Z}_2 \), and \( D_n \) is the semidirect product of \( \langle r \rangle \cong \mathbb{Z}_n \) and \( \langle f \rangle \cong \mathbb{Z}_2 \). However, neither the quaternion group nor \( \mathbb{Z}_8 \) is a semidirect product of \( \mathbb{Z}_4 \) and \( \mathbb{Z}_2 \); to see this is to observe that we cannot find subgroups \( K \cong \mathbb{Z}_4 \) and \( G \cong \mathbb{Z}_2 \) inside either with \( K \cap G = 1 \).

2 Cocycles

As we will see, semidirect products represent a relatively easy way to build an extension. We wish to work with extensions in general. The theory of extensions generally is broken into two cases, \( K \) Abelian and \( K \) non-Abelian. We will restrict to \( K \) Abelian; thus, \( K \) will always denote an Abelian group. If \( E \) is an extension of \( K \) by \( G \), we will produce a homomorphism \( \varphi : G \to \text{Aut}(K) \) in spirit like for semidirect products, but we will construct a fourth object \( f \); we will see that the four objects \( K, G, \varphi, \) and \( f \) completely determine \( E \). To begin, if \( E \) is an extension of \( K \) by \( G \), we fix the short exact sequence \( 1 \to K \to E \xrightarrow{\pi} G \to 1 \) and we identify \( K \) as a subgroup of \( E \) by identifying \( K \) with its isomorphic image in \( E \). The map \( \pi \) is surjective. Thus, for every \( g \in G \) there is an element \( e_g \in E \) with \( \pi(e_g) = g \). In other words, there is a function \( l : G \to E \) with \( \pi \circ l = \text{id} \), and \( e_g = l(g) \). The element \( e_g \) is not uniquely determined by \( G \); in fact, the set \( \{ x : \pi(x) = g \} \) is equal to \( \{ ke_g : k \in K \} \), since \( K = \ker(\pi) \). Thus, \( e_g \) is only determined up to multiplication by an element of \( K \). While it is not absolutely necessary to do so, we make the choice \( e_1 = 1 \); this will cut down some on
technical details later. The function \( l \) need not be a group homomorphism, as we show with an example.

**Example 2.1.** With the quaternion group \( Q \) mentioned above, if \( \pi : Q \to \mathbb{Z}_2 \) has kernel \( K = \langle i \rangle \) and sends \( j \) to \( \overline{1} \), then we may define \( l \) by \( l(\overline{0}) = i \) and \( l(\overline{1}) = j \). Then \( l(\overline{1} + \overline{1}) = l(\overline{0}) = i \), while \( l(\overline{1})l(\overline{1}) = j^2 = -1 \). Thus, \( l \) is not a group homomorphism.

Given the setup before the example, we define a map \( G \to \text{Aut}(K) \) by \( \varphi(g) : k \mapsto e_g k e_g^{-1} \). In other words, \( \varphi(g) \) is the restriction to \( K \) of the inner automorphism of \( e_g \). We show that \( \varphi(g) \) does not depend on the choice of \( g \).

**Lemma 2.2.** Suppose that \( e_g, e'_g \in E \) both map to \( g \) under \( \pi \). Then \( e_g k e_g^{-1} = e'_g k (e'_g)^{-1} \) for all \( k \in K \).

**Proof.** Let \( k \in K \). Since \( \pi(e_g) = \pi(e'_g) \), the element \( e_g^{-1} e'_g \in \ker(\pi) = K \). Thus, because \( K \) is Abelian, \( (e_g^{-1} e'_g) k = k (e_g^{-1} e'_g) \). Multiplying both sides on the left by \( e_g \) and on the right by \( (e'_g)^{-1} \) yields the result. \( \square \)

Because of the lemma we have a well defined map \( \varphi : G \to \text{Aut}(G) \), such that \( \varphi(g) : k \mapsto e_g k e_g^{-1} \). For ease of notation we will write \( \varphi_g \) in place of \( \varphi(g) \). It is clear that \( \varphi \) is a group homomorphism. Note that if \( E \) is Abelian, then \( \varphi_g = \text{id} \) for every \( g \in G \). We will often call \( \varphi \) an *action*. To understand the use of this term, the group \( \text{Aut}(K) \) is a subgroup of the group \( \text{Perm}(K) \) of permutations of the set \( G \). We can view \( \varphi \) as a homomorphism \( G \to \text{Perm}(K) \); this says that the group \( G \) acts on the set \( K \). Since \( \varphi \) has its image in \( \text{Aut}(K) \), we can further refine our terminology to say that \( G \) acts on \( K \) as group automorphisms. Moreover, with some knowledge of group rings, it follows that having an action \( \varphi : G \to \text{Aut}(K) \) is equivalent to making \( K \) a module over the group ring \( \mathbb{Z}[G] \).

Suppose that \( \varphi : G \to \text{Aut}(K) \) is an action. With \( K \), \( G \), and \( \varphi \), we have the appropriate data to define the semidirect product \( K \rtimes_{\varphi} G \). However, this is only one possible extension of \( K \) by \( G \). To determine all extensions we need more data. Define \( f : G \times G \to K \) by

\[
f(g, h) = e_g e_h e_{gh}^{-1} = l(g)l(h)l(gh)^{-1}.
\]

Thus, we see that \( l \) is a group homomorphism if and only if \( f(g, h) = 1 \) for all \( g, h \in G \). Thus, in some sense, \( f \) measures how far \( l \) is from being a group homomorphism. Note that \( f(g, h) \) is an element of \( K \) since \( \pi(f(g, h)) = \pi(e_g e_h e_{gh}^{-1}) = gh(gh)^{-1} = 1 \). The function \( f \) is called a \( 2\)-cocycle, or a *factor set*. We record the main properties of this function.

**Lemma 2.3.** Let \( f \) be the \( 2\)-cocycle defined above. Then \( f(1, g) = f(g, 1) = 1 \) for all \( g \in G \). Furthermore, for all \( g, h, k \in G \), we have

\[
f(g, h)f(gh, k) = \varphi_g(f(h, k)) f(g, hk).
\] (1)
Proof. The first statement follows from the assumption that \( e_1 = 1 \), since \( f(1, g) = e_1 e_g e_g^{-1} = 1 \) and \( f(g, 1) = e_g e_1 e_g^{-1} = 1 \). The second follows from associativity in \( E \); we compute both sides of the equation \( (e_g e_h) e_k = e_g (e_h e_k) \). To help us do this, we note that since \( f(g, h) = e_g e_h e_g^{-1} \), we have \( e_g e_h = f(g, h) e_h \). The left hand side is

\[
(e_g e_h) e_k = f(g, h) e_{gh} e_k = f(g, h) f(gh, k) e_{ghk}
\]

while the right hand side is

\[
e_g (e_h e_k) = e_g (f(h, k) e_{hk}) = e_g f(g, h) e_g^{-1} e_{gh} e_{hk} = \varphi_g(f(h, k)) e_g e_{hk}
\]

\[
= \varphi_g(f(h, k)) f(g, hk) e_{ghk}.
\]

Setting these two final expressions equal and cancelling \( e_{ghk} \) yields the second statement. \( \square \)

Equation 1 above is often called the 2-cocycle condition. As we saw in the proof, it is a consequence of associativity. This fact is very important, and 2-cocycles arise in several situations for similar reasons.

Because the choice of the \( e_g \) is not uniquely determined, the 2-cocycle \( f \) is not uniquely determined. We next see how \( f \) depends on this choice. Recall that \( e_g \) is determined only up to multiplication by an element of \( K \).

Lemma 2.4. Suppose that \( e'_g = k_g e_g \) for some \( k_g \in K \). If \( f'(g, h) = e'_g e'_h (e'_{gh})^{-1} \), then \( f'(g, h) = (k_g \varphi_g(k_h) k_{gh}^{-1}) f(g, h) \).

Proof. This is simply a matter of computing. We have

\[
f'(g, h) = e'_g e'_h (e'_{gh})^{-1} = (k_g e_g) (k_h e_h) (k_{gh} e_{gh})^{-1} = (k_g e_g k_h e_h) e_{gh}^{-1} k_{gh}^{-1}
\]

\[
= (k_g e_g e_h e_k) e_{gh}^{-1} k_{gh}^{-1} = (k_g \varphi_g(k_h) f(g, h) e_{gh}) e_{gh}^{-1} k_{gh}^{-1}
\]

\[
= k_g \varphi_g(k_h) f(g, h) k_{gh}^{-1} = (k_g \varphi_g(k_h) k_{gh}^{-1}) f(g, h);
\]

the final equality holds since \( K \) is Abelian. \( \square \)

While these formulas look messy, things are not as bad as they seem. First of all, we point out that, given an element \( k_g \in K \) defined for each \( g \in G \), the function \( b(g, h) = k_g \varphi_g(k_h) k_{gh}^{-1} \) is a 2-cocycle; the verification of this easy fact is left as an exercise. We call a 2-cocycle of this form a 2-coboundary. The formula of the lemma can be written as \( f'(g, h) = b(g, h) f(g, h) \). Thus, \( f' \) is the product of two 2-cocycles. In fact, if \( f_1 \) and \( f_2 \) are arbitrary 2-cocycles, then the point-wise product \( f_1 f_2 \), defined by \( (f_1 f_2)(g, h) = f_1(g, h) f_2(g, h) \), is a 2-cocycle; all this uses is that \( K \) is Abelian. Moreover, if \( f \) is a 2-cocycle, then we may define \( f^{-1} \) by \( f^{-1}(g, h) = f(g, h)^{-1} \), and \( f^{-1} \) is easily seen to be a 2-cocycle. Thus, the set of 2-cocycles forms an Abelian group under this point-wise multiplication. Furthermore, the set of 2-coboundaries forms a subgroup. The identity cocycle is the cocycle \( c \) with \( c(g, h) = 1 \) for all \( g, h \in G \).
Definition 2.5. We denote by $Z^2(G, K)$ the group of all 2-cocycles $G \times G \to K$ and by $B^2(G, K)$ the subgroup of all 2-coboundaries. The quotient group

$$H^2(G, K) = Z^2(G, K)/B^2(G, K)$$

is called the second cohomology group of $G$ with coefficients in $K$.

An important point we need to make about the notation is that the definition of a cocycle depends on the homomorphism $\varphi : G \to \text{Aut}(K)$. We need to be aware that our notation does not indicate this dependence. The previous lemma says that two cocycles obtained from different choices of preimages under $\pi$ of elements of $G$ differ by a 2-coboundary; thus, they represent the same class in $H^2(G, K)$. We point this out as a corollary.

Corollary 2.6. Let $E$ be an extension of $K$ by $G$. If we choose $e_g \in E$ mapping to $g \in G$, and define $\varphi : G \to \text{Aut}(K)$ by $\varphi(g)(k) = e_g k e_g^{-1}$ and $f : G \times G \to K$ by $f(g, h) = e_g e_h e_h^{-1}$, then the class of $f$ in the group $H^2(G, K)$ is uniquely determined, independent of the choice of the $e_g$.

We give some examples of finding the cocycle corresponding to an extension. To avoid confusing the notation, we will write all of our groups multiplicatively. Thus, to work with cyclic groups we will write $C_n$ for a cyclic group of order $n$.

Example 2.7. Consider the group $E = C_6 = \langle a \rangle$ as a group extension of $C_3 = \langle a^2 \rangle$ by $C_2 = C_6/C_3$. This quotient group is the set $\{\overline{1}, \overline{a}\}$. Because $E$ is Abelian, the homomorphism $\varphi : C_2 \to \text{Aut}(C_3)$ is the trivial homomorphism. We choose the function $l : C_2 \to C_6$ by $l(\overline{1}) = 1$ and $l(\overline{a}) = a$. In other words, $e_1 = 1$ and $e_\pi = a$. Let $f$ be the corresponding cocycle. We have $f(1, 1) = f(1, a) = f(a, 1) = 1$, and $f(\overline{a}, \overline{a}) = e_\pi e_\pi = e_1 = a^2$.

Example 2.8. Next, consider the group $E = C_3 \times C_2$ as an extension of $C_3$ by $C_2$. We identify $C_3$ with its isomorphic copy $C_3 \times \{1\}$ in $E$. Again, since $E$ is Abelian, $\varphi : C_2 \to \text{Aut}(C_3)$ is the trivial homomorphism. Write $C_3 = \langle a \rangle$ and $C_2 = \langle g \rangle$. We may choose $e_1 = (1, 1)$ and $e_g = (1, g)$. Thus, if $f$ is the corresponding cocycle, we have $f(1, 1) = f(1, g) = f(g, 1) = f(g, g)$; we have $f(g, g) = e_g e_g e_1 = (1, g)(1, g)(1, 1) = (1, g^2) = (1, 1)$. Therefore, $f$ is the trivial cocycle.

Example 2.9. Let $K$ and $G$ be groups, and let $\psi : G \to \text{Aut}(K)$ be a group homomorphism. Let $E = K \times_\psi G$ be the corresponding semidirect product. For $g \in G$, set $e_g = (1, g)$. Following our prescription for determining cocycles, we first obtain the homomorphism $\varphi : G \to \text{Aut}(K)$, given by $\varphi_g(k) = e_g k e_g^{-1}$. We are identifying $K = \{(k, 1) : k \in K\}$. Thus, this equation reads

$$\varphi_g(k, 1) = (1, g)(k, 1)(1, g)^{-1} = (1, g)(k, 1)(1, g^{-1}) = (\psi_g(k), g)(1, g^{-1})$$

$$= (\psi_g(k), 1).$$
Thus, \( \varphi_g = \psi_g \). In other words, \( \varphi = \psi \); we recover the original homomorphism. We next determine the cocycle \( f \). We have
\[
f(g, h) = e_g e_h e_{gh}^{-1} = (1, g)(1, h)(1, gh)^{-1} = (1, g)(1, h)(1, (gh)^{-1}) = (1, 1).
\]
Thus, \( f \) is the trivial cocycle.

We have seen that, given an extension of \( K \) by \( G \), we can produce an action \( \varphi : G \to \text{Aut}(K) \) and a cocycle \( f \in Z^2(G, K) \). We will show that this construction reverses. Before we do so, we show how \( E \) is determined by this data.

**Lemma 2.10.** Every element of \( E \) can be written uniquely in the form \( ke_g \) for some \( k \in K \) and \( g \in G \). Furthermore, \( (ae_g)(be_h) = a\varphi_g(b)f(g, h)e_{gh} \) for all \( a, b \in K \) and all \( g, h \in G \).

**Proof.** The first statement is easy, since if \( x \in E \), then set \( g = \pi(x) \). It follows that \( \pi(xe_g^{-1}) = 1 \), so \( xe_g^{-1} \in \ker(\pi) = K \). Writing \( xe_g^{-1} = k \in K \), we get \( x = ke_g \). Moreover, if \( ae_g = be_h \) for some \( a, b \in K \) and \( g, h \in G \). Applying \( \pi \), we get \( g = h \). Then, by cancelling \( e_g \), we get \( a = b \). This proves the uniqueness. For the second statement, we have
\[
(ae_g)(be_h) = ae_g be_g^{-1} e_g e_h = a\varphi_g(b)e_{gh},
\]
which finishes the proof. \( \square \)

Let \( K \) and \( G \) be groups together with a homomorphism \( \varphi : G \to \text{Aut}(K) \) and a cocycle \( f \in Z^2(G, K) \) relative to the action \( \varphi \). We define a group \( E_f \) as follows. As a set, we define \( E_f = K \times G \), and with multiplication given by the formula
\[
(a, g)(b, h) = (a\varphi_g(b)f(g, h), gh).
\]
This looks like the formula for a semidirect product except for the presence of \( f \). In fact, we see that if \( f(g, h) = 1 \) for all \( g, h \), then we recover \( K \rtimes \varphi G \). We leave it as an exercise to prove that \( E_f \) is a group. We do point out that associativity follows precisely from the 2-cocycle condition, the identity of \( E_f \) is \( (1, 1) \), and \( (a, g)^{-1} = (\varphi_{g^{-1}}(af(g^{-1}, g))^{-1}, g^{-1}) \). The assumption that \( f(1, g) = f(g, 1) = 1 \) actually makes the formula for the inverse easier than it would otherwise be. Moreover, we have an extension \( 1 \to K \to E_f \to G \to 1 \), by defining the map \( K \to E_f \) by \( k \mapsto (k, 1) \) and the map \( E_f \to G \) by \( (k, g) \mapsto g \). It is easy to check that this does result in a short exact sequence. Furthermore, by setting \( e_g = (1, g) \), a short exercise shows that the action of this extension is \( \varphi \) and the cocycle class is the class of \( f \).

We would like to show that extensions of \( K \) by \( G \) are in 1-1 correspondence with elements of \( H^2(G, K) \). This is not true. For one thing, to discuss \( H^2(G, K) \) requires fixing the action \( \varphi : G \to \text{Aut}(K) \). Second, distinct elements of \( H^2(G, K) \) do not correspond to distinct, up to isomorphism, groups. We will see this in an example shortly. To understand what \( H^2(G, K) \) represents, we give the following definition.
Two extensions \(1 \to K \xrightarrow{i} E \xrightarrow{\pi} G \to 1\) and \(1 \to K \xrightarrow{i'} E' \xrightarrow{\pi'} G \to 1\) are said to be equivalent if there is an isomorphism \(\sigma : E \to E'\) such that the following diagram commutes.

\[
\begin{array}{ccc}
1 & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \xrightarrow{\sigma} & E' & \xrightarrow{\pi'} & G & \xrightarrow{\text{id}} & 1 \\
\end{array}
\]

If two extensions are equivalent, then the middle groups are isomorphic. However, the following example shows that the middle groups may be isomorphic while the extensions are not equivalent. Therefore, equivalence of extensions is a more subtle notion than isomorphism of groups.

**Example 2.11.** We will see here that there are (at least) 3 equivalence classes of extensions of \(\mathbb{Z}_3\) by \(\mathbb{Z}_3\) while there are only two groups, up to isomorphism, that are extensions of \(\mathbb{Z}_3\) by \(\mathbb{Z}_3\). These groups are \(\mathbb{Z}_3 \times \mathbb{Z}_3\) and \(\mathbb{Z}_9\). The direct product \(\mathbb{Z}_3 \times \mathbb{Z}_3\) corresponds to the trivial cocycle. On the other hand, if \(E = \langle a \rangle\) is cyclic of order 9, then for \(i = 1, 2\), we get a group extension

\[
0 \to \langle a^3 \rangle \to \langle a \rangle \xrightarrow{\pi_i} \mathbb{Z}_3 \to 0
\]

of \(\mathbb{Z}_3\) by \(\mathbb{Z}_3\) by defining \(\pi_i(a) = i \mod 3\). We show that these two extensions are not equivalent. Suppose that \(\varphi : E \to E\) is an isomorphism with \(\varphi|_{\langle a^3 \rangle} = \text{id}\). We must have \(\varphi(a) = a^r\) for some \(r\) with \(\gcd(r, 9) = 1\). Then \(a^3 = \varphi(a^3) = a^{3r}\). This yields \(3r \equiv 3 \mod 9\), so \(r \equiv 1 \mod 3\). We then have \(\pi_2(\varphi(a)) = \pi_2(a^r) = 2r\) while \(\pi_1(a) = 1\). Since \(r \equiv 1 \mod 3\), it is not true that \(2r \equiv 1 \mod 3\). Thus, \(\pi_2 \circ \varphi \neq \pi_1\). Therefore, the two sequences are not equivalent. They are clearly not equivalent to the sequence \(0 \to \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \to 0\) since \(\mathbb{Z}_9\) is not isomorphic to \(\mathbb{Z}_3 \times \mathbb{Z}_3\).

Suppose that \(1 \to K \to E \to G \to 1\) is an extension whose action is \(\varphi\) and whose cocycle class is the class of \(f \in Z^2(G, K)\). From \(f\) we have seen how to construct a group \(E_f\) and an extension \(1 \to K \to E_f \to G \to 1\).

**Lemma 2.12.** Suppose that we have equivalent extensions according to the following diagram.

\[
\begin{array}{ccc}
1 & \xrightarrow{i} & E & \xrightarrow{\pi} & G & \xrightarrow{\sigma} & E' & \xrightarrow{\pi'} & G & \xrightarrow{\text{id}} & 1 \\
\end{array}
\]

Then the action \(G \to \text{Aut}(K)\) is the same for both extensions, and the cocycles describing the two extensions have the same class in \(H^2(G, K)\).

**Proof.** Choose \(e_g \in E\) with \(\pi(e_g) = g\), and set \(e'_g = \sigma(e_g) \in E'\). Then \(\pi'(e'_g) = \pi'(\sigma(e_g)) = \pi(e_g) = g\). Thus, we can built our actions and cocycles from the choices of the \(e_g\) for \(E\) and the \(e'_g\) for \(E'\). The action of \(g \in G\) on \(k \in K\) given by the first extension satisfies
$k \mapsto e_gk^{-1}$, and the action given by the second extension satisfies $k \mapsto e'_g k (e'_g)^{-1}$. We show that $e_gk^{-1} = e'_g k (e'_g)^{-1}$. To interpret this equation, we must remember that we view $K$ as a subgroup of both $E$ and $E'$; the left hand side of this equation is an element of $E$ whereas the right hand side lives in $E'$. If we apply $\sigma$ to the left hand side, we get

$$\sigma(e_gk^{-1}) = \sigma(e_g)\sigma(k)\sigma(e_g)^{-1} = e'_g\sigma(k) (e'_g)^{-1} = e'_g k (e'_g)^{-1}$$

since the commutativity of the diagram shows that $\sigma|_K = \text{id}$. Thus, the actions are the same; we write $\varphi : G \to \text{Aut}(K)$ for this action. Next, the two cocycles for the extensions are given by

$$f(g, h) = e_g e_h e_{gh}^{-1},$$

$$f'(g, h) = e'_g e'_h (e'_{gh})^{-1}$$

for all $g, h \in G$. We have $\sigma(f(g, h)) = f'(g, h)$. Since $f$ has values in $K$ and since $\sigma|_K = \text{id}$, this yields $f(g, h) = f'(g, h) \in K$. The two cocycles $f$ and $f'$ are equal, so they represent the same class in $H^2(G, K)$.

**Theorem 2.13.** Let $K$ and $G$ be groups with $K$ Abelian. If $\varphi : G \to \text{Aut}(K)$ is a homomorphism, then there is a 1-1 correspondence between equivalence classes of extensions of $K$ by $G$ whose action is $\varphi$, and elements of $H^2(G, K)$.

**Proof.** Let $1 \to K \to E \to G \to 1$ be an extension of $K$ by $G$. We have given a procedure for producing an action $G \to \text{Aut}(K)$ and a cocycle class in $H^2(G, K)$ from the extension. Furthermore, the previous lemma shows that equivalent extensions yield the same action and the same cocycle class. Thus, we have a well-defined function from the set of equivalence classes of extensions whose action is $\varphi$ and elements of $H^2(G, K)$. We need to show that this map is injective and surjective. If $f \in Z^2(G, K)$, then we have shown how to produce an extension $1 \to K \to E_f \to G$ whose action is $\varphi$ and whose cocycle class is $f$; this proves surjectivity. Finally, suppose that $1 \to K \to E \overset{\pi}{\to} G \to 1$ and $1 \to K \to E' \overset{\pi'}{\to} G \to 1$ are two extensions whose action is $\varphi$ and whose cocycle classes agree in $H^2(G, K)$. We may then assume that they can be represented by the same cocycle. In other words, there is a cocycle $f$ and choices $e_g \in E$ and $e'_g \in E$ such that $f(g, h) = e_g e_h e_{gh}^{-1}$ and $f(g, h) = e'_g e'_h (e'_{gh})^{-1}$. We define a map $\sigma : E \to E'$ by $\sigma(k e_g) = k e'_g$. Recalling that everything in $E$ (resp. $E'$) has a unique representation in the form $k e_g$ (resp. $k e'_g$) with $k \in K$ and $g \in G$, this map is well-defined. Furthermore, the second part of Lemma 2.10 shows that this map is a group homomorphism. It is then a bijection by the uniqueness of the representation. Finally, $\pi'(\sigma(k e_g)) = \pi'(k e'_g) = g = \pi(k e_g)$. This, together with the fact that $\sigma|_K = \text{id}$, shows that the two extensions are equivalent. This finishes the proof.

In the correspondence of the theorem, the trivial cocycle corresponds to the semidirect product of $K$ by $G$. Therefore, if $H^2(G, K) = 1$, then the semidirect product is the only extension of $K$ by $G$, up to equivalence.
3 Computations and Consequences

In this section we will give some results about $H^2(G, K)$ without proving everything. The appropriate way to study this group in detail is to realize it in its proper context of homological algebra. By using results of homology groups and resolutions, one has better tools for making computations. However, since we are not developing the theory of homological algebra here, we make do with unproven statements and some ad-hoc calculations.

Let $G$ be a group and let $\varphi : G \to \text{Aut}(K)$ be an action of $G$ on an Abelian group $K$. We will write $gk$ in place of $\varphi_g(k)$. Suppose that $G$ is a finite group. We define a map $N : K \to K$ by $N(k) = \prod_{g \in G} gk$. This map is usually called the norm map. We also denote by $K^G$ the $G$-fixed elements of $K$; that is,

$$K^G = \{k \in K : gk = k \text{ for all } g \in G\}.$$ 

It is not hard to see that $N$ is a group homomorphism and the image $N(K) \subseteq K^G$.

**Proposition 3.1.** Let $G$ be a finite cyclic group. Then $H^2(G, K) \cong K^G/N(K)$.

**Example 3.2.** Let $p$ be a prime, and set $G = K = \mathbb{Z}_p$. The only homomorphism $\varphi : \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ is the trivial map. The norm map then satisfies $N(x) = px = 0$ for all $x \in \mathbb{Z}_p$. Also, $K^G = K$ since $g x = x$ for all $g \in G$ and $x \in K$. Thus, $K^G/N(K) \cong K$. Therefore, $H^2(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p$. We conclude that there are $p$ inequivalent extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_p$. However, we know that $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ are the only groups of order $p^2$, up to isomorphism. The trivial cocycle corresponds to the (semi)direct product; i.e., the extension $1 \to \mathbb{Z}_p \to \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \to 1$. The $p - 1$ nontrivial cocycle classes all correspond to extensions whose middle group is $\mathbb{Z}_{p^2}$. This helps to explain Example 2.11, which produced two inequivalent extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_3$ whose middle group is $\mathbb{Z}_9$.

**Example 3.3.** Let $p < q$ be prime numbers such that $p$ divides $q - 1$. This hypothesis shows that there is a nontrivial homomorphism $\varphi : G = \mathbb{Z}_p \to \text{Aut}(\mathbb{Z}_q)$, since $\text{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$. With this action we show that $H^2(\mathbb{Z}_p, \mathbb{Z}_q) = 1$. To see this, we note that $\mathbb{Z}_q^G \neq \mathbb{Z}_q$ since the action is not trivial. However, $\mathbb{Z}_q^G$ is a subgroup of $\mathbb{Z}_q$, and since $q$ is prime, $\mathbb{Z}_q$ has no nontrivial subgroups. Thus, $\mathbb{Z}_q^G = 1$. This can also be seen easily by direct calculation. Thus, by the proposition, $H^2(\mathbb{Z}_p, \mathbb{Z}_q) = 1$. Therefore, with this action, the only extension of $\mathbb{Z}_q$ by $\mathbb{Z}_p$ is the semidirect product. Since the action is nontrivial, this group is a non-Abelian group of order $pq$. If, on the other hand, we use the trivial action, then $\mathbb{Z}_q^G = \mathbb{Z}_q$, and the norm map is given by $N(x) = px$ for all $x \in \mathbb{Z}_q$. However, this map is an isomorphism since $\gcd(p, q) = 1$. Thus, the image of $N$ is $\mathbb{Z}_q$. Consequently, $H^2(\mathbb{Z}_p, \mathbb{Z}_q) = 1$ in this case also. Thus, the only extension of $\mathbb{Z}_q$ by $\mathbb{Z}_p$ with the trivial action is the direct product $1 \to \mathbb{Z}_q \to \mathbb{Z}_q \times \mathbb{Z}_p \to \mathbb{Z}_p \to 1$.

**Example 3.4.** The group $H^2(G, K)$ is an Abelian group. In this example we show that, if $|G| = n$ is finite, then $H^2(G, K)$ is an $n$-torsion group. Let $f \in Z^2(G, K)$. We show that $f^n$
is a 2-coboundary, showing that $\bar{f}^n = 1$ in $H^2(G, K)$. To do this, we play with the cocycle condition. This says, for all $g, h, k \in G$, that

$$f(g, h)f(gh, k) = \varphi_g(f(h, k))f(g, hk).$$

Multiplying both sides by $f(gh, k)^{-1}$, keeping in mind that $K$ is Abelian, and taking a product over all $k \in G$ yields

$$f(g, h)^n = \prod_{k \in G} f(g, h) = \prod_{k \in G} \varphi_g(f(h, k))f(g, hk)f(gh, k)^{-1}.$$ 

Set $c_l = \prod_{k \in G} f(l, k)$ for $l \in G$. Since $G = hG$, we see that $c_l = \prod_{k \in G} f(l, hk)$. Therefore, the equation above reduces to $f(g, h)^n = \varphi_g(c_h)c_g^{-1}$. In other words, $f^n$ is a 2-coboundary, as we wished to prove.

The following result, proved in the 1930’s, is an important generalization of Example 3.3.

**Theorem 3.5 (Schur-Zassenhaus).** Let $K$ and $G$ be finite groups with $\gcd(|K|, |G|) = 1$. Then any extension of $K$ by $G$ is a semidirect product of $K$ by $G$.

**Proof.** We prove this for $K$ Abelian, and we indicate something about the general case. If $K$ is Abelian, what we will do is prove that $H^2(G, K) = 1$ for any action $\varphi : G \to \text{Aut}(K)$. Let $n = |G|$ and $m = |K|$. By the previous example, if $f \in Z^2(G, K)$, then $\bar{f}^n = 1$ in $H^2(G, K)$. Since $K$ is a finite Abelian group whose order is relatively prime to $n$, the map $\sigma : x \mapsto x^n$ is an automorphism of $K$. It is easy to see that automorphisms of $K$ send cocycles to cocycles. Thus, since $f \in Z^2(G, K)$, there is a cocycle $f'$ with $f(g, h) = f'(g, h)^n$ for every $g, h \in G$. In other words, we define $f'$ by $f'(g, h) = \sigma^{-1}(f(g, h))$ and observe that $f'$ is a 2-cocycle. This yields $f = (f')^n$, so $f = 1$ in $H^2(G, K)$. This finishes the proof for the case $K$ is Abelian.

To give some ideas of the general case, a non-homological argument is given on Page 151 of Rotman’s book *Introduction to the Theory of Groups*. We indicate briefly how one can give a homological argument. If $1 \to K \to E \to G \to 1$ is an extension, then we note that the handout *Group Extensions and $H^3$*, it is shown that equivalence classes of extensions of $K$ by $G$ are in 1-1 correspondence with the elements of $H^2(G, Z(K))$. However, since $Z(K)$ is a subgroup of $K$, Lagrange’s theorem implies that $\gcd(|Z(K)|, |G|) = 1$. The Abelian case shows that $H^2(G, Z(K)) = 1$. Thus, any two extensions of $K$ by $G$ (with the same action) are equivalent. Since one corresponds to the semidirect product of $K$ by $G$, this is the unique extension. Thus, $E$ is a semidirect product.