2 Cohomology of groups

This section intends to give a very first introduction to group cohomology. In particular, we want to discuss another setting in which Ext-groups carry meaningful information.

2.1 Definition. Let G be a group, which in general will be non-abelian. By a G-module we mean an abelian group A, written additively, together with an action $\rho\colon G \times A \to A$ of G on A by group automorphisms. In more detail, if we write $g * a$ for $\rho(g, a)$ we should have:

(1) $e * a = a$ and $g_1 * (g_2 * a) = (g_1 g_2) * a$ for all g_1, $g_2 \in G$ and $a \in A$;
(2) $g * (a_1 + a_2) = (g * a_1) + (g * a_2)$ and $g * (-a) = -(g * a)$ for all $g \in G$ and a, a_1, $a_2 \in A$.

The first simply expresses that we have an action of G on the set A; the second expresses that this is an action of G by group automorphisms of A.

2.2 Remark. If A is an abelian group then to give A the structure of a G-module is the same as giving a homomorphism of groups $\theta\colon G \to \mathrm{Aut}(A)$. The correspondence is given by the rule $\theta(g)\big(a\big) = g * a$.

2.3 Definition. If A and B are G-modules then a morphism of G-modules $f\colon A \to B$ is a group homomorphism with the property that $g * f(a) = f(g * a)$ for all $g \in G$ and $a \in A$.

2.4 Remark. Let $\mathbb{Z}[G]$ be the group ring of G. A G-module is then nothing else but a $\mathbb{Z}[G]$-module. Indeed, if we have a $\mathbb{Z}[G]$-module A then we already know what we mean by $g * a$ (which of course is often written as $g \cdot a$). Conversely, if A is a G-module then it has the structure of a $\mathbb{Z}[G]$-module by the rule

$$\Big(\sum_{g \in G} m_g \cdot g\Big) \cdot a = \sum_{g \in G} m_g \cdot (g * a)\,.$$

(Since A is abelian, if we have elements $a_i \in A$ and integers $m_i \in \mathbb{Z}$, we know what we mean by $\sum m_i \cdot a_i$.) Under this correspondence, a morphism of G-modules is the same as a morphism of $\mathbb{Z}[G]$-modules. In what follows we will freely switch between the two notions and rather than introducing a new notation G-Mod for the category of G-modules, we will identify this category with the category $\mathbb{Z}[G]$-Mod of (left) $\mathbb{Z}[G]$-modules. As we will see, in examples the purely group-theoretic notion of a G-module will sometimes be more natural than its module-theoretic equivalent, which is the reason why we have introduced it.

2.5 If A is an abelian group, we can give it the trivial structure of a G-module for which $g * a = a$ for all $g \in G$ and $a \in A$. This gives a fully faithful "inclusion functor" $i\colon \mathsf{Ab} \to \mathbb{Z}[G]$-$\mathsf{Mod}$.

This functor can also be understood as follows. For any group G we have the augmentation homomorphism

$$\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z} \qquad \text{given by} \qquad \sum_{g \in G} m_g \cdot g \mapsto \sum_{g \in G} m_g\,,$$

which is a homomorphism of rings. Thinking of $\mathbb{Z}$ as the group ring of the trivial group, ϵ is the homomorphism induced by the unique homomorphism $G \to \{1\}$. The inclusion functor i is the induced functor between module categories.

The kernel of ϵ is called the augmentation ideal of $\mathbb{Z}[G]$; we denote it by I_G. As one readily checks, it is generated, as an ideal of $\mathbb{Z}[G]$, by the elements $g-1$.

2.6 Definition. If A is a G-module, we define its subgroup of G-invariants $A^G \subset A$ by

$$A^G = \left\{ a \in A \;\middle|\; g * a = a \quad \text{for all } g \in G \right\}.$$

One readily verifies that A^G is indeed a subgroup of A and that a homomorphism of G-modules $A \to B$ restricts to a homomorphism of groups $A^G \to B^G$. This gives us a functor

$$(\ )^G \colon \mathbb{Z}[G]\text{-}\mathsf{Mod} \to \mathsf{Ab}.$$

2.7 Proposition. *The functor* $(\ )^G$ *is left exact.*

Proof. We can suggest three proofs: (1) Verify left exactness by hand, which is not hard. (2) Note that the natural isomorphism $\mathrm{Hom}_{\mathsf{Ab}}(\mathbb{Z}, A) \cong A$ restricts to an isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]\text{-}\mathsf{Mod}}(\mathbb{Z}, A) \cong A^G \tag{2.7.1}$$

(where $\mathbb{Z}$ always denotes $\mathbb{Z}$ with its trivial G-module structure), which gives an isomorphism of functors $\mathrm{Hom}_{\mathbb{Z}[G]\text{-}\mathsf{Mod}}(\mathbb{Z}, -) \cong (\ )^G$. Then use that if R is a ring and M is an R-module, the functor $\mathrm{Hom}_R(M, -)$ is left exact. (3) Note that $(\ )^G$ is right adjoint to the above inclusion-functor i. $\square$

2.8 Remark. By construction, $\mathbb{Z}[G]/I_G \xrightarrow{\sim} \mathbb{Z}$ as $\mathbb{Z}[G]$-modules. Hence we see from (2.7.1) that if we think of A as a $\mathbb{Z}[G]$-module, $A^G \subset A$ is the subgroup of elements that are annihilated by the augmentation ideal I_G.

2.9 Definition. Let G be a group, and let A be a G-module. Then we define the cohomology in degree n of G with coefficients in A, notation $\mathrm{H}^n(G, A)$, to be

$$\mathrm{H}^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A),$$

where $\mathbb{Z}$ is given the trivial G-module structure.

2.10 Remark. By the general properties of Ext-groups, this defines functors

$$\mathrm{H}^n(G, -) \colon \mathbb{Z}[G]\text{-}\mathsf{Mod} \to \mathsf{Ab},$$

and if $0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$ is a short exact sequence of G-modules, we have an associated long exact cohomology sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^0(G, A') \longrightarrow \mathrm{H}^0(G, A) \longrightarrow \mathrm{H}^0(G, A'') \xrightarrow{\delta} \mathrm{H}^1(G, A') \\ \longrightarrow \mathrm{H}^1(G, A) \longrightarrow \mathrm{H}^1(G, A'') \xrightarrow{\delta} \mathrm{H}^2(G, A') \longrightarrow \cdots \end{aligned}$$

2.11 Example. As a very first example, for $n = 0$ we find

$$\mathrm{H}^0(G, A) = A^G$$

by (2.7.1).

2.12 Example. Let $G = \langle\gamma\rangle \cong \mathbb{Z}$ be an infinite cyclic group. In this case the group ring $\mathbb{Z}[G]$ is isomorphic to $\mathbb{Z}[t, t^{-1}]$; the isomorphism is given by $\gamma^i \mapsto t^i$. The augmentation ideal $I_G \subset \mathbb{Z}[G]$ is generated by $\gamma - 1$. As $\mathbb{Z}[G]$ is a domain, it follows that the sequence

$$0 \longrightarrow \mathbb{Z}[G] \xrightarrow{\gamma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is short exact. From the associated long exact sequence and the fact that $\mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) = 0$ for $n > 0$ because $\mathbb{Z}[G]$ is (obviously) a free $\mathbb{Z}[G]$-module, we then find

$$\begin{cases} \mathrm{H}^0(G, A) = A^G \\ \mathrm{H}^1(G, A) = A/(\gamma - 1) \cdot A \\ \mathrm{H}^n(G, A) = 0 & \text{for } n \geq 2. \end{cases}$$

2.13 Example. Let $G = \langle\gamma\rangle$ denote a cyclic group of order n. (So $G \cong \mathbb{Z}/n\mathbb{Z}$.) In this case the group ring $\mathbb{Z}[G]$ is isomorphic to $\mathbb{Z}[t]/(t^n - 1)$, via the map that sends γ^i to the class of t^i. The augmentation ideal I_G is the ideal generated by $\gamma - 1$. In $\mathbb{Z}[G]$, consider the *norm element*

$$N = 1 + \gamma + \gamma^2 + \cdots + \gamma^{n-1}\,.$$

Clearly $(\gamma - 1) \cdot N = \gamma^n - 1 = 0$. But in fact we have something better, namely that the sequences

$$\mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\gamma-1} \mathbb{Z}[G] \qquad \text{and} \qquad \mathbb{Z}[G] \xrightarrow{\gamma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G]$$

are both exact. It follows that the complex

$$R_\bullet : \qquad \cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\gamma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\gamma-1} \mathbb{Z}[G] \longrightarrow 0$$

together with the augmentation map $\epsilon\colon R_\bullet \to \mathbb{Z}$ is a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module. This gives

$$\begin{cases} \mathrm{H}^0(G, A) = \mathrm{Ker}\big(\gamma - 1\colon A \to A\big) = A^G \\ \mathrm{H}^n(G, A) = \mathrm{Ker}\big(N\colon A \to A\big)/\mathrm{Im}\big(\gamma - 1\colon A \to A\big) & \text{if } n \text{ is odd} \\ \mathrm{H}^n(G, A) = A^G/\mathrm{Im}\big(N\colon A \to A\big) & \text{for } n \geq 2 \text{ even.} \end{cases}$$

We will use this in later examples.

2.14 For an arbitrary group G we have seen in Exercise ?? an explicit free resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module, namely the complex

$$B_\bullet(G): \qquad \cdots \longrightarrow \mathbb{Z}[G^3] \xrightarrow{d} \mathbb{Z}[G^2] \xrightarrow{d} \mathbb{Z}[G] \longrightarrow 0$$

with $B_n(G) = \mathbb{Z}[G^{n+1}]$, viewed as a $\mathbb{Z}[G]$-module via the diagonal action $g*(g_0, g_1, \ldots, g_n) = (gg_0, gg_1, \ldots, gg_n)$, and with differentials $d\colon \mathbb{Z}[G^{n+1}] \to \mathbb{Z}[G^n]$ given by

$$d(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i \cdot (g_0, \ldots, \widehat{g_i}, \ldots, g_n)\,.$$

We are going to use this to give an explicit description of the cohomology groups of G with coefficients in a G-module A. This will be particularly useful in low degrees.

The basic observation is that we can identify

$$\mathrm{Hom}_{\mathbb{Z}[G]}\big(\mathbb{Z}[G^{n+1}], A\big) \cong \mathrm{Map}(G^n, A)\,. \tag{2.14.1}$$

This can in fact be done in many ways, and the one that we are going to use does not seem the simplest possible; however, it leads to an explicit description of group cohomology that is very useful in practice. We will work with the identification (2.14.1) given by sending $f\colon \mathbb{Z}[G^{n+1}] \to A$ to the map $\phi\colon G^n \to A$ given by

$$\phi(g_1, \ldots, g_n) = f(1,\, g_1,\, g_1g_2,\, g_1g_2g_3, \ldots,\, g_1g_2\cdots g_n)\,.$$

In the reverse direction, $\phi\colon G^n \to A$ is sent to the $\mathbb{Z}[G]$-homomorphism $f\colon \mathbb{Z}[G^{n+1}] \to A$ given by

$$f(g_0, g_1, \ldots, g_n) = \phi(g_0^{-1}g_1,\, g_1^{-1}g_2,\, \ldots,\, g_{n-1}^{-1}g_n)\,.$$

With these identifications (2.14.1) the cochain complex $\mathrm{Hom}_{\mathbb{Z}[G]}\big(B_\bullet(G), A\big)$ can be identified with a cochain complex

$$0 \longrightarrow \mathrm{Map}(G^0, A) \longrightarrow \mathrm{Map}(G, A) \longrightarrow \mathrm{Map}(G^2, A) \longrightarrow \cdots$$

Note that each $\mathrm{Map}(G^n, A)$ is naturally an abelian group, via the addition in A. Direct calculation shows that the differentials $d^n\colon \mathrm{Map}(G^n, A) \to \mathrm{Map}(G^{n+1}, A)$ are given by

$$\begin{aligned} &d^n(\phi)\big(g_1, \ldots, g_{n+1}\big) \\ &\qquad = g_1 * \phi(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i \cdot \phi(g_1, \ldots, g_ig_{i+1}, \ldots, g_{n+1}) + (-1)^{n+1} \cdot \phi(g_1, \ldots, g_n). \end{aligned}$$

The conclusion of this is that

$$\mathrm{H}^n(G, A) = \frac{\mathrm{Ker}\big(d^n\colon \mathrm{Map}(G^n, A) \to \mathrm{Map}(G^{n+1}, A)\big)}{\mathrm{Im}\big(d^{n-1}\colon \mathrm{Map}(G^{n-1}, A) \to \mathrm{Map}(G^n, A)\big)}\,,$$

where the differentials d^n are given by the above formula.

2.15 Examples. Let us consider some examples in low degree.

Of course, $G^0 = \{1\}$ so that a map $G^0 \to A$ is given by an element $a \in A$. The differential $d^0 \colon \mathrm{Map}(G^0, A) = A \to \mathrm{Map}(G, A)$ sends a to the map $g \mapsto g * a - a$. In degree $n = 0$ we therefore find

$$\mathrm{H}^0(G, A) = \mathrm{Ker}(d^0) = A^G\,,$$

in agreement with what we have found before.

The next differential is $d^1 \colon \mathrm{Map}(G, A) \to \mathrm{Map}(G^2, A)$. It sends a map $\phi \colon G \to A$ to $d^1(\phi) \colon G^2 \to A$ given by

$$d^1(\phi)\bigl(g_1, g_2\bigr) = g_1 * \phi(g_2) - \phi(g_1 g_2) + \phi(g_1)\,.$$

This gives

$$\mathrm{H}^1(G, A) = \frac{\bigl\{\phi \colon G \to A \bigm| \phi(g_1 g_2) = g_1 * \phi(g_2) + \phi(g_1)\bigr\}}{\bigl\{\phi \colon G \to A \bigm| \text{there exists an } a \in A \text{ such that } \phi(g) = g * a - a \text{ for all } g \in G\bigr\}}$$

The maps that appear in the numerator are called *crossed homomorphisms* from G to A. As we have already studied Ext^1-groups in the previous section, we will not elaborate on this. We do note, however, that if G acts trivially on A we simply get $\mathrm{H}^1(G, A) = \mathrm{Hom}_{\mathsf{Ab}}(G, A)$.

The differential $d^2 \colon \mathrm{Map}(G^2, A) \to \mathrm{Map}(G^3, A)$ sends a map $\phi \colon G^2 \to A$ to $d^2(\phi) \colon G^3 \to A$ given by

$$d^2(\phi)\bigl(g_1, g_2, g_3\bigr) = g_1 * \phi(g_2, g_3) - \phi(g_1 g_2, g_3) + \phi(g_1, g_2 g_3) - \phi(g_1, g_2)\,.$$

This gives

$$\mathrm{H}^2(G, A) = \frac{\bigl\{\phi \colon G^2 \to A \bigm| \phi(g_1 g_2, g_3) - \phi(g_1, g_2 g_3) = g_1 * \phi(g_2, g_3) - \phi(g_1, g_2)\bigr\}}{\bigl\{\phi \colon G \to A \bigm| \exists \psi \colon G \to A \text{ such that } \phi(g_1, g_2) = g_1 * \psi(g_2) - \psi(g_1 g_2) + \psi(g_1)\bigr\}}$$

which already looks rather mysterious.

2.16 Group extensions and H^2. Just as in the previous section we have related Ext^1 modules to extensions of modules, we are here going to relate $\mathrm{H}^2(G, A)$ to a problem about extensions of groups.

The starting point for this is that if G and A are groups then by an extension of G by A we mean a short exact sequence of groups

$$1 \longrightarrow A \xrightarrow{\ i\ } \Gamma \xrightarrow{\ \pi\ } G \longrightarrow 1\,. \tag{2.16.1}$$

Note: "short exact" simply means that i is injective, π is surjective and $\mathrm{Im}(i) = \mathrm{Ker}(\pi)$. Similar to the definition for extensions of modules, we will view two such extensions as equivalent if they fit in a diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\mathrm{id}_A"] & \Gamma \arrow[r, "\pi"] \arrow[d, "f"] & G \arrow[r] \arrow[d, "\mathrm{id}_G"] & 0 \\
0 \arrow[r] & A \arrow[r, "i'"] & \Gamma' \arrow[r, "\pi'"] & G \arrow[r] & 0
\end{tikzcd}$$

and the existence of such a diagram implies that f is an isomorphism of groups.

In the rest of the discussion we assume that the group A is abelian. This has an important consequence. Namely, given an extension (2.16.1) we obtain a natural structure of a G-module on A. For this, choose a *set-theoretic* section $s\colon G \to \Gamma$ of the map π, i.e., a map s such that $\pi \circ s = \mathrm{id}_G$. Such a section exists, simply because π is surjective. Note, however, that in general we cannot find a homomorphic section s. Given this section s we obtain an action of G on A by

$$g * a = s(g) \cdot a \cdot s(g)^{-1}\,. \tag{2.16.2}$$

Explanation: we identify A with $\ker(\pi)$ via i, and we calculate $s(g) \cdot a \cdot s(g)^{-1}$ inside the group Γ. Then we observe that this element lies in A because $\pi\bigl(s(g)\cdot a\cdot s(g)^{-1}\bigr) = g\cdot 1\cdot g^{-1} = 1$. One readily checks that (2.16.2) indeed defines a G-module structure on A. Moreover, this G-module structure is independent of the chosen section s. Indeed, any other section is of the form $\sigma(g) = \alpha(g) \cdot s(g)$, where α is a map from G to A. But then we find that

$$\sigma(g) \cdot a \cdot \sigma(g)^{-1} = \alpha(g) \cdot \bigl(s(g) \cdot a \cdot s(g)^{-1}\bigr) \cdot \alpha(g)^{-1} = s(g) \cdot a \cdot s(g)^{-1}$$

because A is abelian.

The problem that we are interested in is to describe, given a group G and a G-module A, all extensions of G by A up to equivalence. Since we have now fixed the structure of a G-module on A this means that we want to consider all extensions (2.16.1) for which the resulting G-module structure (2.16.2) is the given one.

There is always at least one such extension. Namely, if we describe the G-module structure on A as a homomorphism $\theta\colon G \to \mathrm{Aut}(A)$ (see Remark 2.2) we can form the semi-direct product $A \rtimes_\theta G$. Recall that $A \rtimes_\theta G$ is the set of pairs $(a, g) \in A \times G$, with group structure given by

$$(a_1, g_1) \cdot (a_2, g_2) = \Bigl(a_1 + \theta(g_1)\bigl(a_2\bigr),\, g_1 g_2\Bigr)\,.$$

(We write the group structure on A additively.) The maps $i\colon A \to A \rtimes_\theta G$ given by $a \mapsto (a, 1)$ and $\pi\colon A \rtimes_\theta G \to G$ given by $(a, g) \mapsto g$ are homomorphisms that realize $A \rtimes_\theta G$ as an extension of G by A. To see that the corresponding G-module structure on A is the one given by θ note that in this case π has a homomorphic section, namely $s\colon G \to A \rtimes_\theta G$ given by $g \mapsto (0, g)$. Since in $A \rtimes_\theta G$ we have

$$(0, g) \cdot (a, 1) \cdot (0, g^{-1}) = \bigl(\theta(g)\bigl(a\bigr), 1\bigr)$$

we see that, indeed, the G-module structure on A is the one we started with.

Already at this point it is an easy exercise to show that an extension Γ is equivalent to $A \rtimes_\theta G$ if and only if there exists a homomorphic section of $\pi\colon \Gamma \to G$. So we may think of the semi-direct product as being the "trivial" extension of G by A (similar to split extensions of modules) and ask whether there are other, non-equivalent extensions. This is an important question in group theory that can be answered using group cohomology.

2.17 Theorem. *Let G be a group and A be a G-module. Then the set of equivalence classes of extensions of G by A (with its given G-module structure) is in natural bijection with* $\mathrm{H}^2(G, A)$*. Under this bijection the semi-direct product $A \rtimes_\theta G$ corresponds with the zero class in* $\mathrm{H}^2(G, A)$*.*

We will not give the full details of the proof but only explain the key idea, which is a simple one. Namely, given an extension (2.16.1) we choose a (set-theoretic) section $s\colon G \to \Gamma$ of π, and we measure how far s is from being a homomorphism. This leads us to consider the map $\phi_s\colon G^2 \to A$ given by

$$\phi_s(g_1, g_2) = s(g_1g_2) \cdot s(g_2)^{-1} \cdot s(g_1)^{-1}\,.$$

Note that the RHS is calculated in Γ and defines an element of A because it lies in the kernel of π. (In what follows we identify A with the subgroup $\mathrm{Ker}(\pi) \subset \Gamma$.) We claim that $d^2(\phi_s) = 0$, or what is the same, that

$$-\phi_s(g_1, g_2g_3) + \phi_s(g_1g_2, g_3) = g_1 * \phi_s(g_2, g_3) - \phi_s(g_1, g_2)$$

for all g_1, g_2, $g_2 \in G$. The LHS (calculated in the group Γ, which is written multiplicatively) is given by

$$s(g_1)\, s(g_2g_3)\, s(g_1g_2g_3)^{-1}\, s(g_1g_2g_3)\, s(g_3)^{-1}\, s(g_1g_2)^{-1}\;;$$

the RHS is

$$s(g_1)\, s(g_2g_3)\, s(g_3)^{-1}\, s(g_2)^{-1}\, s(g_1)^{-1}\, s(g_1)\, s(g_2)\, s(g_1g_2)^{-1}$$

and we readily see that these two expressions indeed give the same. Therefore, ϕ_s defines a class in $\mathrm{H}^2(G, A)$. This class is independent of the choice of a section s, for if σ is another section then $\sigma(g) = \alpha(g) \cdot s(g)$ for some map $\alpha\colon G \to A$, and then

$$\begin{aligned}
\phi_\sigma(g_1, g_2) &= \alpha(g_1g_2) \cdot s(g_1g_2) \cdot s(g_2)^{-1} \cdot \alpha(g_2)^{-1} \cdot s(g_1)^{-1} \cdot \alpha(g_1)^{-1}\\
&= \alpha(g_1g_2) \cdot \phi_s(g_1, g_2) \cdot \big(s(g_1) * \alpha(g_2)^{-1}\big) \cdot \alpha(g_1)^{-1}\\
&= \phi_s(g_1, g_2) - \big[s(g_1) * \alpha(g_2) - \alpha(g_1g_2) + \alpha(g_1)\big]\\
&= \phi_s(g_1, g_2) - d^1(\alpha)\big(g_1, g_2\big)
\end{aligned}$$

where in the third step we switch from multiplicative notation (in he group Γ) to additive notation (in A). Hence we see that ϕ_s and ϕ_σ define the same class in $\mathrm{H}^2(G, A)$.

This construction gives a map from the set of equivalence classes of extensions of G by the G-module A to $\mathrm{H}^2(G, A)$, and the more precise form of the theorem is that this map is a bijection. Note that indeed the semi-direct product $A \rtimes_\theta G$ is mapped to the zero class, as clearly $\phi_s = 0$ if (and only if) s is a homomorphism.

2.18 Example. Let p be a prime number and let us classify all extensions of $C_p = \mathbb{Z}/p\mathbb{Z}$ by itself. Note that by basic group theory every group of order p^2 has a normal subgroup of order p and can therefore be obtained as an extension of C_p by itself.

As $\mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, there is no other C_p-module structure on $\mathbb{Z}/p\mathbb{Z}$ other than the trivial one. (In case you find this confusing, note that a C_p-module structure is the structure of a module over the group ring $\mathbb{Z}[C_p]$. Of course C_p has a natural structure of a module over the ring $\mathbb{Z}/p\mathbb{Z}$ but that is something different.) By what we have found in Example 2.13,

$$\mathrm{H}^2(C_p, C_p) \cong C_p\,.$$

(With notation as in Example 2.13 the norm element N acts as multiplication by p, which in this case is 0.)

There are two extensions that immediately come to mind: the trivial extension $C_p \times C_p$ and the extension

$$1 \longrightarrow C_p \xrightarrow{i} (\mathbb{Z}/p^2\mathbb{Z}) \xrightarrow{\pi} C_p \longrightarrow 1\,,$$

with i given by $a \bmod p \mapsto p\cdot a \bmod p^2$. However, if we take $c \in (\mathbb{Z}/p\mathbb{Z})^*$ and in this sequence change the map i to $c\cdot i$ given by $a \bmod p \mapsto p\cdot ca \bmod p^2$ then this gives a different equivalence class of extensions. One can check that this gives all possible classes in $\mathrm{H}^2(C_p, C_p) \cong C_p$. The conclusion, therefore, is that every group of order p^2 is isomorphic to $C_p \times C_p$ or to $\mathbb{Z}/p^2\mathbb{Z}$.

2.19 Example. Let $C_2 = \{1, \iota\}$ and C_4 denote the cyclic groups of order 2 and 4, respectively. As $\mathrm{Aut}(C_4) \cong C_2$, there are two possible C_2-module structures on C_4: the trivial one, and the one for which ι acts as $-\mathrm{id}$ on C_4.

Let us first take the trivial C_2-module structure on C_4. By Example 2.13 we have $\mathrm{H}^2(C_2, C_4) \cong C_4/2C_4$. (The norm element N acts as multiplication by 2.) We easily see the two corresponding extensions: the product group $C_4 \times C_2$ and the extension

$$0 \longrightarrow C_4 \longrightarrow \mathbb{Z}/8\mathbb{Z} \longrightarrow C_2 \longrightarrow 0\,.$$

If we take the non-trivial C_2-module structure $\theta\colon C_2 \to \mathrm{Aut}(C_4)$ then we find that $\mathrm{H}^2(C_2, C_4) \cong 2C_4 \cong \mathbb{Z}/2\mathbb{Z}$. (In this case the norm element acts trivially.) Again we can see two extensions:

$$0 \longrightarrow \langle r\rangle \longrightarrow D_4 \xrightarrow{\det} \{\pm 1\} \longrightarrow 1$$

where $D_4 = \langle r, s\rangle$ is the dihedral group of order 8 (with $r \in D_4$ the rotation, of order 4), and

$$0 \longrightarrow \langle i\rangle \longrightarrow Q \longrightarrow C_2 \longrightarrow 1$$

with $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ the quaternion group of order 8. The dihedral group is of course the semidirect product $C_4 \rtimes_\theta C_2$. The quaternion group Q is not semi-direct, as all its elements of order 2 lie in the subgroup $\langle i\rangle \subset Q$, so that the map $Q \to C_2$ has no homomorphic section.