École Polytechnique Fédérale de Lausanne
Mathematics Section

FROM HOMOLOGICAL ALGEBRA TO GROUP COHOMOLOGY

Semester Project By
Maximilien Holmberg-Péroux

Responsible Professor
prof. Jacques Thévenaz

Supervisor
Rosalie Chevalley

Academic year : 2013-2014
Spring Semester

Contents

Introduction

The study of topological spaces through algebraic invariants in algebraic topology introduced new concepts in mathematics, such as category theory or homological algebraic theory, which are nowadays autonomous fields of study. Algebraic topologists introduced the notion of homology and cohomology of groups to describe the behavior of the fundamental group of a topological spaces. This new concept is standing on its own and has become a new branch of algebra. Group cohomology is essential in many aspects of algebra, such as representation theory.

This paper covers standard exercises about homological algebra and group cohomology. Emphasis will be put on concrete computations. We first study basic homological algebra on which group cohomology is grounded. Then we look at group cohomology itself to finish by reviewing the low-dimensional interpretation of group cohomology. We will give an insight of Galois cohomology.

Chapter 1

Elementary Homological Algebra

The exercises of this chapter are based on the theory presented in Chapters 6 and 7 of the reference [Rotman, 2009]. It discusses homology of chain complexes, projective resolutions, and the derived functors Tor and Ext which are crucial for group (co)homology.

1.1 Homology Functors

We first present some exercises that study chain complexes and their homology.

Exercise 1.1.1. *For any chain complex $C_\bullet$, the following are equivalent :*

(a) *$C_\bullet$ is exact;*

(b) *$C_\bullet$ is acyclic;*

(c) *The map $f : 0_\bullet \to C_\bullet$ is a quasi-isomorphism.*

Proof. Let us denote d the differentials of $C_\bullet$.

(a)⇒(b) : For any integer n, by definition of exactness, we have $\operatorname{im} d_{n+1} = \ker d_n$, and thus :

$$H_n(C_\bullet) = \ker d_n \Big/ \operatorname{im}\, d_{n+1} = 0.$$

Therefore $C_\bullet$ is acyclic.

(b)⇒(c) : Since for all n we have $H_n(C_\bullet) = 0$, we get that the diagram commutes for all n :

$$\begin{array}{ccc} H_n(0_\bullet) & \xrightarrow{H_n(f)} & H_n(C_\bullet) \\ \| & & \| \\ 0 & = & 0, \end{array}$$

i.e., f is a quasi-isomorphism.

(c)⇒(a) : Since f is a quasi-isomorphism, we get that $H_n(C_\bullet) \cong H_n(0_\bullet) = 0$ for all n. Therefore, for any z in $\ker d_n$, its homology class $\operatorname{cls}(z) = 0$, i.e., $z \in \operatorname{im} d_{n+1}$. We have just proved that $\ker d_n \subseteq \operatorname{im} d_{n+1}$, for all $n \in \mathbb{Z}$, therefore $\ker d_n = \operatorname{im} d_{n+1}$ for all n. □

Exercise 1.1.2. *Let $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ be a short exact sequence of chain complexes. Show that if two of the three complexes $A_\bullet, B_\bullet, C_\bullet$ are exact, then so is the third.*

Proof. The short exact sequence induces a long exact sequence in homology (see Theorem 6.10 in [ROTMAN, 2009]) :

$$\cdots \longrightarrow H_{n+1}(C_\bullet) \longrightarrow H_n(A_\bullet) \longrightarrow H_n(B_\bullet) \longrightarrow H_n(C_\bullet) \longrightarrow \cdots . \qquad (\star)$$

Recall that, from the previous exercise, a complex $K_\bullet$ is exact if and only if $H_n(K_\bullet) = 0$ for all $n \in \mathbb{Z}$. Since the other cases are similar, let us prove that if $A_\bullet$ and $B_\bullet$ are exact, then so is $C_\bullet$. Since $A_\bullet$ and $B_\bullet$ are exact, we have that $H_n(A_\bullet)$ and $H_n(B_\bullet)$ are trivial for all n. So by exactnes of $(\star)$, we get that $H_n(C\bullet)$ is trivial for every n, so that $C_\bullet$ is exact. □

Exercise 1.1.3. *Let $f : C_\bullet \to D_\bullet$ be a morphism of chain complexes. Show that if* $\ker(f)$ *and* $\operatorname{coker}(f)$ *are acyclic, then f is a quasi-isomorphism.*

Proof. Let us denote by $f^{|\mathrm{im}(f)}$ the corestriction of f onto the subcomplex $\mathrm{im}(f)$ of $D_\bullet$. Let $i : \mathrm{im}(f) \hookrightarrow D_\bullet$ denote the inclusion. Since f is a morphism of chain complexes, we have the following short exact sequences :

$$0 \longrightarrow \ker(f) \hookrightarrow C_\bullet \xrightarrow{f^{|\mathrm{im}(f)}} \mathrm{im}(f) \longrightarrow 0,$$

and :

$$0 \longrightarrow \mathrm{im}(f) \xhookrightarrow{i} D_\bullet \twoheadrightarrow \operatorname{coker}(f) \longrightarrow 0.$$

Since $\ker(f)$ is acyclic, the long exact exact sequence of homology induced by the first short exact sequence implies that for every n : $H_n(C_\bullet) \cong H_n(\mathrm{im}(f))$, via $H_n(f^{|\mathrm{im}(f)})$. Similarly, since $\operatorname{coker}(f)$ is acyclic, we get that $H_n(\mathrm{im}(f)) \cong H_n(D_\bullet)$ via $H_n(i)$, for every n. Composing the isomorphisms, we get that $H_n(C_\bullet) \cong H_n(D_\bullet)$ via $H_n(f^{|\mathrm{im}(f)}) \circ H_n(i) = H_n(f^{|\mathrm{im}(f)} \circ i) = H_n(f)$, for every n. Therefore f is a quasi-isomorphism. □

Exercise 1.1.4. *A chain complex $C_\bullet$, with differential $d_n : C_n \to C_{n-1}$, is called* split exact *if it is exact and if moreover every submodule $Z_n := \ker d_n$ is a direct summand of C_n, i.e., $C_n = Z_n \oplus U_n$, for some module U_n. Show that :*

(a) *If $C_\bullet$ is a split exact complex then $U_n \xrightarrow{\cong} Z_{n-1}$ for all n.*

(b) *The inverse of the previous isomorphism induces a morphism $s_n : C_n \to C_{n+1}$ such that $\ker(s_n) = U_n$ and $\mathrm{im}(s_n) = U_{n+1}$, for all $n \in \mathbb{Z}$.*

(c) *The following are equivalent :*

- *$C_\bullet$ is split exact;*
- *$\mathrm{id}_{C_\bullet}$ and 0 are homotopic;*
- *$C_\bullet$ is exact and there are morphisms $s_n : C_n \to C_{n+1}$ such that $dsd = d$, where d denotes the differentials of $C_\bullet$.*

Proof. (a) For any n, we have : $C_n = Z_n \oplus U_n$. The restriction $d_{n|_{U_n}}$ is an isomorphism onto its image, as we have $\ker(d_{n|_{U_n}}) = \pi_{U_n}(\ker(d_n)) = 0$, where $\pi_{U_n} : Z_n \oplus U_n \to U_n$ is the projection onto the second component. So by exactness :

$$U_n \cong \mathrm{im}\ d_n = \ker d_{n-1} = Z_{n-1},$$

for all $n \in \mathbb{Z}$, i.e., $U_n \xrightarrow{\cong} Z_{n-1}$ via $d_{n|_{U_n}}$.

(b) Let us denote by $f_{n-1} : Z_{n-1} \xrightarrow{\cong} U_n$ the inverse morphism of the previous isomorphism $d_{n|_{U_n}}$, for all n. Define for all $n \in \mathbb{Z}$:

$$\begin{array}{rcl} s_n : C_n = Z_n \oplus U_n & \longrightarrow & Z_{n+1} \oplus U_{n+1} = C_{n+1} \\ z_n + u_n & \longmapsto & 0 + f_n(z_n). \end{array}$$

It is a well-defined morphism, since it is the composite of the projection onto the first component and the isomorphism f_n. From this observation, we get that $\ker(s_n) = U_n$ and $\mathrm{im}(s_n) = U_{n+1}$, as desired.

(c) Suppose first that $C_\bullet$ is split exact, let us prove that $\mathrm{id}_{C_\bullet}$ and 0 are homotopic. We need to prove that $\mathrm{id}_{C_n} = d_{n+1}s_n + s_{n-1}d_n$, for all n, for some homotopy s_n. Choose the morphism s_n defined in question (b), as $C_\bullet$ is split exact. Let us regard d_n as :

$$\begin{array}{rcl} d_n : C_n = Z_n \oplus U_n & \longrightarrow & Z_{n-1} \oplus U_{n-1} = C_{n-1} \\ z_n + u_n & \longmapsto & d_{n|_{U_n}}(u_n) + 0, \end{array}$$

Therefore, for all n and for all $z_n \in Z_n$, $u_n \in U_n$, we have :

$$\begin{array}{rcl} (d_{n+1}s_n + s_{n-1}d_n)(z_n + u_n) & = & d_{n+1}(s_n(z_n + u_n)) + s_{n-1}(d_n(z_n + u_n)) \\ & = & d_{n+1}(0 + f_n(z_n)) + s_{n-1}(d_{n|_{U_n}}(u_n) + 0) \\ & = & \Big(d_{n+1|_{U_{n+1}}}(f_n(z_n)) + 0\Big) + \Big(0 + f_{n-1}(d_{n|_{U_n}}(u_n))\Big) \\ & = & (z_n + 0) + (0 + u_n) \\ & = & z_n + u_n, \end{array}$$

where we used that $d_{n|_{U_n}}$ and f_{n-1} are mutual inverse, for all n. This proves that $\mathrm{id}_{C_n} = d_{n+1}s_n + s_{n-1}d_n$, and so $\mathrm{id}_{C_\bullet}$ and 0 are homotopic.

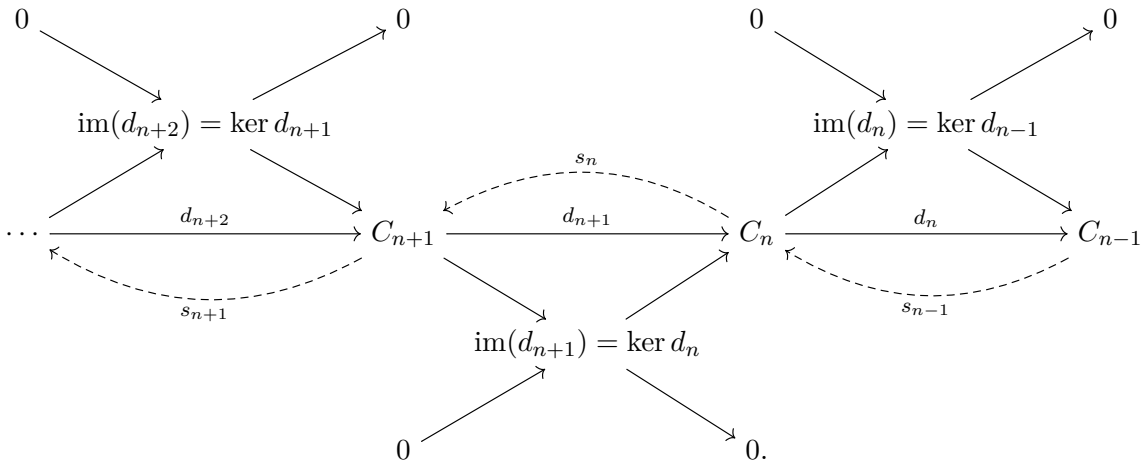
Now suppose that $\mathrm{id}_{C_\bullet}$ and 0 are homotopic. Let us prove that $C_\bullet$ is exact and there are morphisms $s_n : C_n \to C_{n+1}$ such that $dsd = d$. Since $\mathrm{id}_{C_\bullet}$ and 0 are homotopic, there exists a morphism $s_n : C_n \to C_{n+1}$ for all n, such that : $\mathrm{id}_{C_n} = d_{n+1}s_n + s_{n-1}d_n$, for all n in $\mathbb{Z}$. We get :

$$\begin{array}{rcl} d_n & = & d_n \mathrm{id}_{C_n} \\ & = & d_n(d_{n+1}s_n + s_{n-1}d_n) \\ & = & \underbrace{d_n d_{n+1}}_{=0} s_n + d_n s_{n-1} d_n \\ & = & d_n s_{n-1} d_n, \end{array}$$

and so $dsd = d$. It remains to prove that $C_\bullet$ is exact. But this follows from the fact that homotopic maps of chain complexes induce the same map in homology (see Theorem 6.14 in [Rotman, 2009]). Therefore $H_n(\mathrm{id}_{C_\bullet}) = \mathrm{id}_{H_n(C_\bullet)} : H_n(C_\bullet) \to H_n(C_\bullet)$ is the zero map, thus $C_\bullet$ is acyclic, i.e., $C_\bullet$ is exact.

Now let us show that if $C_\bullet$ is exact and there are morphisms $s_n : C_n \to C_{n+1}$ such that $dsd = d$, then $C_\bullet$ is split. The exactness of $C_\bullet$ means that $\mathrm{im}(d_n) = \ker(d_{n-1})$ for every n,

so we have the following situation, where the diagonals and the row are exact sequences :



So we get short exact sequences for every n :

$$0 \longrightarrow \mathrm{im}(d_{n+1}) \hookrightarrow C_n \underset{d_n^{|\mathrm{im}(d_n)}}{\overset{s_{n-1|\mathrm{im}(d_n)}}{\rightleftarrows}} \mathrm{im}(d_n) \longrightarrow 0.$$

Each of these sequences split as $s_{n-1|\mathrm{im}(d_n)}$ is a section. Indeed, any element of $\mathrm{im}(d_n)$ can be written as $d_n(c)$ for some c in C_n. Since $dsd = d$, we get that $(d_n \circ s_{n-1})(d_n(c)) = d_n(c)$. Therefore we get : $d_n^{|\mathrm{im}(d_n)} \circ s_{n|\mathrm{im}(d_n)} = \mathrm{id}_{\mathrm{im}(d_n)}$. Thus $C_\bullet$ splits. □

The next exercise shows that exact sequences need not to be split exact in general.

Exercise 1.1.5. *The complex* $\cdots \overset{\cdot 2}{\to} \mathbb{Z}/4\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}/4\mathbb{Z} \overset{\cdot 2}{\to} \cdots$ *is acyclic, but not split exact.*

Proof. Clearly the morphism $\mathbb{Z}/4\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}/4\mathbb{Z}$ has kernel and image equal to $\{0, 2\} \cong \mathbb{Z}/2\mathbb{Z}$. Therefore its homology at every term is the trivial group, and so the complex is acyclic. However it is not split exact since if it were, we would have $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, which is not true (since $\mathbb{Z}/4\mathbb{Z}$ contains an element of order 4, whereas $\mathbb{Z}/2\mathbb{Z}$ does not). □

We end this part by presenting concrete computations of homology of abelian groups chain complexes, through the next two exercises. Subsequently, we will focus on chain complexes of $\mathbb{Z}$-modules.

Exercise 1.1.6. (a) *Let p be a prime number and let :*

$$\cdots \to 0 \to \mathbb{Z} \overset{\cdot p}{\to} \mathbb{Z} \to 0 \to \cdots,$$

$$\cdots \to 0 \to \mathbb{Z} \overset{0}{\to} \mathbb{Z} \to 0 \to \cdots,$$

$$\cdots \to 0 \to \mathbb{Z}/2\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}/4\mathbb{Z} \to 0 \to \cdots,$$

$$\cdots \to 0 \to \mathbb{Z}/3\mathbb{Z} \overset{\cdot 2}{\to} \mathbb{Z}/6\mathbb{Z} \to 0 \to \cdots,$$

be chain complexes of abelian groups. Compute the homology of each complex.

(b) *Let $C_\bullet$ and $D_\bullet$ be two chain complexes with isomorphic homology groups. Is is true in general that one can find a morphism of chain complexes $f : C_\bullet \to D_\bullet$ such that the induced map in homology $H_\bullet(f)$ is an isomorphism ?*

Proof. (a) We make the convention that the first non trivial term of the chain complex is the term zero. We get :

$$\begin{aligned} H_n(\cdots \to 0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to 0 \to \cdots) &= \begin{cases} \ker(\mathbb{Z} \to 0) \Big/ \mathrm{im}(\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}), & \text{if } n = 0, \\ 0, & \text{otherwise,} \end{cases} \\ &= \begin{cases} \mathbb{Z}/p\mathbb{Z}, & \text{if } n = 0, \\ 0, & \text{otherwise,} \end{cases} \end{aligned}$$

$$\begin{aligned} H_n(\cdots \to 0 \to \mathbb{Z} \xrightarrow{0} \mathbb{Z} \to 0 \to \cdots) &= \begin{cases} \ker(\mathbb{Z} \xrightarrow{0} \mathbb{Z}) \Big/ \mathrm{im}(0 \to \mathbb{Z}), & \text{if } n = 1, \\ \ker(\mathbb{Z} \to 0) \Big/ \mathrm{im}(\mathbb{Z} \xrightarrow{0} \mathbb{Z}), & \text{if } n = 0, \\ 0, & \text{otherwise,} \end{cases} \\ &= \begin{cases} \mathbb{Z}, & \text{if } n = 0, 1, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Similiarly we obtain :

$$\begin{aligned} H_n(\cdots \to 0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \to 0 \to \cdots) &\cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } n = 0, \\ 0, & \text{otherwise,} \end{cases} \\ H_n(\cdots \to 0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/6\mathbb{Z} \to 0 \to \cdots) &\cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } n = 0, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

(b) The anwser is no, as we can find a counter-example. Indeed, if we denote by

$$C_\bullet = \cdots \to 0 \to \mathbb{Z}/3\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/6\mathbb{Z} \to 0 \to \cdots,$$

and by :

$$D_\bullet = \cdots \to 0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/4\mathbb{Z} \to 0 \to \cdots,$$

the previous chain complexes, then we can define a chain map :

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/3\mathbb{Z} & \xrightarrow{\cdot 2} & \mathbb{Z}/6\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \| & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle 0} & & \| & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\cdot 2} & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots. \end{array}$$

This chain map is the only possibility between $C_\bullet$ and $D_\bullet$. However, clearly the homomorphism $H_0(\mathbb{Z}/6\mathbb{Z} \xrightarrow{0} \mathbb{Z}/4\mathbb{Z})$ is not an isomorphism, and so the chain map is not a quasi-isomorphism. □

Exercise 1.1.7. *Consider the following morphism of chain complexes of abelian groups :*

$$\begin{array}{lccccccccccccc} C_\bullet = & \cdots & \xrightarrow{0} & \mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Z} & \xrightarrow{0} & \mathbb{Z} & \xrightarrow{\cdot p} & \mathbb{Z} & \longrightarrow 0 \\ & & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle f} & \\ D_\bullet = & \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow 0. \end{array}$$

Compute the homology of $C_\bullet$ and $D_\bullet$, and show that the chain map is a quasi-isomorphism.

Proof. The homology of $C_\bullet$ is given by :

$$H_0(C_\bullet) = \ker(\mathbb{Z} \to 0) \Big/ \operatorname{im}\left(\mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z}\right) = \mathbb{Z}/p\mathbb{Z},$$

and $H_n(C_\bullet) = 0$ for $n \neq 0$, and similarly :

$$H_0(D_\bullet) = \ker(\mathbb{Z}/p\mathbb{Z} \to 0) \Big/ \operatorname{im}(0 \to \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z},$$

and $H_n(D_\bullet) = 0$ for $n \neq 0$. Therefore the induced homomorphism :

$$\begin{array}{rcl} H_0(f) : \mathbb{Z}/p\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \operatorname{cls}(z) = z + p\mathbb{Z} & \longmapsto & \operatorname{cls}([z]_p) = [z]_p, \end{array}$$

is clearly an isomorphism : it is actually the identity map. □

1.2 Projective Resolutions

The first exercise of this section presents a projective resolution that will be later useful.

Exercise 1.2.1. *Let K be a field. Let us define the ring $R = K[t]/(t^2)$. Let us denote by $\bar{t}$ the class of t in R. The field K can be given a trivial structure of R-module, where $\bar{t}$ acts by zero on K. Let us consider the sequence of R-modules :*

$$\cdots \xrightarrow{\cdot\bar{t}} R \xrightarrow{\cdot\bar{t}} R \xrightarrow{\varepsilon} K \longrightarrow 0,$$

where the morphism ε sends 1 to 1_K, and $\bar{t}$ to 0_K. Show that this sequence is a projective resolution of R-modules of the R-module K.

Proof. Since R is obviously a free R-module, it is projective. It only remains to prove the exactness of the sequence. The map ε is surjective since the class of any constant polynomial in R is sent to its representative in K. By construction, its kernel equals to the ideal $(\bar{t})$. The morphism $R \xrightarrow{\cdot\bar{t}} R$ has kernel and image equal to the ideal $(\bar{t})$, as $\bar{t} \cdot \bar{t} = 0$ in R. Therefore the sequence is exact. □

The next two exercises will make use of the comparison theorem (see Theorem 6.16 in [Rotman, 2009]).

Exercise 1.2.2. *Let $P_\bullet$ be a positive complex of projective modules. Show that $P_\bullet$ is exact if and only if $\mathrm{id}_{P_\bullet}$ and the zero chain map $0_\bullet : P_\bullet \to P_\bullet$ are homotopic.*

Proof. Suppose that $P_\bullet$ is exact. We want to apply the comparison theorem (see Theorem 6.16 in [Rotman, 2009]). We extend by zero our positive complex so that we are in the following situation :

$$\begin{array}{ccccccccccccccc} \cdots & \longrightarrow & P_n & \xrightarrow{d_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \longrightarrow & 0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \| & & \\ \cdots & \longrightarrow & P_n & \xrightarrow{d_n} & P_{n-1} & \longrightarrow \cdots \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \longrightarrow & 0 & \longrightarrow & 0. \end{array}$$

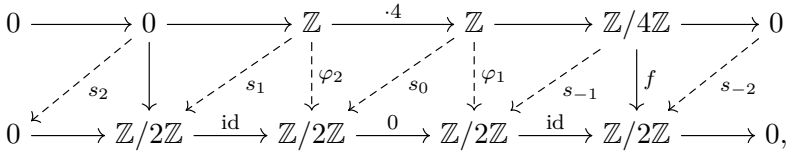
Since each non-trivial element in the top row is projective, and the bottom row is exact, the theorem implies that a chain map $P_\bullet \to P_\bullet$ which makes the above diagram commutes is unique

up to homotopy. It is straightfoward to see that the identity and zero maps are such maps. Therefore, they must be homotopic.

Conversly, if $\mathrm{id}_{P_\bullet}$ and $0_\bullet : P_\bullet \to P_\bullet$ are homotopic, then, by exercise 1.1.4, we get that $P_\bullet$ is split exact, so in particular exact. □

Exercise 1.2.3. *Let $P_\bullet = (0 \to 0 \to Z \xrightarrow{\cdot 4} \mathbb{Z})$ and $Q_\bullet = (0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 0} \mathbb{Z}/2\mathbb{Z})$. Let $f : H_0(P_\bullet) = \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} = H_0(Q_\bullet)$ be the unique non-zero $\mathbb{Z}$-morphism. Find all possible liftings $\varphi_\bullet : P_\bullet \to Q_\bullet$ and construct homotopies between the different liftings.*

Proof. We want to apply the comparison theorem (Theorem 6.16 in [Rotman, 2009]). Knowing the homology at zero, we get the following situation :



where the top row has each term projective, except $\mathbb{Z}/4\mathbb{Z}$ and the bottom row is an exact sequence. Then the comparison theorem states that there exists liftings which are the vertical dashed arrows in the diagrams. But there are only two possible homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$: the zero map, or the natural projection. Since we want a chain map (i.e. a commutative diagram), φ_1 cannot be the zero map, so we have two cases :

$$\{\varphi_2 = 0, \varphi_1 = \mathrm{proj}\} \text{ and } \{\varphi_2 = \mathrm{proj}, \varphi_1 = \mathrm{proj}\}.$$

Let us name the two possible chained maps $\varphi_\bullet^0$ and $\varphi_\bullet^{\mathrm{proj}}$ respectively. The comparison theorem states they are homotopic, so we can find a homotopy $s_n : P_n \to Q_{n+1}$ for each n, which is the diagonal dashed map in the diagram. We proceed as the proof of the theorem. We first set $s_{-2} = 0$ and $s_{-1} = 0$ for convenience, as we regard $\mathbb{Z}/4\mathbb{Z}$ and $\{0\}$ the 0-th and (-1)-st term of $P_\bullet$ and $\mathbb{Z}/2\mathbb{Z}$ and $\{0\}$ the 0-th and (-1)-st term of $Q_\bullet$. Since in both cases we have the same homomorphism φ_1, we easely see that $s_0 = 0$. To get a homotopy, we have the equation $s_1 = \varphi_2^{\mathrm{proj}} - \varphi_2^0 = \varphi_2^{\mathrm{proj}} = \mathrm{proj}$. And obviously we have $s_2 = 0$. So the homotopy s is the the zero map in each term except for s_1 which equals the projection $\mathrm{proj} : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. □

1.3 Tor and Ext

We end this chapter by investigating Tor and Ext.

Exercise 1.3.1. *Prove that if I is an injective R-module, then $\mathrm{Ext}^n_R(M, I) = 0$, for any R-module M, and any $n \geq 1$.*

Proof. An injective resolution for I can be given by :

$$E_\bullet = 0 \longrightarrow I \xrightarrow{\mathrm{id}} I \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots .$$

Therefore $\mathrm{Ext}^n_R(M, I) = H^n(\mathrm{Hom}_R(A, E^I_\bullet)) = 0$ for all $n \geq 1$, as $\mathrm{Hom}_R(M, 0) = 0$. Notice that this argument can be given for any right (covariant) derived functor. □

Exercise 1.3.2 (Tor and Ext for abelian groups)**.** *Let A be a $\mathbb{Z}$-module. Let p be a fixed integer. Show that :*

(a) $\mathrm{Tor}^{\mathbb{Z}}_{\bullet}(A, \mathbb{Z}/p\mathbb{Z})$ *is the homology of the complex* $0 \to A \xrightarrow{\cdot p} A \to 0$*, so that :*

$$\begin{gathered}\mathrm{Tor}^{\mathbb{Z}}_0(A, \mathbb{Z}/p\mathbb{Z}) \cong A/pA,\\ \mathrm{Tor}^{\mathbb{Z}}_1(A, \mathbb{Z}/p\mathbb{Z}) \cong A_p := \{a \in A \mid p \cdot a = 0\},\\ \mathrm{Tor}^{\mathbb{Z}}_n(A, \mathbb{Z}/p\mathbb{Z}) = 0, \ \textit{if } n \geq 2;\end{gathered}$$

(b) $\mathrm{Ext}^{\bullet}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A)$ *is the cohomology of the complex* $0 \to A \xrightarrow{\cdot p} A \to 0$*, so that :*

$$\begin{gathered}\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong A_p,\\ \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) \cong A/pA,\\ \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A) = 0, \ \textit{if } n \geq 2.\end{gathered}$$

Proof. (a) A $\mathbb{Z}$-projective resolution of $\mathbb{Z}/p\mathbb{Z}$ can be given by :

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0.$$

Apply $A \otimes_{\mathbb{Z}} -$ to the complex $P_\bullet$ obtained by the previous projective resolution where we replace $\mathbb{Z}/p\mathbb{Z}$ by 0, we get :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \otimes_{\mathbb{Z}} \mathbb{Z} & \xrightarrow{\cdot(\mathrm{id} \otimes p)} & A \otimes_{\mathbb{Z}} \mathbb{Z} & \longrightarrow & 0\\ & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & A & \xrightarrow{\cdot p} & A & \longrightarrow & 0. \end{array}$$

From the commutativity of the above diagram, it follows that, for any n :

$$\begin{aligned}\mathrm{Tor}^{\mathbb{Z}}_n(A, \mathbb{Z}/p\mathbb{Z}) &= H_n(A \otimes_{\mathbb{Z}} P_\bullet)\\ &\cong H_n(0 \to A \xrightarrow{\cdot p} A \to 0)\\ &= \begin{cases} \ker(A \to 0) \Big/ \mathrm{im}\left(A \xrightarrow{\cdot p} A\right) = A/pA, & \text{if } n = 0,\\ \ker\left(A \xrightarrow{\cdot p} A\right) \Big/ \mathrm{im}(0 \to A) = A_p, & \text{if } n = 1,\\ 0, & \text{if } n \geq 2. \end{cases}\end{aligned}$$

(b) As before, we consider the complex $P_\bullet$ obtained from the projective resolution of $\mathbb{Z}/p\mathbb{Z}$, and we apply $\mathrm{Hom}_{\mathbb{Z}}(-, A)$:

$$\begin{array}{ccccccccc} \mathrm{Hom}_{\mathbb{Z}}(0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) & \xrightarrow{(\cdot p)^*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(0, A)\\ \| & & \downarrow \cong & & \downarrow \cong & & \| \\ 0 & \longrightarrow & A & \xrightarrow{\cdot p} & A & \longrightarrow & 0, \end{array}$$

where the vertical isomorphism is the evaluation at 1. In details, the isomorphism of abelian groups is :

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) &\longrightarrow A\\ f &\longmapsto f(1).\end{aligned}$$

It is vacuous to check that it is a homomorphism, and it is bijective since any abelian group homomorphism $f : \mathbb{Z} \to A$ is entirely determined by its value in 1, since we have the equation $f(k) = kf(1)$, for all $k \in \mathbb{Z}$. We get that $\mathrm{Ext}^\bullet_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, A)$ is the cohomology of the complex $0 \to A \xrightarrow{\cdot p} A \to 0$. he computation of the cohomology at each dimension n is as straightfoward as the previous question (a). □

Exercise 1.3.3. *Let K be a field and $R = K[t]/(t^2)$. As in exercise* 1.2.1*, K can be regarded as a trivial R-module.*

(a) *Show that, for any R-module M :*

$$\mathrm{Ext}^n_R(K, M) \cong \begin{cases} M_t, & \text{if } n = 0, \\ M_t/tM & \text{if } n \geq 1, \end{cases}$$

where $M_t = \{m \in M \mid \bar{t} \cdot m = 0\}$, where $\bar{t}$ is the class of t in R.

(b) *Compute $\mathrm{Ext}^n_R(K, K)$ and $\mathrm{Ext}^n_R(K, R)$, for every $n \geq 1$.*

Proof. (a) In exercise 1.2.1, we have seen that a projective resolution P of R-modules of K can be given by :

$$\cdots \xrightarrow{\cdot\bar{t}} R \xrightarrow{\cdot\bar{t}} R \xrightarrow{\varepsilon} K \longrightarrow 0,$$

where the morphism ε sends 1 to 1_K, and $\bar{t}$ to 0_K. We apply $\mathrm{Hom}_R(-, M)$ to the deleted projective resolution P_K, we get :

$$\begin{array}{ccccccc} \mathrm{Hom}_R(0, M) & \longrightarrow & \mathrm{Hom}_R(R, M) & \xrightarrow{(\cdot\bar{t})^*} & \mathrm{Hom}_R(R, M) & \xrightarrow{(\cdot\bar{t})^*} & \cdots \\ \| & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \longrightarrow & M & \xrightarrow{\cdot\bar{t}} & M & \xrightarrow{\cdot\bar{t}} & \cdots, \end{array}$$

where the vertical isomorphism is the evaluation at the class of 1_K in R (the same that is given in exercise 1.3.2). The result follows.

(b) Let $n \geq 1$. We apply the previous result. Recall that $\bar{t}$ acts as zero on K, therefore :

$$\mathrm{Ext}^n_R(K, K) = K_t/tK = K/\{0\} \cong K.$$

Moreover, one can see that $\mathrm{Ext}^n_R(K, R) = 0$, as R is free, but also by applying (a) and using the fact that $R_t = tR$. □

Exercise 1.3.4. *Show that if $\mathrm{Ext}^1_R(M, N) = 0$, then any short exact sequence :*

$$0 \to N \xrightarrow{i} X \xrightarrow{j} M \to 0,$$

of R-modules, splits.

Proof. We only need to find a retraction $r : X \to N$ of the short exact sequence. We regard the fonctors $\mathrm{Ext}^\bullet_R(-, N)$ as the cohomological extension of the contravariant additive functor $\mathrm{Hom}_R(-, N)$, so there exists a (natural) connecting homomorphism Δ such that we have the following exact sequence (see [Rotman, 2009], Corrolary 6.65) :

$$0 \to \mathrm{Hom}_R(M, N) \xrightarrow{j^*} \mathrm{Hom}_R(X, N) \xrightarrow{i^*} \mathrm{Hom}_R(N, N) \xrightarrow{\Delta} \mathrm{Ext}^1_R(M, N) \longrightarrow \cdots$$

In particular, since $\mathrm{Ext}^1_R(M, N) = 0$, we have that $i^* : \mathrm{Hom}_R(X, N) \to \mathrm{Hom}_R(N, N)$ is surjective. Therefore, there exists $r \in \mathrm{Hom}_R(X, N)$ such that $r \circ i = i^*(r) = \mathrm{id}_N$. So $r : X \to N$ is a retraction. □

Exercise 1.3.5. *Show that if R is hereditary (i.e. all submodules of an R-projective module are projective), then $\mathrm{Tor}_n^R(A,B) = 0$, for all $n \geq 2$, for all R-modules A and B.*

Proof. Define the free R-module F generated by the elements of A, and let $p : F \to A$ be the natural projection. Since F is projective as it is free, then $\ker p$ is also projective, because R is hereditary. Therefore we have found a projective resolution of A of lenght 2 :

$$\cdots \longrightarrow 0 \longrightarrow 0 \longrightarrow \ker p \hookrightarrow F \xrightarrow{p} A \longrightarrow 0.$$

In fact, we have just proved that the global dimension of an hereditary ring is always at most 1. It is then straightfoward that $\mathrm{Tor}_n^R(A,B) = 0$ for all $n \geq 2$. □

Exercise 1.3.6. *Show that if A and B are finite abelian groups, then $\mathrm{Tor}_1^{\mathbb{Z}}(A,B) \cong A \otimes_{\mathbb{Z}} B$.*

Proof. We first argue that it suffices to prove for the case $A = \mathbb{Z}/n\mathbb{Z}$ and $B = \mathbb{Z}/m\mathbb{Z}$. Indeed, suppose we have shown that $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$, for any n and m. From the classification of finite abelian groups, we can write $A = \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$ and $B = \bigoplus_{j=1}^s \mathbb{Z}/m_j\mathbb{Z}$, so we get, by using the compatibility of $\oplus$ with $\otimes$:

$$\begin{aligned}
\mathrm{Tor}_1^{\mathbb{Z}}(A,B) &\cong \mathrm{Tor}_1^{\mathbb{Z}}\left(\bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}, \bigoplus_{j=1}^s \mathbb{Z}/m_j\mathbb{Z}\right) \\
&\cong \bigoplus_{i=1}^r \bigoplus_{j=1}^s \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n_i\mathbb{Z}, \mathbb{Z}/m_j\mathbb{Z}) \\
&\cong \bigoplus_{i=1}^r \bigoplus_{j=1}^s (\mathbb{Z}/n_i\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m_j\mathbb{Z}) \\
&\cong \left(\bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}\right) \otimes_{\mathbb{Z}} \left(\bigoplus_{j=1}^s \mathbb{Z}/m_j\mathbb{Z}\right) \\
&\cong A \otimes_{\mathbb{Z}} B.
\end{aligned}$$

So let us prove $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$. From our work in exercise 1.3.2, we get :

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})_n := \{\overline{k} \in \mathbb{Z}/m\mathbb{Z} \mid n \cdot \overline{k} = 0\} \cong \mathbb{Z}/\gcd(n,m)\mathbb{Z},$$

Since $\mathbb{Z}/\gcd(n,m)\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$, the result follows. □

Exercise 1.3.7. *Prove that if A is an abelian group with $nA = A$ for some positive integer n, then every extension $0 \to A \to X \to \mathbb{Z}/n\mathbb{Z} \to 0$ splits.*

Proof. From exercise 1.3.4, we only need to show that $\mathrm{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/n\mathbb{Z}, A) = A/nA = 0$. But this follows directly from exercise 1.3.2, as $nA = A$. □

Chapter 2

Group Cohomology

The exercises of this chapter are based on the theory of group (co)homology presented in Chapter 9 of [Rotman, 2009] and Chapter IV of [Brown, 1982].

2.1 First Computations

Let us begin by answering what is the cohomology of the trivial group.

Exercise 2.1.1. *Compute the cohomology of the trivial group.*

Proof. Let G be the trivial group, and let A be any $\mathbb{Z}G$-module. In this case, the action of G on A is vacuous, so that A can be any abelian group. In order to compute $H^n(G, A)$, since $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$, we need a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module, i.e., as an abelian group. Such a resolution can be given by :

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mathrm{id}_{\mathbb{Z}}} \mathbb{Z} \longrightarrow 0.$$

So that $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ is given by the cohomology of the cochain :

$$\ldots \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \longrightarrow 0.$$

We obtain : $H^0(G, A) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ (the isomorphism was proven in exercise 1.3.2) and $H^n(G, A) = 0$, whenever $n \geq 0$. □

Recall that the n-th cohomology of an $\mathbb{Z}G$-module A is given by $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$. But one can wonder why we are only interested with $\mathbb{Z}G$-modules, and not KG-modules, where K is a commutative ring. It is actually enough to consider $\mathbb{Z}G$-modules, as shown in the following exercise.

Exercise 2.1.2. *Let K be a commutative ring, let G be a group, and let A be a KG-module.*

(a) *If F is a free $\mathbb{Z}G$-module with $\mathbb{Z}G$-basis S, prove that* $\mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(F, A)$.

(b) *Prove that* $\mathrm{Ext}^n_{KG}(K, A) \cong \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof. (a) Since F is a free $\mathbb{Z}G$-module, then $K \otimes_{\mathbb{Z}} F$ is a free KG-module with basis $\widetilde{S}$ given by $\{1 \otimes s \mid s \in S\}$. Indeed, since F is a free $\mathbb{Z}G$-module, then $F \cong \bigoplus_{i=1}^{r} \mathbb{Z}G$, for some integer $r > 0$. So we get :

$$K \otimes_{\mathbb{Z}} F \cong K \otimes_{\mathbb{Z}} \left(\bigoplus_{i=1}^{r} \mathbb{Z}G \right) \cong \bigoplus_{i=1}^{r} (K \otimes_{\mathbb{Z}} \mathbb{Z}G) \cong \bigoplus_{i=1}^{r} KG,$$

where the last isomorphism stems from the following isomorphism :

$$\begin{array}{rcl} K \otimes_{\mathbb{Z}} \mathbb{Z}G & \longrightarrow & KG \\ \lambda \otimes \sum\limits_{g \in G} m_g g & \longmapsto & \sum\limits_{g \in G} \lambda m_g g. \end{array}$$

So $K \otimes_{\mathbb{Z}} F$ is a free KG-module. We define :

$$\Phi : \mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(F, A),$$

as $\Phi(f)(x) = f(1 \otimes x)$, for any $x \in F$, and any KG-morphism $f : K \otimes_{\mathbb{Z}} F \to A$. Since f is a KG-morphism, we have that $\Phi(f)(gx) = f(1 \otimes gx) = gf(1 \otimes x)$ for any $g \in G$, so $\Phi(f)$ is indeed a $\mathbb{Z}G$-morphism. Thus Φ is clearly a well-defined abelian group homomorphism. For any $\mathbb{Z}G$-morphism $h : F \to A$, we define $\Psi(h) : K \otimes_{\mathbb{Z}} F \to A$ on the basis $\widetilde{S}$ as $\Psi(h)(1 \otimes s) = h(s)$ and extend it KG-linearly, and this defines an abelian group homomorphism :

$$\Psi : \mathrm{Hom}_{\mathbb{Z}G}(F, A) \longrightarrow \mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A).$$

We get directly $(\Phi \circ \Psi)(h)(1 \otimes s) = h(1 \otimes s)$ and $(\Psi \circ \Phi)(f)(s) = f(s)$, for any s in S. Since the maps agree on the basis, we get that $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Hom}_{\mathbb{Z}G}(F,A)}$ and $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A)}$, and so : $\mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(F, A)$.

(b) Let :

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z},$$

be the free standard resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module (see [Brown, 1982] chapter II). We apply the functor $K \otimes_{\mathbb{Z}} -$ and we obtain a free resolution of K as a KG-module :

$$\cdots \longrightarrow K \otimes_{\mathbb{Z}} F_2 \xrightarrow{\mathrm{id}_K \otimes d_2} K \otimes_{\mathbb{Z}} F_1 \xrightarrow{\mathrm{id}_K \otimes d_1} K \otimes_{\mathbb{Z}} F_0 \xrightarrow{\mathrm{id}_K \otimes d_0} K \otimes_{\mathbb{Z}} \mathbb{Z} \cong K.$$

In order to compute $\mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ and $\mathrm{Ext}^n_{KG}(K, A)$, we must apply $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$ and $\mathrm{Hom}_{KG}(-, A)$ respectively on the appropriate free resolutions. The previous isomorphism in part (a) defines an isomorphism of chain complexes :

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F_0, A) & \longrightarrow & \mathrm{Hom}_{KG}(K \otimes_{\mathbb{Z}} F_1, A) & \longrightarrow & \cdots \\ & & \Phi_0 \downarrow \cong & & \Phi_1 \downarrow \cong & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(F_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) & \longrightarrow & \cdots . \end{array}$$

It is straightfoward to check the commutativity of the above diagram. Since the cochains of complexes are isomorphic, their cohomology are also isomorphic (see Proposition 6.8 in [Rotman, 2009]), and therefore, for all $n \geq 0$: $\mathrm{Ext}^n_{KG}(K, A) \cong \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$. □

Exercise 2.1.3 (The Augmentation Ideal)**.** *Let G be any group, we denote its unit $1 = 1_G$. Let $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ be the augmentation map : $\varepsilon(g) = 1$ for all g in G. Let $IG = \ker \varepsilon$ be the augmentation ideal.*

(a) *Prove that IG is a free $\mathbb{Z}$-module with basis $\{g - 1 \mid g \in G \setminus \{1\}\}$.*

(b) *Prove that if S is a set of generators of G, then IG is generated as a $\mathbb{Z}G$-module by the set $\{s - 1 \mid s \in S\}$.*

(c) *Prove that for every* $n \geq 1$, $H^n(G, A) \cong \mathrm{Ext}^{n-1}_{\mathbb{Z}G}(IG, A)$ *and* $H_n(G, B) \cong \mathrm{Tor}^{\mathbb{Z}}_{n-1}(IG, B)$.

(d) *If* A *and* B *are trivial* $\mathbb{Z}G$*-modules, we get isomorphisms :* $H^1(G, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$ *and* $H_1(G, B) \cong IG \otimes_{\mathbb{Z}G} B$.

(e) *Set* $G_{\mathrm{Ab}} := G/[G, G]$. *Prove that* $(IG/(IG)^2, +) \cong (G_{\mathrm{Ab}}, \cdot)$, *via the map* $\overline{g-1} \mapsto \overline{g}$.

(f) *If* A *and* B *are trivial* $\mathbb{Z}G$*-modules, then we get the following sequence of abelian group isomorphisms :*

$$\begin{aligned} H^1(G, A) &\cong \mathrm{Hom}_{\mathbb{Z}G}(IG, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2, A) \cong \mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2, A) \\ &\cong \mathrm{Hom}_{\mathbb{Z}}(G_{\mathrm{Ab}}, A) \cong \mathrm{Hom}_{\mathscr{G}r}(G, A), \end{aligned}$$

where $\mathrm{Hom}_{\mathscr{G}r}(G, A)$ *is the group of all group homomorphisms* $G \to A$*; and :*

$$H_1(G, B) \cong IG \otimes_{\mathbb{Z}G} B \cong IG/(IG)^2 \otimes_{\mathbb{Z}G} B \cong IG/(IG)^2 \otimes_{\mathbb{Z}} B \cong G_{\mathrm{Ab}} \otimes_{\mathbb{Z}} B.$$

(g) $H_1(G, \mathbb{Z}) \cong G_{\mathrm{Ab}}$ *and, if* G *is finite,* $H^1(G, \mathbb{Z}) = 0$.

Proof. (a) If $x = \sum_{g \in G} \lambda_g g \in IG$, then $\sum_{g \in G} \lambda_g = 0$. Therefore :

$$x = x - (\sum_{g \in G} \lambda_g)1 = \sum_{g \in G} \lambda_g g - (\sum_{g \in G} \lambda_g)1 = \sum_{g \in G \setminus \{1\}} \lambda_g (g - 1),$$

so any $x \in IG$ is spanned by $\{g-1 \mid g \in G \setminus \{1\}\}$. Let us prove that the set is independant : $\sum_{g \neq 1} \lambda_g (g-1) = 0$ implies that $\sum_{g \neq 1} \lambda_g g - (\sum_{g \neq 1} \lambda_g) = 0$, but $\mathbb{Z}G$ is free abelian, so $\lambda_g = 0$ for all $g \neq 1$.

(b) We can express any element of the $\mathbb{Z}$-basis $\{g - 1 \mid g \in G \setminus \{1\}\}$ as an element of the $\mathbb{Z}G$-module generated by the set $\{s - 1 \mid s \in S\}$, via the formulas :

$$gh - 1 = g(h - 1) + (g - 1),$$

$$g^{-1} - 1 = -g^{-1}(g - 1),$$

for any $g \in G \setminus \{1\}$, as any element of G is a product of elements of S and their inverses.

(c) This is straightfoward from the properties of Tor and Ext (see [Rotman, 2009] Corrolary 6.23), take the standard resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module :

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \cong \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0.$$

As $IG = \ker \varepsilon = \mathrm{im}\, d_1$, we obtain a projective resolution of IG as a $\mathbb{Z}G$-module by corestricting d_1 to its image :

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} IG \longrightarrow 0.$$

So when we compute $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}G}(\mathbb{Z}, A)$ and $H_n(G, A) = \mathrm{Tor}^{\mathbb{Z}G}_n(\mathbb{Z}, B)$, we simply compute $\mathrm{Ext}^{n-1}_{\mathbb{Z}G}(IG, A)$ and $\mathrm{Tor}^{\mathbb{Z}G}_{n-1}(IG, B)$ respectively, as long as $n \geq 2$, for any $\mathbb{Z}G$-modules A and B.

(d) In previous question we had the exact sequences :

$$\cdots \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

$$d_1^{|IG} \searrow \quad \nearrow \hookrightarrow$$

$$IG$$

$$\nearrow \quad \searrow$$

$$0 \qquad\qquad 0.$$

Therefore, when we apply $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$, as it is a left exact contravariant functor, we get :

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \xrightarrow{\varepsilon^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \xrightarrow{d_1^*} \mathrm{Hom}_{\mathbb{Z}G}(F_1, A) \xrightarrow{d_2^*} \cdots$$

$$\searrow \quad \nearrow$$

$$\mathrm{Hom}_{\mathbb{Z}G}(IG, A)$$

$$\nearrow$$

$$0.$$

But in this case, as A has a trivial $\mathbb{Z}G$-structure, we get that ε^* is an isomorphism, as we can find an inverse :

$$\begin{array}{rcl} \mathrm{res} : \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \\ f & \longmapsto & f_{|\mathbb{Z}}, \end{array}$$

where $f_{|\mathbb{Z}}(k) := f(k \cdot 1_G)$, for any $k \in \mathbb{Z}$. It is well-defined as $f(g) = gf(1_G) = f(1_G)$, for all $g \in G$. It is then straightfoward to see that $\varepsilon^* \circ \mathrm{res} = \mathrm{id}_{\mathbb{Z}G(\mathbb{Z}G,A)}$ and $\mathrm{res} \circ \varepsilon^* = \mathrm{id}_{\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},A)}$. Thus by exactness we have :

$$H^1(G, A) = \ker d_2^* / \mathrm{im}\ d_1^* = \mathrm{Hom}_{\mathbb{Z}G}(IG, A) / \ker \varepsilon^* = \mathrm{Hom}_{\mathbb{Z}G}(IG, A).$$

(e) We begin by noticing that we have the following relation in $\mathbb{Z}G$:

$$\underbrace{(g-1) \cdot (h-1)}_{\in (IG)^2} = (gh-1) - (g-1) - (h-1). \qquad (\star)$$

Define $\varphi' : IG \to G_{\mathrm{Ab}}$ as the composite of :

$$\begin{array}{rcl} \varphi : IG & \longrightarrow & G \\ \displaystyle\sum_{g \in G \setminus \{1\}} \lambda_g (g-1) & \longmapsto & \displaystyle\prod_{g \in G \setminus \{1\}} g^{\lambda_g}, \end{array}$$

with the natural projection : $G \twoheadrightarrow G_{\mathrm{Ab}} = G/[G, G]$. It is straightfoward that φ is a group homomorphism, and so φ' is also a group homomorphism. Denote by $\overline{g}$ the class of g in G_{Ab}. We argue that $(IG)^2 \subseteq \ker \varphi'$. Indeed, let $x \in (IG)^2$, so that :

$$\begin{aligned} x &= \left(\sum_{g \in G \setminus \{1\}} \lambda_g (g-1) \right) \cdot \left(\sum_{h \in G \setminus \{1\}} \mu_h (h-1) \right) \\ &= \sum_{g,h \in G \setminus \{1\}} \lambda_g \mu_h \left((g-1)(h-1) \right) \\ &= \sum_{g,h \in G \setminus \{1\}} \lambda_g \mu_h \left((gh-1) - (g-1) - (h-1) \right), \end{aligned}$$

by $(\star)$. Therefore we get :

$$\begin{aligned}\varphi(x) &= \varphi\left(\sum_{g,h\in G\setminus\{1\}} \lambda_g\mu_h\left((gh-1)-(g-1)-(h-1)\right)\right)\\ &= \prod_{g,h\in G\setminus\{1\}} \varphi((gh-1)-(g-1)-(h-1))^{\lambda_g\mu_h}\\ &= \prod_{g,h\in G\setminus\{1\}} (ghg^{-1}h^{-1})^{\lambda_g\mu_h} \in [G,G],\end{aligned}$$

so that $(IG)^2 \subseteq \ker\varphi'$. By the universal property of the quotient, there is a unique group homomorphism $\Phi : IG/(IG)^2 \to G_{\mathrm{Ab}}$ such that the following diagram commutes :

$$\begin{array}{ccccc} IG & \xrightarrow{\ \varphi\ } & G & \twoheadrightarrow & G_{\mathrm{Ab}} \\ \downarrow & & & \nearrow_{\Phi} & \\ IG/(IG)^2. & & & & \end{array}$$

In particular $\Phi(\overline{g-1}) = \overline{g}$, where $\overline{g-1}$ denotes the class of $g-1$ in $IG/(IG)^2$.
We now define its inverse :

$$\begin{aligned}\psi : G &\longrightarrow IG/(IG)^2\\ g &\longmapsto \overline{g-1}.\end{aligned}$$

We argue that ψ is indeed a group homomorphism. Indeed, from $(\star)$, we have :

$$\begin{aligned}\psi(gh) &= \overline{gh-1}\\ &= \overline{(g-1)} + \overline{(h-1)}\\ &= \psi(g)+\psi(h),\end{aligned}$$

for any $g, h \in G$. Since IG is abelian, then $[G,G] \subseteq \ker\psi$, by the universal property of the abelianization (see [Lang, 1974] Theorem 7.8 of Chapter II). Therefore, by the universal property of the quotient, there is a unique homomorphism $\Psi : G_{\mathrm{Ab}} \to IG/(IG)^2$ such that the following diagram commutes :

$$\begin{array}{ccc} G & \xrightarrow{\ \psi\ } & IG/(IG)^2 \\ \downarrow & \nearrow_{\Psi} & \\ G_{\mathrm{Ab}}. & & \end{array}$$

In particular $\Psi(\overline{g}) = \overline{g-1}$. It is straightfoward that Φ and Ψ are mutally inverse, using that IG has the set $\{g-1\}_{g\neq 1}$ as a $\mathbb{Z}$-basis.

(f) From (d), we have $H^1(G,A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG,A)$. We show the rest of the abelian group isomorphisms step by step.

- Let us prove that :

$$\mathrm{Hom}_{\mathbb{Z}G}(IG,A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2,A).$$

Let us name $\pi : IG \to IG/(IG)^2$ the projection. It induces, for a fixed $\mathbb{Z}G$-module A, an isomorphism of groups between the group formed by the $\mathbb{Z}G$-morphisms $IG \to A$ containing $(IG)^2$ in their kernel, and $\mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2, A)$. We have seen in question (c) that the elements $(gh-1)-(g-1)-(h-1)$ for $g, h \neq 1$ in G, span $(IG)^2$. For any $\mathbb{Z}G$-morphism $\varphi : IG \to A$, we get :

$$\begin{aligned}\varphi((gh-1)-(g-1)-(h-1)) &= \varphi(gh-1)-\varphi(g-1)-\varphi(h-1)\\ &= \varphi(g(h-1)+(g-1))-\varphi(g-1)-\varphi(h-1)\\ &= g\varphi(h-1)+\varphi(g-1)-\varphi(g-1)-\varphi(h-1),\end{aligned}$$

as any g acts trivially on $\varphi(h-1)$ since A is a trivial $\mathbb{Z}G$-module. Therefore we obtain $(IG)^2 \subseteq \ker\varphi$, for any $\mathbb{Z}G$-morphism $\varphi : IG \to A$. We obtained the isomorphism of abelian groups :

$$\mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, A),$$

via π_*, by the universal property of the quotient.

- We now claim we have the isomorphism of abelian groups :

$$\mathrm{Hom}_{\mathbb{Z}G}(IG/(IG)^2, A) \cong \mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2, A).$$

This follows directly from the fact that both $IG/(IG)^2$ and A are trivial $\mathbb{Z}G$-modules. Indeed, for any $h \in G \setminus \{1\}$, and any $g \in G$, from the relation $(\star)$, we get :

$$\begin{aligned}g\cdot(h-1) &= gh-g\\ &= (gh-1)-(g-1)\\ &= (g-1)\cdot(h-1)+(h-1),\end{aligned}$$

and so, in $IG/(IG)^2$, we get $g\cdot\overline{h-1} = \overline{h-1}$. Therefore $IG/(IG)^2$ is a trivial $\mathbb{Z}G$-module.

- The isomorphism in (e) induces the isomorphism of abelian groups :

$$\mathrm{Hom}_{\mathbb{Z}}(IG/(IG)^2, A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{\mathrm{Ab}}, A).$$

- Since A is abelian, we have $G/(\ker\varphi)$ is an abelian group for any group homomorphim $\varphi : G \to A$, and so $[G,G] \subseteq \ker\varphi$ and φ defines uniquely an abelian group homorphism $G_{\mathrm{Ab}} \to A$. Therefore, the universal property of the quotient implies that we have the isomorphism of abelian groups :

$$\mathrm{Hom}_{\mathscr{G}r}(G, A) \cong \mathrm{Hom}_{\mathbb{Z}}(G_{\mathrm{Ab}}, A).$$

And so, this finishes the proof that $H^1(G, A) \cong \mathrm{Hom}_{\mathscr{G}r}(G, A)$.

We now want to prove that, for B a trivial $\mathbb{Z}G$-module :

$$H_1(G, B) \cong IG \otimes_{\mathbb{Z}G} B \cong IG/(IG)^2 \otimes_{\mathbb{Z}G} B \cong IG/(IG)^2 \otimes_{\mathbb{Z}} B \cong G_{\mathrm{Ab}} \otimes_{\mathbb{Z}} B.$$

All the isomorphisms are shown similarly, except $IG \otimes_{\mathbb{Z}G} B \cong IG/(IG)^2 \otimes_{\mathbb{Z}G} B$. Let us define $\mu : IG \times B \to IG/(IG)^2 \otimes_{\mathbb{Z}G} B$ as the composite of :

$$IG \times B \xrightarrow{\pi \times \mathrm{id}_B} IG/(IG)^2 \times B \twoheadrightarrow IG/(IG)^2 \otimes_{\mathbb{Z}G} B.$$

The map μ is $\mathbb{Z}G$-bilinear. Indeed the additivity in the two variable is clear. We now want to check that $\mu((h-1)\cdot g, b) = \psi(h-1, gb)$, for all $g \in G$, $h \in G \setminus \{1\}$, and $b \in B$. Since $IG/(IG)^2$ and B are both trivial $\mathbb{Z}G$-modules, we get :

$$\mu((h-1)\cdot g, b) = (\overline{h-1}\cdot g)\otimes b = \overline{h-1}\otimes b = \overline{h-1}\otimes gb = \mu(h-1, gb).$$

So μ is bilinear. From the universal property of the tensor product, we get there exists a unique abelian group homomorphism $\overline{\mu}$, such that the diagram commutes :

$$\begin{array}{ccc} IG\times B & \xrightarrow{\ \mu\ } & IG/(IG)^2\otimes_{\mathbb{Z}G} B \\ \downarrow & \nearrow_{\overline{\mu}} & \\ IG\otimes_{\mathbb{Z}G} B. & & \end{array}$$

We now define an inverse of $\overline{\mu}$. Define the $\mathbb{Z}G$-bilinear map :

$$\begin{array}{rcl} \nu : IG/(IG)^2\times B & \longrightarrow & IG\otimes_{\mathbb{Z}G} B \\ (\overline{g-1}, b) & \longmapsto & (g-1)\otimes b. \end{array}$$

We must show it is well defined, i.e., for any $g_1, g_2 \neq 1$ in G such that $\overline{g_1-1} = \overline{g_2-1}$, we have $\nu(\overline{g_1-1}, b) = \nu(\overline{g_2-1}, b)$, for every $b \in B$. By linearity, as $\overline{g_1-1} = \overline{g_2-1}$, we can assume without loss of generality that there exist $g, h \neq 1$ in G such that :

$$(g_1-1) = (g_2-1) + (gh-1) - (g-1) - (h-1).$$

Then we get :

$$\nu(\overline{g_1-1}, b) \;=\; \nu(\overline{g_2-1}, b) + ((gh-1)-(g-1)-(h-1))\otimes b.$$

But we have :

$$\begin{array}{rcl} ((gh-1)-(g-1)-(h-1))\otimes b & = & (gh-1)\otimes b - (g-1)\otimes b - (h-1)\otimes b \\ & = & (g(h-1)+(g-1))\otimes b - (g-1)\otimes b - (h-1)\otimes b \\ & = & (g(h-1))\otimes b - (h-1)\otimes b \\ & = & (h-1)\otimes (gb) - (h-1)\otimes b \\ & = & (h-1)\otimes b - (h-1)\otimes b \\ & = & 0. \end{array}$$

Therefore $\nu(\overline{g_1-1}, b) = \nu(\overline{g_2-1}, b)$. So ν is well-defined. It is straightfoward to see that ν is indeed $\mathbb{Z}G$-bilinear. Therefore by the universal property of the tensor product, there exists a unique abelian group homomorphism $\overline{\nu}$ such that the diagram commutes :

$$\begin{array}{ccc} IG/(IG)^2\times B & \xrightarrow{\ \nu\ } & IG\otimes_{\mathbb{Z}G} B \\ \downarrow & \nearrow_{\overline{\nu}} & \\ IG/(IG)^2\otimes_{\mathbb{Z}G} B, & & \end{array}$$

as B is a trivial $\mathbb{Z}G$-module.

(g) We apply the previous result :

$$H_1(G,\mathbb{Z}) \cong G_{\mathrm{Ab}} \otimes_{\mathbb{Z}} \mathbb{Z} \cong G_{\mathrm{Ab}},$$

and if G is finite, there is only one homomorphism $G \to \mathbb{Z}$, that is the trivial map, since we must have $|G| \cdot f(g) = 0$ for any $g \in G$ and any group homomorphism $f : G \to \mathbb{Z}$, where $|G|$ denotes the order of G. Therefore $H^1(G,\mathbb{Z}) \cong \mathrm{Hom}_{\mathscr{G}r}(G,\mathbb{Z}) = 0$. □

We are now interested in the cohomology of the infinite cyclic group. For finite cyclic groups, we refer the reader to chapter III.1 in [Brown, 1982].

Exercise 2.1.4 (Cohomology of infinite cyclic groups)**.** *Let $G := \langle g \rangle$ be an infinite cyclic group.*

(a) *Prove that $0 \to \mathbb{Z}G \xrightarrow{m_{g-1}} \mathbb{Z}G$ is a projective resolution of $\mathbb{Z}$, where m_{g-1} is the multiplication by $g-1$.*

(b) *Compute $H^n(G,A)$ for all $n \geq 0$, and all $\mathbb{Z}G$-module A.*

Proof. (a) As $\mathbb{Z}G$ is a free $\mathbb{Z}G$-module, we must only prove that the sequence :

$$0 \longrightarrow \mathbb{Z}G \xrightarrow{m_{g-1}} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

is exact, where ε is the augmentation map. The map ε is obviously surjective. By exercise 2.1.3, the augmentation ideal $\ker\varepsilon =: IG$ is the $\mathbb{Z}G$-module generated by the element $g-1$, i.e., we get $\mathrm{im}\, m_{g-1} = \ker\varepsilon$. It only remains to prove that m_{g-1} is injective. For this matter, take $x \in \mathbb{Z}G$: there exists finitely many non-zero integers λ_i such that :

$$x = \sum_{i\in\mathbb{N}} \lambda_i g^i.$$

Suppose that $x \in \ker m_{g-1}$, i.e., $m_{g-1}(x) = 0$. We get :

$$\begin{aligned} 0 &= (g-1)\sum_{i\in\mathbb{N}} \lambda_i g^i \\ &= \sum_{i\in\mathbb{N}} \lambda_i g^{i+1} - \sum_{i\in\mathbb{N}} \lambda_i g^i, \end{aligned}$$

so that : $\sum_{i\in\mathbb{N}} \lambda_i g^{i+1} = \sum_{i\in\mathbb{N}} \lambda_i g^i$, i.e., $\lambda_i = \lambda_{i+1}$, for all $i \in \mathbb{N}$. But since $\lambda_i = 0$ for all $i \in \mathbb{N}$ except for finitely many, we get that $\lambda_i = 0$ for all $i \in \mathbb{N}$, i.e., $x = 0$. Therefore m_{g-1} is injective.

(b) The abelian group $H^n(G,A)$ is given by the cohomology of the cochain complex :

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) & \xrightarrow{(m_{g-1})^*} & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots, \\ & & \downarrow\cong & & \downarrow\cong & & & & & & \\ 0 & \longrightarrow & A & \xrightarrow{\cdot(g-1)} & A & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

and so $H^n(G,A) = 0$ whenever $n \geq 2$, and

$$H^0(G,A) = \ker((m_{g-1})^*) \cong \ker(\cdot(g-1)) = \{a \in A \mid ga = a\},$$

and $H^1(G,A) \cong A_G = A/\langle ga - a\rangle_{a\in A}$. □

2.2 Group Extensions and Low-Dimensional Cohomology

A better understanding of the low-dimensional cohomology will be given by the following exercises. We want prove again the result of exercise 2.1.4.

Exercise 2.2.1. *Let G be a group. Let A be a $\mathbb{Z}G$-module. Let $A \rtimes G$ be the set $A \times G$ with the group law :*

$$\begin{array}{rcl} (A \times G) \times (A \times G) & \longrightarrow & A \times G \\ ((a,g),(b,h)) & \longmapsto & (a,g) \cdot (b,h) := (a + gb, gh). \end{array}$$

(a) *Prove that $A \rtimes G$ is indeed a group.*

(b) *Prove that the set of derivations :*

$$\mathrm{Der}(G,A) := \{d : G \to A \text{ function} \mid d(gh) = d(g) + gd(h), \forall g,h \in G\},$$

is in bijection with the set $\mathrm{Hom}'(G, A \rtimes G)$ of sections of the exact sequence of groups :

$$0 \longrightarrow A \xrightarrow{i} A \rtimes G \xrightarrow{\pi} G \longrightarrow 1,$$

where $i(a) = (a, 1_G)$ for all $a \in A$, and $\pi(a,g) = g$ for all $(a,g) \in A \rtimes G$.[1]

Proof. (a) Let us prove that the three axioms hold for $(A \rtimes G, \cdot)$.

Associativity : Let a, b, c be in A and g, h, k in G. We need to prove that :

$$((a,g) \cdot (b,h)) \cdot (c,k) = (a,g) \cdot ((b,h) \cdot (c,k)).$$

We have on the one hand :

$$\begin{array}{rcl} ((a,g) \cdot (b,h)) \cdot (c,k) & = & (a + gb, gh) \cdot (c,k) \\ & = & (a + gb + (gh)c, g(hk)), \end{array}$$

and on the other hand :

$$\begin{array}{rcl} (a,g) \cdot ((b,h) \cdot (c,k)) & = & (a,g) \cdot (b + hc, hk) \\ & = & (a + g(b + hc), g(hk)) \\ & = & (a + gb + g(hc), g(hk)) \\ & = & (a + gb + (gh)c, (gh)k), \end{array}$$

using the associativity of G, and associativity of the action of G on A. Therefore the associativity holds.

Neutral element : We claim that $1_{A \rtimes G} = (0_A, 1_G)$. Indeed, for any $(a,g) \in A \rtimes G$, we have :

$$(a,g) \cdot (0_A, 1_G) = (a + g \cdot 0_A, g \cdot 1_G) = (a,g),$$

and :

$$(0_A, 1_G) \cdot (a,g) = (0_A + 1_A \cdot a, 1_G \cdot g) = (a,g).$$

[1] The maps i and π are indeed group homomorphism.

Inverse element : For any $(a, g) \in A \rtimes G$, we claim that $(a, g)^{-1} = (-g^{-1}a, g^{-1})$. Indeed, we have :

$$(a, g) \cdot (-g^{-1}a, g^{-1}) = (a - (gg^{-1})a, gg^{-1}) = (a - a, 1_G) = (0_A, 1_G),$$

and :

$$(-g^{-1}a, g^{-1}) \cdot (a, g) = (-g^{-1}a + g^{-1}a, g^{-1}g) = (0_A, 1_G).$$

(b) Let us investigate on what a section means in this situation. If we consider $s : G \to A \rtimes G$ a function (not necessarily a homomorphism) with the condition that $\pi \circ s = \mathrm{id}_G$, then we get that s is uniquely determined by some function $d : G \to A$ as follows : $s(g) = (d(g), g)$, for any $g \in G$, since we have $\pi \circ s = \mathrm{id}_G$. Let us notice that, for any $g, h \in G$:

$$s(g) \cdot s(h) = (d(g), g) \cdot (d(h), h) = (d(g) + gd(h), gh).$$

Thereby, we get :

$$\begin{array}{rcl} s \text{ is a homomorphism} & \iff & s(gh) = s(g) \cdot s(h), \forall g, h \in G \\ & \iff & d(gh) = d(g) + gd(h), \forall g, h \in G \\ & \iff & d \text{ is a derivation.} \end{array}$$

Therefore, we have shown the correspondance between $\mathrm{Der}(G, A)$ and $\mathrm{Hom}'(G, A \rtimes G)$. In details, if we name $p_1 : A \rtimes G \to A$ the set map defined by $p_1(a, g) = a$, for all $(a, g) \in A \rtimes G$, the bijection is given by :

$$\begin{array}{rcl} \mathrm{Hom}'(G, A \rtimes G) & \longleftrightarrow & \mathrm{Der}(G, A) \\ s : G \to A \rtimes G & \longmapsto & p_1^*(s) = p_1 \circ s : G \to A. \quad \square \end{array}$$

Exercise 2.2.2. *Let G be a group and A a $\mathbb{Z}G$-module. Prove that* $\mathrm{Der}(G, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$ *as abelian groups.*

Proof. For the sake of clarity we will simply write 1 for the unit 1_G. Recall that IG is a free $\mathbb{Z}$-module with basis $\{g - 1 \mid g \in G \setminus \{1\}\}$, by exercise 2.1.3. Let us define the map $\Phi : \mathrm{Der}(G, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$ as follows. For any derivation $d : G \to A$, we define :

$$\begin{array}{rcl} \Phi(d) : IG & \longrightarrow & A \\ \displaystyle\sum_{g \neq 1} \lambda_g (g - 1) & \longmapsto & \displaystyle\sum_{g \neq 1} \lambda_g d(g). \end{array}$$

It is obviously well-defined, meaning that $\Phi(d)$ is a $\mathbb{Z}G$-morphism, for all derivation $d : G \to A$, as $\Phi(d)$ extends linearly the map $(g - 1) \mapsto d(g)$. It is straighfoward to see that Φ is an abelian group homomorphism.
We now define its inverse. Recall that for any derivation $d : G \to A$, we have $d(1) = 0$, as we have :

$$d(1) = d(1 \cdot 1) = d(1) + 1 \cdot d(1) = d(1) + d(1).$$

Let $\Psi : \mathrm{Hom}_{\mathbb{Z}G}(IG, A) \longrightarrow \mathrm{Der}(G, A)$ be the map defined as follows, for all $\mathbb{Z}G$-morphism $f : IG \to A$:

$$\begin{array}{rcl} \Psi(f) : G & \longrightarrow & A \\ g & \longmapsto & \begin{cases} f(g - 1), & \text{if } g \neq 1 \\ 0, & \text{if } g = 1. \end{cases} \end{array}$$

We must argue that $\Psi(f)$ is indeed a derivation, for all $f \in \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$. We must prove that for all $g, h \in G$, the following equality holds :

$$\Psi(f)(gh) = \Psi(f)(g) + g(\Psi(f)(h)).$$

If $g = 1$, or $h = 1$, or $g = h^{-1}$, the equality follows easily. So let us consider the case $g \neq 1 \neq h$ and $g \neq h^{-1}$. We have :

$$\begin{aligned} \Psi(f)(gh) &= f(gh - 1) \\ &= f((g-1) + g(h-1)) \\ &= f(g-1) + gf(h-1), \text{ since } f \text{ is a } \mathbb{Z}G\text{-morphism}, \\ &= \Psi(f)(g) + g\Psi(f)(h). \end{aligned}$$

Thereby $\Psi(f)$ is a derivation. It is straightfoward to see that Ψ is a homomorphism. Notice now that for all $f \in \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$, $d \in \mathrm{Der}(G, A)$ and $g \in G \setminus \{1\}$:

$$\begin{aligned} (\Phi \circ \Psi)(f)(g-1) &= \Psi(f)(g) \\ &= f(g-1), \end{aligned}$$

and forall $g \in G$ and $d \in \mathrm{Der}(G, A)$:

$$\begin{aligned} (\Psi \circ \Phi)(d)(g) &= \begin{cases} \Phi(d)(g-1), & \text{if } g \neq 1 \\ 0, & \text{if } g = 1. \end{cases} \\ &= d(g). \end{aligned}$$

Therefore $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Hom}_{\mathbb{Z}G}(IG,A)}$ and $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Der}(G,A)}$. Thus $\mathrm{Der}(G, A) \cong \mathrm{Hom}_{\mathbb{Z}G}(IG, A)$. □

Exercise 2.2.3. *Recall that a group F is said to be free on a set X if X is a subset of F with the following universal property : for every group G and every set map $\varphi : X \to G$, the map φ extends uniquely to a group homomorphism $\widetilde{\varphi} : F \to G$:*

$$\begin{array}{ccc} X & \xrightarrow{\varphi} & G \\ \downarrow & \nearrow_{\widetilde{\varphi}} & \\ F. & & \end{array}$$

(a) *Prove that an infinite cyclic group $F = \langle f \rangle$ is free on the set $\{f\}$.*

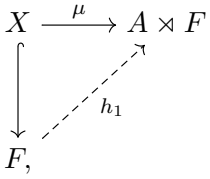
(b) *Prove that if F is a free group on a set X, then the augmentation ideal IF is a free $\mathbb{Z}F$-module on the set $X - 1 := \{x - 1 \mid x \in X\}$.*

Proof. (a) A group homomorphism $\langle f \rangle \to G$ is uniquely determined by its value on the generator f. Therefore $F = \langle f \rangle$ is free on the set $\{f\}$: for any associated value $\varphi(f)$ on G of f, we define the group homomorphism $\widetilde{\varphi}(f^n) = \varphi(f)^n$, for any $n \in \mathbb{N}$. The extension $\widetilde{\varphi} : F \to G$ is uniquely determined.

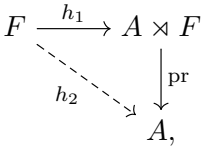
(b) Let A be a $\mathbb{Z}F$-module. Given a set map $h : X - 1 \to A$, we must prove there exists a unique extension $\widetilde{h} : IF \to A$ that is a $\mathbb{Z}F$-morphism (see Theorem 2.1 of Chapter IV in [Lang, 1974]). We define the set map :

$$\begin{aligned} \mu : X &\longrightarrow A \rtimes F \\ x &\longmapsto (h(x-1), x). \end{aligned}$$

Since F is a free group on the set X, there exists by the universal property a unique group homomorphism $h_1 : F \to A \rtimes F$, such that the diagram commutes :



i.e., such that $h_1(x) = (h(x-1), x)$ for all $x \in X$. It follows in particular that h_1 is in $\mathrm{Hom}'(F, A \rtimes F)$ (see notation in exercise 2.2.1). By exercise 2.2.1, the homomorphism h_1 factorizes uniquely a derivation $h_2 : F \to A$:



i.e., $h_2 \in \mathrm{Der}(F, A)$ such that $h_2(x) = h(x-1)$ for all $x \in X$. By exercise 2.2.2, it defines uniquely $\widetilde{h} := \Phi(h_2) \in \mathrm{Hom}_{\mathbb{Z}F}(IF, A)$. This implies $\widetilde{h}(x-1) = h_2(x)$ for all $x \in X$, by definition of the isomorphism Φ given in exercise 2.2.2. Therefore $\widetilde{h}$ is uniquely determined by its restriction on the set map $h : X - 1 \to A$. □

Exercise 2.2.4. *Let F be a free group on a set X.*

(a) *Prove that $0 \to IF \hookrightarrow \mathbb{Z}F$ is a free resolution of $\mathbb{Z}$ as a trivial $\mathbb{Z}F$-module.*

(b) *Prove that $H^n(F, A) = 0$ for all $n \geq 2$.*

(c) *Prove that if A is a trivial $\mathbb{Z}F$-module, then $H^1(F, A) \cong \prod_{x \in X} A$.*

(d) *Solve again exercise* 2.1.4 *for a trivial module.*

Proof. (a) We have the exact sequence of $\mathbb{Z}F$-modules :

$$0 \longrightarrow IF \hookrightarrow \mathbb{Z}F \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

where $\varepsilon : \mathbb{Z}F \to \mathbb{Z}$ is the augmentation map. From exercise 2.2.3, we have that IF is a free $\mathbb{Z}F$-module. Since $\mathbb{Z}F$ is also free, we have proved that $0 \to IF \hookrightarrow \mathbb{Z}F$ is a free resolution of $\mathbb{Z}$ as a trivial $\mathbb{Z}F$-module.

(b) The value of $H^n(F, A)$ is given by the cohomology of the following cochain complex :

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}F}(\mathbb{Z}F, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}F}(IF, A) \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots .$$

We get directly then that $H^n(F, A) = 0$ for $n \geq 2$.

(c) From exercise 2.1.3, as A is trivial, we have the isomorphism of groups :

$$H^1(F, A) \cong \mathrm{Hom}_{\mathscr{G}r}(F, A).$$

But from the universal property of the free groups, the bijection between the set maps $X \to A$ and the extended group homomorphisms $F \to A$ induces an isomorphism :

$$\mathrm{Hom}_{\mathscr{G}r}(F, A) \cong \mathrm{Hom}_{\mathscr{S}et}(X, A),$$

where $\mathrm{Hom}_{\mathscr{S}et}(X, A)$ denotes the group formed by the set maps $X \to A$ and where the group law is given by pointwise addition in the abelian group A. This group is isomorphic to the group product $\prod_{x \in X} A$ via :

$$\begin{array}{rcl} \mathrm{Hom}_{\mathscr{S}et}(X, A) & \longrightarrow & \prod_{x \in X} A \\ (\varphi : X \to A) & \longmapsto & \Big(\ \varphi(x) \ \Big)_{x \in X}. \end{array}$$

Therefore we get : $H^1(F, A) \cong \prod_{x \in X} A$.

(d) If $G = \langle g \rangle$ is an infinite cyclic group, then G is free on the singleton $\{g\}$ by exercise 2.2.3. Therefore, by the previous results, we get :

$$H^n(G, A) = 0,$$

for $n \geq 2$, and since A is trivial, we find that $H^1(G, A) \cong A$ by question (d). □

The following exercise shows that in the category of groups, split exact sequences need to have a retraction.

Exercise 2.2.5. *Let $1 \to A \xrightarrow{i} E \to G \to 1$ be a short exact sequence of groups, where we regard i as the inclusion and A is normal in E. Prove that the following are equivalent.*

(a) *The inclusion i has a retraction, i.e., there exists a group homomorphism $r : E \to A$ such that $r \circ i = \mathrm{id}_A$.*

(b) *A has a normal complement in E, i.e., there exists a normal subgroup H of E such that $AH = E$ and $A \cap H = 1$.*

(c) *There is a normal subgroup H of E such that $E \cong A \times H$.*

Find an example of an exact sequence of groups that admits a section but not a retraction.

Proof. Let us show that (a) implies (b). Define $H := \ker r$. For any $e \in E$, we have :

$$e = r(e)r(e)^{-1}e = r(e)(r(e)^{-1}e).$$

Since r is an homomorphism of groups which is the identity on A, we get :

$$r(r(e)^{-1}e) = r(\underbrace{r(e)^{-1}}_{\in A})r(e) = r(e)^{-1}r(e) = 1,$$

so $r(e)^{-1}e \in H = \ker r$, and $r(e) \in A$, thus $e \in AH$. Therefore $E = AH$. Now consider $e \in A \cap H$. We have that $e \in \ker r$ and since $r \circ i = \mathrm{id}_A$:

$$1 = r(e) = e,$$

so $A \cap H = 1$. Thereby, A has a normal complement H in E.

Let us show now that (b) implies (c). We first argue that if A has a normal complement H in E, then each $e \in E$ has a unique expression $e = ah$, where $a \in A$ and $h \in H$. Indeed suppose there exists also $b \in A$ and $k \in H$ such that $e = ah = bk$. Then we get :

$$hk^{-1} = a^{-1}b \in A \cap H = 1,$$

so $a = b$ and $h = k$.
We define a map :

$$\begin{array}{rcl} \Phi : E = AH & \longrightarrow & A \times H \\ e = ah & \longmapsto & (a, h). \end{array}$$

We now argue that Φ is a homomorphism. We must check that : $\Phi((ah)(bk)) = \Phi(ah)\Phi(bk)$, for all $a, b \in A$ and $h, k \in H$. We get :

$$\begin{array}{rcl} \Phi((ah)(bk)) = \Phi(ah)\Phi(bk) & \iff & ahbk = abhk \\ & \iff & bk = h^{-1}bhk. \end{array}$$

Since A is normal in E we get that $h^{-1}bh \in A$, so by uniqueness of expression in AH, we get that $b = h^{-1}bh$. So Φ is a homomorphism. It is bijective by uniquess of expressions in AH, therefore $E \cong A \times H$ via Φ.

Finally, let us show that (c) implies (a). Let $\Phi : E \xrightarrow{\cong} A \times H$ be an isomorphism. Let $A' := \Phi(A) \cong A$ so that it fits into the diagram :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xhookrightarrow{i} & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \cong\downarrow{\scriptstyle \Phi_{|A}} & & {\scriptstyle \Phi}\downarrow\cong & & & & \\ 1 & \longrightarrow & A' & \hookrightarrow & A \times H. & & & & \end{array} \tag{2.1}$$

Let $p_1 : A \times H \to A$ be the projection on the first variable. It is an homomorphism of groups. Define $r' : A \times H \to A'$ a group homomorphism as the composite :

$$A \times H \xrightarrow{p_1} A \xrightarrow{\Phi_{|A}} A'.$$

It is a retraction of the inclusion map $i' : A' \hookrightarrow A \times H$. Now define $r : A \times H \to A$ the group homomorphism defined as the composite :

$$E \xrightarrow{\Phi} A \times H \xrightarrow{r'} A' \xrightarrow{\Phi^{-1}_{|A}} A.$$

From the commutativity of the diagram (2.1), we get that r is a retraction of i.

Let us find an example of an exact sequence of groups that admits a section but not a retraction. Let us denote $\mathfrak{S}_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ the symmetric group of degree 3, and $A_3 = \{\mathrm{id}, (123), (132)\}$ its alternating group. Recall that A_3 is normal in $\mathfrak{S}_3$ and that we have the isomorphism : $\mathfrak{S}_3/A_3 \cong \{\pm 1\} = C_2$ via the signature homomorphism. Therefore, we get an exact sequence of groups :

$$1 \longrightarrow A_3 \hookrightarrow \mathfrak{S}_3 \xrightarrow{\mathrm{sign}} \{\pm 1\} \longrightarrow 1.$$

This sequence does not admit a retraction, as if it were, then we would have the isomorphism $\mathfrak{S}_3 \cong A_3 \times \{\pm 1\}$, and so $\mathfrak{S}_3$ would be abelian : which is not the case. But it admits a section, define :

$$\begin{array}{rcl} s : \{\pm 1\} & \longrightarrow & \mathfrak{S}_3 \\ 1 & \longmapsto & \mathrm{id} \\ -1 & \longmapsto & (12), \end{array}$$

It is a well-defined homomorphism and we have $\mathrm{sign} \circ s = \mathrm{id}_{C_2}$. So s is a section. □

Exercise 2.2.6. *Any group extension $1 \to A \to E \to F \to 1$, with F a free group, splits.*

Proof. Let us name the right homomorphism $p : E \to F$. Let us assumed that F is free on a subset X. For any $x \in X$, as p is surjective, we can choose[2] an element $e_x \in E$ such that $p(e_x) = x$. This defines a set map :

$$\begin{array}{rcl} s : X & \longrightarrow & E \\ x & \longmapsto & e_x. \end{array}$$

It satisfies the condition $p \circ s = \mathrm{id}_X$. So by the universal property of the free group, we get that there exists a unique group homomorphism $\widetilde{s} : F \to E$ such that the diagram commutes :

$$\begin{array}{ccc} X & \xrightarrow{s} & E \\ \downarrow & \nearrow_{\widetilde{s}} & \\ F. & & \end{array}$$

Recall that an element of F can be regarded as a reduced word formed by the elements of X and their inverse (see Corollary 11.5 in [Rotman, 1995]). So since $\widetilde{s}$ is a group homomorphism, we get $p \circ \widetilde{s} = \mathrm{id}_F$. Therefore the extension splits. □

Let us investigate on the interpretation of the cohomology in dimension 2. We first do a more categorical exercise.

Exercise 2.2.7 (Functorial properties of $\mathscr{E}(G, A)$)**.** *Let G be a group and A a $\mathbb{Z}G$-module. We denote by $\mathscr{E}(G, A)$ the set of all extensions of G by A, up to equivalence. Given an extension $0 \to A \to E \to G \to 1$ and a group homomorphism $\alpha : G' \to G$, where G' is any group, show that there is an extension $0 \to A \to E' \to G' \to 1$, characterized up to equivalence by the fact that it fits into the following commutative diagram :*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G' & \longrightarrow & 1. \end{array} \tag{2.2}$$

Deduce that a homomorphism $\alpha : G' \to G$ induces a mapping $\mathscr{E}(G, A) \to \mathscr{E}(G', A)$, which corresponds to $H^2(\alpha, A) : H^2(G, A) \to H^2(G', A)$.

[2] For the infinite case, we rely on the Axiom of choice (see [Lang, 1974] Prerequisites, part 7).

Proof. We denote by $p : E \to G$ the given surjective homomorphism, and $i : A \to E$ the injective homomorphism. We define E' by the following pullback square (see [Borceux, 1994] point 2.5) :

$$\begin{array}{ccc} E' & \xrightarrow{\mathrm{pr}_{G'}} & G' \\ {\scriptstyle \mathrm{pr}_E}\downarrow & & \downarrow{\scriptstyle \alpha} \\ E & \xrightarrow{p} & G. \end{array}$$

In other words we have : $E' = E \times_G G' = \{(e, g') \in E \times G' \mid p(e) = \alpha(g')\}$. We denote by pr_E and $\mathrm{pr}_{G'}$ the natural projections. Let us show we have an exact sequence of groups :

$$0 \longrightarrow A \xrightarrow{i'} E' \xrightarrow{\mathrm{pr}_{G'}} G' \longrightarrow 1,$$

which fits into the diagram (2.2), where $i' : A \to E'$ is defined as $a \mapsto (i(a), 1_{G'})$. Since $p(i(a)) = 1_G$ by exactness and $\alpha(1_{G'}) = 1_G$ as α is a homomorphism, we see that the range of i' is indeed in E'. Since i is injective, we see that i' is also injective. Clearly $\mathrm{pr}_{G'}$ is surjective. Since $\mathrm{im}\ i = \ker p$, we get :

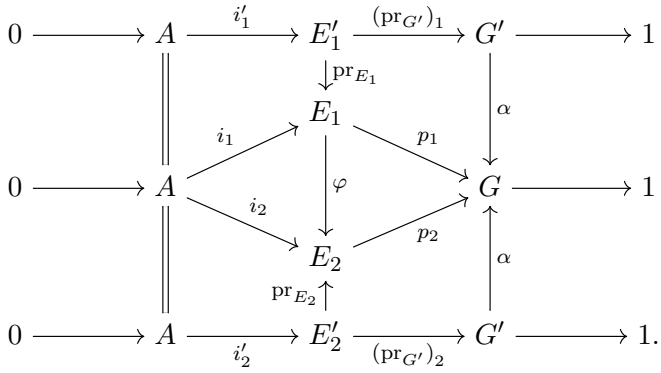
$$\begin{aligned} \ker \mathrm{pr}_{G'} &= E \times_G \{1_{G'}\} \\ &= \ker p \times \{1_{G'}\} \\ &= \mathrm{im}\ i \times \{1_{G'}\} \\ &= \mathrm{im}\ i' \end{aligned}$$

So the sequence is exact.

Let us prove now that $\alpha : G' \to G$ induce the desired mapping. By our previous work, we are able to define :

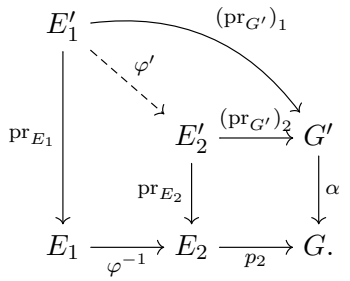
$$\begin{array}{rcl} \mathscr{E}(G, A) & \longrightarrow & \mathscr{E}(G', A) \\ (0 \to A \to E \to G \to 1) & \longmapsto & (0 \to A \to E' \to G' \to 1). \end{array}$$

We only need to show it is well-defined, that is, for two extensions E_1 and E_2 of G by A which are equivalent, their image E_1' and E_2' are also equivalent. Let us name $\varphi : E_1 \to E_2$ the isomorphism, we have the following commutative diagram :

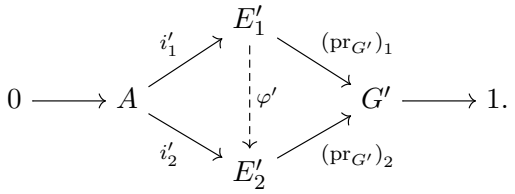


By the universal property of the pullback, we get there exists a unique group homomorphism

$\varphi' : E'_1 \to E'_2$ such that the following diagram commutes :



Combining the two previous diagrams, we get the following commutative diagram :



So φ' is an isomorphism and the two extensions E'_1 and E'_2 are indeed equivalent.

Let us prove now that this mapping corresponds to the map :

$$\begin{array}{rcl} H^2(\alpha, A) : H^2(G, A) & \longrightarrow & H^2(G', A) \\ [f] & \longmapsto & [f'] \,, \end{array}$$

where here we regard $H^2(G, A)$ as the quotient $Z^2(G, A)/B^2(G, A)$, and $[f]$ is the class of an element $f \in Z^2(G, A)$ in $H^2(G, A)$, and where f' is defined as :

$$\begin{array}{rcl} f' : G' \times G' & \longrightarrow & A \\ (g', h') & \longmapsto & f(\alpha(g'), \alpha(h')). \end{array}$$

Let us remind how the correspondance between $\mathscr{E}(G, A)$ and $H^2(G, A)$ works. For any extension $0 \to A \xrightarrow{i} E \to G \to 1$, apply the forgetful functor $\mathscr{G}r \to \mathscr{S}et_*$ from the category of groups to the category of pointed sets so that we regard this sequence in $\mathscr{S}et_*$. In this category, all exact sequences split. Choose a section $s : G \to E$, and define $f : G \times G \to A$ as a map in $\mathscr{S}et_*$ that measures the failure of s being a group homomorphism, for all $g, h \in G$:

$$s(g)s(h) = i(f(g, h))s(gh). \tag{2.3}$$

It turns out that $f \in Z^2(G, A)$, and changing the choice of the section s corresponds precisely to modifying the cocycle f by a coboundary (see chapter IV in [Brown, 1982] for more details). So take an extension $0 \to A \xrightarrow{i} E \to G \to 1$ in $\mathscr{E}(G, A)$ and choose a section $s : G \to E$ of pointed sets, so that it defines by equation (2.3) a 2-cocycle $f : G \times G \to A$. Our mapping $\mathscr{E}(G, A) \to \mathscr{E}(G', A)$ maps the pointed set map $s : G \to E$ to the pointed set map :

$$\begin{array}{rcl} s' : G' & \longrightarrow & E' \\ g' & \longmapsto & (s(\alpha(g')), g'), \end{array}$$

since the diagram (2.2) must commute. As s is a section, $p(s(\alpha(g'))) = \alpha(g')$, for any $g' \in G$, so s' is indeed well-defined. Now this pointed set section s' defines a 2-cocycle f' in $Z^2(G', A)$, by the following equation, for all $g', h' \in G'$:

$$s'(g')s'(h') = i'(f'(g', h'))s'(g'h').$$

We apply the definition of s' :

$$(s(\alpha(g')), g') \cdot (s(\alpha(h'), h') = (i(f'(g', h')), 1_{G'}) \cdot (s(\alpha(g'h')), g'h').$$

We multiply the terms, so that it is equivalent :

$$(s(\alpha(g'))s(\alpha(h'))), g'h') = (i(f'(g', h'))s(\alpha(g'h')), g'h').$$

But by equation (2.3), we get :

$$i(f(\alpha(g'), f(\alpha(h'))s(\alpha(g'h')) = s(\alpha(g'))s(\alpha(h')) = i(f'(g', h'))s(\alpha(g'h')).$$

Since i is injective, we finally obtain :

$$f(\alpha(g'), \alpha(h'))) = f'(g', h').$$

The last equation shows that $[f']$ is indeed the image of $[f]$ by the homomorphism $H^2(\alpha, A)$. Therefore our mapping $\mathscr{E}(G, A) \to \mathscr{E}(G', A)$ corresponds to the abelian group homomorphism $H^2(\alpha, A) : H^2(G, A) \to H^2(G', A)$. □

The next exercise shows how much information the group cohomology in dimension 2 contains. We look at the group of order 2, and we see we can deduce all the group of order 8. It is an example of a basic application of group cohomology in algebra.

Exercise 2.2.8 (Application of Group Cohomology)**.** *Let $A := C_4$ and $G := C_2$ be the cyclic groups of order 4 and of order 2 respectively.*

(a) *Find all linear actions of G on A.*

(b) *For each such action, compute $H^2(G, A)$.*

(c) *For each such action, describe all extensions of A by G.*

(d) *Find all groups of order 8.*

Proof. We will write $G = \langle g \rangle$ multiplicatively, and $A = \mathbb{Z}/4\mathbb{Z}$ additively.

(a) Let us denote $\mathrm{Aut}(A)$ the group formed by all the automorphisms $A \to A$. Each linear action of G on A is determined uniquely by a group homomorphism :

$$h : G \to \mathrm{Aut}(A),$$

where $g \cdot a = h(g)(a)$, for all $a \in A$. We only specify the action of g since $1_G \cdot a = a$ for all a. Since h is a group homomorphism, we have $h(1_G) = \mathrm{id}_A$, and $h(gg) = h(g) \circ h(g)$, therefore $h(g)$ is its own inverse, i.e. of order 2 in $\mathrm{Aut}(A)$, for any homomorphism h. Since $h(g) \in \mathrm{Aut}(A)$ and A is a cyclic group generated by 1, the automorphism $h(g)$ is determined uniquely by its value in 1. Since $h(g)$ must be its own inverse, we see that $h(g)(1) = 1$ and $h(g)(1) = 3$ are the only possibilities. So either h is the trivial map

(sending all its elements to the identity id_A), and so A is a trivial $\mathbb{Z}G$-module, either h is the homomorphism which sends g to the automorphism :

$$\begin{array}{rccc} h(g) : & A & \longrightarrow & A \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 3 \\ & 2 & \longmapsto & 2 \\ & 3 & \longmapsto & 1. \end{array}$$

We will refer to this homomorphism by h subsequently. Notice that actually $h(g)(a) = -a$, for all $a \in A$, so it is the inversion homomorphism. The homomorphism h gives rise to a $\mathbb{Z}G$-structure on A. Thereby, there are only two linear actions of G on A : the trivial action and the action induced by h.

(b) Let us write $t = 1_G + g \in \mathbb{Z}G$. Since G is a finite cyclic group, we know that (see [Brown, 1982], chapter III.1) :

$$H^2(G, A) = A^G/(t \cdot A),$$

where A^G are the fixed elements of A by the action of G. So if A has the trivial $\mathbb{Z}G$-structure, then $H^2(G, A) = A/(\{0, 2\}) \cong \mathbb{Z}/2\mathbb{Z}$, and if A has the $\mathbb{Z}G$-structure induced by h, we have $H^2(G, A) = \{0, 2\}/\{0\} \cong \mathbb{Z}/2\mathbb{Z}$. Therefore, for any action of G on A, we have $H^2(G, A) \cong \mathbb{Z}/2\mathbb{Z}$.

(c) We will determine all the extensions up to equivalence. Let us recall the correspondance between $H^2(G, A)$ and $\mathscr{E}(G, A)$ (see [Brown, 1982], chapter IV.3 for more details). Choose a 2-cocycle $f : G \times G \to A$ modulo a 2-coboundary in $H^2(G, A)$, it determines an extension :

$$0 \longrightarrow A \xrightarrow{\ i\ } E_f \xrightarrow{\ p\ } G \longrightarrow 1,$$

where E_f is the set $A \times G$ together with a group law given by, for all $a, b \in A$ and $g, k \in G$:

$$(a, g) \cdot (b, k) = (a + gb + f(g, k), gk), \tag{2.4}$$

and i and p are group homomorphisms defined by $i(a) := (a, 1_G)$ and $p(a, g) = g$, for all $a \in A$ and $g \in G$.
Now recall that a 2-cocycle f satisfies the identity, for all $g, k, \ell \in G$:

$$gf(k, \ell) - f(gk, \ell) + f(g, k\ell) - f(g, k) = 0.$$

But since $G = \langle g \rangle$, the previous equation reduces to :

$$g \cdot f(g, g) = f(g, g),$$

since to be a 2-cocycle also requires that $f(1, g) = f(1, 1) = f(g, 1) = 0$. Therefore, we get that a 2-cocycle f in our case is only determined by its value $f(g, g)$ and that $f(g, g) \in A^G$.

So if A has a trivial action of G, since $H^2(G, A) = \mathbb{Z}/2\mathbb{Z}$ and $A^G = A$, we get that there are four 2-cocycles $f : G \times G \to A$, and up to a 2-coboundary, there are two 2-cocycles. Recall that a 2-coboundary is a function $f : G \times G \to A$ such that there exists a function $c : G \to A$ such that $c(1_G) = 0$ and for all $g, k \in G$:

$$f(g, k) = gc(g) - c(gk) + c(k).$$

In our case, this means that $f(g,g) = 2c(g)$. So, for $i = 0, 1, 2, 3$, let us name by $f_i : G \times G \to A$ the 2-coboundary such that $f(g,g) = i$. We get that the set of 2-coboundary is $B^2(G,A) = \{f_0, f_2\}$. Therefore, we choose f_0 and f_1 as the two representatives of $H^2(G,A)$. Thus we get two extensions : E_{f_0} and E_{f_1}. Now for E_{f_0}, the group law (2.4) simply becomes :

$$(a,g) \cdot (b,k) = (a+b, gk).$$

Therefore E_{f_0} is an abelian group of order 8 and we see directly that $E_{f_0} = A \times G$.
Similarly, we get that the group law (2.4) in E_{f_1} becomes :

$$(a,g) \cdot (b,k) = (a+b+f_1(g,k), gk).$$

It is therefore an abelian group of order 8 as $f_1(g,k) = f_1(k,g)$ for all $g, k \in G$. Now we compute :

$$(1,g)^2 = (3,1_G), (1,g)^3 = (0,g), (1,g)^4 = (2,1_G), (1,g)^5 = (3,g),$$

$$(1,g)^6 = (1,1_G), (1,g)^7 = (2,g), (1,g)^8 = (0,1_G),$$

so $(1,g)$ is an element of order 8 that generates E_{f_1}, so we get $E_{f_1} = \langle (1,g) \rangle \cong \mathbb{Z}/8\mathbb{Z}$. Therefore, if we write now $G = \mathbb{Z}/2\mathbb{Z}$, when G acts trivially on A, we have the following two extensions of G by A, up to equivalence :

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{i_0} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{p_0} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{i_1} \mathbb{Z}/8\mathbb{Z} \xrightarrow{p_1} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

where i_0, i_1, p_0 and p_1 are determined by our previous isomorphisms on E_{f_0} and E_{f_1}. In details, we see that $i_0([a]_4) = ([a]_4, 0)$ and $p_0([a]_4, [b]_2) = [b]_2$, where we used the bracket notations to remind in which class are the elements. And we see that $i_1([a]_4) = 6 \cdot [a]_8$ and $p_1([b]_8) = [b]_2$.

Let us now look the case where G acts on A with h. We get back to the previous notation $G = \langle g \rangle$. In this case $A^G = \{0, 2\}$ and $H^2(G,A) = \mathbb{Z}/2\mathbb{Z}$. So we get directly that $f_0, f_2 : G \times G \to A$ are the 2-cocycle of $H^2(G,A)$. For E_{f_0}, the group law (2.4) becomes :

$$(a,g) \cdot (b,k) = (a + h(g)(b), gk).$$

If we call $r = (1, 1_G)$ and $s = (1, g)$, we get that (we do not write down the computations as they are not enlightening) :

$$E_{f_0} = \left\langle r, s \mid r^4 = (0,1_G), s^2 = (0,1_G), srs = r^{-1} \right\rangle.$$

Therefore $E_{f_0} \cong D_8$ the dihedral group of order 8 (see [Brown, 1982] chapter IV for the definition of D_8 with generators).
For E_{f_2}, the group law (2.4) becomes :

$$(a,g) \cdot (b,k) = (a + h(g)(b) + f_2(g,k), gk).$$

Let us name $x = (1, 1_G)$ and $y = (1, g)$. We get :

$$E_{f_2} = \left\langle x, y \mid x^4 = (0,1_G), x^2 = y^2, yxy^{-1} = x^{-1} \right\rangle.$$

Therefore $E_{f_2} \cong Q$, the quaternion group (see [Brown, 1982] chapter IV for the definition of Q with generators). Therefore, if we write now $G = \mathbb{Z}/2\mathbb{Z}$, when G acts by h on A, we have the following two extensions of G by A, up to equivalence :

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{i_3} D_8 \xrightarrow{p_3} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{i_4} Q \xrightarrow{p_4} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

where i_3, i_4, p_3 and p_4 are determined by our previous isomorphisms on E_{f_0} and E_{f_2}. In details, we see that $i_3(a) = r^a$ and $p_3(r^a s^b) = [b]_2$, and $i_4(a) = x^a$ and $p_4(x^a y^b) = [b]_2$.

(d) Let E be a group of order 8. If E contains an element of order 4, say a, then $\langle a \rangle \cong \mathbb{Z}/4\mathbb{Z}$ is a normal subgroup of E, of index 2. Therefore it fits into a short exact sequence :

$$0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow E \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

In question (c), we have classified all these short exact sequence up to equivalence.
If E does not contain an element of order 4 then, by Lagrange's theorem, it contains an element a of order 8 or of order 2. If a is of order 8, then a^2 is of order 4, which is impossible. So if E does not contain an element of order 4, then all its elements are at most of order 2. Then we claim that in that case E is abelian. To prove this, we need to show $xy = yx$ for all x and y in E. As E is a group, xy is in E, and it is of order 2, so it is its own inverse. Therefore :

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

So E is abelian and so we have : $E \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Therefore, all the groups of order 8, up to isomorphism, are :

$$\mathbb{Z}/8\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ D_8,\ Q. \qquad \square$$

We finish this paper by presenting a proof of Hilbert's Theorem 90 using group cohomology. It is a founding result for classifying cyclic extensions of fields. The only difficulty is the change of notation : the group law of the modules will be written multiplicatively instead of additively.

Exercise 2.2.9 (Galois Cohomology, a first result)**.** *Let K be a field, and $E \supseteq K$ be a Galois extension, with Galois group $G := \mathrm{Gal}(E, K)$. The multiplicative group E^* is a KG-module, and $H^1(G, E^*) = 0$.*

Proof. The extension E is a K-vector space, and G acts on E^* by the inclusion homomorphism :

$$G \longhookrightarrow \mathrm{Aut}(E^*),$$

so E^* is indeed a KG-module.

Let $d : G \to E^*$ be a derivation (i.e. a 1-cocycle). We must show that d is actually a principal derivation (i.e. a 1-coboundary), that is, there exists $b \in E^*$ such that $d(\sigma) = b\sigma(b)^{-1}$,

for all $\sigma \in G$. Let us write d_σ instead of $d(\sigma)$. Since d is a derivation, we have for all σ and τ in G (remember that E^* is written mutliplicatively) :

$$d_{\sigma\circ\tau} = d_\sigma \sigma(d_\tau),$$

and so, as E^* is abelian, we obtain the equation :

$$\sigma(d_\tau) = d_{\sigma\circ\tau} d_\sigma^{-1}. \tag{2.5}$$

By the linear independence of automorphisms (see [Rotman, 2003] Proposition 4.30), there exists $e \in E^*$ such that :

$$b := \sum_{\tau\in G} d_\tau \tau(e) \neq 0.$$

In particular, we have $b \in E^*$. Therefore, for all $\sigma \in G$:

$$\begin{aligned}
\sigma(b) &= \sum_{\tau\in G} \sigma(d_\tau)\sigma(\tau(e)), \text{ as } \sigma \text{ is an automorphism,} \\
&= \sum_{\tau\in G} d_{\sigma\circ\tau} d_\sigma^{-1} \sigma(\tau(e)), \text{ by equation (2.5)} \\
&= d_\sigma^{-1} \sum_{\sigma\in G} d_{\sigma\circ\tau}\sigma(\tau(e)) \\
&= d_\sigma^{-1} \sum_{\tau'\in G} d_{\tau'}\tau'(e) \\
&= d_\sigma^{-1} b.
\end{aligned}$$

Thus $d_\sigma = b\sigma(b)^{-1}$, for all $\sigma \in G$. Whence d is a principal derivation. Therefore $H^1(G, E^*)$ is trivial. □

Exercise 2.2.10 (Hilbert's Theorem 90)**.** *Let E be a finite cyclic extension of K and let $\beta \in E^*$. Then $N_K^E(\beta) = 1_E$ if and only if there exists $\alpha \in E^*$ such that $\beta = \alpha\sigma(\alpha)^{-1}$, where σ is the generator of $G = \mathrm{Gal}(E, K)$.*

Proof. We refer the reader to the definition 7.1 of Chapter V of the reference [Lang, 1974] for the definition the norm N_K^E of an extension. Let n be the degree of extension of E over K. Recall that the cohomology of a finite cyclic group is given by (see [Brown, 1982], chapter III.1) :

$$H^1(G, E^*) = \ker N/\mathrm{im}\ D,$$

where N is the multiplication by $\mathrm{id} \cdot \sigma \cdot \sigma^2 \cdots \sigma^{n-1}$, i.e., $N(e) = N_K^E(e)$, and $D(e) = \sigma(e)e^{-1}$. By previous exercise, we have $H^1(G, E^*) = 0$, so $\ker N = \mathrm{im}\ D$. Hence, if $\beta \in E^*$, then $N_K^E(\beta) = 1_E$ if and only if there is $\alpha \in E^*$ such that $D(\alpha) = \beta$, i.e., $\beta = \alpha\sigma(\alpha)^{-1}$. □

References

[Borceux, 1994] Borceux, F. (1994). *Handbook of Categorical Algebra*, vol. 1. Cambridge University Press.

[Brown, 1982] Brown, K.S. (1982). *Cohomology of Groups*. Springer.

[Lang, 1974] Lang, S. (1974). *Algebra*. Springer.

[Rotman, 1995] Rotman, J.J. (1995). *An Introduction to the Theory of Groups*. Springer.

[Rotman, 2003] Rotman, J.J. (2003). *Advanced Modern Algebra*. Prentice Hall.

[Rotman, 2009] Rotman, J.J. (2009). *An Introduction to Homological Algebra*. Springer.