Cohomology of Groups - Part 1

Ergün Yalçın
Bilkent University

July 5, 2024

Contents

1 Introduction

These are the first draft of the lecture notes (Part 1) for the Graduate Course Math 626 Cohomology of Groups, offered in Spring 2024 at Bilkent University. Over the years, it will be revised and expanded. I thank all the students that took the course for taking the course and for the feedbacks and corrections.

The second part of these lecture notes will cover the topics like Topological Definition of Group Cohomology, Homology of a Groups, Restriction and Transfer, Product Structure and Structure Theorems. Through the student term projects, we also hope to cover the following topics: Group Actions on Simplicial Complexes, Cohomology of Small Categories, LHS-Spectral Sequence, etc.

These lecture notes are based on some well-known books on Group Cohomology where the author learned the material from. We list some of these books here:

1. Kenneth S. Brown, *Cohomology of Groups*, Springer-Verlag, 1994.
2. A. Adem and R. J. Milgram, *Cohomology of Finite Groups*, Springer-Verlag, 2004.
3. D. Benson, *Representations and Cohomology I, II*, Cambridge University Press, 1998.
4. J. Carlson, et al, *Cohomology Rings of Finite Groups*, Springer, 2003.
5. A. Weibel, *Introduction to Homological Algebra*, Cambridge University Press, 1994.
6. J. J. Rotman, *An Introduction to Homological Algebra*, Second Edition, Springer, 2009.

Conventions: Throughout these notes when we say G is a group we also mean G is a discrete group. Our focus will be mostly finite groups. In these notes every ring R is associative and unital. When we say M is an R-module, we mean M is left R-module. For the composition of two morphisms f and g, we write gf instead of $g \circ f$.

2 Preliminaries on Algebra

2.1 Modules

Definition 1. Let R be a ring with a unit element $1 \in R$. A (left) R**-module** M is an abelian group with operation

$$R \times M \to M$$
$$(r, m) \to rm$$

such that for every $r, r_1, r_2 \in R$, $m, m_1, m_2 \in M$

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $(r_1 r_2)m = r_1(r_2 m)$
3. $(r_1 + r_2)m = r_1 m + r_2 m$
4. $1m = m$.

Example 2. If $R = \mathbb{F}$ is a field, then an R-module is a $\mathbb{F}$-vector space. The most common fields that we use in these notes are the field of rational numbers $\mathbb{Q}$ and the field $\mathbb{F}_p$ with p-elements.

Example 3. If $R = \mathbb{Z}$, the integers, then a $\mathbb{Z}$-module is the same as an abelian group.

Example 4. If k is a commutative ring (say $k = \mathbb{Z}$, or $k = \mathbb{F}$ a field) and G is a discrete group, then the group ring kG is defined to be the ring whose elements are formal sums

$$x = \sum_{g \in G} a_g g$$

with $a_g \in k$ such that $a_g = 0$ for all but finitely many $g \in G$. The addition is defined by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g.$$

and the multiplication is defined by the formula

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{\substack{h,k \in G \\ hk = g}} a_k b_k \right) g$$

Group rings play an important role for defining group cohomology. Note that a $\mathbb{Z}G$-module M is an abelian group together with a left multiplication by the elements in $\mathbb{Z}G$. Since as an abelian group $\mathbb{Z}G$ is generated by the elements of G, we can define a $\mathbb{Z}G$-module also as follows:

Definition 5. An abelian group M is called a (left) G**-module** if there is a G-action on M satisfying the condition that for every $g \in G$ and $m_1, m_2 \in M$,

$$g(m_1 + m_2) = gm_1 + gm_2.$$

A G-module M can be viewed as a $\mathbb{Z}G$-module via the $\mathbb{Z}G$-action defined by

$$(\sum_{g\in G} a_g g)m = \sum_{g\in G} a_g(gm).$$

Conversely a $\mathbb{Z}G$-module can be viewed as a G-module by considering G as a subset of $\mathbb{Z}G$ in a natural way. A morphism of G-modules $f : M \to N$ is defined to be an abelian group homomorphism such that for every $g \in G$ and $m \in M$, $f(gm) = gf(m)$.

A morphism of R-modules is defined as follows:

Definition 6. Let M and N are R-modules. An **R-module homomorphism**, an **R-homomorphism**, or an **R-linear map** $f : M \to N$ is an abelian group homomorphism that satisfies

$$f(rm) = rf(m)$$

for every $r \in R$ and $m \in M$.

If the R-module homomorphism $f : M \to N$ is a bijection, then its inverse is also an R-module homomorphism. In this case we say f is an **R-module isomorphism**.

Example 7. Let G be a group and $R = \mathbb{Z}G$. We can consider $\mathbb{Z}G$ as a $\mathbb{Z}G$-module via multiplication from left. Let $\mathbb{Z}$ denote the trivial $\mathbb{Z}G$-module with the G-action defined by $gn = n$ for all $g \in G$ and $n \in N$. Consider the group homomorphism $\epsilon : \mathbb{Z}G \to \mathbb{Z}$ defined by

$$\epsilon\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} a_g.$$

It is easy to check that this defines an $\mathbb{Z}G$-module homomorphism. This homomorphism is called the **augmentation map**.

Definition 8. The **category of R-modules** is the category whose objects are R-modules and whose morphisms are given by R-module homomorphisms. We denote this category by R-Mod.

Remark 9. From the definitions above the category of $\mathbb{Z}G$-modules can be identified with the category of G-modules. From now on we will use this identification when are describing $\mathbb{Z}G$-modules and $\mathbb{Z}G$-homomorphisms.

In a similar way to left R-modules, one can also define a category of right R-modules using a right action on M. A **right R-module** M is an abelian group with operation

$$M \times R \to M$$

$$(m, r) \to mr$$

satisfying the properties analogous to the left version. An R-module homomorphism $f : M \to N$ is an abelian (right) group homomorphism that satisfies

$$f(mr) = f(m)r$$

for every $m \in M$, $r \in R$. The category of right R-modules is denoted by Mod-R.

For modules over a group rings, the categories left and right modules are isomorphic. This is because a right kG-module M can be viewed as a left kG-module via the G-action given by $gm = mg^{-1}$. Throughout these notes unless it is specifically declared, all R-modules will be left R-modules.

We now recall some standard definitions for R-modules.

Definition 10. Let M be an R-module.

1. A subgroup $N \subseteq M$ is called a **submodule** of M if for every $r \in R$ and $n \in N$, $rn \in N$.
2. Let N be a submodule of M. The **quotient module** M/N is defined to be the quotient group M/N together with the multiplication given by
$$r(m + N) = rm + N$$
for every $r \in R$ and $m \in M$.

Example 11. Let M be an R-module and U, V be two submodules of M. Then the set
$$U + V = \{u + v \,|\, u \in U,\, v \in V\}$$
is a submodule of M. This follows easily from the fact that $r(u + v) = ru + rv$ for every $u \in U$ and $v \in V$.

Example 12. Let $G = C_2 = \langle g \,|\, g^2 = 1\rangle$ be the cyclic group of order 2 and $R = \mathbb{Z}G$. Let $M = \mathbb{Z}G$ and $N \subseteq M$ be the submodule $\{(1 + g)a \,|\, a \in \mathbb{Z}\}$ generated by $(1 + g) \in M$. Note that N is isomorphic to the trivial $\mathbb{Z}G$-module $\mathbb{Z}$. The quotient module M/N is isomorphic to $\mathbb{Z}$ as an abelian group but it is not a trivial $\mathbb{Z}G$-module. Note that in M/N, for every $m \in M$, we have $gm + N = -m + N$. So, M/N is the $\mathbb{Z}G$-module whose underlying abelian group is $\mathbb{Z}$ where $g \in G$ acts by $g \cdot 1 = -1$. This $\mathbb{Z}G$-module is denoted by $\widetilde{\mathbb{Z}}$.

Definition 13. Given a set of elements X of M, the set of all linear combinations
$$\langle X\rangle = \Big\{\sum_{i=1}^{n} r_i x_i \,|\, r_i \in R, x_i \in X, n \text{ is a positive integer}\Big\}$$
is a submodule of M. If X is a subset of M such that $M = \langle X\rangle$, then we say M **is generated by** X. An R-module M is **finitely generated** if there is a finite set X that generates M.

Definition 14. Given an R-module homomorphism $f : M \to N$, we define

1. the **kernel** of f to be the submodule of M defined by
$$\ker f = \{m \in M \mid f(m) = 0\}$$
2. the **image** of f as the submodule of N defined by
$$\operatorname{im} f = \{n \in N \mid \text{there exist an } m \in M \text{ such that } n = f(m)\}$$
3. the **coker** of f to be the quotient module
$$\operatorname{coker} f = N/\operatorname{im} f.$$

There are isomorphism theorems for R-modules similar to the isomorphism theorems in group theory:

Theorem 15.

1. *If $f : M \to N$ is an R-module homomorphism then there is an R-module isomorphism*

$$\varphi : M/\ker f \to \operatorname{im} f$$

given by $\varphi(m + \ker f) = f(m)$ for all $m \in M$.

2. *If U and V are submodules of an R-module M, then R-module homomorphism $U \to (U + V)/V$ defined by $u \to u + V$ induces an R-isomorphism*

$$U/(U \cap V) \to (U + V)/V.$$

3. *Let M be an R-module, and V and U be submodules of M such that $V \subseteq U \subseteq M$. Then the R-module homomorphism $M/V \to M/U$ defined by $m + V \to m + U$ induces an R-isomorphism*

$$(M/V)/(U/V) \to M/U.$$

Exercise 16. Prove the isomorphism theorems stated above.

Definition 17. Given a sequence of homomorphism

$$A \xrightarrow{f} B \xrightarrow{g} C,$$

we say that the sequence is **exact** at B if $\operatorname{im} f = \ker g$. Note that in this case the composition gf is zero. A sequence of R-module homomorphisms

$$M_0 \to M_1 \to \cdots \to M_n \to M_{n+1}$$

is a **long exact sequence** if it is exact at $M_1, \ldots, M_n$.

Note that the sequence $0 \to M \xrightarrow{f} N$ is exact if and only if f is injective. The sequence $M \xrightarrow{f} N \to 0$ is exact if and only if f is surjective. A n exact sequence of the form

$$0 \to M \xrightarrow{i} M' \xrightarrow{\pi} M'' \to 0$$

is called a **short exact sequence**, or an **extension of R-modules**. Note that in this case there are isomorphisms $M \cong \operatorname{im} i$ and $M'/\operatorname{im} i \cong M''$.

Exercise 18. Let $G = C_n = \langle g \,|\, g^n = 1 \rangle$ be the cyclic group of order n and let $N_G = 1 + g + \cdots + g^{n-1}$. Then show that the sequence of $\mathbb{Z}G$-modules

$$\mathbb{Z}G \xrightarrow{1-g} \mathbb{Z}G \xrightarrow{N_G} \mathbb{Z}G \xrightarrow{1-g} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is exact.

2.2 Direct sums

Definition 19. Let M and N be R-modules. Then the **(externel) direct sum** of M and N is the R-module

$$M \oplus N = \{(m, n) \,|\, m \in M, n \in N\}$$

where the addition and the R-module structure are defined by

$$(m, n) + (m', n') = (m + m', n + n')$$
$$r(m, n) = (rm, rn)$$

for every $m, m' \in M$, $n, n' \in N$, and $r \in R$.

There are R-module homomorphisms $i_1 : U \to U \oplus V$ and $i_2 : V \to U \oplus V$, called **injections**, defined by $u \to (u, 0)$ and $v \to (0, v)$. On the other direction there are R-module homomorphisms $\pi_1 : U \oplus V \to U$ and $\pi_2 : U \oplus V \to V$, called **projections**, defined by $(u, v) \to u$ and $(u, v) \to v$. Note that injections and projections satisfies the following equations:

$$\pi_1 i_1 = id_U, \quad \pi_2 i_2 = id_V, \quad \pi_1 i_2 = 0, \quad \pi_2 i_1 = 0, \quad \text{and} \quad i_1\pi_1 + i_2\pi_2 = 1_M.$$

Conversely if M, U, and V are R-modules together with the R-module homomorphisms $i_1 : U \to M$, $i_2 : V \to M$, $\pi_1 : M \to U$, and $\pi_2 : M \to V$ satisfying the above equations, then $M \cong U \oplus V$.

Exercise 20. Give a proof for the previous statement.

Lemma 21. *Suppose that M is an R-module, and U and V are submodules of M such that*

$$U + V = M \quad \text{and} \quad U \cap V = 0.$$

Then $M \cong U \oplus V$. In this case we say M is an **internal direct sum** *of U and V.*

Proof. Consider the R-module homomorphism $\varphi : U \oplus V \to M$ defined by $\varphi(u, v) = u + v$. Since $M = U + V$, φ is surjective. If $\varphi(u, v) = \varphi(u', v')$, then $u + v = u' + v'$. Then $u - u' = v - v'$ is in $U \cap V = 0$. This implies $u = u'$ and $v = v'$. So, φ is injective. □

Remark 22. Note that an external direct sum $U \oplus V$ is an internal direct sum of its submodules $i_1(U)$ and $i_2(V)$ in $U \oplus V$.

When U, V, M are as in Lemma 21, then we say U and V are called direct summands of M. The submodule V is called a **complement** of $U \subseteq M$. Note that there can be more than one complement of a submodule.

Example 23. Let M be a two dimensional vector space over a field $\mathbb{F}$. If $U = \langle(1, 0)\rangle$, then both $V = \langle(0, 1)\rangle$ and $V' = \langle(1, 1)\rangle$ are complements of U.

Now we discuss direct sums in the context of short exact sequences of R-modules.

Definition 24. A short exact sequence

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} L \to 0$$

is a **split exact sequence** if there is an R-module homomorphism $s : L \to M$ such that $\pi s = \mathrm{id}_L$.

Note that if $M = U \oplus V$, then the sequence

$$0 \to U \xrightarrow{i_1} M \xrightarrow{\pi_2} V \to 0$$

is a split exact sequence with splitting $i_2 : V \to M$. Conversely we have the following:

Lemma 25. *If the short exact sequence* $0 \to N \xrightarrow{i} M \xrightarrow{\pi} L \to 0$ *is a split exact sequence, then* $M \cong N \oplus L$.

Proof. Let $s : L \to M$ be an R-module homomorphism such that $\pi s = \mathrm{id}_L$. For every $m \in M$, $\pi(m - s\pi(m)) = \pi(m) - \pi s\pi(m) = 0$, so there is a unique $n \in N$ such that $i(n) = m - s\pi(m)$. This defines an R-module homomorphism $t : M \to N$ such that $i(t(m)) = m - s\pi(m)$ for all $m \in M$. Consider the R-homomorphisms $\varphi : M \to N \oplus L$ and $\psi : N \oplus L \to M$ defined by $\varphi(m) = (t(m), \pi(m))$ and $\psi((n, l)) = i(n) + s(l)$ for all $m \in M$, $n \in N$, and $l \in L$. By direct calculation, we can show that $\psi\varphi = \mathrm{id}_M$ and $\varphi\psi = \mathrm{id}_{N \oplus L}$. Hence $\psi : M \to N \oplus L$ is an isomorphism. □

Exercise 26. Let

$$0 \to N \xrightarrow{i} M \xrightarrow{\pi} L \to 0$$

be a short exact sequence. Show that if there is an R-homomorphism $t : M \to N$ such that $ti = \mathrm{id}_N$, then this sequence is split and $M \cong N \oplus L$.

The direct sum of a finite collection of modules $M_1, \ldots, M_n$ is defined to be the R-module

$$M_1 \oplus \cdots \oplus M_n = \{(m_1, \ldots, m_n) \,|\, m_i \in M_i\}$$

with coordinate-wise addition. The multiplication with $r \in R$ is defined by $r(m_1, \ldots, m_n) = (rm_1, \ldots, rm_n)$. Given a finite collection $M_1, \ldots, M_n$ of submodules of M, we have $M \cong M_1 \oplus \cdots \oplus M_n$ if $M_1 + \cdots + M_n = M$ and for every $i \in \{1, \ldots, n\}$,

$$M_i \cap (M_1 + \cdots + \widehat{M_i} + \cdots + M_n) = 0.$$

Here the notation $\widehat{M_i}$ means the i-th term in the sum is removed.

Definition 27. Let $\{M_i\}_{i \in I}$ be an arbitrary collection of R-modules.

1. The **direct product** $\prod_{i \in I} M_i$ is defined to the the R-module whose elements are tuples $(m_i)_{i \in I} \in \prod_{i \in I} M_i$ with coordinate-wise addition $(m_i) + (m_i') = (m_i + m_i')$ and the scalar multiplication defined by $r(m_i) = (rm_i)$ for every $m_i, m_i' \in M_i$ and $r \in R$.
2. The **direct sum** $\bigoplus_{i \in I} M_i$ is the submodule of $\prod_{i \in I} M_i$ consists of all tuples $(m_i)_{i \in I}$ where $m_i = 0$ for all but finitely many $i \in I$.

For each $j \in I$, there is an injection $i_j : M_j \to \prod_{i \in I} M_i$ defined by $i_i(m_j) = (u_i)$ where $u_i = m_j$ if $i = j$ and $u_i = 0$ if $i \neq j$. For each $j \in I$, the projection $p_j : \prod_{i \in I} M_i \to M_j$ is defined by $p_j((m_i)_{i \in I}) = m_j$. The injections and projections induces injections and projections on the submodule $\bigoplus_{i \in I} M_i \subseteq \prod_{i \in I} M_i$.

2.3 Free R-Modules

Throughout, R is an associative unital ring.

Definition 28. Let M be an R-module. A subset $\mathcal{B} \subseteq M$ is called a **basis** for M if for every $m \in M$ there exists a unique set of elements $\{r_b\}_{b\in B}$ with only finitely many r_b's nonzero, such that

$$m = \sum_{b\in\mathcal{B}} r_b b.$$

An R-module M is a said to be a **free R-module** if it has a basis.

Example 29. By standard theorems in linear algebra, if $\mathbb{F}$ is a field then every $\mathbb{F}$-module has a basis, hence every $\mathbb{F}$-module is free.

Example 30. Let A be an abelian group. An element $a \in A$ is called a **torsion element** if there is a nonzero integer $n \in \mathbb{Z}$ such that $na = 0$. By the classification of finitely generated abelian groups, a finitely generated abelian group A is a free $\mathbb{Z}$-module if and only if there are no nonzero torsion elements in A.

Lemma 31. *An R-module M is free if and only if $M \cong \bigoplus_{i\in I} R$ for some indexing set I.*

Proof. Let M be a free R-module with basis $\mathcal{B}$. For each $b \in B$, the submodule $\langle b\rangle = \{rb \,|\, r \in R\} \subseteq M$ is isomorphic to R. Since $\mathcal{B}$ spans M, we have $\sum_{b\in\mathcal{B}}\langle b\rangle = M$. Using the linear independence we can show that for every $b_0 \in B$, $\langle b_0\rangle \cap \sum_{b\in\mathcal{B}\setminus b_0}\langle b\rangle = 0$. Hence

$$M \cong \bigoplus_{b\in B}\langle b\rangle \cong \bigoplus_{b\in B} R.$$

Conversely let $\varphi : \oplus_{i\in I}R \to M$ be an isomorphism. For each $j \in I$, consider the element $e_j = (r_i) \in \prod_{i\in I} R$ such that $r_j = 1$ and $r_i = 0$ for all $i \neq j$. For each $j \in I$, let $b_j = \varphi(e_j) \in M$. We claim that $\mathcal{B} = \{b_i | i \in I\}$ is a basis for M. Since φ is surjective, for every $m \in M$, there is $(r_i) \in \oplus_{i\in I}R$ such that $\varphi((r_i)) = m$. Then since $(r_i) = \sum_{i\in I} r_i e_i$, we have $m = \sum_i r_i b_i$. Note that in this sum only finitely many r_i's are nonzero. This shows that $\mathcal{B}$ spans M. For linear independence assume that $\sum r_i b_i = 0$ for some r_i. Then we get $\varphi((r_i)) = 0$. Since φ is injective, we obtain $r_i = 0$ for all i. Hence $\mathcal{B}$ is a basis for M. □

Lemma 32. *If M is a finitely generated free R-module, then it has a finite basis.*

Proof. Let F be a free module with basis $\mathcal{B}$. Assume that F has a finite generating set X. Each element $x \in X$ can be written as a finite linear combination of elements in $\mathcal{B}$. Let $\mathcal{B}_x$ be the finite set of elements in $\mathcal{B}$ used in the linear combination for x. Then the set $\cup_{x\in X}\mathcal{B}_x$ spans M, hence it is a finite basis for F. □

Note that for an arbitrary ring R, a free R-module may have two basis with different number of elements when R is not commutative.

Proposition 33. *For any set X there is a free R-module with basis X, denoted by RX.*

Proof. Consider the set of all formal sums $\sum_{x\in X} a_x x$ with $a_x \in R$ where $a_x \neq 0$ for only finitely many $x \in X$. A formal sum can be defined as a function $f : X \to R$ with $f(x) \neq 0$ for only finitely many $x \in X$. Then for each $x \in X$, the coefficient $a_x \in R$ will be $f(x) \in R$.

The sum of two formal sums is defined by

$$\sum_{x\in X} a_x x + \sum_{x\in X} b_x x = \sum_{x\in X} (a_x + b_x)x.$$

The multiplication with $r \in R$ is defined by

$$r(\sum_{x\in X} a_x x) = \sum_{x\in X} r a_x x.$$

By definition this is a free R-module with basis given by X. □

An immediate corollary of this is the following:

Theorem 34. *For every R-module M, there is a surjective R-linear map $\varphi : F \to M$ where F is a free R-module. Moreover, M is finitely generated if and only if there is an R-linear map $\varphi : F \to M$ with F is finitely generated free R-module.*

Proof. Let X be a generating set for M. Let $F = RX$ be the free R-module with basis X. Consider the R-module homomorphism $\varphi : RX \to M$ defined by

$$\varphi(\sum_{x\in X} r_x x) = \sum_{x\in X} r_x x$$

where the first sum is in RX and the second sum is the sum in M which is defined even when X is infinite since $r_x = 0$ for all but finitely many $x \in X$. It is clear that φ defines an R-module homomorphism and it is surjective because the image includes X.

For the second sentence, note that if M is finitely generated we can take X as a finite set, so F is finitely generated. For the other direction, by Lemma 32, if F is a finitely generated free R-module, then it has a finite basis B. The set $\{\varphi(b) \mid b \in \mathcal{B}\}$ is a finite generating set for M, hence M is finitely generated. □

2.4 Hom Functor

Let R be an associative ring with unity. For two R-modules M and N, let $\mathrm{Hom}_R(M, N)$ denote the set of all R-module homomorphisms $f : M \to N$. Given two R-module homomorphisms $f, g \in \mathrm{Hom}_R(M, N)$, we define their sum to be the homomorphism $f + g$ defined by $(f+g)(m) = f(m)+g(m)$ for all $m \in M$. Together with this addition operation, $\mathrm{Hom}_R(M, N)$ is an abelian group. The zero element is the zero homomorphism which sends every $m \in M$ to 0.

Definition 35. 1. Let N be an R-module. Given an R-module homomorphism $\varphi : M \to M'$, there is an abelian group homomorphism

$$\varphi^* : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N)$$

defined $\varphi^*(f) = f\varphi$ for every $f \in \mathrm{Hom}_R(M', N)$.

2. Let M be an R-module. Given an R-module homomorphism $\varphi : N \to N'$, there is an abelian group homomorphism

$$\varphi^* : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N')$$

defined $\varphi_*(f) = \varphi f$ for every $f \in \mathrm{Hom}_R(M, N)$.

Because of the induced maps defined above the assignment $(M, N) \to \mathrm{Hom}_R(M, N)$ defines a functor

$$\mathrm{Hom}_R(-,-) : (R\text{-Mod})^{op} \times R\text{-Mod} \to Ab$$

where Ab is the category of abelian groups. We call this functor, the **Hom-functor**.

For each R-module M, the functor $\mathrm{Hom}_R(M, -)$ is a covariant functor R-Mod $\to Ab$, and for each R-module N, the functor $\mathrm{Hom}_R(-, N)$ is a contravariant functor $(R\text{-Mod})^{op} \to Ab$. Neither of these two functors take the exact sequences to exact sequences. However they both satisfy a property called left exactness as stated in the following lemma.

Lemma 36.

1. *Let N be an R-module. Given an exact sequence of R-module homomorphisms*

$$0 \to M_1 \xrightarrow{j} M_2 \xrightarrow{\pi} M_3 \to 0,$$

the sequence

$$0 \to \mathrm{Hom}_R(M_3, N) \xrightarrow{\pi^*} \mathrm{Hom}_R(M_2, N) \xrightarrow{j^*} \mathrm{Hom}_R(M_1, N)$$

is exact.

2. *Let M be an R-module. Given an exact sequence of R-module homomorphisms*

$$0 \to N_1 \xrightarrow{j} N_2 \xrightarrow{\pi} N_3 \to 0,$$

the sequence

$$0 \to \mathrm{Hom}_R(M, N_1) \xrightarrow{j_*} \mathrm{Hom}_R(M, N_2) \xrightarrow{\pi_*} \mathrm{Hom}_R(M, N_3)$$

is exact.

Proof. (1) Let $f \in \ker \pi_*$. Then $f : M_3 \to N$ such that $\pi^*(f) = f\pi = 0$. Since π is surjective, this shows f is the zero homomorphism. So π^* is injective. So the sequence is exact at $\mathrm{Hom}_R(M_3, N)$.

To show the exactness at $\mathrm{Hom}_R(M_2, N)$, first observe that $j^*\pi^* = (\pi j)^* = 0$. Hence $\mathrm{im}\, \pi^* \subseteq \ker j^*$. Let $f \in \ker j^*$. Then $fj = 0$. Since $\mathrm{im}\, j = \ker \pi$, this shows that $f(m) = 0$ for every $m \in \ker \pi$. Consider the R-module homomorphism $\overline{f} : M_3 \to N$ defined as follows: For every $m \in M_3$ there is an $\widehat{m} \in M_2$ such that $\pi(\widehat{m}) = m$. Note that the element $\widehat{m}$ is not uniquely determined by m. The different choices of $\widehat{m}$ for a given m differ by an element in $\ker \pi$. We define $\overline{f}$ to be the map such that $\overline{f}(m) = f(\widehat{m})$ for every $m \in M_3$. Note that $\overline{f}$ is well defined because $f(m) = 0$ for all $m \in \ker \pi$. By construction $\pi^*(\overline{f}) = \overline{f}\pi = f$, so $f \in \mathrm{im}\, \pi^*$. The proof of (2) can be given in a similar way. □

There are many examples of short exact sequences where the exactness of the Hom-functor fails. Before we give such examples, we prove a useful lemma.

Lemma 37. *For any R-module M, $\mathrm{Hom}_R(R, M) \cong M$ as abelian groups. More generally if RX is the free R-module with basis given by X, then*

$$\mathrm{Hom}_R(RX, M) \cong \{f : X \to M\}$$

as abelian groups.

Proof. Every element in RX can be uniquely written as $\sum_{x \in X} r_x x$ with $r_x \in R$ being nonzero only for finitely many $x \in X$. Hence an R-module homomorphism $\varphi : RX \to M$ is uniquely determined by its values on $x \in X$. This gives the following correspondence: To an homomorphism $\varphi : RX \to M$, we can associate a function $f : X \to M$ defined by $f(x) = \varphi(x)$ for all $x \in X$. Conversely every function $f : X \to M$ defines an R-module homomorphism $\varphi : RX \to M$ defined by $\varphi(\sum_x r_x x) = \sum_x r_x f(x)$. This gives a bijection between these two sets. The abelian group structure on $f : X \to M$ is defined by the coordinate-wise addition. So the correspondence given above preserves the addition. □

Example 38. Consider the short exact sequence of abelian groups

$$0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{m_2} \mathbb{Z}/2 \to 0 \tag{1}$$

where m_2 denotes the mod-2 reduction map. Applying the functor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$, we obtain a sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \to 0.$$

Since there are no nonzero group homomorphism from $\mathbb{Z}/2$ to $\mathbb{Z}$, the first term is zero. By Lemma 37, we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$. So we get a sequence of the form

$$0 \to 0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to 0$$

which is not exact at the second $\mathbb{Z}$ because the map $\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$ is not a surjective map. Similarly if we apply the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, -)$ to the short exact sequence in (1) then we get a sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/2) \to 0.$$

Since $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}) = 0$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/2) \cong \mathbb{Z}/2$, this is a sequence of the form

$$0 \to 0 \to 0 \to \mathbb{Z}/2 \to 0$$

which is not exact.

In some cases the abelian group $\mathrm{Hom}_R(M, N)$ has more than an abelian group structure. It has a module structure with respect to another ring.

Definition 39. Let R and S be two rings. Then we say M is an **R-S-bimodule** if M is a left R-module and a right S-module such that for every $r \in R$, $s \in S$, and $m \in M$, we have $(rm)s = r(ms)$.

Lemma 40.

1. *Let M be an R-S-bimodule and N be a left R-module. Then $\mathrm{Hom}_R(M,N)$ is a left S-module with the multiplication given by $(sf)(m) = f(ms)$ for all $s \in S$ and $m \in M$.*
2. *Let M be an R-S-bimodule and N be a right S-module. Then $\mathrm{Hom}_R(M,N)$ is a right R-module with the multiplication given by $(fr)(m) = f(rm)$ for all $r \in R$ and $m \in M$.*
3. *Let N be an R-S-bimodule and M be an R-module. Then $\mathrm{Hom}_R(M,N)$ is a right S-module with the multiplication given by $(fs)(m) = f(m)s$ for all $s \in S$ and $m \in M$.*

Proof. (1) For $s_1, s_2 \in S$, and for $m \in M$, we have

$$((s_1 s_2)f)(m) = f(m(s_1 s_2)) = f((ms_1)s_2) = (s_2 f)(ms_1) = (s_1(s_2 f))(m).$$

Hence the defined action is a left action. The other conditions are easy to check. The proof of (2) and (3) are similar. □

Example 41. The module structures described above are useful in several occasions. Let M be an R-module and A be an abelian group. Then we can consider M as a R-$\mathbb{Z}$-bimodule with right $\mathbb{Z}$-module structure given by $mn = m + \cdots + m$ (n times). Similarly we can consider A as a right $\mathbb{Z}$-module. Then applying Lemma 40 (2), we see that $\mathrm{Hom}_{\mathbb{Z}}(M,A)$ is a right R-module. Similarly, if M is a right R-module, we can consider it as a $\mathbb{Z}$-R-bimodule. Then for any abelian group A, $\mathrm{Hom}_{\mathbb{Z}}(A,M)$ has a right R-module structure.

Example 42. If R is a commutative ring, then an R-module M can be considered also as a left R-module with the multiplication given by $mr := rm$ for every $r \in R$ and $m \in M$. Because of the commutativity of R, we have

$$(mr)s = (rm)s = s(rm) = (sr)m = m(sr) = m(rs)$$

for every $m \in M$ and $r, s \in R$. Because of this when R is commutative, $\mathrm{Hom}_R(M,N)$ has an R-module structure given by $(rf)(m) = f(rm)$.

The Hom-functor distributes over a direct sum. This means that for R-modules M, N, and L, we have abelian group isomorphisms

$$\mathrm{Hom}_R(M, N \oplus L) \cong \mathrm{Hom}_R(M,N) \oplus \mathrm{Hom}_R(M,L)$$

$$\mathrm{Hom}_R(M \oplus N, L) \cong \mathrm{Hom}_R(M,L) \oplus \mathrm{Hom}_R(N,L).$$

For infinite collections, we have similar isomorphisms. For a family of R-modules $\{N_i\}_{i\in I}$, let $p_j : \prod_{i\in I} N_i \to N_j$ denote the projection map $p_j((n_i)_{i\in I}) = n_j$. Similarly for a family of R-modules $\{M_i\}_{i\in I}$, let $i_j : M_j \to \prod_{i\in I} M_i$ denote the inclusion map $i_j(m) = (m_i)_{i\in I}$ where $m_i = m$ for $i = j$ and $m_i = 0$ for $i \neq j$.

Theorem 43.

1. *Let M be an R-module and $\{N_i\}_{i\in I}$ be a family of R-modules. Then the R-module homomorphism*
$$\varphi : \mathrm{Hom}_R(M, \prod_{i\in I} N_i) \to \prod_{i\in I} \mathrm{Hom}_R(M, N_i)$$
defined by $\varphi(f) = (p_i f)_{i\in I}$ is an isomorphism of abelian groups. If R is commutative, then it is an isomorphism of R-modules.

2. *Let $\{M_i\}_{i\in I}$ be a family of R-modules and N be an R-module. Then the R-module homomorphism*

$$\varphi : \mathrm{Hom}_R(\bigoplus_{i\in I} M_i, N) \to \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$$

defined by $\varphi(f) = (fi_j)_{j\in I}$ is an isomorphism of abelian groups. If R is commutative, then it is an isomorphism of R-modules.

Exercise 44. Prove the above theorem. Study the Example 2.25 in Chapter 2 of Rotman to see why the other possible isomorphisms don't work.

3 Chain Complexes and Homology

3.1 Chain Complexes of R-Modules

Throughout R is an associative unital ring.

Definition 45. A **chain complex** C_* of R-modules consists of a family $\{C_n\}_{n\in\mathbb{Z}}$ of R-modules together with R-module homomorphisms

$$d_n : C_n \to C_{n-1}$$

such that for every $n \in \mathbb{Z}$, the composition

$$d_n d_{n+1} : C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1}$$

is the zero homomorphism. The maps $\{d_n\}$ are called the **boundary maps** or the **differentials** of C_*.

We often write a chain complex as a sequence of homomorphisms:

$$C_* : \cdots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_1} C_0 \xrightarrow{d_0} C_{-1} \xrightarrow{d_{-1}} C_{-2} \xrightarrow{d_{-2}} \cdots$$

A chain complex is **bounded from below** (resp. **above**) if there is an $m \in \mathbb{Z}$ such that $C_i = 0$ for all $i \leq m$ (resp. for all $i \geq m$). In algebraic topology one often deals with chain complexes which are **non-negative**, i.e. $C_i = 0$ for all $i < 0$.

For each $n \in \mathbb{Z}$, the kernel of d_n is called the module of n-cycles of C_*, denoted by $Z_n = Z_n(C_*)$. The image of $d_{n+1} : C_{n+1} \to C_n$ is the module of n-boundaries of C_* denoted by $B_n = B_n(C_*)$. Since the composition $d_n d_{n+1}$ is zero, for every $n \in \mathbb{Z}$, we have

$$0 \subseteq B_n \subseteq Z_n \subseteq C_n.$$

Definition 46. Let C_* be a chain complex of R-modules. For each $n \in \mathbb{Z}$, the **n-th homology module of** C_* is the subquotient

$$H_n(C_*) := Z_n/B_n.$$

The homology class represented by $x \in Z_n(C_*)$ is denoted by $[x]$.

Note that if $H_n(C_*) = 0$, then the sequence $C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1}$ is exact at C_n. The n-th homology group $H_n(C_*)$ of a chain complex C_* measures how far the sequence is from the exactness at C_n. A chain complex C_* is called **acyclic** if $H_n(C_*) = 0$ for all $n \in \mathbb{Z}$. Such a chain complex C_* is exact at C_n for every $n \in \mathbb{Z}$.

Example 47. Consider the chain complex C_* of $\mathbb{Z}$-modules where $C_n = \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $d_n : C_n \to C_{n-1}$ is equal to the identity map if n is odd and is equal to the zero map if n is even. We can write C_* as

$$\cdots \to \mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\mathrm{id}} \cdots \to \mathbb{Z} \xrightarrow{0} \mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z} \xrightarrow{0} \cdots .$$

It is easy to see that $H_n(C_*) = 0$ for all $n \in \mathbb{Z}$. Hence C_* is an acyclic complex.

Example 48. Let $C_n = \mathbb{Z}/8$, integers mod 8, for all $n \geq 0$ and $C_n = 0$ for $n < 0$. Suppose that d_n is defined by $d_n(x) = 4x \pmod 8$ for all $n \geq 1$. Then we have

$$\cdots \to \mathbb{Z}/8 \xrightarrow{d_{n+1}} \mathbb{Z}/8 \xrightarrow{d_n} \mathbb{Z}/8 \xrightarrow{d_{n-1}} \cdots \to \mathbb{Z}/8 \xrightarrow{d_1} \mathbb{Z}/8 \xrightarrow{d_0} 0 \to 0 \to \ldots.$$

Observe that C_* is a chain complex since $d_n d_{n+1}(x) = d_n(4x) = 4(4x) = 16x = 0 \pmod 8$. For each $n \geq 1$, we have

$$H_n(C_*) = \frac{\ker d_n}{\operatorname{im} d_{n+1}} = \frac{\{x \in \mathbb{Z}/8 \mid 4x = 0\}}{\{4y \mid y \in \mathbb{Z}_8\}} = \frac{\{0,2,4,6\}}{\{0,4\}} \cong \mathbb{Z}/2$$

and

$$H_0(C_*) = \frac{\ker d_0}{\operatorname{im} d_1} = \frac{C_0}{\operatorname{im} d_1} = \frac{\mathbb{Z}/8}{4 \cdot \mathbb{Z}/8} \cong \mathbb{Z}/4.$$

Note that $H_n(C_*) = 0$ for all $n < 0$.

Definition 49. A sequence of R-module homomorphisms $\{f_n : C_n \to D_n\}_{n \in \mathbb{Z}}$ is called a **chain map** if for every $n \in \mathbb{Z}$,

$$d_n^D f_n = f_{n-1} d_n^C.$$

A chain map $f_* : C_* \to D_*$ is usually expressed as a sequence of commuting diagrams:

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}^C} & C_n & \xrightarrow{d_n^C} & C_{n-1} & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\ldots & \longrightarrow & D_{n+1} & \xrightarrow{d_{n+1}^D} & D_n & \xrightarrow{d_n^D} & D_{n-1} & \longrightarrow & \ldots
\end{array}$$

Exercise 50. Show that a morphism $f_n : C_n \to D_n$ of chain complexes sends boundaries to boundaries, cycles to cycles and for each $n \in \mathbb{Z}$ induces an R-module homomorphism $H_n(f_*) : H_n(C_*) \to H_n(D_*)$.

Definition 51. A morphism $f_* : C_* \to D_*$ of chain complexes is called a **quasi-isomorphism** if for every $n \in \mathbb{Z}$, the induced map $H_n(f_*) : H_n(C_*) \to H_n(D_*)$ is an isomorphism.

3.2 Chain Homotopy

Definition 52. Let C_* and D_* be two chain complexes of R-modules. The chain maps $f_*, g_* : C_* \to D_*$ are said to be **chain homotopic** if for each $n \in \mathbb{Z}$, there is an R-module homomorphism $s_n : C_n \to D_{n+1}$ such that

$$f_n - g_n = d_{n+1}^D s_n + s_{n-1} d_n^C$$

for every $n \in \mathbb{Z}$. We can express this in a diagram as follows:

$$\begin{array}{ccccccccccccccccc}
\cdots & \longrightarrow & C_{n+2} & \xrightarrow{d_{n+2}^C} & C_{n+1} & \xrightarrow{d_{n+1}^C} & C_n & \xrightarrow{d_n^C} & C_{n-1} & \cdots & \longrightarrow & C_2 & \xrightarrow{d_2^C} & C_1 & \xrightarrow{d_1^C} & C_0 & \longrightarrow 0 \\
 & & \downarrow & \swarrow{\scriptstyle s_{n+1}} & \downarrow & \swarrow{\scriptstyle s_n} & \downarrow & \swarrow{\scriptstyle s_{n-1}} & \downarrow{\scriptstyle f_{n-1}-g_{n-1}} & & & \downarrow & \swarrow{\scriptstyle s_1} & \downarrow & \swarrow{\scriptstyle s_0} & \downarrow{\scriptstyle f_0-g_0} & \\
\cdots & \longrightarrow & D_{n+2} & \xrightarrow[d_{n+2}^D]{} & D_{n+1} & \xrightarrow[d_{n+1}^D]{} & D_n & \xrightarrow[d_n^D]{} & D_{n-1} & \cdots & \longrightarrow & D_2 & \xrightarrow[d_2^D]{} & D_1 & \xrightarrow[d_1^D]{} & D_0 & \longrightarrow 0
\end{array}$$

The collection of R-module homomorphisms $\{s_n : C_n \to D_{n+1}\}_{n \in \mathbb{Z}}$ is called a **chain homotopy** between f_* and g_*. When f_* and g_* are chain homotopic, then we write $f_* \simeq g_*$. If f_* is homotopic to the zero chain map, then we say f_* is null homotopic.

Exercise 53. Show that chain homotopy defines an equivalence relation on the set of chain maps $C_* \to D_*$.

Lemma 54. *If f_* and g_* are chain homotopic, then the maps induced by f_* and g_* on homology are equal, i.e. for each $n \in \mathbb{Z}$,*

$$H_n(f_*) = H_n(g_*) : H_n(C_*) \to H_n(D_*).$$

Proof. Suppose there is a homotopy $h_* : C_* \to D_{*+1}$ such that for every $n \in \mathbb{Z}$, the equation $f_n - g_n = d^D_{n+1}s_n + s_{n+1}d^C_n$ holds. Then for every $x \in Z_n(C_*)$, we have

$$f_n(x) - g_n(x) = d^D_{n+1}s_n(x) + s_{n+1}d^C_n(x) = d^D_{n+1}s_n(x) \in B_n(D_*).$$

Hence

$$H_n(f_*)([x]) - H_n(g_*)([x]) = [f_n(x) - g_n(x)] = 0$$

in $H_n(D_*)$. □

Definition 55. The chain complexes C_* and D_* are **chain homotopy equivalent** if there are chain maps $f_* : C_* \to D_*$ and $g_* : D_* \to C_*$ such that $g_*f_* \simeq \mathrm{id}_{C_*}$ and $f_*g_* \simeq \mathrm{id}_{D_*}$. In this case we write $C_* \simeq D_*$ and say f_* is a chain homotopy equivalence.

Corollary 56. *If $f_* : C_* \to D_*$ is a chain homotopy equivalence, then it is a quasi-isomorphism.*

Proof. If f_* is a chain homotopy equivalence, then there is a $g_* : D_* \to C_*$ such that $g_*f_* \simeq \mathrm{id}_{C_*}$ and $f_*g_* \simeq \mathrm{id}_{D_*}$. Since homotopic chain maps induces the same maps on homology, for each $n \in \mathbb{Z}$, we have $H_n(g_*) \circ H_n(f_*) = \mathrm{id}_{H_n(C_*)}$ and $H_n(f_*) \circ H_n(g_*) = \mathrm{id}_{H_n(D_*)}$. This proves that $H_n(f_*)$ is an isomorphism for each $n \in \mathbb{Z}$. □

A special case of a chain homotopy equivalence is when a chain complex C_* is chain homotopy equivalent to the zero chain complex, i.e. the chain complex with all chain modules are zero module. In this case we say the complex C_* is **contractible**. If C_* is a contractible complex, there is a chain homotopy between the identity map $\mathrm{id}_{C_*} : C_* \to C_*$ and the zero map. This chain homotopy is called a **contracting homotopy**. Note that if C_* is contractible, then C_* is acyclic, i.e. $H_n(C_*) = 0$ for every $n \in \mathbb{Z}$.

Example 57. Consider the chain complex C_* in Example 47 where $C_n = \mathbb{Z}$ for all $n \in \mathbb{Z}$ and $d_n : C_n \to C_{n-1}$ is equal to the identity map if n is odd, and is equal to the zero map if n is even. The complex C_* is contractible. A contracting homotopy $s_* : C_* \to C_{*+1}$ can be defined as follows: For each $n \in \mathbb{Z}$, let $s_n : C_n \to C_{n+1}$ be the identity map $\mathrm{id}_{\mathbb{Z}}$ if n is even and be the zero map if n is odd. It is easy to check that for every $n \in \mathbb{Z}$,

$$\mathrm{id}_{C_n} = d^D_{n+1}s_n + s_{n+1}d^C_n.$$

Note that $H_n(C_*) = 0$ for all $n \in \mathbb{Z}$.

Example 58. A complex C_* can be acyclic but not chain homotopy equivalent to the zero complex. Consider the chain complex of abelian groups

$$\cdots \to 0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \xrightarrow{m_2} \mathbb{Z}/2 \to 0 \to \cdots$$

where $C_0 = \mathbb{Z}/2$ and $d_1 : C_1 \to C_0$ is the mod-2 reduction map $m_2 : \mathbb{Z} \to \mathbb{Z}/2$. It is easy to see that $H_n(C_*) = 0$ for all $n \in \mathbb{Z}$. If there were a chain homotopy $s_* : C_* \to C_{*+1}$ between the identity map and the zero map, then we would have an abelian group homomorphism $s_0 : \mathbb{Z}/2 \to \mathbb{Z}$ such that $m_2 s_0 = \mathrm{id}_{\mathbb{Z}/2}$. But there is no nonzero homomorphism from $\mathbb{Z}/2$ to $\mathbb{Z}$ sinc there is no integer $n \in \mathbb{Z}$ such that $2n = 0$ except $n = 0$.

Exercise 59. Show that if $f, g : C_* \to D_*$ are chain homotopic and $f', g' : D_* \to E_*$ are chain homotopic, then the compositions $f' \circ f$ and $g' \circ g$ are chain homotopic.

Exercise 60. Let $\mathbb{F}$ be a field and C_* be a chain complex of $\mathbb{F}$-vector spaces. Show that there exist two subcomplexes A_* and B_* of C_* satisfying the following properties (all of them):

1. $C_* = A_* \oplus B_*$
2. A_* is nullhomotopic (i.e. homotopic to the zero complex).
3. B_* has zero differentials (i.e. $d^B_* = 0$).

3.3 Simplicial and Singular Homology

Chain complexes were first introduced in algebraic topology to define (co)homology groups of topological spaces. Topological spaces can be studied sometimes as Topological Spaces, CW-complexes, simplicial complexes, or smooth manifolds. In each of these categories there is a different way to define homology of the object in that category. The general idea is to first build a chain complex $C_*(X)$ associated to an object X in one of these categories, and then define the homology groups of X to be the homology groups of the chain complex $C_*(X)$. We first start explaining the simplicial homology of a simplicial complex which is relatively easier to compute if the complex is small.

3.3.1 Simplicial Homology

A set of points $\{x_0, \ldots, x_k\}$ in $\mathbb{R}^n$ is called **affinely independent** if the set of vectors $\{x_1 - x_0, \ldots, x_k - x_0\}$ is linearly independent. For $k = 0$, we assume by convention that the set $\{x_0\}$ is affinely independent.

Definition 61. For an affinely independent set $\{x_0, \ldots, x_k\}$ in $\mathbb{R}^n$, the **geometric k-simplex** with vertices $x_0, \ldots, x_k$ is the subspace

$$\langle x_0, \ldots, x_k \rangle = \{t_0 x_0 + \ldots, t_k x_k \mid \sum_{i=0}^{n} t_i = 1, t_i \geq 0\} \subseteq \mathbb{R}^n$$

whose topology is given by the subspace topology in $\mathbb{R}^n$.

For every nonempty subset $\{x_{i_0}, \ldots, x_{i_r}\}$ of $\{x_0, \ldots, x_k\}$, the r-simplex with vertices $x_{i_0}, \ldots, x_{i_r}$ is called a **face** of $\langle x_0, \ldots, x_k \rangle$.

Definition 62. For each $k \geq 0$, the standard k-simplex Δ^k is defined as the geometric k-simplex whose vertices are the standard basis $\{e_0, \ldots, e_k\}$ in $\mathbb{R}^{k+1}$. In other words, the k-simplex is the subspace

$$\Delta^k = \{(t_0, \ldots, t_k) \in \mathbb{R}^{k+1} \mid \sum_{i=0}^{k} t_i = 1, t_i \geq 0\} \subseteq \mathbb{R}^{k+1}.$$

Standard k-simplex plays an important role when we are defining singular homology. Note that all k-simplices are homeomorphic to the standard k-simplex Δ^k. For $k = 0$, the 0-simplex Δ^0 is a point, 1-simplex Δ^1 is a line segment. The 2-simplex Δ^2 is a triangle with its interior, and the 3-simplex Δ^3 is a tetrahedron with its interior. Using these as building blocks and by gluing them in an appropriate way, we can build many interesting spaces such as spheres, torus, surfaces, real-projective space, etc, up to homeomorphism.

Definition 63. A collection K of simplices in $\mathbb{R}^n$ is called a **simplicial complex** if it satisfies the following properties:

1. If $\sigma \in K$ and τ is a face of σ, then $\tau \in K$.
2. If σ and τ are simplices in K such that $\sigma \cap \tau \neq \emptyset$, then $\sigma \cap \tau$ is a face of σ and τ.
3. If K has infinitely many simplices, then we require that every point in $\mathbb{R}^n$ has a neighborhood intersecting finitely many simplices of K.

Example 64. Consider the set of integers $\mathbb{Z}$ in $\mathbb{R}$. For every $j \in \mathbb{Z}$, we can consider the 1-simplex $\langle j, j+1\rangle$ in $\mathbb{R}$. The collection $K = \{\langle j, j+1\rangle \mid j \in \mathbb{Z}\}$ is a simplicial complex with infinitely many simplices. The intersection of two simplices σ and τ is either empty or the simplices are of the form $\sigma = \langle j-1, j\rangle$ and $\tau = \langle j, j+1\rangle$ and there intersection $\sigma \cap \tau = \langle j\rangle$ is a face of σ and τ. It is clear that every point in $\mathbb{R}^n$ has a neighborhood which intersect with only finitely many simplices in K.

Definition 65. The **geometric realization** of a simplicial complex K in $\mathbb{R}^n$ is defined as the union

$$|K| = \bigcup_{\sigma \in K} \sigma$$

with subspace topology in $\mathbb{R}^n$.

If X is a topological space and K is a simplicial complex such that $|K|$ is homeomorphic to X, then we say K is a **triangulation** of X. Every smooth manifold can be triangulated.

Example 66. Let K be the collection of all proper faces of the standard simplex Δ^n. A proper face of a simplex σ is a face of σ which is different than σ. Note K is a simplicial complex since the nonempty intersection of any two faces is again a proper face of Δ^n, so it is in K. This simplicial complex is usually called the boundary of Δ^n, and it is denoted by $\partial\Delta^n$. For $n \geq 1$, the realization of $\partial\Delta^n$ is homeomorphic to the sphere S^{n-1}. So it gives a triangulation of S^{n-1}. As an example note that the boundary of 2-simplex Δ^2 is a triangle which gives a triangulation of circle S^1.

A 0-simplex in a simplicial complex K is usually called a vertex of K. Since every geometric simplex $\sigma = \langle x_0, \ldots, x_k\rangle$ is uniquely defined by its vertex set $\{x_0, \ldots, x_k\}$, a simplicial complex can also be described using the subsets of its vertex set.

Definition 67. A **abstract simplicial complex** K consists of set $V(K)$, called vertex set, and a set $S(K)$ of finite nonempty subsets of $V(K)$, called simplex set, satisfying the following properties:

1. For every $v \in V(K)$, $\{v\} \in S(K)$.

2. If $\sigma \in S(K)$ and $\emptyset \neq \tau \subseteq \sigma$, then $\tau \in S(K)$.

A simplex $\{v_0, \ldots, v_k\} \in S(K)$ with $k+1$ elements is called a **k-simplex** in K. We say K is **finite-dimensional** if there is an integer d such that K has a simplex of dimension d and no simplices of dimension $d+1$. In that case we say K is **d-dimensional**. A simplicial complex is **finite** if its vertex set is finite. An abstract complex K is called **locally finite** if each $v \in V(K)$ is in finitely many simplices in $S(K)$.

Example 68. Let K be a simplicial complex where $V(K) = \{1, 2, 3, 4\}$ and

$$S(K) = \{\{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}, \{1, 2, 3\}\}.$$

Then K is a finite 2-dimensional simplicial complex.

Given a geometric simplicial complex K_{geo} with vertex set V, we can define an abstract simplicial complex K_{abs} to be the simplicial complex whose vertex set is V and such that $\sigma = \{v_0, \ldots, v_k\}$ is a simplex K_{abs} if and only if $\langle v_0, \ldots, v_k \rangle$ is a simplex in K_{geo}.

Conversely given a abstract simplicial complex K_{abs} with finite vertex set $V = \{v_0, \ldots, v_n\}$, we can construct a geometric simplicial complex K_{geo} in $\mathbb{R}^{n+1}$ as follows: Consider the standard simplex Δ^n in $\mathbb{R}^{n+1}$. A geometric k-simplex $\langle e_{i_0}, \ldots, e_{i_k} \rangle$ in Δ^n is a simplex in K_{geo} if and only if the set $\{v_{i_0}, \ldots, v_{i_k}\}$ is a simplex in K_{abs}. It is easy to see that K_{geo} is a geometric simplicial complex because nonempty intersection of two faces of Δ^n is also a face of Δ^n. More generally we can construct a geometric simplicial complex for a locally finite abstract simplicial complex using the infinite dimensional real vector space $\mathbb{R}^\infty$.

There are two different ways to construct a simplicial complex associated to an (abstract) simplicial complex.

Ordered simplicial homology:

Let K be a simplicial complex with vertex set $V(K)$. Choose a total ordering for $V(K)$. Then for each k-simplex $\{v_0, \ldots, v_k\}$ in $S(K)$, we can write a tupple $[v_0, \ldots, v_k]$ where $v_0 < \cdots < v_k$ in $V(K)$. Such tuples are called the ordered k-simplices of K. For each $k \geq 0$, we define the chain group $C_k^{ord}(K)$ to be the free abelian group with basis given by all ordered k-simplices of K. For each $k \geq 1$, the boundary map $\partial_k : C_k^{ord}(K) \to C_{k-1}^{ord}(K)$ is defined by

$$\partial_k([v_0, \ldots, v_k]) = \sum_{i=0}^{k} (-1)^i [v_0, \ldots, \widehat{v_i}, \ldots, v_k]$$

where the notation $[v_0, \ldots, \widehat{v_i}, \ldots, v_k]$ means that the i-th vertex is removed from the list. All the other chain groups are taken to be zero, in particular, $C_i^{ord}(K) = 0$ for $i < 0$ and $C_i^{ord}(K) = 0$ if $i > \dim K$. By direct calculation one can show that for every $k \in \mathbb{Z}$, $\partial_{k-1}\partial_k = 0$, hence $C_*^{ord}(K)$ is a chain complex. For $n \geq 0$, the n-th homology group of the complex $C_*^{ord}(K)$ are called the ***n*-th ordered simplicial homology group** of the complex K and denoted by $H_n^{ord}(K)$.

Example 69. Consider the simplicial complex in Example 68 with vertex set $V(K) = \{1, 2, 3, 4\}$. Take the natural ordering $1 < 2 < 3 < 4$ as the total order on $V(K)$. then

the chain groups $C_k^{ord}(K)$ can be describe as follows:

$$C_2^{ord}(K) = \mathbb{Z}[1,2,3]$$
$$C_1^{ord}(K) = \mathbb{Z}[1,2] \oplus \mathbb{Z}[1,3] \oplus \mathbb{Z}[2,3] \oplus \mathbb{Z}[1,4]$$
$$C_0^{ord}(K) = \mathbb{Z}[1] \oplus \mathbb{Z}[2] \oplus \mathbb{Z}[3] \oplus \mathbb{Z}[4]$$

We have a chain complex of the form

$$0 \to C_2^{ord}(K) \xrightarrow{\partial_2} C_1^{ord}(K) \xrightarrow{\partial_1} C_0^{ord}(K) \to 0$$

where $\partial_1([i,j]) = [j] - [i]$ for every basis element in $C_1^{ord}(K)$ and

$$\partial_2([1,2,3]) = [2,3] - [1,3] + [1,2].$$

Note that

$$\begin{aligned}\partial_1\partial_2([1,2,3]) &= \partial_1([2,3] - [1,3] + [1,2]) \\ &= ([3] - [2]) - ([3] - [1]) + ([2] - [1]) = 0\end{aligned}$$

Note that $Z_2^{ord}(K) = \ker \partial_2 = 0$, so $H_2^{ord}(K) = 0$. By direct calculation one can show that $Z_1^{ord}(K)$ is generated by $[1,2] - [1,3] + [1,2]$ which is a boundary. So, $H_1^{ord}(K) = 0$. Finally, since $[i] - [j]$ is a boundary for every i, j such that $[i,j]$ is 1-simplex in K, we have $H_1^{ord}(K) \cong \mathbb{Z}$. In general, $H_0^{ord}(K) \cong \mathbb{Z}^m$ where m is the number of connected components of K.

Oriented simplicial homology:

Let K be a simplicial complex. For each simplex $\{v_0, \ldots, v_k\}$ choose a total order for the vertices $v_0, \ldots, v_k$ and write $(v_0, \ldots, v_k)$ for the $k+1$-tuple with the correct ordering. Such a tuple is called an **oriented** k-simplex. Let $C_*^{ori}(K)$ denote the free abelian group with basis given by all oriented k-simplices of K. For the tuples of vertices ordered in a different way, we have the following identification: For every permutation $\sigma : \{0, \ldots, k\} \to \{0, \ldots, k\}$, define

$$(v_{\sigma(0)}, \ldots, v_{\sigma(k)}) = \text{sign}(\sigma)(v_0, \ldots, v_k)$$

in $C_k^{ori}(K)$. For each $k \geq 1$, the boundary map $\partial : C_k^{ori} \to C_{k-1}^{ori}$ is defined in a similar way:

$$\partial_k((v_0, \ldots, v_k)) = \sum_{i=0}^{k} (-1)^i (v_0, \ldots, \widehat{v_i}, \ldots, v_k).$$

The only difference is that since each simplex is oriented, possibly in a noncompatible way, the tuple $(v_0, \ldots, \widehat{v_i}, \ldots, v_k)$ may not the ordered in a correct way, we may have to introduce a minus sign when we change its orientation to the correct one.

Example 70. Consider the simplicial complex in Example 68 with vertex set $V(K) = \{1,2,3,4\}$. Orient the simplices as $(1,2)$, $(2,3)$, $(3,1)$, $(4,1)$, and $(2,3,1)$, then $C_k^{ori}(K)$ can be describe as follows:

$$C_2^{ori}(K) = \mathbb{Z}(2,3,1)$$
$$C_1^{ori}(K) = \mathbb{Z}(1,2) \oplus \mathbb{Z}(3,1) \oplus \mathbb{Z}(2,3) \oplus \mathbb{Z}(4,1)$$
$$C_0^{ori}(K) = \mathbb{Z}(1) \oplus \mathbb{Z}(2) \oplus \mathbb{Z}(3) \oplus \mathbb{Z}(4)$$

We have a chain complex of the form

$$0 \to C_2^{ori}(K) \xrightarrow{\partial_2} C_1^{ori}(K) \xrightarrow{\partial_1} C_0^{ori}(K) \to 0$$

where $\partial_1((i,j)) = (j) - (i)$ for every basis element in $C_1^{ori}(K)$ and

$$\partial_2((2,3,1)) = (3,1) - (2,1) + (2,3). = (3,1) + (1,2) + (2,3) = (2,3) + (3,1) + (1,2).$$

Note that thinking $(2,3) + (3,1) + (1,2)$ as a boundary of $(2,3,1)$ is more natural than the formula with minus signs. As before we have $Z_2^{ori}(K) = \ker \partial_2 = 0$, so $H_2^{ori}(K) = 0$. By direct calculation one can show that $Z_1^{ori}(K)$ is generated the 2-cycle by $(2,3)+(3,1)+(1,2)$ which is a boundary of $(2,3,1)$. So, $H_1^{ori}(K) = 0$. Finally, as before we have $H_1^{ori}(K) \cong \mathbb{Z}$.

3.3.2 Singular Homology

Let X be a topological space and R be any commutative ring. For each n, let Δ^n denote the standard n-simplex defined as

$$\Delta^n = \{(t_0, \cdots, t_n) \in \mathbb{R}^{n+1} \mid \sum_{i=0}^{n} t_i = 1, t_i \geq 0\}.$$

The n-simplex Δ^n is a topological space with subspace topology. For each $i \in \{0, \ldots, n\}$, there are continuous face maps $d^i : \Delta^{n-1} \to \Delta^n$ defined by

$$d^i(t_0, \cdots, t_{n-1}) = (t_0, \cdots, t_{i-1}, 0, t_i, \ldots, t_n).$$

For $n \geq 0$, consider the set X_n of all continuous functions $\sigma : \Delta^n \to X$. Let $C_n(X; R)$ be the free R-module with basis given by X_n. For each $n \geq 1$, the boundary map $\partial_n : C_n(X; R) \to C_{n-1}(X; R)$ is defined by

$$\partial_n(\sigma) = \sum_{i=0}^{n} (-1)^i \sigma \circ d^i$$

for every continuous function $f : \Delta^n \to X$. By direct calculation, similar to the one we did for simplicial chain complex, we can show that ∂_n is a derivation, so $C_*(X; R)$ is a chain complex.

Definition 71. For each $n \geq 0$, the n-th homology group the chain complex $C_*(X; R)$ is called the **n-th singular homology group** of the space X with coefficients in R.

Since the chain groups $C_n(X; R)$ are not finitely generated, it is in general not possible to calculate the homology groups $H_n(X; R)$ using the chain complex like we did in the case of simplicial homology. There are other methods for calculation of the singular homology, such as Mayer-Vietoris theorem, excision, etc. We show here one sample calculation which actually uses the chain complex:

Example 72. If $X = pt$ is a point, i.e. $X = \{x_0\}$, then for each $n \geq 0$, every continuous map $\Delta^n \to X$ is the constant map $c : \Delta^n \to \{x_0\}$ which sends every $t \in \Delta^n$ to x_0. Then for

every $n \geq 0$, the chain group $C_n(pt; R) \cong R$ generated by the constant map. Since $c \circ d^i$ is also the constant map, we have

$$\partial_n(c) = \sum_{i=0}^{n} (-1)^i c = \begin{cases} c & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd .} \end{cases}$$

So the chain complex $C_*(X; R)$ is of the form

$$\cdots \to R \xrightarrow{\mathrm{id}_R} R \xrightarrow{0} R \xrightarrow{\mathrm{id}_R} \cdots \xrightarrow{0} R \xrightarrow{\mathrm{id}_R} R \xrightarrow{0} R \to 0.$$

So, we conclude that

$$H_n(pt; R) = \begin{cases} R & \text{if } n = 0 \\ 0 & \text{if } n > 0. \end{cases}$$

Even though the singular homology is harder to calculate by using the singular chain complex, certain properties are easy to show.

Lemma 73. *Let $f : X \to Y$ be a continuous map between two topological spaces. Then there is an induced R-module homomorphism $H_n(f) : H_n(X; R) \to H_n(Y; R)$ between the corresponding singular homology groups.*

Proof. Consider the R-module homomorphism $f_n : C_n(X; R) \to C_n(Y; R)$ defined by $f_n(\sigma) = f \circ \sigma$ for every $\sigma : \Delta^n \to X$. It is easy to see that the R-module homomorphisms $\{f_n\}_{n \geq 0}$ commutes with the boundary maps ∂_n. Hence $\{f_n\}$ defines a chain map $f_* : C_*(X; R) \to C_*(Y; R)$. We define $H_n(f)$ to the R-module map induced by the chain map f_*. □

The continuous functions $f, g : X \to Y$ are **homotopic** if there is a continuous function $H : X \times [0, 1] \to Y$ such that $H(x, 0) = f(x)$ and $H(x, 1) = g(x)$ for all $x \in X$. Homotopic maps has the following property.

Theorem 74. *Let R be any commutative ring. If $f, g : X \to Y$ are homotopic, then for every $n \geq 0$, the induced R-module homomomorphisms $H_n(f), H_n(g) : H_n(X; R) \to H_n(Y; R)$ are equal.*

For further information about singular homology we refer the reader to one of the standard textbooks on algebraic topology.

3.4 Cochain Complexes and Cohomology

Definition 75. A cochain complex C^* of R-modules is a family $\{C^n\}_{n \in \mathbb{Z}}$ of R-modules together with maps $d^n : C^n \to C^{n+1}$ such that the composition

$$d^n d^{n-1} : C^{n-1} \xrightarrow{d^{d-1}} C^n \xrightarrow{d^n} C^{n+1}$$

is zero map. We define

$$Z^n(C^*) = \ker d^n \quad (n\text{-cocycles}),$$
$$B^n(C^*) = \operatorname{im} d^{n-1} \quad (n\text{-coboundaries}),$$

and the n-th cohomology module of C^* is defined by

$$H^n(C^*) := \frac{\ker d^n}{\operatorname{im} d^{n-1}}$$

Remark 76. A cochain complex can be considered as a chain complex and a chain complex can be considered as a cochain complex if we reindex the complexes as follows: For each $n \in \mathbb{Z}$, let $C^n = C_{-n}$ and $d^n = d_{-n}$. Then we have

$$\begin{array}{ccccccccccccc} \ldots & \longrightarrow & C_1 & \xrightarrow{d_1} & C_0 & \xrightarrow{d_0} & C_{-1} & \xrightarrow{d_{-1}} & C_{-2} & \longrightarrow & \ldots \\ & & \| & & \| & & \| & & \| & & \\ \ldots & \longrightarrow & C^{-1} & \xrightarrow{d^{-1}} & C^0 & \xrightarrow{d^0} & C^1 & \xrightarrow{d^1} & C^2 & \longrightarrow & \ldots \end{array}$$

Because of this the category of chain complexes and the category of cochain complexes are equivalent. Note that for each $n \in \mathbb{Z}$, $H_n(C_*) \cong H^{-n}(C^{-*})$.

Another way to obtain a cochain complex from a given chain complex C_* is to apply the Hom-functor $\mathrm{Hom}_R(-, M)$ to C_* for some R-module M. In this case we obtain a cochain complex $C^* = \mathrm{Hom}_R(C_*, M)$ of abelian groups. The cohomology of the complex C^* is related to the homology of C_*, however depending on the module M the relation between these two complexes can be complicated to explain. We can also apply the Hom-functor $\mathrm{Hom}_{\mathbb{Z}}(C_*; A)$ for some abelian group A and obtain a cochain complex of right R-modules. A third possibility is to start with a chain complex of abelian groups C_* and apply $\mathrm{Hom}_{\mathbb{Z}}(-, M)$ to C_* for some R-module M. In this case we again obtain a cochain complex of R-modules. We discuss all of these constructions below.

Example 77. Let C_* be a chain complex of R-modules and M be an R-module. Consider the cochain complex $C^* := \mathrm{Hom}_R(C_*, M)$ of abelian groups where for each $n \in \mathbb{Z}$,

$$d^n : \mathrm{Hom}_R(C_n, M) \to \mathrm{Hom}_R(C_{n+1}, M)$$

is defined by $d^n(f)(x) = (-1)^{n+1} f(d_{n+1}x)$ for every $f : C_n \to M$ and $x \in C_{n+1}$.

One special case of this situation is where $R = \mathbb{Z}$, M is an abelian group, and C_* is the simplicial or singular chain complex of a simplicial complex or a topological space X. Then the cohomology of the cochain complex $C^*(X; A) := \mathrm{Hom}_{\mathbb{Z}}(C_*(X), A)$ is called the cohomology of the space X with coefficients in A.

Example 78. Consider the Hom-functor in Example 77 with $R = \mathbb{Z}G$. Suppose that C_* is a positive chain complex of free $\mathbb{Z}G$-modules which has homology of a point. Given a $\mathbb{Z}G$-module, we can consider the cochain complex $C^*(G; M) := \mathrm{Hom}_{\mathbb{Z}G}(C_*, M)$. Cohomology groups of this cochain complex is called the cohomology of the group G with coefficients in M (see Section 4). These cohomology groups are the main objective of these notes.

Example 79. Let C_* be a chain complex of R-modules, and A be an abelian group. In this case

$$C^* = \mathrm{Hom}_{\mathbb{Z}}(C_*, A)$$

is a cochain complex of right R-modules. For $f \in \mathrm{Hom}_{\mathbb{Z}}(C_*, A)$, the R-module structure is defined by $(fr)(x) = f(rx)$ for every $r \in R$ and $x \in C_n$. One special case where we use this construction is when C_* is a chain complex of $\mathbb{Z}G$-modules and $A = \mathbb{Z}$. Then the cochain complex $C^* = \mathrm{Hom}_{\mathbb{Z}}(C_*; \mathbb{Z})$ is a cochain complex of right $\mathbb{Z}G$-modules. By using the G-action via $gf = fg^{-1}$ we can consider this cochain complex as the cochain complex of

(left) $\mathbb{Z}G$-modules. When C_* is a chain complex of free abelian groups, and for each $n \in \mathbb{Z}$, the homology group $H_n(C_*)$ is a free abelian group, then for every $n \in \mathbb{Z}$, we have

$$H^n(\mathrm{Hom}_{\mathbb{Z}}(C_*, \mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(H_n(C_*), \mathbb{Z})$$

as $\mathbb{Z}G$-modules.

Example 80. Let C_* be a chain complex of $\mathbb{Z}$-modules and M be an R-module. Then the cochain complex $C^* = \mathrm{Hom}_{\mathbb{Z}}(C_*; M)$ is complex of R-modules where the R-module structure is given by $(rf)(x) = rf(x)$ for $r \in R$, $x \in C_n$ and $f : C_* \to M$. One of ways we use this construction is when C_* is a chain complex of free abelian groups and $M = \mathbb{F}_p$ is a field with p-elements. then in this case there is an isomorphism

$$H^n(\mathrm{Hom}_{\mathbb{Z}}(C_*, \mathbb{F}_p)) \cong \mathrm{Hom}_{\mathbb{Z}}(H_n(C_*), \mathbb{F}_p)$$

if and only if $H_n(C_*)$ has no p-torsion elements, i.e. elements $u \in H_n(C_*)$ such that $pu = 0$.

If C_* is a chain complex of abelian groups and A is any abelian group, then the homology groups of the cochain complex $C^* = \mathrm{Hom}_{\mathbb{Z}}(C_*, A)$ can be computed using the homology of the chain complex C_* using the Hom-functor and the Ext-groups. This relationship is explained by the universal coefficient theorem.

Theorem 81. *Let C_* be a chain complex of free abelain groups and A be any abelian group. Then there is a split exact sequence of abelian groups*

$$0 \to \mathrm{Ext}_{\mathbb{Z}}(H_{n-1}(C_*), A) \to H^n(\mathrm{Hom}_{\mathbb{Z}}(C_*, A)) \to \mathrm{Hom}_{\mathbb{Z}}(H_n(C_*), A) \to 0.$$

Here the ext-groups denote the first derived functors of the hom-functor. The definition of ext-groups will be given in the second part of the lecture notes.

In algebraic topology, to each topological space (or simplicial complex or simplicial set) X, we associate a chain complex $C_*(X)$ of free abelian groups (in the case of simplicial complexes, the basis of $C_n(X)$ is given by the n-simplices in X). The homology of the chain complex $C_*(X)$ is called the homology of the space X, denoted by $H_*(X)$. For an abelian group A, the cochain complex $\mathrm{Hom}_{\mathbb{Z}}(C_*(X), A)$ is usually denoted by $C^*(X; A)$ and its cohomology is called the cohomology of the space X with coefficient in A, denoted by $H^*(X; A)$. The relation between $H^*(X; A)$ and $H_*(X)$ has been an important question for algebraic topology and lead the development of homological algebra as we know today. By universal coefficient theorem we conclude that there is an exact sequence of abelian groups

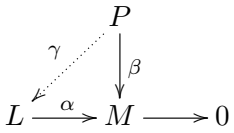
$$0 \to \mathrm{Ext}_{\mathbb{Z}}(H_{n-1}(X), A) \to H^n(X; A) \to \mathrm{Hom}_{\mathbb{Z}}(H_n(X), A) \to 0.$$

Exercise 82. Show that in Example 79 if we take $A = \mathbb{Q}$ the rational numbers, then for any chain complex C_* of abelian groups, there is an isomorphism of abelian groups $H^n(\mathrm{Hom}_{\mathbb{Z}}(C_*, \mathbb{Q})) \cong \mathrm{Hom}_{\mathbb{Z}}(H_n(C_*), \mathbb{Q})$.

4 Algebraic Definition of Group Cohomology

4.1 Projective Resolutions

Definition 83. An R-module P is **projective** if for every commuting diagram



where the row sequence is exact (α is surjective), there exists an R-linear map $\gamma : P \to L$ such that $\alpha\gamma = \beta$.

Lemma 84. *Every free R-module is projective.*

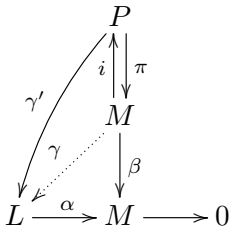
Proof. Let F be a free module with basis $\mathcal{B}$. Consider the above diagram with P replaced with F. For each $b \in \mathcal{B}$ choose an element $l_b \in L$ such that $\alpha(l_b) = \beta(b)$. Define $\gamma : F \to L$ to be the R-linear map such that

$$\gamma(\sum_{b\in\mathcal{B}} r_b b) = \sum_{b\in\mathcal{B}} r_b l_b.$$

Since F is free this is a well-defined map. It is clear that γ is R-linear and $\alpha\gamma = \beta$. □

Lemma 85. *A summand of a projective module is also projective.*

Proof. Let P be a projective R-module and $P \cong M \oplus N$. Let $\pi : P \to M$ and $i : M \to P$ denote the projection and inclusion maps for the summand M. Consider the diagram:



Since P is projective, there is a $\gamma' : P \to L$ that satisfies $\alpha\gamma' = \beta\pi$. Let $\gamma = \gamma' i$. Then we have

$$\alpha\gamma = \alpha\gamma' i = \beta\pi i = \beta.$$

So M is projective. □

For projective modules the following equivalent conditions hold.

Lemma 86. *Let P be an R-module. Then the following are equivalent:*

1. *P is projective.*
2. *P is a direct summand of a free module.*

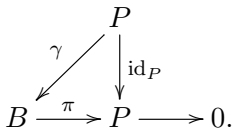
3. *Every exact sequence of the form*

$$0 \to A \xrightarrow{j} B \xrightarrow{\pi} P \to 0$$

splits.

4. *If $\alpha : L \to M$ is a surjective R-linear map, then the induced map $\alpha_* : \mathrm{Hom}_R(P, L) \to \mathrm{Hom}_R(P, M)$ is also surjective.*

Proof. It is clear from the definitions that (1) and (4) are equivalent.
(1) $\Rightarrow$ (3) Assume P is projective. Then there is a γ such that the following diagram commutes:



The R-linear map γ gives a splitting for the short exact sequence in (3).
(3) $\Rightarrow$ (2) By Theorem 34, there is a surjective R-linear map $\varphi : F \to P$ where F is free R-module. By (3), the short exact sequence $0 \to \ker(\varphi) \to F \to P \to 0$ splits giving that P is a direct summand of F.
(2) $\Rightarrow$ (1) Since every free module is projective, this follows from Lemma 85. □

Definition 87. A **projective resolution** of an R-module M is a non-negative complex P_* of projective R-modules together with a homomorphism $\varepsilon : P_0 \to M$ such that

$$\cdots \to P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

is exact.

Lemma 88. *For every R-module M, there is a projective resolution $P_* \xrightarrow{\varepsilon} M$.*

Proof. By Theorem 34, for every R-module M there is surjective R-linear map $\varepsilon : F \to M$ where F is a free R-module. Since free modules are projective we can take P_0 as F. Then we have a short exact sequence of R-modules

$$0 \to \ker \varepsilon \xrightarrow{j} P_0 \xrightarrow{\varepsilon} M \to 0.$$

Now applying the same argument to $\ker \varepsilon$, we can find a surjective R-linear map $\varphi_1 : P_1 \to \ker \varepsilon$ with P_1 projective. This gives an exact sequence of R-modules

$$0 \to \ker \partial_1 \to P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} M \to 0$$

where $\partial_1 = j\varphi_1$. Continuing this way, we obtain a projective resolution for M. □

Example 89. Let $G = \langle g \,|\, g^2 = 1 \rangle$ be the cyclic group of order 2 and k be any field with characteristic 2. We can consider k as the trivial kG-module with the G-action given by $g \cdot 1 = 1$. If we follow the construction given above, we obtain a projective resolution for k as a kG-module of the following form:

$$(P_*, \varepsilon) : \ldots \longrightarrow kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{\varepsilon} k \longrightarrow 0$$

where for all $n \geq 0$, $P_n = kG$, and for $n \geq 1$, the boundary maps $\partial_n : P_n \to P_0$ are given by the multiplication with $1 + g$ in kG. The map $\varepsilon : kG \to k$ is the augmentation map defined by $\varepsilon(a + bg) = a + b$. By construction this chain complex is exact, so it is a projective (free) resolution of k as a kG-module.

Exercise 90. Show that if G is the cyclic group of order 2, there is a projective resolution of the trivial module $\mathbb{Z}$ as a $\mathbb{Z}G$-module of the following form:

$$(P_*, \varepsilon) : \ldots \longrightarrow \mathbb{Z}G \xrightarrow{1+g} \mathbb{Z}G \xrightarrow{1-g} \mathbb{Z}G \xrightarrow{1+g} \mathbb{Z}G \xrightarrow{1-g} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

Example 91. In some cases it is possible to find a projective resolution P_* for an $\mathbb{Z}G$-module M such that P_* bounded. As an example consider the group of integers $\mathbb{Z}$ with the addition operation. Using the multiplicative notation we can write $G = \langle t \rangle$. Then the group ring $\mathbb{Z}G$ is isomorphic to $\mathbb{Z}[t, t^{-1}]$. We can write a two step projective resolution

$$(P_*, \varepsilon) : 0 \longrightarrow \mathbb{Z}G \xrightarrow{1-t} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where $P_1 = P_0 = \mathbb{Z}G$, the boundary map $\partial_1 : P_1 \to P_0$ is defined by the multiplication with $1 - t$, and the morphism ε is the augmentation map that takes t to 1.

For a given R-module M, there are many different projective resolutions for M, however as we show below they are all chain homotopy equivalent to each other. To see this we first prove the following:

Proposition 92. *Let $P_* \xrightarrow{\varepsilon} M$ be a projective resolution of the R-module M and*

$$\cdots \to B_2 \xrightarrow{\partial'_2} B_1 \xrightarrow{\partial'_1} B_0 \xrightarrow{\varepsilon'} N \to 0$$

be an exact sequence of R-modules. For every R-linear map $f : M \to N$ there exists a chain map $\mu_* : P_* \to B_*$ such that the diagram

$$\begin{array}{ccc} P_0 & \xrightarrow{\varepsilon} & M \\ \downarrow{\scriptstyle \mu_0} & & \downarrow{\scriptstyle f} \\ B_0 & \xrightarrow{\varepsilon'} & N \end{array}$$

commutes. Moreover if μ_* and η_* are two such chain maps then they are chain homotopic.

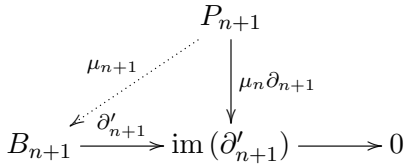
Proof. Since $B_0 \xrightarrow{\partial'} N$ is surjective and P_0 is projective, there is a R-linear map $\mu_0 : P_0 \to B_0$ such that $\varepsilon' \mu_0 = f\varepsilon$. By induction assume that we have constructed $\mu_i : P_i \to B_i$ for $i = 0, \ldots, n$. Consider the diagram:

$$\begin{array}{ccccccc} P_{n+1} & \xrightarrow{\partial_{n+1}} & P_n & \xrightarrow{\partial_n} & P_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \mu_n} & & \downarrow{\scriptstyle \mu_{n-1}} & & \\ B_{n+1} & \xrightarrow{\partial'_{n+1}} & B_n & \xrightarrow{\partial'_n} & B_{n-1} & \longrightarrow & \cdots \end{array}$$

If $n = 0$, in the above diagram assume $P_{-1} = M$, $B_{-1} = N$, $\partial_n = \varepsilon$, $\partial' = \varepsilon'$ and $\mu_{-1} = f$. Since $\partial'_n \mu_n \partial_{n+1} = \mu_{n-1}\partial_n\partial_{n+1} = 0$, we have

$$\operatorname{im}(\mu_n\partial_{n+1}) \subseteq \ker(\partial'_n) = \operatorname{im}(\partial'_{n+1}).$$

This gives a diagram of the form

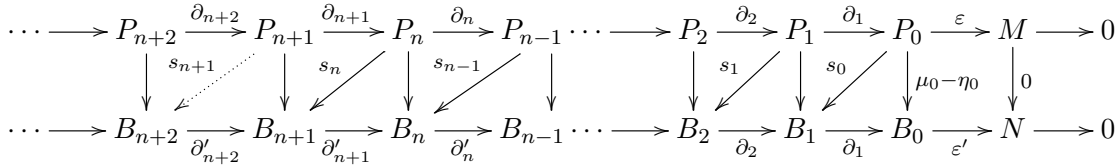


We define μ_{n+1} to be the R-linear map that makes this diagram commutes. So, by induction for all $n \geq 0$, the map $\mu_n : P_n \to B_n$ with the desired properties is constructed.

Let μ_* and η_* are two chain maps satisfying the given conditions. Then $\varepsilon'(\mu_0 - \eta_0) = 0$. This gives that $\operatorname{im}(\mu_0 - \eta_0) \subseteq \ker \varepsilon' = \operatorname{im} \partial'_1$. Since P_0 is projective there exists an R-linear map $s_0 : P_0 \to B_1$ such that $\partial'_1 s_0 = \mu_0 - \eta_0$. Now suppose that for $i = 0, \ldots, n$, we constructed $s_n : P_n \to B_{n+1}$ such that the equality

$$\mu_n - \eta_n = \partial'_{n+1}s_n + s_{n-1}\partial_n$$

holds. For this to make sense at $n = 0$, we take $P_{-1} = M$, $B_{-1} = N$, and $s_{-1} = 0$. We can view this as a commuting diagram:



where the vertical arrows are $\mu_n - \eta_n : P_n \to B_n$ for all $n \geq 0$. Let $k_{n+1} = \mu_{n+1} - \eta_{n+1} - s_n\partial_{n+1}$. Then

$$\begin{aligned}
\partial'_{n+1}k_{n+1} &= \partial'_{n+1}(\mu_{n+1} - \eta_{n+1}) - \partial'_{n+1}s_n\partial_{n+1} \\
&= (\mu_n - \eta_n)\partial_{n+1} - \partial'_{n+1}s_n\partial_{n+1} \\
&= (\mu_n - \eta_n - \partial'_{n+1}s_n)\partial_{n+1} = s_{n-1}\partial_n\partial_{n+1} = 0.
\end{aligned}$$

Hence $\operatorname{im}(k_{n+1}) \subseteq \ker \partial'_{n+1} = \operatorname{im}(\partial'_{n+2})$. Since P_{n+1} is projective, this gives that there is an R-linear map $s_{n+1} : P_{n+1} \to B_{n+2}$ such that $\partial'_{n+2}s_{n+1} = k_{n+2}$. Thus s_{n+2} satisfies the equation

$$\mu_{n+1} - \eta_{n+1} = \partial'_{n+2}s_{n+1} + s_n\partial_{n+1}.$$

This completes the inductive step. Hence we can conclude that μ_* and η_* are chain homotopic. □

Corollary 93. *Let $P_* \xrightarrow{\varepsilon} M$ and $Q_* \xrightarrow{\varepsilon'} M$ be two projective resolutions of an R-module M. Then there is a chain map $\mu_* : P_* \to Q_*$ that lifts the identity map on M. Moreover any two such chain maps are chain homotopic.*

Proof. Since $P_* \xrightarrow{\varepsilon} M$ is a projective resolution and the chain complex

$$\cdots \longrightarrow Q_2 \longrightarrow Q_1 \longrightarrow Q_0 \xrightarrow{\varepsilon'} M \longrightarrow 0$$

is exact, the corollary follows from Proposition 92. □

From these we can conclude:

Theorem 94. *Let $P_* \xrightarrow{\varepsilon} M$ and $Q_* \xrightarrow{\varepsilon'} M$ be two projective resolutions of an R-module M. Then the chain complexes P_* and Q_* are chain homotopy equivalent.*

Proof. By Corollary 93, there are chain maps $f_* : P_* \to Q_*$ and $g_* : Q_* \to P_*$ lifting the identity map on M. Then the compositions

$$g_* f_* : P_* \to P_* \qquad f_* g_* : Q_* \to Q_*$$

also lift the identity maps. But then they are chain homotopic to the identity chain maps on P_* and Q_*. This gives that f_* is a chain homotopy equivalence. □

In Section 4.3.3, we give examples of chain homotopy between projective resolutions after we discuss the standard resolution.

4.2 Definition of Group Cohomology via Projective Resolutions

Let G be a discrete group and k be a commutative ring. As before we denote by kG the group ring of G over k.

Definition 95. Let

$$(P_*, \varepsilon) : \qquad \cdots \longrightarrow P_{n+1} \xrightarrow{\partial_{n+1}} P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\varepsilon} k \longrightarrow 0$$

be a projective kG-resolution of the trivial module k. Let M be a kG-module. Applying the Hom-functor $\mathrm{Hom}_{kG}(-, M)$ to (P_*, ε), we obtain a cochain complex

$$0 \to \mathrm{Hom}_{kG}(P_0, M) \xrightarrow{\delta^0} \mathrm{Hom}_{kG}(P_1, M) \xrightarrow{\delta^1} \cdots \to \mathrm{Hom}_{kG}(P_n, M) \xrightarrow{\delta^n} \mathrm{Hom}_{kG}(P_{n+1}, M) \to \cdots$$

where $\delta^n(f)(x) = (-1)^{n+1} f(\partial_{n+1} x)$ for all $f \in \mathrm{Hom}_{kG}(P_n, M)$ and all $x \in P_{n+1}$.

The **n-th cohomology group** $H^n(G; M)$ of the group G with coefficients in M is defined to be the cohomology of the cochain complex $\mathrm{Hom}_{kG}(P_*, M)$, i.e.. $H^0(G; M) = \ker \delta^0$ and for all $n \geq 1$,

$$H^n(G; M) := \frac{\ker \delta^n}{\mathrm{im}\, \delta^{n-1}}.$$

Example 96. Let $G = \langle g \,|\, g^2 = 1 \rangle$ be the cyclic group of order 2, and let k be any field with characteristic 2. Consider the projective resolution of k as a kG-module given in Example 89:

$$(P_*, \varepsilon) : \ldots \longrightarrow kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{\varepsilon} k \longrightarrow 0$$

Applying the Hom-functor $\mathrm{Hom}_{kG}(-;k)$, we obtain a cochain complex of the form

$$0 \longrightarrow \mathrm{Hom}_{kG}(kG,k) \xrightarrow{\delta^0} \mathrm{Hom}_{kG}(kG,k) \xrightarrow{\delta^1} \mathrm{Hom}_{kG}(kG,k) \xrightarrow{\delta^2} \cdots$$

where the coboundary maps δ^i are induced by the map $kG \xrightarrow{1+g} kG$. there is an isomorphism $\mathrm{Hom}_{kG}(kG,k) \cong k$, and the coboundary maps $k \xrightarrow{\delta^i} k$ are equal to the zero map (note that k has characteristic 2). Hence the cochain complex $\mathrm{Hom}_{kG}(P_*,k)$ is of the form

$$0 \longrightarrow k \xrightarrow{0} k \xrightarrow{0} k \xrightarrow{0} \cdots \longrightarrow k \xrightarrow{0} k \longrightarrow \cdots.$$

From this we conclude that for every $n \geq 0$, we have $H^n(G;k) \cong k$ as k-vector spaces.

Example 97. Let $G = \langle t \rangle \cong \mathbb{Z}$ denote the group of integers (written multiplicatively). In Example 91 we showed that there is a two step projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module

$$(P_*, \varepsilon) : 0 \longrightarrow \mathbb{Z}G \xrightarrow{1-t} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where ε is the augmentation map that takes t to 1. Applying Hom-functor to this resolution we obtain a cochain complex

$$0 \longrightarrow \mathbb{Z} \xrightarrow{0} \mathbb{Z} \longrightarrow 0$$

where $C^0 \cong C^1 \cong \mathbb{Z}$ and $\delta^0 = 0$. This shows that $H^n(G;\mathbb{Z}) \cong \mathbb{Z}$ for $n = 0, 1$ and $H^n(G;\mathbb{Z}) = 0$ for $n \neq 0, 1$.

If M is a $\mathbb{Z}G$-module, then the cochain complex $C^* = \mathrm{Hom}_{\mathbb{Z}G}(P_*, M)$ is of the form

$$0 \longrightarrow M \xrightarrow{1-t} M \longrightarrow 0$$

and the cohomology of G with coefficients in M can be calculated as

$$H^n(G;M) \cong \begin{cases} \ker\{M \xrightarrow{1-t} M\} & \text{if } n = 0 \\ \mathrm{coker}\,\{M \xrightarrow{1-t} M\} & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Note that here we took advantage of the fact that $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, M)$ has a (left) $\mathbb{Z}G$-module structure coming from the right G-action on $\mathbb{Z}G$. We use this action to explain the coboundary maps in a convenient way.

4.2.1 Independence from the projective resolution

The definition of the group cohomology given in Definition 95 uses projective resolutions. For this definition to make sense we need to show that the cohomology of the Hom-complex $\mathrm{Hom}_{kG}(P_*, M)$ is independent of the chosen resolution.

Theorem 98. *Let G be a group and k be a commutative ring. Suppose that (P_*, ε) and (Q_*, ε') are two projective kG-resolutions of k. Then for any kG-module M, the cohomology of the cochain complexes $\mathrm{Hom}_{kG}(P_*, M)$ and $\mathrm{Hom}_{kG}(Q_*, M)$ are isomorphic. Hence the cohomology $H^n(G;M)$ does not depend on the choice of the projective resolution of k.*

Proof. Let (P_*, ε) and (Q_*, ε') be two projective kG-resolutions of k. Then by Theorem 94, there are chain maps $f_* : P_* \to Q_*$ and $g_* : Q_* \to P_*$ such that

$$g_* f_* \simeq_{s_*} \mathrm{id}_{P_*} \quad \text{and} \quad f_* g_* \simeq_{t_*} \mathrm{id}_{Q_*}$$

where $s_* : P_* \to P_{*+1}$ and $t_* : Q_* \to Q_{*+1}$ are the corresponding chain homotopies. Applying the Hom-functor $\mathrm{Hom}_{kG}(-, M)$ to these chain maps, we obtain chain maps

$$\overline{f}_* : \mathrm{Hom}_{kG}(Q_*, M) \to \mathrm{Hom}_{kG}(P_*, M)$$

and

$$\overline{g}_* : \mathrm{Hom}_{kG}(P_*, M) \to \mathrm{Hom}_{kG}(Q_*, M)$$

and chain homotopies

$$\overline{s}_* : \mathrm{Hom}_{kG}(P_*, M) \to \mathrm{Hom}_{kG}(P_{*-1}, M) \text{ and } \overline{t}_* : \mathrm{Hom}_{kG}(Q_*, M) \to \mathrm{Hom}_{kG}(Q_{*-1}, M)$$

Note that the equalities for chain homotopy will still hold, so we have chain homotopies

$$\overline{f}_* \overline{g}_* \simeq_{\overline{s}_*} \mathrm{id}_{\mathrm{Hom}_{kG}(P_*, M)} \quad \text{and} \quad g_* f_* \simeq_{\overline{t}_*} \mathrm{id}_{\mathrm{Hom}_{kG}(Q_*, M)}.$$

This shows that the cochain complexes $\mathrm{Hom}_{kG}(P_*, M)$ and $\mathrm{Hom}_{kG}(Q_*, M)$ are chain homotopy equivalent, hence they have isomorphic cohomology groups. □

4.3 The Standard Resolution and the Bar Complex

4.3.1 The Standard Resolution

We defined the group cohomology $H^n(G; M)$ to be the cohomology of the cochain complex $\mathrm{Hom}_{kG}(P_*, M)$ for some projective kG-resolution P_* of k. Even though we showed that the projective resolutions always exist, it is useful to have a standard one where all projective modules P_n can be described in terms of G without any dependency to the structure of the group G. For this purpose, a free resolution, called standard resolution, is introduced.

Definition 99. Let G be a group and k be a commutative ring. Consider the chain complex

$$(F_*, \varepsilon) : \cdots \xrightarrow{\partial_4} kG^{\otimes 4} \xrightarrow{\partial_3} kG^{\otimes 3} \xrightarrow{\partial_2} kG \otimes kG \xrightarrow{\partial_1} kG \xrightarrow{\varepsilon} k \longrightarrow 0$$

where $F_n = kG^{\otimes(n+1)}$ for all $n \geq 0$ and the boundary maps $\partial_n : F_n \to F_{n-1}$ are the kG-module homomorphisms defined by

$$\partial_n(g_0 \otimes \cdots \otimes g_n) = \sum_{i=0}^{n} (-1)^i (g_0 \otimes \cdots \otimes \widehat{g}_i \otimes \cdots \otimes g_n).$$

Here the notation $\widehat{g}_i$ means the i-th term g_i is removed from the tensor product. The map $\varepsilon : kG \to k$ is the augmentation map that takes $\sum_{g \in G} a_g g$ to $\sum_{g \in G} a_g$ in k.

Lemma 100. *The chain complex (F_*, ε) defined in Definition 99 is a free resolution of k as a kG-module.*

Proof. The G-action on $F_n = kG^{\otimes(n+1)}$ given by the diagonal action

$$g(g_0 \otimes \cdots \otimes g_n) = gg_0 \otimes \cdots \otimes gg_n.$$

Hence for each $n \geq 0$, $F_n = kG^{\otimes(n+1)}$ is a free kG-module and the boundary maps ∂_n are kG-module homomorphisms.

Let $\widetilde{F}_*$ denote the complex obtained form F_* by adding $\widetilde{F}_{-1} = k$ and $\partial_0 : F_0 \xrightarrow{\varepsilon} F_{-1} = k$ to the complex F_*. To prove that the chain complex (F_*, ε) is a resolution of k, we need to show that the augmented complex $\widetilde{F}_*$ is acyclic. For this we show that there is contracting homotopy $s_* : \widetilde{F}_* \to \widetilde{F}_{*+1}$. for $\widetilde{F}_*$. Note that s_* will defined as a k-linear map, since in general there is no contraction for $\widetilde{F}_*$ as a chain complex of kG-modules.

Let $s_{-1} : k \to kG$ be the k-linear map which sends $\lambda \in k$ to $\lambda \cdot 1 \in kG$. For every $n \geq 0$, we define $s_n : F_n \to F_{n+1}$ to be the k-linear map such that

$$s_n(g_0 \otimes \cdots \otimes g_n) = 1 \otimes g_0 \otimes \cdots \otimes g_n$$

for every $g_0, \ldots, g_n \in G$. For $n = 0$, and for any $g_0 \in G$, we have

$$(\partial_1 s_0 + s_{-1}\partial_0)(g_0) = \partial_1(1 \otimes g_0) + s_{-1}(1) = g_0 - 1 + 1 = g_0.$$

Hence, the equality $\partial_{n+1}s_n + s_{n-1}\partial_n = \mathrm{id}_{F_*}$ holds in this case. For $n \geq 1$, we have

$$\begin{aligned}
&(\partial_{n+1}s_n + s_{n-1}\partial_n)(g_0 \otimes \cdots \otimes g_n) \\
&= \partial_{n+1}(1 \otimes g_0 \otimes \cdots \otimes g_n) + s_{n-1}(\sum_{i=0}^{n}(-1)^i(g_0 \otimes \cdots \otimes \widehat{g}_i \otimes \cdots \otimes g_n) \\
&= (g_0 \otimes \cdots \otimes g_n) + \sum_{i=0}^{n}(-1)^{i+1}(1 \otimes g_0 \otimes \cdots \otimes \widehat{g}_i \otimes \cdots \otimes g_n) \\
&+ \sum_{i=0}^{n}(-1)^i(1 \otimes g_0 \otimes \cdots \otimes \widehat{g}_i \otimes \cdots \otimes g_n) = g_0 \otimes \cdots \otimes g_n
\end{aligned}$$

This shows that s_* is a contracting homotopy for $\widetilde{F}_*$, hence it is acyclic. We conclude that (F_*, ε) is a free kG-resolution for k. □

4.3.2 The Bar Notation

Using the standard resolution one can give a more explicit cochain complex for calculating the group cohomology. For this, first note that for $n \geq 0$, $F_n = kG^{(n+1)}$ is a k-vector space with basis given by $G^{(n+1)} = G \times \cdots \times G$ ($(n+1)$-fold product). We write the basis elements as $(n+1)$-tuples $(g_0, \ldots, g_n)$. Using this basis we can express the boundary maps by

$$\partial_n(g_0, \ldots, g_n) = \sum_{i=0}^{n}(-1)^i(g_0, \ldots, \widehat{g}_i, \ldots, g_n).$$

Note that G acts on the the basis $G^{(n+1)}$ for F_n by $g(g_0, \ldots, g_n) = (gg_0, \ldots, gg_n)$ and this action is free. Note that since $(g_0, \ldots, g_n) = g_0(1, g_0^{-1}g_1, \ldots, g_0^{-1}g_n)$ the set of all tuples with the first coordinate equal to 1 forms a basis for F_n as a free kG-module. We go further and define **bar notation** for these basis elements.

Definition 101. For every $g_1, \ldots, g_n \in G$, let $[g_1|g_2|\ldots|g_n]$ denote the $(n+1)$-tuple

$$(1, g_1, g_1g_2, g_1g_2g_3, \ldots, g_1 \cdots g_n)$$

in $G^{(n+1)}$.

Note that every $(n+1)$-tuple $(g_0, g_1, \ldots, g_n)$ can be written as $g_0[g_0^{-1}g_1|g_1^{-1}g_2|\ldots|g_{n-1}^{-1}g_n]$ using the bar notation. The motivation for introducing the bar notation becomes more clear later when we discuss group extensions and factor sets. Using the bar notation for each $n \geq 1$, we can take the basis for the free kG-module F_n as the set

$$\mathcal{B}_n = \{[g_1|\ldots|g_n] \,|\, g_1, \ldots, g_n \in G\}.$$

For $n = 0$, we take $\mathcal{B}_0 = \{[\,]\}$. With respect to this basis the formulas for boundary maps changes.

$$\begin{aligned}
\partial_1([g_1]) &= \partial_1((1, g_1)) = (g_1) - (1) = g_1[\,] - [\,] \\
\partial_2([g_1|g_2]) &= \partial_2((1, g_1, g_1g_2)) = (g_1, g_1g_2) - (1, g_1g_2) + (1, g_1) \\
&= g_1[g_2] - [g_1g_2] + [g_1] \\
\partial_3([g_1|g_2|g_3]) &= \partial_3((1, g_1, g_1g_2, g_1g_2g_3)) \\
&= (g_1, g_1g_2, g_1g_2g_3) - (1, g_1g_2, g_1g_2g_3) + (1, g_1, g_1g_2g_3) - (1, g_1, g_1g_2) \\
&= g_1[g_2|g_3] - [g_1g_2|g_3] + [g_1|g_2g_3] - [g_1|g_2]
\end{aligned}$$

Lemma 102. *Using the bar notation, for $n \geq 1$, for the boundary maps $\partial_n : F_n \to F_{n-1}$ we have the following formula:*

$$\partial_n([g_1|\ldots|g_n]) = g_1[g_2|\ldots|g_n] + \sum_{i=1}^{n-1}(-1)^i[g_1|\ldots|g_ig_{i+1}|\ldots|g_n] + (-1)^n[g_1|\ldots|g_{n-1}].$$

Proof. For every $g_1, \ldots, g_n \in G$, we have

$$\begin{aligned}
\partial_n([g_1|\ldots|g_n]) &= \partial_n((1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n)) \\
&= (g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n) \\
&\quad + \sum_{i=1}^{n-1}(-1)^i(1, g_1, g_1g_2, \ldots, g_1 \cdots g_{i-1}, g_1 \cdots g_{i+1}, \ldots, g_1 \cdots g_n) \\
&\quad + (-1)^n(1, g_1, \ldots, g_1 \cdots g_{n-1}) \\
&= g_1[g_2|\ldots|g_n] + \sum_{i=1}^{n-1}(-1)^i[g_1|\ldots|g_ig_{i+1}|\ldots|g_n] + (-1)^n[g_1|\ldots|g_{n-1}].
\end{aligned}$$

□

Remark 103. The bar notation defines a change of basis for the k-vector space $F_n = kG^{(n+1)}$ induced by a bijection $\psi : G^{n+1} \to G \times G^n$ that sends $(g_0, \ldots, g_n)$ to $(g_0, (g_0^{-1}g_1, \ldots, g_{n-1}^{-1}g_n))$. The inverse of ψ is the function that sends $(g_0, (g_1, \ldots, g_n))$ to $(g_0, g_0g_1, \ldots, g_0 \cdots g_n)$. Note

that the function ψ is a G-equivariant function if we take the G-action on G^{n+1} to be the diagonal action and on $G \times G^n$ to be the action defined by multiplication on the first coordinate, This follows from the following calculation:

$$\begin{aligned}\psi(g(g_0, g_1, \ldots, g_n)) &= \psi((gg_0, gg_1, \ldots, gg_n)) = (gg_0, (g_0^{-1}g_1, \ldots, g_{n-1}^{-1}g_n)) \\ &= g\psi(g_0, g_1, \ldots, g_n).\end{aligned}$$

Using the bar notation, we can give a definition of group cohomology as cohomology an explicitly defined cochain complex for any kG-module.

Definition 104. Let G be a group and k a commutative ring. For every kG-module M, the **bar complex** $C^*(G; M)$ is defined as the cochain complex such that for all $n \geq 0$, $C^0(G; M) \cong M$ and $C^n(G; M) = \{f : G^n \to M\}$ with coboundary maps $\delta^n : C^n(G; M) \to C^{n+1}(G; M)$ defined by $(\delta^0 m)(g) = gm - m$ and for all $n \geq 1$

$$\begin{aligned}(\delta^n f)(g_1, \ldots, g_{n+1}) = g_1 f(g_2, \ldots, g_n) &- \sum_{i=2}^{n-1} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n).\end{aligned}$$

Proposition 105. *Let G be a group and k a commutative ring. For every kG-module M, and for all $n \geq 0$, we have*

$$H^n(G; M) \cong H^n(C^*(G; M)) = \frac{\ker \delta^n : C^n(G; M) \to C^{n+1}(G; M)}{\operatorname{im} \delta^{n-1} : C^{n-1}(G : M) \to C^n(G; M)}.$$

Proof. Let (F_*, ε) denote the standard resolution. We will show that the cochain complex $\mathrm{Hom}_{kG}(F_*, M)$ is isomorphic to the bar complex $C^*(G; M)$ as cochain complexes of k-vector spaces. The isomorphism is given by the chain map

$$\tau_* : \mathrm{Hom}_{kG}(F_*, M) \to C^*(G; M)$$

defined as follows: For each $n \geq 0$, let τ_n be the k-linear map that sends a kG-module homomorphism $\varphi : F_n \to M$ to $f : G^n \to M$ where

$$f(g_1, \ldots, g_n) = \varphi(1 \otimes g_1 \otimes g_1 g_2 \otimes \cdots \otimes g_1 \ldots g_n).$$

The inverse of the τ_n is the k-linear map that sends $f : G^n \to M$ to the kG-homomorphism defined by

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

A calculation similar to the one performed in the proof of Lemma 102 shows that the map τ_* and its inverse are chain maps giving the desired chain isomorphism. □

Proposition 105 gives us a quick way to calculate the low dimensional group cohomology.

Example 106. For any kG-module M, $C^0(G; M) = M$ and $C^1(G; M) = \{f : G \to M\}$. For every $m \in M$ and $g \in G$, we have $\delta^0(m)(g) = gm - m$. Then

$$H^0(G; M) = \ker \delta^0 = M^G$$

where $M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}$ denotes the submodule of invariant elements in M.

Example 107. Let M be a kG-module. For every $f \in C^1(G;M)$ and $g_1, g_2 \in G$,

$$\delta^1(f)(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_2).$$

The kernel of δ^1 is the set of all functions $f : G \to M$ such that for every $g_1, g_2 \in G$,

$$f(g_1 g_2) = g_1 f(g_2) + f(g_1).$$

A function $f : G \to M$ satisfying this equation for every $g_1, g_2 \in G$ is called a **derivation**. A function $f : G \to M$ is an **inner derivation** if there is an $m \in M$ such that for every $g \in G$, $f(g) = gm - m$. Note that this is equivalent to saying $f = \delta^0(m)$. We denote the set of all derivations $f : G \to M$ by $\mathrm{Der}(G;M)$ and the subgroup of inner derivations by $\mathrm{IDer}(G;M)$. By the definition of group cohomology, we have

$$H^1(G;M) \cong \frac{\mathrm{Der}(G;M)}{\mathrm{IDer}(G;M)}.$$

If $M = A$ is a trivial kG-module (a k-module A with $ga = a$ for all $g \in G$ and $a \in A$), then

$$H^1(G;A) \cong \mathrm{Hom}_{Group}(G, A)$$

where $\mathrm{Hom}_{Group}(G, A)$ denotes the group of all group homomorphisms $f : G \to A$. In particular when G is a finite group and $A = \mathbb{Z}$, then $H^1(G;\mathbb{Z}) = 0$.

4.3.3 The normalized cochain complex

For group cohomology calculations it is possible to work with a small resolution than the bar complex using the normalized standard resolution. Let (F_*, ε) be the standard resolution. Consider the subcomplex D_* of F_* where for each $n \geq 0$, $D_n \subseteq F_n = kG^{\otimes(n+1)}$ the subspace generated by elements of the form $(g_0, \ldots, g_n)$ where for some $i \geq 0$, $g_i = g_{i+1}$. From the formula for boundary maps $\partial_n : F_n \to F_{n-1}$, it is easy to see that D_* is chain complex with boundary maps induced from F_*. Also note that D_* is a subcomplex as a chain complex of kG-modules. In terms of the bar notation D_* is the free kG-subcomplex of F_* generated by the basis elements $[g_1|\ldots|g_n]$ where $g_i = 1$ for some $i \geq 1$.

Definition 108. Let D_* be the kG-subcomplex of the standard resolution F_*. The **normalized standard resolution** $\overline{F}_*$ is defined to the quotient complex F_*/D_*.

Applying the Hom-functor to the normalized standard resolution $\overline{F}_*$ gives a normalized bar complex $\overline{C} * (G;M)$ where

$$\overline{C}^n(G;M) = \{f : G^n \to M \mid f(g_1, \ldots, g_n) = 0 \text{ if } g_i = 1 \text{ for some } i\}.$$

We have following observation:

Proposition 109. *For every kG-module M, the group cohomology $H^*(G;M)$ is isomorphic to the cohomology of the normalized bar complex $\overline{C}_*(G;M)$.*

Proof. The chain complex

$$D_* : \cdots \longrightarrow D_n \xrightarrow{\partial_n} D_{n-1} \xrightarrow{\partial_{n-1}} \cdots \longrightarrow D_2 \xrightarrow{\partial_2} D_1 \xrightarrow{\partial_1} D_0 \longrightarrow 0$$

has the property that $D_0 = 0$, D_1 is the 1-dimensional free kG-module with basis [1], and D_n is the free kG-module with basis

$$\mathcal{B}_n = \{[g_1|\dots|g_n] \,|\, g_1, \dots, g_n \in G,\ g_i = 1 \text{ for some } i\}.$$

The contracting homotopy $s_* : F_* \to F_{*+1}$ for the standard resolution sends $g[g_1|\cdots|g_n]$ to $[g|g_1|\cdots|g_n]$. From this it is easy to see that s_* takes elements in D_* to D_*, hence it induces a contracting homotopy for the quotient complex $\overline{F}_*$. This gives that $\overline{F}_*$ also gives a free resolution for k as a kG-module. Hence F_* and $\overline{F}_*$ are chain homotopy equivalent as chain complexes of free kG-modules. From this we can conclude that for every kG-module M, the cochain complexes $\mathrm{Hom}_{kG}(F_*, M)$ and $\mathrm{Hom}_{kG}(\overline{F}_*, M)$ have isomorphic cohomology groups. The second cocomplex is isomorphic to the normalized complex $\overline{C}^*(G; M)$. □

Note that for $H^1(G; M)$, calculation using the normalized bar resolution does not make any difference because a derivation $f : G \to M$ is always normalized. This is because if we take $g_1 = 1$ in the formula for derivations, we get $f(g_2) = f(g_2) + f(1)$ which implies that $f(1) = 0$.

For $H^2(G; M)$ calculation, we see that the group of normalized 2-cycles is smaller than the group of all 2-cycles. This plays an important role when we are studying group extensions.

Example 110. Let M be a G-module. Let $f : G \times G \to M$ be an element in $C^2(G; M)$. For every $g_1, g_2, g_3 \in G$, we have

$$\delta^2(f)(g_1, g_2, g_3) = g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2).$$

So f is a 2-cocycle if for every $g_1, g_2, g_3 \in G$, the equation

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0 \tag{2}$$

holds. If $f \in C^2(G; M)$ is also a normalized 2-cocycle then we also have

$$f(g, 1) = f(1, g) = 0 \tag{3}$$

for all $g \in G$. A function $f : G \times G \to M$ is called a **factor set** if it is a normalized 2-cocycle, i.e. if it satisfies the equations (2 and 3). We denote the set of all factor sets $f : G \times G \to M$ by $\mathrm{Factor}(G; M)$.

A function $f : G \times G \to M$ is a 2-boundary if there is a function $\xi : G \to M$ such that $f = \delta^1(\xi)$. In this case, for every $g_1, g_2 \in G$, we have

$$f(g_1, g_2) = g_1 \xi(g_2) - \xi(g_1 g_2) + \xi(g_1).$$

If ξ is a normalized function, i.e. if $\xi(1) = 0$, then $f\delta^1(\xi)$ is a normalized 2-cocycle, i.e a factor set. We call such a factor set **trivial factor set** and denote the subgroup of the trivial factor sets by $\mathrm{TFactor}(G; M)$. By definition of group cohomology, we have

$$H^2(G; M) \cong \frac{\mathrm{Factor}(G; M)}{\mathrm{TFactor}(G; M)}.$$

Another interesting example is the case where $G = C_2$ where the normalized standard resolution gives a periodic free resolution.

Example 111. Let $G = \langle g \,|\, g^2 = 1\rangle$ be the cyclic group of order 2 and k be a field with characteristic 2. Then every element $[g_1|\cdots|g_n]$ is in D_n except the element $z_n = [g|\cdots|g]$. So, in this case $\overline{F}_n$ is a 1-dimensional free kG-module generated by z_n. Applying the boundary operator to the element z_n, we get

$$\partial_n(z_n) = g[g|\ldots|g] + \sum_{i=1}^{n-1}[g|\cdots|1|\cdots|g] + [g|\cdots|g] \equiv (g+1)[g|\cdots|g]$$

mod D_{n-1}. So, in this case the normalized standard resolution is isomorphic to the resolution

$$(P_*, \varepsilon) : \cdots \longrightarrow kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{1+g} kG \xrightarrow{\varepsilon} k \longrightarrow 0$$

given in Example 89. We know that this projective resolution is chain homotopy equivalent to any projective resolution of k, in particular it is homotopy equivalent to the standard resolution

$$(Q_*, \varepsilon) : \cdots \xrightarrow{\partial_4} kG^{\otimes 4} \xrightarrow{\partial_3} kG^{\otimes 3} \xrightarrow{\partial_2} kG \otimes kG \xrightarrow{\partial_1} kG \xrightarrow{\varepsilon} k \longrightarrow 0\,.$$

However it is not always easy to write down the chain homotopy $\mu_* : P_* \to Q_*$ even when we know it exists.

One way to write the chain homotopy $\mu_* : P_* \to Q_*$ and its homotopy inverse $\eta_* : Q_* \to P_*$ is to use the k-linear contracting homotopies $s_* : P_* \to P_{*+1}$ and $t_* : Q_* \to Q_{*+1}$. Note that a kG-module homomorphism from a free kG-module F to any kG-module M is uniquely determined by where the basis elements of F are mapped in M. Since both P_* and Q_* are chain complexes of free kG-modules, we can use the contracting homotopies s_* and t_*. For $n \geq 0$, let x_n denote the generator for $P_n \cong kG$. The basis vectors for Q_n will be taken as the elements $[g_1|\ldots|g_n]$ with $g_1, \ldots, g_n \in G$.

We define $\mu_n : P_n \to Q_n$ inductively as follows: Take μ_0 as the identity map, i.e. the map that takes x_0 to $[\,]$. For each $n \geq 1$, let $\mu_n = t_{n-1}\mu_{n-1}\partial_n^P$. Then we have

$$\mu_1(x_1) = t_0\mu_0\partial_1^P(x_1) = t_{n_1}((1+g)[\,]) = [1] + [g].$$

Similar calculation shows

$$\mu_2(x_2) = t_1((1+g)([1]+[g])) = [1|1] + [1|g] + [g|1] + [g|g]$$

and

$$\mu_3(x_3) = [1|1|1] + [1|1|g] + [1|g|1] + [1|g|g] + [g|1|1] + [g|1|g] + [g|g|1] + [g|g|g].$$

By induction, one can easily show that for every $n \geq 0$,

$$\mu_n(x_n) = \sum_{g_1,\ldots,g_n \in G} [g_1|\ldots|g_n]$$

i.e. $\mu_n(x_n)$ is the sum of all basis elements in $\mathcal{B}_n$ for Q_n defined using the bar notation.

Using a similar argument one can calculate the chain map $\eta_n : Q_n \to P_n$. Note that $s_n : P_n \to P_{n+1}$ is the k-linear map that sends $(1+g)x_n$ to x_{n+1} and x_n to 0. Then we take $\eta_0 = \mathrm{id}$ and for all $n \geq 1$, we have $\eta_n = s_{n-1}\eta_{n-1}\partial_n^Q$. By induction we see that η_n takes $[g_1|\dots|g_n]$ to x_n if $g_1 = \cdots = g_n = g$ and to zero otherwise. From the calculations for μ_* and η_*, it is easy to see that $\eta_*\mu_* = \mathrm{id}_{P_*}$. In the other direction there is a chain homotopy h_* between $\mu_*\eta_*$ and id_{Q_*}.

Exercise 112. Write a formula for the chain homotopy $h_* : Q_* \to Q_{*+1}$ between $\mu_*\eta_*$ and id_{Q_*}.

4.3.4 Functoriality of Group Cohomology

The cohomology of a group is functorial with respect ot the groups G and $\mathbb{Z}G$-module M in the following sense. Let $\varphi : H \to G$ be a group homomorphism and $\nu : M \to N$ be an abelian group homomorphism between a G-module M and an H-module N such that for every $h \in H$ and $m \in M$,

$$\nu(\varphi(h) \cdot m) = h \cdot \nu(m).$$

There is a chain map $(\varphi, \eta)^* : C^*(G; M) \to C^*(H; N)$ defined by

$$(\varphi, \eta)^* f(h_1, \dots, h_n) = \nu(f(\varphi(h_1), \dots, \varphi(h_n)))$$

for every $f : G^n \to M$ and $h_1, \dots, h_n \in H$. It is easy to check that $(\varphi, \nu)^*$ defines a chain map: Let $f' = (\varphi, \mu)^* f$ and $g_i = \varphi(h_i)$ for all i. Then

$$\begin{aligned}
(\delta^n f')(h_1, \dots, h_{n+1}) =& h_1 f'(h_2, \dots, h_{n+1}) - \sum_{i=2}^{n-1} (-1)^i f'(h_1, \dots, h_i h_{i+1}, \dots, h_{n+1}) \\
&+ (-1)^{n+1} f'(h_1, \dots, h_n) \\
=& h_1 \nu(f(g_2, \dots, g_n)) - \sum_{i=2}^{n-1} (-1)^i \nu(f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1})) + (-1)^{n+1} \nu(f(g_1, \dots, g_n)) \\
=& \nu(g_1 f(g_2, \dots, g_n)) - \sum_{i=2}^{n-1} (-1)^i \nu(f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1})) + (-1)^{n+1} \nu(f(g_1, \dots, g_n)) \\
=& \nu((\delta^n f)(g_1, \dots, g_{n+1})).
\end{aligned}$$

Hence for each $n \geq 0$, the chain map $(\varphi, \nu)^*$ induces an abelian group homomorphism

$$H^n(\varphi, \nu) : H^n(G; M) \to H^n(H; N).$$

Sometimes $H^n(\varphi, \nu)$ is denoted by $(\varphi, \nu)^*$. When M and N are both equal to the trivial $\mathbb{Z}G$-module A, and ν is the identity map, then the induced map is written as

$$\varphi^* : H^n(G; A) \to H^*(H; A).$$

4.4 Cohomology of Cyclic Groups

Let n be a positive integer and $G = \langle g \,|\, g^n = 1\rangle$ be the cyclic group of order n. Let X be the 1-dimensional simplicial complex X with n-vertices and n-edges whose realization is a regular n-gon. The group G acts on X with the action defined by rotation by $2\pi/n$ degrees. The simplicial chain complex for X is of the form

$$0 \longrightarrow C_1(X) \xrightarrow{\partial_1} C_0(X) \longrightarrow 0$$

where $C_0(X)$ and $C_1(X)$ are the free abelian groups with the basis given by the vertices of X and edges of X. The chain groups $C_0(X)$ and $C_1(X)$ are both $\mathbb{Z}G$-modules with the G-action induced by the G-action on X.

Since G acts freely on the vertices of X (for every $x \in X$, we have $gx = x$ implies $g = 1$), we can choose a vertex v of X and write the set of vertices of X as the set $V = \{v, gv, \ldots, g^{n-1}v\}$. We can assume that V is ordered with the ordering given by $g^i v \leq g^j v$ if $i \leq j$. The chain module

$$C_0(X) = \mathbb{Z} \cdot [v] \oplus \cdots \oplus \mathbb{Z} \cdot [g^{n-1}v] \cong \mathbb{Z}G[v]$$

is a free $\mathbb{Z}G$-module with $\mathbb{Z}G$-basis given by $x_0 = [v]$.

The set of edges of X is also permuted freely by G. Let $e = \{v, gv\}$ denote the edge between v and gv. Then we can write the set of edges as $E = \{e, ge, g^2e, \ldots, g^{n-1}e\}$ where g^ie is the edge $\{g^iv, g^{i+1}\}$. Note that $C_1(X)$ is the free abelian group with basis given by the ordered edges, so we have

$$C_1(X) = \mathbb{Z} \cdot [v, gv] \oplus \mathbb{Z} \cdot [gv, g^2v] \oplus \cdots \oplus \mathbb{Z} \cdot [g^{n-1}v, v]\}.$$

Hence $C_1(X)$ is the 1-dimensional free $\mathbb{Z}G$-module with $\mathbb{Z}G$-basis given by $x_1 = [v, gv]$. The boundary map is defined by

$$\partial_1(g^i x_1) = \partial_1([g^iv, g^{i+1}v]) = [g^{i+1}v] - [g^iv] = g^i(g-1)x_0.$$

The homology groups of X are easy to calculate. Since X is connected $H_0(X) \cong \mathbb{Z}$ generated by an equivalence class of vertices. The kG-module homomorphism $\varepsilon : C_0(X) \to \mathbb{Z}$ sends every $[g^iv]$ to this equivalence class, so after the identification $C_1(X) \cong \mathbb{Z}G$, the map ε is the augmentation map that sends g^i to 1 for all i. The first homology group $H_1(X)$ is also isomorphic to $\mathbb{Z}$ generated by the 1-cycle

$$\begin{aligned} z &= [v, gv] + [gv, g^2v] + \cdots + [g^{n-1}v, v] \\ &= x_1 + gx_1 + \cdots + g^{n-1}x_1 = (1 + g + \cdots + g^{n-1})x_1 \end{aligned}$$

and after the identifications $H_1(X) \cong \mathbb{Z}$ and $C_0(X) \cong \mathbb{Z}G$, the map $\eta : H_1(X) \to C_1(X)$ is the $\mathbb{Z}G$-module homomorphism $\mathbb{Z} \to \mathbb{Z}G$ that sends 1 to $N_G := 1 + g + \cdots + g^{n-1}$. Note that the boundary map $\partial_1 : C_1(X) \to C_0(X)$ takes x_1 to $(g-1)x_0$. So after identifications $C_1(X) \cong \mathbb{Z}G$ and $C_0(X) \cong \mathbb{Z}G$, we can consider ∂_1 as the map defined by multiplication with $g - 1$ in $\mathbb{Z}G$.

Lemma 113. *Let n be a positive integer and $G = \langle g \,|\, g^n = 1\rangle$ denote the cyclic group of order n. Then there is a short exact sequence of $\mathbb{Z}G$-modules*

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

where η is the group homomorphism that sends 1 to N_G and ε is the augmentation map.

Proof. This follows from the above homology group calculations for the simplicial complex X whose realization is an n-gon. □

Putting together the short exact sequences of the form given in Lemma 113 we obtain a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}G$-module.

Proposition 114. *Let n be a positive integer and $G = \langle g \,|\, g^n = 1\rangle$ denote the cyclic group of order n. Then there is a free resolution (F_*, ε) of $\mathbb{Z}$ as a $\mathbb{Z}G$-module where for all $n \geq 0$, $F_n \cong \mathbb{Z}G$ and*

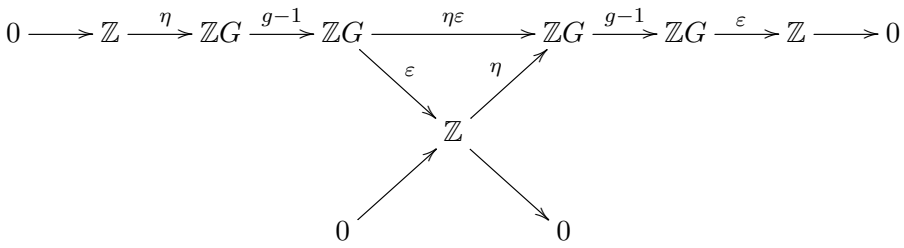
$$\partial : F_n \to F_{n-1} = \begin{cases} g-1 & \text{if } n = odd \\ N_G & \text{if } n = even \end{cases}$$

The free resolution (F_*, ε) can be written as

$$\cdots \longrightarrow \mathbb{Z}G \xrightarrow{N_G} \mathbb{Z}G \xrightarrow{g-1} \mathbb{Z}G \xrightarrow{N_G} \mathbb{Z}G \xrightarrow{g-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

where ε is the augmentation map.

Proof. Splicing two short exact sequence given in Lemma 113, we get a diagram of the form:



Note that the composition $\eta\epsilon : \mathbb{Z}G \to \mathbb{Z}G$ is $\mathbb{Z}G$-module homomorphism defined by the multiplication with $N_G \in \mathbb{Z}G$. The resulting long sequence of $\mathbb{Z}G$-modules is exact by construction. Repeating this splicing process infinitely many times gives the projective resolution in the proposition. □

For any $\mathbb{Z}G$-module M, let

$$M^G = \{m \in M \,|\, gm = m \text{ for all } g \in G\}$$

denote the submodule of G-invariant elements in M. Note that if G is a cyclic group generated by $g \in G$, then $M^G = \ker\{M \xrightarrow{g-1} M\}$.

Proposition 115. *Let n be a positive integer and $G = \langle g \,|\, g^n = 1\rangle$ denote the cyclic group of order n. Then for every $\mathbb{Z}G$-module M, we have*

$$H^n(G; M) \cong \begin{cases} M^G & \text{if } n = 0 \\ \ker\{M \xrightarrow{N_G} M\}/(g-1)M & \text{if } n = odd \\ M^G/N_G M & \text{if } n = even > 0 \end{cases}$$

Proof. Let M be a $\mathbb{Z}G$-module and (F_*, ε) denote the free resolution constructed in Proposition 114. The cochain complex $C^* = \mathrm{Hom}_{\mathbb{Z}G}(F_*, M)$ is of the form

$$0 \longrightarrow M \xrightarrow{1-g} M \xrightarrow{N_G} M \xrightarrow{1-g} M \xrightarrow{N_G} M \longrightarrow \cdots.$$

Calculating the cohomology of G using this cochain complex gives the cohomology groups stated in the proposition. □

When M is the trivial $\mathbb{Z}G$-module then we have the following calculation:

Corollary 116. *Let n be a positive integer and $G = \langle g \,|\, g^n = 1 \rangle$ denote the cyclic group of order n. Then for every $\mathbb{Z}G$-module M, we have*

$$H^n(G; M) \cong \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ \mathbb{Z}/n\mathbb{Z} & \text{if } n = \text{even} > 0 \\ 0 & \text{if } n = \text{odd} \end{cases}$$

Note that for the cyclic group of order $n \geq 0$, the free resolution we constructed is periodic in the sense that for every $n \geq 1$, the chain maps $\partial_n : F_n \to F_{n-1}$ and $\partial_{n+2} : F_{n+2} \to F_{n+1}$ are exactly the same. This gives that for $n \geq 1$, $H^n(G; M) \cong H^{n+2}(G; M)$.

5 Group Cohomology and Group Extensions

5.1 Group Extensions and $H^1(G; M)$

Let G be a group and M be a $\mathbb{Z}G$-module.

Definition 117. An extension of G by M is a sequence of group homomorphisms

$$1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$$

such that

1. i is injective, π is surjective, and $\operatorname{im} i = \ker \pi$,
2. For every $\gamma \in \Gamma$ and $m \in M$, $\gamma i(m)\gamma^{-1} = i(\pi(\gamma)m)$.

The condition (2) can be rephrased by saying that the G-module structure on M coincides with the G-module structure on M induced by the conjugation action in Γ. The G-module structure induced by Γ can be described as follows: For each $g \in G$, choose a $\gamma \in \Gamma$ such that $\pi(\gamma) = g$. Then we can define gm to the element such that $i(gm) = \gamma i(m)\gamma^{-1}$. Note that this action is well defined because M is an abelian group, so the different choices of γ gives the same action of $g \in G$.

Example 118. If N is an abelian normal subgroup of the group Γ, then there is a group extension

$$1 \to N \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$$

where $G = \Gamma/N$, i is the inclusion map and π is the quotient map $\Gamma \to \Gamma/N$. The G-action on N is the one induced by the conjugation action of Γ on N. As special cases of this example we can list the following well-known group extensions:

1. Let $\Gamma = S_3$ be the symmetric group on 3 elements and $N = C_3$ in Γ. Then $G = G/N \cong C_2$. Then there is a group extension of the form

   $$1 \to C_3 \to S_3 \to C_2 \to 1$$

   where C_2-action on C_3 is given by $gx = x^{-1}$ for $1 \neq g \in C_2$ and $x \in C_3$.

2. Let $\Gamma = D_\infty = \langle a, b \,|\, a^2 = b^2 = 1\rangle$ denotes the infinite dihedral group. Then $N = \langle ab\rangle$ is a normal subgroup of Γ which is isomorphic to $\mathbb{Z}$. The quotient group Γ/N is isomorphic to C_2. This gives a group extension of the form

   $$1 \to \mathbb{Z} \to \Gamma \to C_2 \to 1$$

   where the C_2-action on $\mathbb{Z}$ is given by $g \cdot 1 = -1$ for $1 \neq g$ in C_2. To see this note that $a(ab)a^{-1} = aaba = ba = (ab)^{-1}$.

3. Let $\Gamma = D_8 = \langle r, s \,|\, r^4 = s^2 = 1, srs = r^{-1}\rangle$. Then $N = \langle r^2, s\rangle \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ is a normal subgroup of Γ and $G = \Gamma/N = \langle \overline{r}\rangle \cong C_2 \cong \mathbb{Z}/2$. This gives an extension of the form

   $$1 \to \mathbb{Z}/2 \times \mathbb{Z}/2 \to D_8 \to \mathbb{Z}/2 \to 1$$

such that the G-action on N is given by

$$\overline{r} \cdot s = rsr^{-1} = rrs = r^2 s.$$

So if we take s and $r^2 s$ as the generators for $N \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, then the C_2-action is the action that swaps these generators. So as a C_2-module, N is isomorphic to the free module $\mathbb{Z}C_2$.

There is an equivalence relation defined on the set of all extensions of a group G by a $\mathbb{Z}G$-module M which is defined as follows:

Definition 119. Let G be a group and M be a $\mathbb{Z}G$-module. Then two extension $\mathcal{E}_1 : 1 \to M \xrightarrow{i_1} \Gamma_1 \xrightarrow{\pi_1} G \to 1$ and $\mathcal{E}_2 : 1 \to M \xrightarrow{i_2} \Gamma_2 \xrightarrow{\pi_2} G \to 1$ are **equivalent** if there is a group homomorphism $\varphi : \Gamma_1 \to \Gamma_2$ which makes the following diagram commute:

$$\begin{array}{ccccccccc} & & & & \Gamma_1 & & & & \\ & & & \overset{i_1}{\nearrow} & \downarrow{\scriptstyle \varphi} & \overset{\pi_1}{\searrow} & & & \\ 0 & \longrightarrow & M & & & & G & \longrightarrow & 1 \\ & & & \underset{i_2}{\searrow} & \downarrow & \underset{\pi_2}{\nearrow} & & & \\ & & & & \Gamma_2 & & & & \end{array} \tag{4}$$

It is easy to show that if there is a group homomorphism $\varphi : \Gamma_1 \to \Gamma_2$ satisfying the above properties, then it is an isomorphism and its inverse also satisfies the given properties, i.e. makes the diagram commute in the other direction. So the relation above is indeed an equivalence relation. We denote by $\mathcal{E}(G; M)$ the set of all equivalence classes of the extensions of G by M.

One question we can ask is the following:

Question 120. *Given a group G and a $\mathbb{Z}G$-module M, can we classify all extensions of G by M up to the equivalence relation defined above?*

We answer this question completely in Section 5.2. The first step for understanding the extensions of G by M is answering the following question:

Question 121. *Given a group and a G-module M, does there always exist an extension of G by M?*

The answer to the second question is given by the semidirect product construction.

Definition 122. Let G be a group and M be a $\mathbb{Z}G$-module. The **semidirect product** $M \rtimes G$ is the group whose elements are the pairs (m, g) with $m \in M$ and $g \in G$, and the multiplication is defined by

$$(m, g)(m', g') = (m + gm', gg').$$

It is easy to show that the product defined above is associative and the zero element of $M \rtimes G$ is $(0, 1)$. The inverse of (m, g) in $M \rtimes G$ is the element $(-g^{-1}m, g^{-1})$.

Lemma 123. *The semidirect product defines a group extension*

$$1 \to M \to M \rtimes G \to G \to 1$$

where the induced G-action on M coincides with the G-module structure on M.

Proof. To see this note that for every $m \in M$ and $g \in G$, we have

$$(0,g)(m,1)(0,g)^{-1} = (gm,g)(0,g^{-1}) = (gm,1).$$

So M is normal in $M \rtimes G$ and the induced action by conjugation coincides with the G-module action. □

Given a group extension

$$\mathcal{E} : 1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$$

a function $s : G \to \Gamma$ such that $\pi s = \mathrm{id}_G$ is called a **section** of $\mathcal{E}$. If there is a section $s : G \to \Gamma$ which is a group homomorphism, then s is called a **splitting for** $\mathcal{E}$. In this case extension $\mathcal{E}$ is called a **split extension**.

Lemma 124. *Let $\mathcal{E} : 1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$ be an extension of G. If there is a splitting $s : G \to \Gamma$ for $\mathcal{E}$, then the extension $\mathcal{E}$ is equivalent to the extension defined by the semidirect product $M \rtimes G$.*

Proof. Consider the group homomorphism defined by $\varphi : \Gamma \to M \rtimes G$ defined by $\varphi(\gamma) = (m, \pi(\gamma))$ where m is the element in M such $i(m) = \gamma(s\pi(\gamma))^{-1}$. For every $m \in M$, we have $\varphi(i(m)) = (m,1)$ and for every $\gamma \in \Gamma$, $\pi\varphi(\gamma) = \pi(\gamma)$. So φ defines an equivalence of extensions. Note that the inverse of φ is defined by $\varphi^{-1}(m,g) = i(m)s(g)$. □

Let

$$\mathcal{E} : 1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$$

be a split extension. We say two splitting $s_1, s_2 : G \to \Gamma$ are **conjugate** if there is a $m \in M$ such that for every $g \in G$, $s_2(g) = i(m)s_1(g)i(m)^{-1}$. It is easy to see that being conjugate defines an equivalence relation on the set of all splittings. We denote the set of equivalence classes of all splittings of a split extension $\mathcal{E}$ by $\mathrm{Split}(\mathcal{E})$.

If $\mathcal{E}_1$ and $\mathcal{E}_2$ are two equivalent split extensions, using the isomorphism $\varphi : \Gamma_1 \to \Gamma_2$, we can show that there is a bijection $\mathrm{Split}(\mathcal{E}_1) \xrightarrow{\cong} \mathrm{Split}(\mathcal{E}_2)$ which sends an equivalance class $[s]$ of a splitting $s : G \to \Gamma_1$ to the equivalence class $[s\varphi^{-1}]$ where $s\varphi^{-1} : G \to \Gamma_2$ is a splitting for $\mathcal{E}_2$. It is easy to show that this mapping is well-defined.

The argument above shows that for any split extension $\mathcal{E}$, the set $\mathrm{Split}(\mathcal{E})$ is isomorphic to the set $\mathrm{Split}(\mathcal{E}_0)$ where

$$\mathcal{E}_0 : 1 \to M \xrightarrow{i} M \rtimes G \xrightarrow{\pi} G \to 1$$

is the split extension defined by the semidirect product. Here the map i and π are defined by $i(m) = (m,1)$ and $\pi(m,g) = g$. So a splitting for $\mathcal{E}_0$ must be of the form $s(g) = (\xi(g), g)$

for some function $\xi : G \to M$. The function s defined this way is a group homomorphism if for every g_1, g_2 the equation

$$(\xi(g_1), g_1)(\xi(g_2), g_2) = (\xi(g_1 g_2), g_1 g_2)$$

holds. Applying the product rule for semidirect products, we obtain that s is a group homomorphism if for every $g_1, g_2 \in G$,

$$\xi(g_1) + g_1 \xi(g_2) = \xi(g_1 g_2).$$

This is the condition for ξ to be a derivation. We proved the following:

Lemma 125. *Let $\mathcal{E}_0$ be the extension for the semidirect product $M \rtimes G$ and $\xi : G \to M$ be a function. Then the function $s : G \to M \rtimes G$ defined by $s(g) = (\xi(g), g)$ for all $g \in G$ is a splitting for $\mathcal{E}_0$ if and only if ξ is a derivation.*

If two splittings s_1 and s_2 for $\mathcal{E}_0$ defined by $s_1(g) = (\xi_1(g), g)$ and $\xi_2(g), g)$ are equivalent then there is a $m \in M$ such that for every $g \in G$

$$(\xi_2(g), g) = (m, 1)(\xi_1(g), g)(m, 1)^{-1}.$$

This gives the equation $\xi_1(g) - \xi_2(g) = gm - m$. Since $gm - m = \delta^0(m)(g)$, $\xi_1 - \xi_2$ is an inner derivation. Conversely running this argument backwards, we can see that if $\xi_1 - \xi_2$ is an inner derivation, then the corresponding splittings are equivalent.

Proposition 126. *Let G be a group, M be a G-module, and $\mathcal{E}_0$ denote the extension for the semidirect product $M \rtimes G$. Then there is a bijection*

$$\mathrm{Split}(\mathcal{E}_0) \cong H^1(G; M).$$

Proof. Every function $s : G \to M \rtimes G$ satisfying $\pi s = id_G$ is of the form $s(g) = (\xi(g), g)$ for some $\xi : G \to M$. We showed that s is splitting for $\mathcal{E}_0$ if and only if ξ is a derivation. By the argument above two splitting are equivalent if and only if the corresponding derivations differ by an inner derivation. Hence there is a well-defined bijection

$$\mathrm{Split}(\mathcal{E}_0) \to \frac{\mathrm{Der}(G; M)}{\mathrm{IDer}(G; M)} = H^1(G; M)$$

which takes the equivalence class $[s]$ to $\xi + \mathrm{IDer}(G; M)$ were ξ is the derivation corresponding to the splitting s. □

5.2 Group Extensions and $H^2(G; M)$

Let G be a group and M be a G-module. In this section we consider the classification problem stated in Question 120, i.e., we want to calculate the set $\mathcal{E}(G, M)$ of equivalence classes of extension of G by M. We will show that the set $\mathcal{E}(G; M)$ is isomorphic to $H^2(G; M)$.

Let

$$\mathcal{E} : 1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$$

be an extension of G by M. Let $s : G \to M$ be a set-map such that $\pi s = \mathrm{id}$, i.e. a section for $\mathcal{E}$. For simplicity of calculations we assume that $s(1) = 1$. We call such a section **normalized section** for $\mathcal{E}$.

For every $\gamma \in \Gamma$, we have $\pi(s\pi(\gamma)) = \pi(\gamma)$. Hence for every $\gamma \in \Gamma$ there is a unique $m \in M$ such that $\gamma = i(m)s\pi(\gamma)$. This shows that every $\gamma \in \Gamma$ can be uniquely written as

$$\gamma = i(m)s(g)$$

where $g = \pi(\gamma)$ and $m \in M$ is such that $\gamma = i(m)s(g)$. This gives a one-to-one correspondence between Γ and the product $M \times G$ given by the function $\tau_s : \Gamma \to M \times G$ that sends $\gamma \in \Gamma$ to the pair $(m, g) \in M \times G$ such that $\gamma = i(m)s(g)$. We will now show that there is a suitable defined group operation on $M \times G$ that makes this correspondence a group isomorphism.

Lemma 127. *Let $\mathcal{E}$ be an extension of G by M and $s : G \to M$ be a section for $\mathcal{E}$. Suppose that $f : G \times G \to M$ is the function defined by $i(f(g, h)) = s(g)s(h)s(gh)^{-1}$ for every $g, h \in G$. Then f is a factor set.*

Proof. By the definition of $f : G \times G \to M$, for every $g, h \in G$, we have

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

Let $g_1, g_2, g_3 \in G$. Then we have

$$\begin{aligned}(s(g_1)s(g_2))s(g_2) &= i(f(g_1, g_2))s(g_1g_2)s(g_3)\\ &= i(f(g_1, g_2))i(f(g_1g_2, g_3))s(g_1g_2g_3)\\ &= i(f(g_1, g_2) + f(g_1g_2, g_3))s(g_1g_2g_3)\end{aligned}$$

and

$$\begin{aligned}s(g_1)(s(g_2)s(g_3)) &= s(g_1)i(f(g_1, g_2))s(g_2g_3)\\ &= i(g_1f(g_2, g_3))s(g_1)s(g_2g_3)\\ &= i(g_1f(g_2, g_3))i(f(g_1, g_2g_3))s(g_1g_2g_3)\\ &= i(g_1f(g_2, g_3) + f(g_1, g_2g_3))s(g_1g_2, g_3).\end{aligned}$$

The associativity of the product in Γ gives that the equality

$$g_1f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3) - f(g_1, g_2) = 0$$

holds. Since $s(1) = 1$, for every $g \in G$, we have $s(1)s(g) = i(f(g, 1))s(g)$ which implies $f(g, 1) = 0$. Similarly $s(g)s(1) = i(f(1, g))s(g)$ which gives $f(1, g) = 0$. Hence f is a factor set. □

There is a construction in the opposite direction as well.

Lemma 128. *Let G be a group, M be a G-module, and $f : G \times G \to M$ be factor set. Consider the binary operation on the set $M \times G$ defined by*

$$(m_1, g_1)(m_2, g_2) = (m_1 + g_1m_2 + f(g_1, g_2), g_1g_2).$$

Then $M \times G$ is a group with this operation where the unit element is $(0, 1)$. This group is denoted by $M \times_f G$.

Proof. For every $m_1, m_2, m_3 \in M$ and $g_1, g_2, g_3 \in G$, we have

$$\begin{aligned}((m_1, g_1)(m_2, g_2))(m_3, g_3) &= (m_1 + g_1 m_2 + f(g_1, g_2), g_1 g_2)(m_3, g_3) \\ &= (m_1 + g_1 m_2 + f(g_1, g_2) + g_1 g_2 m_3 + f(g_1 g_2, g_3), g_1 g_2 g_3)\end{aligned}$$

and

$$\begin{aligned}(m_1, g_1)((m_2, g_2)(m_3, g_3)) &= (m_1, g_1)(m_2 + g_2 m_3 + f(g_2, g_3), g_2 g_3) \\ &= (m_1 + g_1 m_2 + g_1 g_2 m_3 + g_1 f(g_2, g_3) + f(g_1, g_2 g_3), g_1 g_2 g_3).\end{aligned}$$

So after cancellations, the associativity of the operation defined in Lemma 128 is equivalent to the equation

$$f(g_1, g_2) + f(g_1 g_2, g_3) = g_1 f(g_2, g_3) + f(g_1, g_2 g_3).$$

Since f is factor set this equation holds.

f is a factor set also implies that for every $g \in G$, the equations $f(1, g) = f(g, 1) = 0$ hold. Then for every $m \in M$ and $g \in G$, we have

$$(0, 1)(m, g) = (m + f(1, g), g) = (m, g)$$

and

$$(m, g)(0, 1) = (m + f(g, 1), g) = (m, g).$$

This shows $(0, 1)$ is the unit element. We claim that the inverse of an element (m, g) is $(-g^{-1}m - g^{-1}f(g, g^{-1}), g^{-1})$. To see this observe that

$$(m, g)(-g^{-1}m - g^{-1}f(g, g^{-1}), g^{-1}) = (0, 1).$$

For the other direction, consider the product

$$(-g^{-1}m - g^{-1}f(g, g^{-1}), g^{-1})(m, g) = (-g^{-1}f(g, g^{-1}) + f(g^{-1}, g), 1).$$

This product is equal to $(0, 1)$ because the factor set equation for the triple (g^{-1}, g, g^{-1}) gives

$$g^{-1}f(g, g^{-1}) - f(1, g^{-1}) + f(g^{-1}, 1) - f(g^{-1}, g) = 0$$

which implies $g^{-1}f(g, g^{-1}) = f(g^{-1}, g)$. Hence $M \times_f G$ is a group with unit element $(0, 1)$. □

We also have the following:

Lemma 129. *Let $M \times_f G$ be the group defined in Lemma 128 . Then there is a group extension*

$$\mathcal{E}_f : 1 \to M \xrightarrow{i} M \times_f G \xrightarrow{\pi} G \to 1$$

where $i(m) = (m, 1)$ and $\pi(m, g) = g$ for every $m \in M$ and $g \in G$. Moreover if we take $s : G \to \Gamma$ to be the function $s(g) = (0, g)$, then the associated factor set is f.

Proof. It is easy to see from the definition of group operation in $M \times_f G$ that $i : M \to M \times_f G$ and $\pi : M \times_f G \to G$ are group homomorphisms. It is also clear that $\ker \pi = \operatorname{im} i$. So, $\mathcal{E}_f$ is a group extension. If $s : G \to \Gamma$ is the section defined by $s(g) = (0, g)$, then an easy calculation shows that the factor set associated to this section is equal to f. □

The formula chosen for the group operation for $M \times_f G$ is not random, it comes from the 1-1 correspondence τ_s between the sets Γ and $M \times G$. In fact the operation for $M \times_f G$ is the operation that makes τ_s a group isomorphism. We have the following:

Proposition 130. *Let $\mathcal{E} : 1 \to M \to \Gamma \to G \to 1$ be an extension of G by M and $s : G \to \Gamma$ be a section for $\mathcal{E}$. Suppose that f is the factor set associated to the section s. Then the group $M \times_f G$ is isomorphic to Γ and the extensions $\mathcal{E}$ and $\mathcal{E}_f$ are equivalent.*

Proof. Consider the map $\tau_s : \Gamma \to M \times G$ that takes $\Gamma = i(s)\pi(g)$ to the pair (m, g). Let $\gamma_1, \gamma_2 \in \Gamma$ such that $\gamma_1 = i(m_1)g_1$ and $\gamma_2 = i(m_2)g_2$ for some $m_1, m_2 \in M$ and $g_1, g_2 \in G$. Then we have

$$\begin{aligned}\gamma_1\gamma_2 &= i(m_1)s(g_1)i(m_2)s(g_2)\\ &= i(m_1)i(g_1m_2)s(g_1)s(g_2)\\ &= i(m_1)i(g_1m_2)i(f(g_1,g_2))s(g_1g_2)\\ &= i(m_1 + gm_2 + f(g_1,g_2))s(g_1g_2).\end{aligned}$$

This gives $\tau_s(\gamma_1\gamma_2) = \tau_s(\gamma_1)\tau_s(\gamma_2)$, hence τ_s is a group homomorphism. Since τ is a bijection, it defined a group isomorphism. It is easy to see that τ gives a commuting diagram of group extensions with the inclusion and projection maps defined as above. □

Remark 131. The Proposition 130 is very useful when one is working with group extensions. It allows us replace a given extension $\mathcal{E} : 1 \to M \to \Gamma \to G \to 1$ with an extension $\mathcal{E}_f : 1 \to M \to M \times_f G \to G \to 1$ where the group elements in $M \times_f G$ are the pairs of (m, g) with a specific formula for the group operation

$$(m_1, g_1)(m_2, g_2) = (m_1 + g_1m_2 + f(g_1, g_2), g_1g_2)$$

where $f : G \times G \to M$ is the factor set for the extension $\mathcal{E}$ associated to some section $s : G \to \Gamma$. So for computation purposes we can always assume a given extension $\mathcal{E}$ is of the form $\mathcal{E}$ for some $\mathcal{E}_f$.

To classify all extensions of G by M we need to understand what happens when we replace the section s with another section for $\mathcal{E}$.

Lemma 132. *Suppose that s, s' are two sections for the extension $\mathcal{E} : 1 \to M \to \Gamma \to G \to 1$, and $f, f' : G \times G \to M$ are the corresponding factor sets. Then there is a function $\xi : G \to M$ satisfying $\xi(1) = 0$ such that $f' - f = \delta^1(\xi)$.*

Proof. Let $\xi : G \to M$ be the function such that for every $g \in G$,

$$s'(g) = i(\xi(g))s(g).$$

Note that since $s(1) = s'(1) = 1$, we have $\xi(1) = 0$. For every $g_1, g_2 \in G$, we have

$$\begin{aligned}i(f'(g_1,g_2)) &= s'(g_1)s'(g_2)s'(g_1g_2)^{-1}\\ &= i(\xi(g_1))s(g_1)i(\xi(g_2))s(g_2)s(g_1g_2)^{-1}i(\xi(g_1g_2))^{-1}\\ &= i(\xi(g_1))i(g_1s(g_2))s(g_1)s(g_2)s(g_1g_2)^{-1}i(\xi(g_1g_2))^{-1}\\ &= i(\xi(g_1) + g_1s(g_2))i(f(g_1,g_2)i(\xi(g_1g_2))^{-1}\\ &= i(\xi(g_1) + g_1\xi(g_2) + f(g_1,g_2) - \xi(g_1g_2)).\end{aligned}$$

This gives the equation

$$f'(g_1, g_2) - f(g_1, g_2) = \xi(g_1) + g_1\xi(g_2) - \xi(g_1g_2) = (\delta^1\xi)(g_1, g_2).$$

Hence $f' - f = \delta^1(\xi)$ for some function $\xi : G \to M$ satisfying $\xi(1) = 0$. □

We also have the following:

Lemma 133. *Let $f, f' : G \times G \to M$ be two factor sets such that $f' - f = \delta^1(\xi)$ for some function $\xi : G \to M$ such that $\xi(1) = 0$. Then the extensions*

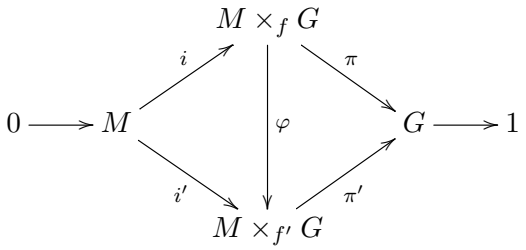
$$\mathcal{E}_f : 1 \to M \xrightarrow{i} M \times_f G \xrightarrow{\pi} G \to 1 \quad \text{and} \quad \mathcal{E}_{f'} : 1 \to M \xrightarrow{i'} M \times_{f'} G \xrightarrow{\pi'} G \to 1$$

are equivalent.

Proof. Consider the map $\varphi : M \times_f G \to M \times_{f'} G$ defined by $\varphi(m, g) = (m + \xi(g), g)$. Then for every $m_1, m_2 \in M$ and $g_1, g_2 \in G$, we have

$$\begin{aligned}
\varphi((m_1, g_1)(m_2, g_2)) &= \varphi((m_1 + g_1m_2 + f(g_1, g_2), g_1g_2)) \\
&= (m_1 + g_1m_2 + f(g_1, g_2) + \xi(g_1g_2), g_1g_2) \\
&= (m_1 + g_1m_2 + f'(g_1, g_2) + g_1\xi(g_2) + \xi(g_2), g_1g_2) \\
&= (m_1 + \xi(g_1), g_1)(m_2 + \xi(g_2), g_2) \\
&= \varphi(m_1, g_2)\varphi(m_2, g_2).
\end{aligned}$$

So, φ is a group homomorphism. Consider the diagram



.

For every $m \in M$, we have

$$(\varphi i)(m) = \varphi(m, 1) = (m + \xi(1), 1) = (m, 1) = i'(m).$$

Also for every $m \in M$, $g \in G$, we have $(\pi'\varphi)(m, g) = (\pi'(m + \xi(g), g) = g = \pi(m, g)$. So the diagram above commutes.

□

Now we are ready to prove the main result of this section.

Theorem 134. *Let G be a group and M be a $\mathbb{Z}G$-module. Then there is a bijection between the set $\mathcal{E}(G; M)$ of equivalence classes of all extensions of G by M and the second cohomology group $H^2(G; M)$.*

Proof. Let $\mathcal{E} : 1 \to M \xrightarrow{i} \Gamma \xrightarrow{\pi} G \to 1$ be an extension of G by M. Choose a section $s : G \to M$ for $\mathcal{E}$. By Lemma 127, the function $f : G \times G \to M$ defined by

$$i(f(g_1, g_1))s(g_1g_2) = s(g_1)s(g_2)$$

for all $g_1, g_2 \in G$ is a factor set, i.e f is a normalized 2-cocycle. By Lemma 132, if we choose a different section s' for $\mathcal{E}$, then the factor set f' differs from f by a normalized coboundary, i.e there is a function $\xi : G \to M$ satisfying $\xi(1) = 0$ such that $f' - f = \delta^1(\xi)$. This shows that the cohomology class $[f] \in H^2(G; M)$ for the extension $\mathcal{E}$ is independent from the section that is chosen. Hence we can define a well-defined function

$$\Psi : \{\text{Extensions of } G \text{ by } M\} \to H^2(G; M)$$

that sends each extension $\mathcal{E}$ to the cohomology class $[f] \in H^2(G; M)$ where f is a factor set associated to some section for $\mathcal{E}$.

If two extensions $\mathcal{E}_1$ and $\mathcal{E}_1$ are equivalent then there is commuting diagram as in Equation 4. Let $s_1 : G \to \Gamma_1$ be a section for the extension $\mathcal{E}_1$ and f_1 be the factor set associated to s. Let $s_2 : G \to \Gamma_2$ be the function defined by $s_2 = \varphi s_1$. Note that $\pi_2 s_2 = \pi_2 \varphi s_1 = \pi_1 s_1 = \mathrm{id}$, so s_2 is section for Γ_2. Let f_2 be the factor set for $\mathcal{E}_2$ associated to the section s_2. Then for every $g, h \in G$, we have

$$\begin{aligned} i_2(f_2(g,h)) &= s_2(g)s_2(h)(s_2(gh))^{-1} \\ &= \varphi(s_1(g))\varphi(s_2(h))\varphi(s_2(gh))^{-1} \\ &= \varphi(s_1(g)s_1(h)s_1(gh)^{-1}) \\ &= \varphi i_1(f_1(g,h)) = i_2(f_1(g,h)) \end{aligned}$$

Hence $f_2 = f_1$. Since the image of an extension under Ψ does not depend on the section that is chosen, we obtain that $\Psi(\mathcal{E}_1) = \Psi(\mathcal{E}_2)$. Hence Ψ induces a well-defined map

$$\overline{\Psi} : \mathcal{E}(G; M) \to H^2(G; M).$$

For each $[f] \in H^2(G; M)$, consider the extension

$$\mathcal{E}_f : 1 \to M \to M \times_f G \to G \to 1$$

constructed in Lemmas 128 and 129. By Lemma 129 if we choose the section for $\mathcal{E}_f$ as the function $s : G \to M \times_f G$ defined by $s(g) = (0, g)$ for all $g \in G$, then the associated factor set is equal to f. So we have $\Psi(\mathcal{E}_f) = [f]$. This shows that Ψ is surjective. To prove injectivity of $\overline{\Psi}$, let $\mathcal{E}$ and $\mathcal{E}'$ be two extension such that for some section s and s', the corresponding sections f and f' satisfy $[f] = [f']$. By Proposition 130, we have $\mathcal{E} \sim \mathcal{E}_f$ and $\mathcal{E}' \sim \mathcal{E}_{f'}$. Since $[f] = [f']$, there is a function $\xi : G \to M$ satisfying $\xi(1) = 0$ such that $f' - f = \delta^i(\xi)$. By Lemma 133 we have $\mathcal{E}_f \sim \mathcal{E}_{f'}$. Hence we conclude that $\mathcal{E} \sim \mathcal{E}'$. This shows that $\overline{\psi}$ is injective. □