

# Homological Algebras

Guo Haoyang

March 2025

## Contents

<b>1 Additive and abelian category</b>	<b>2</b>
<b>2 Chain complexes</b>	<b>2</b>
2.0.1 Categorical complexes . . . . .	2
2.0.2 Exact sequence of complexes . . . . .	3
2.0.3 Classifying exact sequences: First encounter . . . . .	4
2.0.4 Exact functors . . . . .	4
<b>3 Homology of a chain complex</b>	<b>4</b>
3.1 Homology as a functor . . . . .	4
3.1.1 Homology . . . . .	5
3.1.2 Functoriality of $H_n$ . . . . .	5
3.2 Making new exact sequences from old . . . . .	5
<b>4 Injective, Projective and Flat modules</b>	<b>7</b>
4.1 Definitions and properties . . . . .	7
4.2 Resolutions . . . . .	7
<b>5 Derived functors</b>	<b>8</b>
5.1 Homotopic morphisms between complexes . . . . .	8
5.2 Left derived functors . . . . .	10
5.3 Right derived functors . . . . .	13
5.3.1 Covariant right derived functors . . . . .	13
5.3.2 Contravariant right-derived functors . . . . .	14
5.4 Exact sequences and derived functors . . . . .	14
5.5 A little summary . . . . .	14
<b>6 Examples for left-derived functors</b>	<b>14</b>
6.1 Tor functor . . . . .	14
6.1.1 Tor functor . . . . .	15
6.1.2 Axiomatic characterization of $\text{Tor}_n$ functors . . . . .	16
6.1.3 Applications of Tor functor . . . . .	16
<b>7 Examples for right-derived functors</b>	<b>17</b>
7.1 Ext functor . . . . .	17
7.1.1 Applications of Ext 1: Classifying extensions of $R$ -modules . . . . .	17
7.1.2 Application of Ext 2: Baer sum . . . . .	19
7.2 Sheaf cohomology . . . . .	19
7.3 Group cohomology . . . . .	19
7.3.1 Calculation of cohomology groups 1: Choosing resolutions . . . . .	20
7.3.2 Calculations of group cohomology 2: formal calculations . . . . .	22
7.3.3 Application of group cohomology: Number theory . . . . .	23
7.3.4 Application of group cohomology: Group extension . . . . .	26
<b>8 Introduction to spectral sequences</b>	<b>29</b>

# 1 Additive and abelian category

## Definition 1.1: Preadditive category

A category  $\mathcal{C}$  is a **preadditive category**  $\Leftrightarrow$

- (1)  $\forall A, B \in \text{Ob}(\mathcal{C})$ ,  $\text{Mor}_{\mathcal{C}}(A, B)$  has an abelian group structure. The group law here is addition  $+$ .
- (2)  $\forall X, Y, Z \in \text{Ob}(\mathcal{C})$ , the composition map

$$\text{Mor}_{\mathcal{C}}(Y, Z) \times \text{Mor}_{\mathcal{C}}(X, Y) \rightarrow \text{Mor}_{\mathcal{C}}(X, Z) \quad (g, f) \mapsto g \circ f$$

is bilinear. If we write the map in the group law explicitly, then  $\forall f_1, f_2, f \in \text{Mor}_{\mathcal{C}}(X, Y)$ ,  $g_1, g_2, g \in \text{Mor}_{\mathcal{C}}(Y, Z)$ ,

$$(g_1 + g_2) \circ f = g_1 \circ f + g_2 \circ f, \quad g \circ (f_1 + f_2) = g \circ f_1 + g \circ f_2$$

## Lemma 1.1: Characterization of zero element in additive categories

Let  $\mathcal{C}$  be a preadditive category.  $Z \in \text{Ob}(\mathcal{C})$  is an zero object  $\Leftrightarrow \text{Mor}_{\mathcal{C}}(Z, Z)$  has unique element, the trivial map.

**Proof:**  $\Rightarrow Z$  is zero  $\Rightarrow Z$  is initial  $\Leftrightarrow \forall A \in \text{Ob}(\mathcal{C})$ ,  $\text{Mor}_{\mathcal{C}}(Z, A)$  contains unique element. Let  $A := Z$ .

$\Leftarrow$  Since  $\mathcal{C}$  is an preadditive category, the zero map  $0_{ZZ} \in \text{Mor}_{\mathcal{C}}(Z, Z)$ ,  $0_{ZZ} = \text{id}_Z$ . We will show  $Z$  is initial and the fact that  $Z$  is terminal/final is similar:  $\forall A \in \text{Ob}(\mathcal{C})$ ,  $\forall f \in \text{Mor}_{\mathcal{C}}(A, Z)$ ,  $f = \text{id}_Z \circ f = 0_{ZZ} \circ f = 0_{ZZ}$ . So, the morphism from  $A$  to  $Z$  is unique. Then,  $Z$  is initial.  $\square$

## Definition 1.2: Additive category

A category  $\mathcal{C}$  is an **additive category**  $\Leftrightarrow \mathcal{C}$  is a preadditive category admitting all finitary biproducts.

???

## Definition 1.3: Abelian category

# 2 Chain complexes

## 2.0.1 Categorical complexes

### Definition 2.1: Complexes and differentials

Let  $\mathcal{A}$  be an abelian category. A **complex** in  $\mathcal{A}$ , denoted  $(A_{\bullet}, d_{\bullet})$ , is a sequence of objects and morphisms in  $\mathcal{A}$ , where  $A_{\bullet} := \{A_i\}_i$  and  $d_{\bullet} := \{d_i^A\}_i$ :

$$\cdots \longrightarrow A_{n+1} \xrightarrow{d_{n+1}^A} A_n \xrightarrow{d_n^A} A_{n-1} \xrightarrow{d_{n-1}^A} \cdots$$

such that  $\forall n$ ,  $d_{n+1}^A \circ d_n^A = 0$ . The maps  $d_n^A$  are called **differentials**.

### Definition 2.2: Morphism pf complexes

Let  $(A_\bullet, d_\bullet^A)$  and  $(B_\bullet, d_\bullet^B)$  be two complexes in an abelian category  $\mathcal{A}$ . A morphism between two complexes

$$f_\bullet : (A_\bullet, d_\bullet^A) \rightarrow (B_\bullet, d_\bullet^B)$$

is a collection of morphisms  $f_n : A_n \rightarrow B_n$  such that all the squares in the following diagram commute, i.e.  $\forall n, d_{n+1}^B \circ f_{n+1} = f_n \circ d_{n+1}^A$ :

$$\begin{array}{ccccccc} \cdots & \xrightarrow{d_{n+2}^A} & A_{n+1} & \xrightarrow{d_{n+1}^A} & A_n & \xrightarrow{d_n^A} & A_{n-1} \xrightarrow{d_{n-1}^A} \cdots \\ & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} \\ \cdots & \xrightarrow{d_{n+2}^B} & B_{n+1} & \xrightarrow{d_{n+1}^B} & B_n & \xrightarrow{d_n^B} & B_{n-1} \xrightarrow{d_{n-1}^B} \cdots \end{array}$$

As the definitions suggest, there is a category whose objects are complexes in the Abelian category  $\mathcal{A}$ ,  $(A_\bullet, d_\bullet^A)$  and morphisms  $\forall (A_\bullet, d_\bullet^A), (B_\bullet, d_\bullet^B) \in \text{Ob}(R - \mathbf{Comp})$ ,

$$\text{Mor}((A_\bullet, d_\bullet^A), (B_\bullet, d_\bullet^B)) = \{f_\bullet : A_\bullet \rightarrow B_\bullet\}$$

Elementwise,  $(f_\bullet)_n := f_n$ . If there are two morphisms  $f_\bullet : (A_\bullet, d_\bullet^A) \rightarrow (B_\bullet, d_\bullet^B)$  and  $g_\bullet : (B_\bullet, d_\bullet^B) \rightarrow (C_\bullet, d_\bullet^C)$ . The composition  $g_\bullet \circ f_\bullet$  works elementwise as  $(g_\bullet \circ f_\bullet)_n := (g_\bullet)_n \circ (f_\bullet)_n := g_n \circ f_n$ . This definition satisfies those regulations on composition maps.

So, this category can be denoted as  $\mathbf{Comp}(\mathcal{A})$ ,  $\mathbf{Ch}(\mathcal{A})$ . If  $\mathcal{A}$  is understood, it is written in the notation  $\mathbf{Comp}$ . When  $\mathcal{A} =_R \mathbf{Mod}$ , this category is usually written as  $\mathbf{Comp}_{(R\mathbf{Mod})}$  or  $R\mathbf{Comp}$ .

In fact, there is more information on  $\mathbf{Comp}(\mathcal{A})$ , it is not only a category, but also an abelian category.

### Proposition 2.1: $\mathbf{Comp}(\mathcal{A})$ is an abelian category

#### 2.0.2 Exact sequence of complexes

There are two questions concerning the introducing the following concepts:

- Why study exact sequences?
- Why study the short exact sequences?

They are equally important. But, we will see the second one is independent of the first one. Let's explain the first question why study exact sequences

### Definition 2.3: Exact sequence

### Definition 2.4: Short exact sequence

One reason is that the following observation allows us to break up every exact complex into a larger number of short exact sequences.

$$\begin{array}{ccccccc}
& & 0 & & 0 & & \\
& & \searrow & & \swarrow & & \\
& & \text{im}d_{i+1} = \ker d_i & & & & \\
& & \nearrow d_{i+1} & \leftrightarrow & \swarrow d_{i+1} & & \\
M_{i+2} & \xrightarrow{d_{i+2}} & M_{i+1} & \xrightarrow{d_{i+1}} & M_i & \xrightarrow{d_i} & M_{i-1} \\
& \downarrow d_{i+2} & \swarrow \leftrightarrow & & \downarrow d_i & \swarrow \leftrightarrow & \\
& \text{im}d_{i+2} = \ker d_{i+1} & & & \text{im}d_i = \ker d_{i-1} & & \\
& \nearrow & \searrow & & \nearrow & \searrow & \\
& 0 & & 0 & & 0 & 
\end{array}$$

This technique is used in the definition 4.2

### Lemma 2.1: Five lemma

Let  $\mathcal{A}$  be an abelian category. All objects are taken from  $\mathcal{A}$  or **Gp** in the following diagram:

$$\begin{array}{ccccccc}
A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D & \longrightarrow & E \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' & \longrightarrow & E'
\end{array}$$

### 2.0.3 Classifying exact sequences: First encounter

To classify all exact sequences, we need introduce the decomposition as follows.

### Definition 2.5: Split exact sequence

A short exact sequence of  $R$ -modules

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

splits if it is isomorphic to another exact<sup>a</sup> sequence

$$0 \longrightarrow M'_1 \longrightarrow M'_1 \oplus M'_2 \longrightarrow M'_2 \longrightarrow 0$$

such that the following diagram commutes, where  $\sim$  means isomorphism.

$$\begin{array}{ccccccc}
0 & \longrightarrow & M_1 & \longrightarrow & N & \longrightarrow & M_2 & \longrightarrow & 0 \\
& & \downarrow \sim & & \downarrow \sim & & \downarrow \sim & & \\
0 & \longrightarrow & M'_1 & \longrightarrow & M'_1 \oplus M'_2 & \longrightarrow & M'_2 & \longrightarrow & 0
\end{array}$$

<sup>a</sup>from  $m'_1 \mapsto (m'_1, 0)$  and  $(m'_1, m'_2) \mapsto m'_2$

In the upper definition, the exact sequence is classified by the isomorphism and reduced to a simpler form. The classification has not yet done until introducing the tool-Ext functor.

### 2.0.4 Exact functors

## 3 Homology of a chain complex

### 3.1 Homology as a functor

### 3.1.1 Homology

#### Definition 3.1: Homology

Let the following be a complex in an abelian category  $\mathcal{A}$ :

$$M_\bullet : \cdots \xrightarrow{d_{i+2}} M_{i+1} \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

The  $i$ -th homology of that complex  $M_\bullet$  is an object in  $\mathcal{A}$ :

$$H_i(M_\bullet) = \frac{\ker d_i}{\text{im } d_{i+1}}$$

And  $H_\bullet(M_\bullet)$  is a collection of  $R$ -modules indexed by  $\mathbb{Z}$ .

**Remark** Here  $i$  indicates the module  $M_i$  and consider the two components lying inside  $M_i$ .

Notice that

$$H_i(M_\bullet) = 0 \Leftrightarrow \ker d_i = \text{im } d_{i+1} \Leftrightarrow \text{the complex } M_\bullet \text{ is exact at } M_i$$

So, if the sequence is not exact at somewhere, say  $M_i$ , then  $H_i(M_\bullet) \neq 0$ . The homology measures the failure of a complex from being exact.

Sometimes  $\ker d_i$  and  $\text{im } d_{i+1}$  have 'geometric' names and notations.  $M_n$  is called *n-chains*;  $Z_n(M_\bullet) := \ker d_n$  is called *n-cycles* and  $B_n(M_\bullet)$  is called *n-boundaries*. In these notations,

$$H_n(M_\bullet) = \frac{Z_n(M_\bullet)}{B_n(M_\bullet)}$$

### 3.1.2 Functoriality of $H_n$

#### Proposition 3.1: $H_n$ as a functor

Let  $\mathcal{A}$  be an abelian category.  $\forall n, H_n : \mathbf{Comp}(\mathcal{A}) \rightarrow \mathcal{A}$  is an additive functor.

## 3.2 Making new exact sequences from old

#### Lemma 3.1: The snake lemma

Let

$$\begin{array}{ccccccc} A_1 & \xrightarrow{\alpha_1} & B_1 & \xrightarrow{\beta_1} & C_1 & \longrightarrow 0 \\ \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A_2 & \xrightarrow{\alpha_2} & B_2 & \xrightarrow{\beta_2} & C_2 \end{array}$$

be a commutative diagram of  $R$ -modules with exact rows. Then there is an exact sequence

$$\begin{array}{ccccc} \ker f & \xrightarrow{\alpha_1^\circ} & \ker g & \xrightarrow{\beta_1^\circ} & \ker h \\ \downarrow & & \downarrow & & \downarrow \\ \text{coker } f & \xrightarrow{\alpha_2^\circ} & \text{coker } g & \xrightarrow{\beta_2^\circ} & \text{coker } h \end{array}$$

**Remark** If the morphism of two exact sequences is given as (a extended version):

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\alpha_1} & B_1 & \xrightarrow{\beta_1} & C_1 & \longrightarrow 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & \\ 0 & \longrightarrow & A_2 & \xrightarrow{\alpha_2} & B_2 & \xrightarrow{\beta_2} & C_2 & \longrightarrow 0 \end{array}$$

then there is a corresponding exact sequence:

$$0 \longrightarrow \ker f \xrightarrow{\alpha_1^\circ} \ker g \xrightarrow{\beta_1^\circ} \ker h \xrightarrow{\delta} \text{coker } f \xrightarrow{\alpha_2^\circ} \text{coker } g \xrightarrow{\beta_2^\circ} \text{coker } h \longrightarrow 0$$

### Proof: Well-definedness of each map:

We will define  $\alpha_1^\circ, \beta_1^\circ, \alpha_2^\circ, \beta_2^\circ$  and  $\delta$  and show they are well-defined.

- The definitions of  $\alpha_1^\circ$  and  $\beta_1^\circ$  are as follows:

$$\alpha_1^\circ := \alpha_1|_{\ker f}^{\ker g} : A_1 \supseteq \ker f \longrightarrow \ker g \subseteq B_1 \quad \beta_1^\circ := \beta_1|_{\ker g}^{\ker h} : B_1 \supseteq \ker g \longrightarrow \ker h \subseteq C_1$$

Here it is enough to show  $\alpha_1^\circ$  is well-defined, and the case for  $\beta_1^\circ$  is similar.  $\forall x \in \ker f, g(\alpha_1(x)) = \alpha_2(f(x)) = \alpha_2(0) = 0$ , since  $\alpha_2$  is a homomorphism.

- $\alpha_2^\circ, \beta_2^\circ$  are defined as follows:

$$\alpha_2^\circ : \text{coker } f \rightarrow \text{coker } g \quad a_2 + \text{im } f \mapsto \alpha_2(a_2) + \text{im } g$$

The definition for  $g$  is similar and is omitted here. This  $\alpha_2^\circ$  is well-defined because it is independent of choice of representatives:  $\forall a_2, a'_2 \in A_2$  such that  $a_2 - a'_2 \in \text{im } f, \exists a \in A_1$  makes  $a_2 - a'_2 = f(a)$ . So,  $\alpha_2(a_2 - a'_2) = \alpha_2(f(a)) = g(\alpha_1(a)) \in \text{im } g$ . There is no worry about the image of  $A_2/\text{im } f$  is not in  $B_2/\text{im } g$ .

- Let's define  $\delta$  right now. The proof is constructive and the construction of  $\delta$  is a diagram chasing illustrated in the following diagram:

$$\begin{array}{ccccccc}
 & \ker f & \xrightarrow{\alpha_1^\circ} & \ker g & \xrightarrow{\beta_1^\circ} & \ker h & \\
 & \downarrow \iota & & \downarrow \iota & & \downarrow \iota & \\
 A_1 & \xrightarrow{\alpha_1} & B_1 & \xrightarrow{\beta_1} & C_1 & \longrightarrow 0 & \\
 & \downarrow f & \downarrow g & \downarrow h & & & \\
 0 & \xrightarrow{\alpha_2} & A_2 & \xrightarrow{\beta_2} & B_2 & \xrightarrow{\delta} & C_2 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & \xrightarrow{\alpha_2^\circ} & \text{coker } f & \xrightarrow{\beta_2^\circ} & \text{coker } g & \xrightarrow{\delta^\circ} & \text{coker } h
 \end{array}$$

$x$   
 $\downarrow \{(1)\}$   
 $y \xleftarrow{(2.1.1)} x$   
 $\downarrow \{(2.1.2)\}$   
 $z \xleftarrow{(3)} g(y) \dashrightarrow h(x)$   
 $\downarrow \{(2.2)\}$   
 $z + \text{im } f$

(1) Starting from an element in  $\ker h$ ,  $\ker h$  has an inclusion to  $C_1$ . So,  $\iota(x) = x$  is an element in  $C_1$ . (2) The exactness of  $C_1$  implies that  $\beta_1$  is surjective. So,  $\exists y \in B_1$  such that  $\beta_1(y) = x$ . Consider  $g(y)$ .  $g(y) \in \ker \beta_2$ , since

$$\beta_2 \circ g(y) \stackrel{\dagger}{=} h \circ \beta_1(y) = h(x) \stackrel{\ddagger}{=} 0$$

$\dagger$ : from the commutativity of the diagram

$\ddagger$ :  $x \in \ker h$

(3) Then exactness of  $B_2$  implies  $\ker \beta_2 = \text{im } \alpha_2$ . So,  $g(y) \in \text{im } \alpha_2$ . Since  $\alpha_2$  is injective, there is a unique element  $z \in A_2$  such that  $\alpha_2(z) = g(y)$ . (4) The natural projection maps  $z$  to  $z + \text{im } f$ .

Therefore,

$$\boxed{\delta(x) := z + \text{im } f}$$

It remains to prove that  $\delta$  is well-defined and a homomorphism. Also,  $\delta$  makes  $\ker h$  and  $\text{coker } f$  being exact.

The well-definedness starts from this  $x \in \ker h$ . The first time we choose a representative is in  $\beta_1^{-1}(\{x\})$ . Suppose that there are two  $y_1, y_2 \in B_1$  such that  $\beta_1(y_1) = \beta_1(y_2) = x$ . Because  $\beta_1(y_1 - y_2) = \beta_1(y_1) - \beta_1(y_2) = 0$ ,  $y_1 - y_2 \in \ker \beta_1 = \text{im } \alpha_1$ . So,  $\exists w \in A_1$ , making  $y_1 - y_2 = \alpha_1(w)$ . In the definition of  $\delta$ , for  $g(y_1), g(y_2)$  (all of them  $\in \ker \beta_2 = \text{im } \alpha_2$ ),  $\exists!$  elements  $z_1, z_2 \in A_2$  so that  $\alpha_2(z_1) = g(y_1), \alpha_2(z_2) = g(y_2)$ . Notice that

$$\alpha_2(f(w)) \stackrel{\dagger}{=} g(y_1 - y_2) \stackrel{\ddagger}{=} \alpha_2(z_1 - z_2)$$

$\dagger$ :  $\alpha_2(f(w)) = g(\alpha_1(w)) = g(y_1 - y_2)$

$\ddagger$ :  $\alpha_2(z_1 - z_2) = \alpha_2(z_1) - \alpha_2(z_2) = g(y_1) - g(y_2) = g(y_1 - y_2)$

Since  $\alpha_2$  is injective,  $z_1 - z_2 = f(w) \in \text{im } f$ , showing that  $\delta$  is well-defined.

### Exactness at each position:

- The exactness of  $\ker g$ :  $\text{im } \alpha_1^\circ \subseteq \ker \beta_1^\circ$  is because  $\forall x \in \ker f, (\beta_1^\circ \circ \alpha_1^\circ)(x) = (\beta_1 \circ \alpha_1)(x) = 0$ .

To see  $\ker \beta_1^\circ \subseteq \text{im } \alpha_1^\circ$ , let's start from an arbitrary element  $x \in \ker \beta_1^\circ = \ker g \cap \ker \beta_1$ . Rewriting  $\text{im } \alpha_1^\circ$ ,  $\text{im } \alpha_1^\circ = \alpha_1(\ker f)$ . For one thing,  $x \in \ker \beta_1$ . So,  $\exists a \in A_1, x = \alpha_1(a)$ . For another thing,  $x \in \ker g$ . Hence,  $0 = g(x) =$

$g(\alpha_1(a)) = \alpha_2(f(a))$ .  $\alpha_2$  is a monomorphism. Therefore,  $f(a) = 0$  and  $a \in \ker f$ .

- Exactness of  $\ker h$ :
- Exactness of  $\text{coker } f$ :
- Exactness of  $\text{coker } g$ :

□

### Theorem 3.1: Sequence of complexes to sequence of homology

Let  $0 \rightarrow A_\bullet \xrightarrow{\alpha_\bullet} B_\bullet \xrightarrow{\beta_\bullet} C_\bullet \rightarrow 0$  be a short exact sequence of  $R$ -complexes. This  $R$ -complex induces a long exact sequence of homology:

$$\dots \xrightarrow{\beta_{n+1}} H_{n+1}(C_\bullet) \xrightarrow{\delta_{n+1}} \boxed{H_n(A_\bullet) \xrightarrow{\alpha_n} H_n(B_\bullet) \xrightarrow{\beta_n} H_n(C_\bullet)} \xrightarrow{\delta_n} \boxed{H_{n-1}(A_\bullet) \xrightarrow{\alpha_{n-1}} H_{n-1}(B_\bullet) \xrightarrow{\beta_{n-1}} H_{n-1}(C_\bullet)} \xrightarrow{\delta_{n-1}} \dots$$

**Proof:**

### Lemma 3.2: Naturality of the triangle

## 4 Injective, Projective and Flat modules

### 4.1 Definitions and properties

### 4.2 Resolutions

#### Definition 4.1: Projective, Injective resolutions and Enough projective/Injective

Let  $\mathcal{A}$  be an abelian category. Let  $M \in \text{Ob}(\mathcal{A})$ .

An **injective resolution** of  $M$  is an *exact* sequence

$$\mathbf{I} : 0 \rightarrow M \xrightarrow{\eta} I_0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} I_2 \xrightarrow{d^2} \dots$$

such that  $\forall j \geq 0$ ,  $I_j$  is injective.

A **projective resolution** of  $M$  is an *exact* sequence

$$\mathbf{P} : \dots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \rightarrow 0$$

such that  $\forall j \geq 0$ ,  $P_j$  is projective.

**A** is **enough injective**  $\Leftrightarrow \forall M \in \text{Ob}(\mathbf{A})$ ,  $M$  has an injective resolution.

**A** is **enough projective**  $\Leftrightarrow \forall M \in \text{Ob}(\mathbf{A})$ ,  $M$  has a projective resolution.

**Remark** Beyond injective and projective resolutions, the notion *deleted injective resolution* and *deleted projective resolution* are useful:

A **deleted injective resolution** of  $M$  is the *complex*

$$\mathbf{I}^M : 0 \rightarrow I_0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} I_2 \xrightarrow{d^2} \dots$$

Similarly, a **deleted surjective resolution** of  $M$  is the *complex*

$$\mathbf{P}_M : \dots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \rightarrow 0$$

These deleted forms do not cause any loss of information comparing to the original complex. For the deleted injective resolution case,  $M \cong \eta(M) = \text{im } \eta = \ker d^0$ . So,  $M$  is engraved in the kernel of  $d^0$ . For projective (or free, flat) case, deleting loses nothing, for  $\text{coker } d_1 \cong M$ .

The reverse process, recovering a resolution from its deleted form is called *augmenting*.

After this definition, a very natural question is: Do projective and injective resolutions exist for every objects of every abelian category, or at least for a special kind of abelian category,  $\mathbf{RMod}$ . The answer should be positive. Otherwise, the definition is not useful enough. The next theorem gives a definite answer to this question.

### Proposition 4.1: Existence of resolutions in $\text{RMod}$

#### Definition 4.2: Syzygy and cosyzygy

Let  $\mathcal{A}$  be an abelian category. Let  $M \in \text{Ob}(\mathcal{A})$ .

For an injective resolution of  $M$ ,  $\mathbf{I} : 0 \rightarrow M \xrightarrow{\eta} I_0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} I_2 \xrightarrow{d^2} \cdots$ , define  $V_0 := \text{coker } \eta$  and  $\forall n \geq 0$ ,  $V_n := \text{coker } d^{n-1}$ . Then,  $V^n$  is the  $n$ -th **cosyzygy** of  $\mathbf{I}$ .

For a projective resolution of  $M$ ,  $\mathbf{P} : \cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \rightarrow 0$ , define  $K_0 := \ker \epsilon$  and  $\forall n \geq 1$ ,  $K_n := \ker d_n$ . Then,  $K_n$  is the  $n$ -th **syzygy** of  $\mathbf{P}$ .

Another definition is 'flat resolution'. It arises analogous to projective and injective resolutions but does not appear very often.

#### Definition 4.3: Flat resolution

## 5 Derived functors

### 5.1 Homotopic morphisms between complexes

#### Definition 5.1: Homotopic morphisms

Let  $f_\bullet, g_\bullet$  be two extensions of  $f$  as morphisms between two complexes  $(P_\bullet, d_\bullet)$  and  $(Q_\bullet, d'_\bullet)$  as follows:

$$\begin{array}{ccccccc} \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 \xrightarrow{\epsilon} A \longrightarrow 0 \\ & & f_2 \downarrow h_2 & & f_1 \downarrow h_1 & & f_0 \downarrow h_0 \\ \dots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} & Q_0 \xrightarrow{\epsilon'} B \longrightarrow 0 \end{array}$$

$f_\bullet$  and  $g_\bullet$  are called **homotopic**, denoted  $f_\bullet \simeq g_\bullet \Leftrightarrow \exists$  homomorphisms  $s_i : P_i \rightarrow Q_{i+1}$  for all  $i$  such that the following relation holds

$$\forall n, f_n - h_n = s_{n-1} \circ d_n + d'_{n+1} \circ s_n$$

#### Lemma 5.1: Homotopy induces same map on homology

If  $f_\bullet \simeq g_\bullet$ , then they induces the same map  $H_\bullet(P_\bullet) \rightarrow H_\bullet(Q_\bullet)$  on homology.

### Lemma 5.2: Comparison lemma

If there is a commutative diagram of two rows of complexes

$$\begin{array}{ccccccc} \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 \xrightarrow{\epsilon} A \longrightarrow 0 \\ & & & & & & \downarrow f \\ \dots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} & Q_0 \xrightarrow{\epsilon'} B \longrightarrow 0 \end{array}$$

where  $P_\bullet \rightarrow A \rightarrow 0$  is a projective resolution of  $A$  and  $Q_\bullet \rightarrow B \rightarrow 0$  is exact, then  $\exists$  a morphism of complex  $f_\bullet$  which extends  $f$ .

$$\begin{array}{ccccccc} \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 \xrightarrow{\epsilon} A \longrightarrow 0 \\ & & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 \\ \dots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} & Q_0 \xrightarrow{\epsilon'} B \longrightarrow 0 \end{array}$$

Moreover, any two such morphisms extending  $f$  are homotopic to each other.

**Proof:** First, we will prove the existence by induction:

(1.1) Base case: since the lower row is exact, the map  $Q_0 \twoheadrightarrow B$  is surjective. The projectivity of  $P_0$  implies the existence of  $f_0$  which makes the following diagram commute:

$$\begin{array}{ccccc} & & P_0 & & \\ & \nearrow \exists f_0 & \downarrow \epsilon & \searrow f \circ \epsilon & \\ Q_0 & \xrightarrow{\epsilon'} & A & \xrightarrow{f} & B \longrightarrow 0 \end{array}$$

(1.2) Inductive hypothesis+inductive step: suppose that  $\exists f_0, f_1, \dots, f_n$  where each  $f_i$  makes the square formed by  $P_{i-1}, Q_{i-1}, P_i, Q_i$  commute. So, we have the diagram

$$\begin{array}{ccccc} & & P_{n+1} & & \\ & & \downarrow f_n \circ d_{n+1} & & \\ Q_{n+1} & \xrightarrow{d'_{n+1}} & Q_n & \xrightarrow{d'_n} & Q_{n-1} \end{array}$$

The problem is  $d'_{n+1}$  is not necessarily surjective and  $d'_n$  might not goes to zero. To use the projectivity of  $P_{n+1}$ ,  $Q_n$  can be replaced by  $\ker d'_n = \text{im } d'_{n+1}$ .

One thing is left to check: to make the map  $f_n \circ d_{n+1} : P_{n+1} \rightarrow Q_n$  work,  $\text{im } f_n \circ d_{n+1} \subseteq \text{im } d'_{n+1} = \ker d'_n$  remains to check. But this is true from the following:  $\forall x \in P_{n+1}$ ,

$$d'_n \circ (f_n \circ d_{n+1})(x) = (d'_n \circ f_n) \circ d_{n+1}(x) \stackrel{\dagger}{=} (f_{n-1} \circ d_n) \circ d_{n+1}(x) = f_{n-1} \circ (d_n \circ d_{n+1})(x) \stackrel{\ddagger}{=} 0$$

$\dagger$ : from the commutativity of the square

$\ddagger$ : because the upper row is a complex

Hence, the projectivity of  $P_{n+1}$  implies the existence of  $f_{n+1}$  which makes the square consisting of  $P_{n+1}, P_n, Q_{n+1}$  and  $Q_n$  commute.

$$\begin{array}{ccccc} & & P_{n+1} & & \\ & \nearrow \exists f_{n+1} & \downarrow f_n \circ d_{n+1} & & \\ Q_{n+1} & \xrightarrow{\text{im } d'_{n+1}} & \text{im } d'_{n+1} & \xrightarrow{d'_n} & 0 \end{array}$$

Second, suppose that there are two morphisms of these complexes which are homotopic, i.e.  $\exists f_\bullet \simeq g_\bullet$ . Equivalently, let  $g_n := f_n - h_n$ , then we want to construct  $\{s_n\}_n$  making the following diagram commute:

$$\begin{array}{ccccccc}
& \cdots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} P_0 \xrightarrow{0} 0 \\
& & s_2 \swarrow & \downarrow g_2 & s_1 \swarrow & \downarrow g_1 & s_0 \swarrow \quad \downarrow g_0 \quad s_{-1} \swarrow \\
& \cdots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} Q_0 \xrightarrow{0} 0
\end{array}$$

where each square is a commutative diagram. The commutativity of each square comes from the commutativity concerning  $f_n$  and  $g_n$ .

- for  $s_{-1}$ ,  $s_{-1} = 0$
- for  $s_0$ : Notice that  $B$  is deleted, so the lower sequence might not be exact at  $Q_0$  in this new sequence. Using the exactness of the old sequence, let's replace  $Q_0$  by  $\text{im}d'_{n+1} = \ker \epsilon'$ . As the argument above, the well-definedness of  $g_0 : P_0 \rightarrow \text{im}d'_{n+1}$  is from:

$$\epsilon' \circ f_0 = \epsilon' \circ g_0 = f \circ \epsilon \Rightarrow \epsilon' \circ g_0 = 0 \Leftrightarrow \text{im}g_0 \subseteq \ker \epsilon' = \text{im}d'_1$$

Then, the projectivity of  $P_1$  implies the existence of  $s_0$  such that  $g_0 = d'_1 \circ s_0 + s_{-1} \circ d'_0$ , where  $d'_0 := 0$ .

$$\begin{array}{ccc}
& P_0 & \\
\exists s_0 \swarrow & \downarrow g_0 & \\
Q_1 & \xrightarrow{d'_1} \text{im}d'_1 & \xrightarrow{0} 0
\end{array}$$

- Suppose this works for all  $s_0, s_1, \dots, s_{n-1}$  and the equation  $g_i = d'_{i+1} \circ s_i + s_{i-1} \circ d_i$  holds for each  $s_i$  ( $i \leq n-1$ ). Then, still, we can replace each  $Q_n$  by  $\text{im}d'_{n+1}$ . There is a subtlety: we need to check  $\text{im}(g_n - s_{n-1} \circ d_n) \subseteq \text{im}d'_{n+1}$ . The exactness at each  $Q_n \Rightarrow \ker d'_n = \text{im}d'_{n+1}$ . So, it suffices to check  $d'_n \circ (g_n - s_{n-1} \circ d_n) = 0$ ,

$$d'_n \circ (g_n - s_{n-1} \circ d_n) \stackrel{\dagger}{=} g_{n-1} \circ d_n - (d'_n \circ s_{n-1}) \circ d_n \stackrel{\ddagger}{=} g_{n-1} \circ d_n - (g_{n-1} - s_{n-2} \circ d_{n-1}) \circ d_n = -s_{n-2} \circ (d_{n-1} \circ d_n) \stackrel{\dagger\dagger}{=} 0$$

$$\dagger: d'_n \circ g_n = g_{n-1} \circ d_n$$

$$\ddagger: \text{By assumption, } g_{n-1} = d'_n \circ s_{n-1} + s_{n-2} \circ d_{n-1}.$$

$$\dagger\dagger: \text{The upper chain is a complex. Hence, } d_{n-1} \circ d_n = 0.$$

Hence, the projectivity of  $P_{n+1}$  implies the existence of  $s_{n+1}$  such that the following diagram commutes:

$$\begin{array}{ccc}
& P_{n+1} & \\
\exists s_{n+1} \swarrow & \downarrow g_n - s_{n-1} \circ d_n & \\
Q_{n+1} & \xrightarrow{d'_{n+1}} \text{im}d'_{n+1} & \xrightarrow{d'_n} 0
\end{array}$$

The commutativity of this diagram is exactly the equation  $g_n = s_{n-1} \circ d_n + d'_{n+1} \circ s_{n+1}$ , showing that  $f_\bullet \simeq g_\bullet$ .  $\square$

## 5.2 Left derived functors

Left(right) derived functors are defined for right-exact functors(left-exact). One way to think of left-derived(right-derived) functors is to consider them as recovering the information being lost by right-exact functors(correspondingly, left-exact functors): Suppose  $F$  is a right exact functor between two abelian categories,  $\mathcal{A}$  and  $\mathcal{C}$ ,  $F : \mathcal{A} \rightarrow \mathcal{C}$ . So, applying  $F$  to an exact sequence  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ , there is a right exact sequence  $FA \rightarrow FB \rightarrow FC \rightarrow 0$ . This  $F$  guarantees the exactness at  $FB$  and  $FC$ . But, it loses the information of exactness of  $FA$ , in other words, the injectivity of  $FA \rightarrow FB$ . To measure the loss of injectivity,  $\ker(FA \rightarrow FB)$  is a good candidate because ??

Let's try to give the definition of left-derived functor of another functor:

Let  $F : \mathcal{A} \rightarrow \mathcal{C}$  be a right-exact covariant functor between two abelian categories, where  $\mathcal{A}$  is enough projective. Let  $A, B \in \text{Ob}(\mathcal{A})$  be arbitrary objects and  $f \in \text{Mor}_{\mathcal{A}}(A, B)$  be an arbitrary morphism. The *left derived functor* of  $F$  at  $n$ , denoted  $L_n F$ , is defined by the action on  $A, B$  and  $f$  as follows:

- For objects, take the projective resolutions of  $A$  and  $B$ . Then, we get two exact sequences which are projective resolutions of  $A$  and  $B$

$$\begin{aligned}
\mathbf{P}: \cdots & \xrightarrow{\tilde{d}_3} P_2 \xrightarrow{\tilde{d}_2} P_1 \xrightarrow{\tilde{d}_1} P_0 \xrightarrow{\tilde{d}_0} A \longrightarrow 0 \\
\mathbf{Q}: \cdots & \xrightarrow{\tilde{d}'_3} Q_2 \xrightarrow{\tilde{d}'_2} Q_1 \xrightarrow{\tilde{d}'_1} Q_0 \xrightarrow{\tilde{d}'_0} B \longrightarrow 0
\end{aligned}$$

Let  $\mathbf{P}_A$  and  $\mathbf{Q}_B$  be the  $A$ -deleted sequence and  $B$ -deleted sequences, respectively. Since there is a morphism  $f : A \rightarrow B$ , by the Comparison lemma 5.2, a morphism between two sequences,  $f_\bullet = \{f_n\}_n$ , can be constructed between two deleted sequences  $\mathbf{P}_A$  and  $\mathbf{Q}_B$  Exactness of deleted sequences

$$\begin{array}{ccccccc} \mathbf{P}_A : & \cdots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} P_0 \xrightarrow{d_0} 0 \\ & \downarrow f_\bullet & & \downarrow f_2 & & \downarrow f_1 & \downarrow f_0 \\ \mathbf{Q}_B : & \cdots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} Q_0 \xrightarrow{d'_0} 0 \end{array}$$

where the maps  $d_i = \tilde{d}_i$  for all  $i \geq 1$  and  $d_0 := 0$ , the maps  $d'_i := \tilde{d}'_i$  for all  $i \geq 1$  and  $d'_0 := 0$ . The right-exact functor  $F$  induces these chains and morphism in  $\mathcal{C}$  as

$$\begin{array}{ccccccc} F\mathbf{P}_A : & \cdots & \xrightarrow{Fd_3} & FP_2 & \xrightarrow{Fd_2} & FP_1 & \xrightarrow{Fd_1} FP_0 \xrightarrow{Fd_0} 0 \\ \downarrow Ff_\bullet & & & \downarrow Ff_2 & & \downarrow Ff_1 & \downarrow Ff_0 \\ F\mathbf{Q}_B : & \cdots & \xrightarrow{Fd'_3} & FQ_2 & \xrightarrow{Fd'_2} & FQ_1 & \xrightarrow{Fd'_1} FQ_0 \xrightarrow{Fd'_0} 0 \end{array}$$

So,  $L_n F$  acting on  $A$  as  $[L_n F(A) := H_n(F\mathbf{P}_A)]^1$ . In particular,  $L_0 F(A) = F(A)$ , since  $L_0 F(A) := \ker Fd_0 / \text{im } Fd_1 \cong F(A)$ .

$\dagger$ : Truncating the long sequence  $\mathbf{P}$  into  $P_1 \rightarrow P_0 \rightarrow A \rightarrow 0$ , apply the right-exactness of  $F$  to this truncated sequence. Then,  $F(P_0)$  is exact. Hence,  $\text{im } Fd_1 = \ker Fd_0$ . Exactness of  $FA \Rightarrow FP_0 \rightarrow FA$  is a surjective homomorphism. With  $FP_0 = \ker Fd_0$  and  $\text{im } Fd_0 = \text{im } Fd_0$ ,  $FP_0 / \ker Fd_0 \cong F(A)$ .

As a functor, we have

$$[L_0 F \cong F]$$

$\cong$  in what sense

- For morphisms, let  $f : A \rightarrow B$  be a morphism in the category  $\mathcal{A}$ .  $L_n F$  has a natural way sending  $f$  to  $L_n F(f)$ .  $L_n F$  just goes into the category  $\mathbf{Comp}(\mathcal{C})$  and applies the functor  $H_n$  to objects there. Analogously, apply  $H_n$  to the morphism  $Ff_\bullet$ . The 'natural' definition is  $[L_n F(f) := H_n(Tf_\bullet)]$ . Explicitly:

$$L_n F(f) : H_n(F\mathbf{P}_A) =: L_n F(A) \longrightarrow L_n F(B) := H_n(F\mathbf{P}_B) \quad z + \text{im } Fd_{n+1} \mapsto Ff_n(z) + \text{im } Fd'_{n+1}$$

The definition of  $L_n F$  is completed, the work flow of defining  $L_n F$  is illustrated in the following diagram:

$$\begin{array}{ccc} \mathcal{A} & & A \xrightarrow{f} B \\ \downarrow & \curvearrowright \mathbf{Comp}(\mathcal{A}) & \downarrow \\ \mathbf{Comp}(\mathcal{A}) & & (P_\bullet^A, d_\bullet^A) \xrightarrow{f_\bullet} (P_\bullet^B, d_\bullet^B) \\ \downarrow F & \curvearrowright L_n F & \downarrow F \\ \mathbf{Comp}(\mathcal{C}) & & (FP_\bullet^A, Fd_\bullet^A) \xrightarrow{Ff_\bullet} (FP_\bullet^B, Fd_\bullet^B) \\ \downarrow H_n & \curvearrowright \mathcal{C} & \downarrow H_n \\ \mathcal{C} & & H_n(FP_\bullet^A, Fd_\bullet^A) \xrightarrow{H_n Ff_\bullet} H_n(FP_\bullet^B, Fd_\bullet^B) \end{array}$$

There is some subtlety on the definition:  $L_F(A)$  depends on the choice of some resolution of  $A$ . It is crucial to make sure that two different resolutions never lead to different  $L_n F(A)$ . Otherwise, it would be problematic. To prove the two facts: independence of resolution and being an additive functor. The following two lemmas are needed.

**Lemma 5.1 (Homotopy commutes with additive functors)** *Let  $\mathcal{A}, \mathcal{C}$  be abelian categories and  $F : \mathcal{A} \rightarrow \mathcal{C}$  be an additive functor. Then, homotopic extended morphisms of complexes in  $\mathcal{A}$  is still homotopic after applying  $F$ . More precisely, let  $(X_\bullet, d_\bullet^X)$  and  $(Y_\bullet, d_\bullet^Y)$  be two complexes of  $\mathcal{A}$ . If  $f_\bullet, g_\bullet : (X_\bullet, d_\bullet^X) \rightarrow (Y_\bullet, d_\bullet^Y)$  are two morphisms such that  $f_\bullet \simeq g_\bullet$ , then  $Ff_\bullet \simeq Fg_\bullet$ .*

**Proof:** (1)  $\{F(f_n)\}_n$  and  $\{F(g_n)\}_n$  are lifts/extensions of  $Ff$  and  $Fg$  respectively:

Let's denote  $h_\bullet := \{F(f_n)\}_n$  and  $k_\bullet := \{F(g_n)\}_n$ . The assumption  $f_\bullet \simeq g_\bullet$  implies the existence of  $\{s_i\}_{i \geq -1}$ , such that  $\forall n, f_n - g_n = d_{n+1}^Y \circ s_n + s_{n-1} \circ d_n^X$  (\*). Apply the functor  $F$  to (\*). Using the additivity and functoriality of  $F$ , we have

$$\forall n, F(f_n) - F(g_n) = F(d_{n+1}^Y) \circ F(s_n) + F(s_{n-1}) \circ F(d_n^X)$$

<sup>1</sup>This definition is not meaningless. If there is an sequence  $P_\bullet$  that is exact at each place, the sequence being applied by a right-exact functor  $FP_\bullet$  is not necessarily exact at each position. We will see a classical counterexample,  $(-) \otimes M$ .

Since each  $F(f_n) : F(X_n) \rightarrow F(Y_n)$  is a morphism that makes every square in the induced morphism  $Ff_\bullet$  commutative,  $\{F(f_n)\}_n$  serves as an extension of  $Ff$ . So is  $F(g_n)$ . Define  $s'_i := F(s_i)$ . The existence of  $\{s'_i\}_i$  yields  $h_\bullet \simeq k_\bullet$ .

(2.) Consider arbitrary extensions,  $(Ff)_\bullet$  and  $(Fg)_\bullet$ , of  $Ff$  and  $Fg$ , respectively. We have

$$(Ff)_\bullet \xrightarrow{\dagger} h_\bullet \xrightarrow{(2.1)} k_\bullet \xrightarrow{\dagger} (Fg)_\bullet$$

†: By comparison lemma 5.2, both  $(Ff)_\bullet$  and  $h_\bullet$  are extensions of  $Ff$  and both  $(Fg)_\bullet$  are extensions of  $k_\bullet$ .  $\square$

**Lemma 5.2 (Homotopy induces same homology)** *In an abelian category  $\mathcal{C}$ , if two maps between two complexes  $\phi_\bullet, \psi_\bullet : (X_\bullet, d_\bullet^X) \rightarrow (Y_\bullet, d_\bullet^Y)$ , are two morphisms such that  $\phi_\bullet \simeq \psi_\bullet$ , then  $\forall n, H_n(\phi_\bullet) = H_n(\psi_\bullet)$ .*

**Proof:**  $\phi_\bullet \simeq \psi_\bullet$  implies that  $\exists$  a collection of morphisms,  $\{s_n : X_n \rightarrow Y_{n+1}\}_n$ , such that  $\phi_n - \psi_n = d_{n+1}^Y \circ s_n + s_{n-1} \circ d_n^X$ . Evaluating this map at an element  $w \in \ker d_n^X$ ,

$$(\phi_n - \psi_n)(w) = (d_{n+1}^Y \circ s_n)(w) + (s_{n-1} \circ d_n^X)(w) \xrightarrow{d_n^X(w)=0} d_{n+1}^Y(s_n(w))$$

Hence,  $\forall w \in \ker d_n^X, \forall n, \phi_n(w) - \psi_n(w) \in \text{im} d_{n+1}^Y \Rightarrow \forall w, \forall n, [\phi_n(w)] = [\psi_n(w)]$ , implying that  $H_n(\phi_\bullet) = H_n(\psi_\bullet)$ , for  $H_n(\phi_\bullet) : [w] \mapsto [\phi_n(w)]$  and  $H_n(\psi_\bullet) : [w] \mapsto [\psi_n(w)]$ .  $\square$

### Theorem 5.1: Independency of choice of resolution

The definition of  $L_n F$  for an additive functor  $F : \mathcal{A} \rightarrow \mathcal{C}$  between two abelian categories is independent of the choice of resolutions. More precisely, if  $P_\bullet : \mathbf{P}_A \rightarrow A \rightarrow 0$  and  $Q_\bullet : \mathbf{Q}_A \rightarrow A \rightarrow 0$  are two projective resolutions of  $A$ , then  $H_n(F\mathbf{P}_A) \cong H_n(F\mathbf{Q}_A)$ .

**Remark** This enlightens us how to calculate the  $L_n F(A)$  for some  $A \in \text{Ob}(\mathcal{A})$ , because the resolution of  $A$  can be chosen as simple as possible.

**Proof:** Let  $P_\bullet : \mathbf{P}_A \rightarrow A \rightarrow 0$  and  $Q_\bullet : \mathbf{Q}_A \rightarrow A \rightarrow 0$  be two projective resolutions of  $A$ . The comparison lemma 5.2 extends the identity map  $\text{id}_A$  between  $P_\bullet$  and  $Q_\bullet$  to  $f_\bullet, Q_\bullet$  and  $P_\bullet$  to  $g_\bullet$  illustrated as follows:

$$\begin{array}{ccccccc} P_\bullet : & \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \longrightarrow 0 \\ \downarrow f_\bullet & & & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow \text{id}_A \\ Q_\bullet : & \dots & \xrightarrow{d'_3} & Q_2 & \xrightarrow{d'_2} & Q_1 & \xrightarrow{d'_1} Q_0 \xrightarrow{d'_0} A \longrightarrow 0 \\ \downarrow g_\bullet & & & \downarrow g_2 & & \downarrow g_1 & & \downarrow g_0 & & \downarrow \text{id}_A \\ P_\bullet : & \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \longrightarrow 0 \end{array}$$

Notice that  $g_\bullet \circ f_\bullet \simeq (\text{id}_A)_\bullet$  by the diagram. Applying  $F$  to this homotopy and applying the lemma 5.1, we have

$$F(g_\bullet \circ f_\bullet) \simeq F((\text{id}_A)_\bullet)$$

By functoriality of  $F$ , the left hand side is  $F(g_\bullet \circ f_\bullet) = F(g_\bullet) \circ F(f_\bullet)$  and the right hand side is  $F((\text{id}_A)_\bullet) = (\text{id}_{F(A)})_\bullet$ . The lemma 5.2 further implies that  $H_n(F(g_\bullet \circ f_\bullet)) = H_n(F((\text{id}_A)_\bullet))$ . Hence,

$$L_n F(g_\bullet \circ f_\bullet) = L_n F((\text{id}_A)_\bullet)$$

Functoriality of  $H_n$  implies that  $L_n F(g_\bullet \circ f_\bullet) = L_n F(g_\bullet) \circ L_n F(f_\bullet)$  and  $L_n F((\text{id}_A)_\bullet) = \text{id}_{L_n F A}$ . So,

$$L_n F(g_\bullet) \circ L_n F(f_\bullet) = \text{id}_{L_n F A}$$

showing that  $L_n F(f_\bullet) : L_n F(P_\bullet) \rightarrow L_n F(Q_\bullet)$  is an isomorphism.  $\square$

It remains to check that  $L_n F$  is indeed a functor.

### Theorem 5.2: Functoriality of 'Left-derived functors'

Let  $\mathcal{A}, \mathcal{C}$  be two abelian categories and  $\mathcal{A}$  is enough projective. If  $F : \mathcal{A} \rightarrow \mathcal{C}$  is an additive covariant (contravariant) functor, then  $\forall n, L_n F : \mathcal{A} \rightarrow \mathcal{C}$  is also an additive covariant (contravariant) functor.

**Proof:** *Claim 1:*  $(f + g)_\bullet \simeq f_\bullet + g_\bullet$ .

$\forall X, Y \in \text{Mor}_{\mathcal{A}}(X, Y)$ , fix resolutions of  $X$  and  $Y$ . The left hand side is an arbitrary extension morphisms of  $f + g$  between fixed resolutions. The right hand side is elementwise defined as  $(f_\bullet + g_\bullet)_n := (f_\bullet)_n + (g_\bullet)_n = f_n + g_n$ . The fact that each  $f_n + g_n : X_n \rightarrow Y_n$  is a morphism ( $\mathcal{A}$  is additive) and the commutativity **more** of diagram shows that  $f_\bullet + g_\bullet$  is also an extension of  $f + g$ . By the comparison lemma 5.2, they are homotopic to each other.

With lemmas 5.1, 5.2, it is straightforward to show: •  $L_n F$  is a covariant functor; •  $L_n F$  is additive.

$L_n F$  is a functor: **need**

Additivity: From claim 1 and 2,  $F(f + g)_\bullet \simeq F(f_\bullet + g_\bullet) \stackrel{\clubsuit}{=} Ff_\bullet + Fg_\bullet$ , where  $\clubsuit$  is by the additivity of  $F$ . Overall,

$$L_n F((f + g)_\bullet) = H(F(f + g)_\bullet) \xrightarrow{\text{Lemma 5.2}} H(Ff_\bullet + Fg_\bullet) = L_n F(f) + L_n F(g)$$

□

## 5.3 Right derived functors

### 5.3.1 Covariant right derived functors

Still, let  $F : \mathcal{A} \rightarrow \mathcal{C}$  be a left-exact covariant functor between two abelian categories, where  $\mathcal{A}$  is enough injective. Let  $A, B \in \text{Ob}(\mathcal{A})$  be arbitrary objects and  $f \in \text{Mor}_{\mathcal{A}}(A, B)$  be an arbitrary morphism. The *right derived functor* of  $F$  at  $n$ , denoted  $R^n F$ , is defined by the action on  $A, B$  and  $f$  as follows:

- For objects, take the injective resolutions of  $A$  and  $B$ . Then, we get two exact sequences which are injective resolutions of  $A$  and  $B$

$$\begin{aligned} \mathbf{I} : \quad 0 &\longrightarrow A \xrightarrow{\eta} I_0 \xrightarrow{d^0} I_1 \xrightarrow{d^1} I_2 \xrightarrow{d^2} \dots \\ \mathbf{J} : \quad 0 &\longrightarrow B \xrightarrow{\eta'} J_0 \xrightarrow{d^0} J_1 \xrightarrow{d'^1} J_2 \xrightarrow{d^2} \dots \end{aligned}$$

Let  $\mathbf{I}^A$  and  $\mathbf{J}^B$  be the  $A$ -deleted sequence and  $B$ -deleted sequences, respectively. Since there is a morphism  $f : A \rightarrow B$ , by the Comparison lemma 5.2, a morphism between two sequences,  $f_\bullet = \{f_n\}_n$ , can be constructed between two deleted sequences  $\mathbf{I}^A$  and  $\mathbf{J}^B$  **Exactness of deleted sequences**

$$\begin{array}{ccccccc} \mathbf{I}^A : & 0 & \longrightarrow & I_0 & \xrightarrow{d^0} & I_1 & \xrightarrow{d'^1} & I_2 & \xrightarrow{d^2} \dots \\ & \downarrow f_\bullet & & \downarrow f_0 & & \downarrow f_1 & & \downarrow f_2 & \\ \mathbf{J}^B : & 0 & \longrightarrow & J_0 & \xrightarrow{d'^0} & J_1 & \xrightarrow{d'^1} & J_2 & \xrightarrow{d'^2} \dots \end{array}$$

where the maps  $d_i = \tilde{d}_i$  for all  $i \geq 1$  and  $d_0 := 0$ , the maps  $d'_i := \tilde{d}'_i$  for all  $i \geq 1$  and  $d'_0 := 0$ . The right-exact functor  $F$  induces these chains and morphism in  $\mathcal{C}$  as

$$\begin{array}{ccccccc} F\mathbf{P}_A : & \dots & \xrightarrow{Fd_3} & FP_2 & \xrightarrow{Fd_2} & FP_1 & \xrightarrow{Fd_1} & FP_0 \xrightarrow{Fd_0} 0 \\ & \downarrow Ff_\bullet & & \downarrow Ff_2 & & \downarrow Ff_1 & & \downarrow Ff_0 \\ F\mathbf{Q}_B : & \dots & \xrightarrow{Fd'_3} & FQ_2 & \xrightarrow{Fd'_2} & FQ_1 & \xrightarrow{Fd'_1} & FQ_0 \xrightarrow{Fd'_0} 0 \end{array}$$

So,  $L_n F$  acting on  $A$  as  $[L_n F(A) := H_n(F\mathbf{P}_A)]^2$ . In particular,  $L_0 F(A) = F(A)$ , since  $L_0 F(A) := \ker Fd_0 / \text{im } Fd_1 \cong^\dagger F(A)$ .

†: Truncating the long sequence  $\mathbf{P}$  into  $P_1 \rightarrow P_0 \rightarrow A \rightarrow 0$ , apply the right-exactness of  $F$  to this truncated sequence. Then,  $F(P_0)$  is exact. Hence,  $\text{im } Fd_1 = \ker Fd_0$ . Exactness of  $FA \Rightarrow FP_0 \rightarrow FA$  is a surjective homomorphism. With  $FP_0 = \ker Fd_0$  and  $\text{im } Fd_0 = \text{im } Fd_0$ ,  $FP_0 / \ker Fd_0 \cong F(A)$ .

As a functor, we have

$$[L_0 F \cong F]$$

**≈ in what sense**

- For morphisms, let  $f : A \rightarrow B$  be a morphism in the category  $\mathcal{A}$ .  $L_n F$  has a natural way sending  $f$  to  $L_n F(f)$ .

<sup>2</sup>This definition is not meaningless. If there is an sequence  $P_\bullet$  that is exact at each place, the sequence being applied by a right-exact functor  $F\mathbf{P}_\bullet$  is not necessarily exact at each position. We will see a classical counterexample,  $(-) \otimes M$ .

$L_n F$  just goes into the category  $\mathbf{Comp}(\mathcal{C})$  and applies the functor  $H_n$  to objects there. Analogously, apply  $H_n$  to the morphism  $Ff_\bullet$ . The 'natural' definition is  $[L_n F(f) := H_n(Ff_\bullet)]$ . Explicitly:

$$L_n F(f) : H_n(F\mathbf{P}_A) =: L_n F(A) \longrightarrow L_n F(B) := H_n(F\mathbf{P}_B) \quad z + \text{im}Fd_{n+1} \mapsto Ff_n(z) + \text{im}Fd'_{n+1}$$

The definition of  $L_n F$  is completed, the work flow of defining  $L_n F$  is illustrated in the following diagram:

$$\begin{array}{ccc} \mathcal{A} & & A \xrightarrow{f} B \\ \downarrow & \text{Comp}(\mathcal{A}) \curvearrowright & \downarrow \\ \mathcal{C} & \xrightarrow{L_n F} & (P_\bullet^A, d_\bullet^A) \xrightarrow{f_\bullet} (P_\bullet^B, d_\bullet^B) \\ \downarrow & \text{Comp}(\mathcal{C}) & \downarrow \\ & & (FP_\bullet^A, Fd_\bullet^A) \xrightarrow{Ff_\bullet} (FP_\bullet^B, Fd_\bullet^B) \\ \downarrow & H_n & \downarrow \\ H_n(FP_\bullet^A, Fd_\bullet^A) & \xrightarrow{H_n Ff_\bullet} & H_n(FP_\bullet^B, Fd_\bullet^B) \end{array}$$

### 5.3.2 Contravariant right-derived functors

## 5.4 Exact sequences and derived functors

### 5.5 A little summary

Let's recall the process how we define each two functors and compare the difference at the object level: let  $\mathcal{A}$  be an abelian category. For  $A, B \in \text{Ob}(\mathcal{A})$ ,

$$\begin{array}{ccc} A & & B \\ \downarrow \text{proj reso} & & \nearrow \text{inj reso} \\ \mathbf{P} & & \mathbf{I} \\ \downarrow \text{delete } A & & \downarrow \text{delete } B \\ \mathbf{P}_A & & \mathbf{I}_B \\ \downarrow F \text{ covariant} & & \downarrow F \text{ covariant} \\ F\mathbf{P}_A & & F\mathbf{I}_B \\ \downarrow & & \downarrow \\ L_n F(A) := H_n(F\mathbf{P}_A) & & R^n F(B) := H_n(F\mathbf{I}_B) \\ & & \\ & & \nearrow \text{proj reso} \\ & & \mathbf{P} \\ & & \downarrow \text{delete } B \\ & & \mathbf{P}_B \\ & & \downarrow G \text{ contravariant} \\ & & \mathbf{GP}_B \\ & & \downarrow \\ & & R^n G(B) := H_n(G\mathbf{P}_B) \end{array}$$

In each definition, the direction of the sequence applied by  $F$  is in the same direction. For  $L_n F$ , there is nothing to mention. For  $R^n F$  and  $R_n G$ ,  $\mathbf{FI}_B$  and  $\mathbf{GP}_B$  are in the same direction. Left and right derived functor depends on a functor  $F$ , so

Exactness and derived-functors				
Functors $F$	covariant		contravariant	
Exactness of $F$	right-exact	left-exact	right-exact	left-exact
Resolution applied	projective	injective	injective	projective
Derived functors applied	left-derived	right-derived	left-derived	right-derived
Examples of $F$	$(-) \otimes_R N$	$\text{Hom}_R(M, -), \Gamma(X, -), (-)^G$	uncommon	$\text{Hom}_R(-, N)$

From this table, one important observation is that the exactness of  $F$  and the direction of the derived functors are strongly related: the left-exact functor is binded with the right-derived functor, and the right-exact functor is binded with the left-derived functor. Each 'pack' of this property has no relation to any other properties.

## 6 Examples for left-derived functors

### 6.1 Tor functor

As we mentioned earlier,  $(-) \otimes_R M$  and  $\text{Hom}(-, M)$  are two very important examples for right-exact and left-exact functors respectively. In previous subsections, we deal with abstract categories and functors, the most general

abelian categories and additive functors. It is time to be down-to-earth and to embrace the categories and functors we are familiar with, the categories of  $R$ -modules  $_R\mathbf{Mod}$  or  $\mathbf{Mod}_R$ , and the functors  $(-) \otimes_R M$  together with  $\text{Hom}(-, M)$ .

### 6.1.1 Tor functor

Here we give the definition for Tor and  $\text{tor}$  functors and then show they are equivalent. For  $A \in \text{Ob}\mathbf{Mod}_R$  and  $B \in \text{Ob}_R\mathbf{Mod}$ , we have two covariant right-exact functors:  $(-) \otimes_R B$  and  $A \otimes_R (-)$ .

#### Definition 6.1: Tor and $\text{tor}$ functors

For  $A \in \text{Ob}\mathbf{Mod}_R$  and  $B \in \text{Ob}_R\mathbf{Mod}$ ,  $\text{Tor}$  and  $\text{tor}$  are defined to be the left-derived functors

$$\text{Tor}_n(-, B) := L_n((-) \otimes_R B) \quad \text{tor}_n(A, -) := L_n(A \otimes_R (-))$$

**Remark** Explicitly,

$$\text{Tor}_n(A, B) = L_n((-) \otimes_R B)(A) = H_n(((-) \otimes_R B)\mathbf{P}_A) = H_n(\mathbf{P}_A \otimes_R B)$$

and

$$\text{tor}_n(A, B) = H_n(A \otimes_R \mathbf{P}_B)$$

One nice result about these two functors is  $\forall n, \forall A, \forall B$ ,

$$\boxed{\text{Tor}_n(A, B) \cong \text{tor}_n(A, B)}$$

This is the theorem **ss**. To prove this, we need the following lemmas:

#### Corollary 6.1: Subscript reducing isomorphism

Let  $\mathcal{A}$  be an abelian category with enough projectives and  $A \in \text{Ob}(\mathcal{A})$ . Let  $P_\bullet$  be a projective resolution of  $A$ :

$$P_\bullet : \dots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \longrightarrow 0$$

Let  $K_0 := \ker \epsilon, \forall i \geq 1, K_i := \ker d_i$ . Then,

$$(L_{n+1}F)A \cong (L_nF)K_0 \cong (L_{n-1}F)K_1 \cong \dots \cong (L_1F)K_{n-1}$$

**Remark** In particular, when  $\mathcal{A} =_R \mathbf{Mod}$ ,  $B \in \text{Ob}(\mathcal{A})$  and  $F = (-) \otimes_R B$ , take the projective resolution of  $A$  and  $K_i$  as above. Then,

$$\text{Tor}_{n+1}(A, B) \cong \text{Tor}_n(K_0, B) \cong \text{Tor}_{n-1}(K_1, B) \cong \dots \cong \text{Tor}_1(K_{n-1}, B)$$

**Proof:** The basic idea is to shortcut the sequence so that the truncated sequence is a projective resolution of some element in the original sequence.

For the sake of consistency,  $\epsilon =: d_{-1}$  and  $A =: K_{-1}$ . Exactness of  $P_\bullet \Rightarrow K_0 := \ker d_{-1} = \text{im}d_0$ . So, the new sequence

$$\begin{array}{ccccccc} \dots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & K_0 \longrightarrow 0 \\ & & \parallel & & \parallel & & \parallel \\ P'_\bullet & \dots & \xrightarrow{\delta_2} & P'_1 & \xrightarrow{\delta_1} & P'_0 & \xrightarrow{\delta_0} K_0 \longrightarrow 0 \end{array}$$

is exact, where  $\forall n, P'_n = P_{n+1}$  and  $\delta_n := d_{n+1}$ . The lower sequence is hence a projective resolution of  $K_0$ . Let  $(P'_\bullet)^{K_0}$  be the deleted projective resolution of  $K_0$  and  $(P_\bullet)_A$  be the deleted projective resolution of  $A$ . We have  $\forall n$ ,

$$L_n F(K_0) \stackrel{\dagger}{\cong} H_n(FP'_\bullet) = \frac{\ker \delta_n}{\text{im} \delta_{n+1}} \quad \text{by definition of } K_0 \quad (1)$$

$$= \frac{\ker d_{n+1}}{\text{im} d_{n+2}} \quad \text{by definition of } \delta_n \quad (2)$$

$$= H_{n+1}(FP_\bullet^A) \stackrel{\dagger}{\cong} L_{n+1}F(A) \quad \text{by definition of } A \quad (3)$$

† from the theorem 5.1.

Iterating this process by truncating the sequence to  $K_1, \dots, K_n$ , those isomorphisms follows.

### Theorem 6.1: Equivalence of Tor and tor

Let  $A \in \text{Ob}(\mathbf{Mod}_R)$  and  $B \in \text{Ob}(_R\mathbf{Mod})$ . Then,  $\forall n$ ,  $\text{Tor}_n(A, B) \cong \text{tor}_n(A, B)$ .

**Proof:** (A.Zaks) This inducts on  $n$ .

Base case: when  $n = 0$ ,

Inductive hypothesis: Suppose that for  $n$ ,  $\text{Tor}_n(A, B) \cong \text{tor}_n(A, B)$ .

Inductive step: Consider a projective resolution of  $A$  and  $B$  respectively and factor it into SESs:

$$P_\bullet : \cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} A \rightarrow 0 \quad Q_\bullet : \cdots \xrightarrow{d'_2} Q_1 \xrightarrow{d'_1} Q_0 \xrightarrow{\epsilon'} B \rightarrow 0$$

The factorization of  $P_\bullet$  by syzygies into short exact sequence is:

X 0 W

Y

**Remark** There is another direct proof. That version would not be introduced until the spectral sequence is studied.

In this proof, the projective resolution is not fully exploited. Each module in this projective resolution is projective hence flat. The proof only utilizes the flatness of each term in the resolution. So, instead, the Tor and tor functor can be defined by taking flat resolutions (see [Rot09]).

### 6.1.2 Axiomatic characterization of $\text{Tor}_n$ functors

### 6.1.3 Applications of Tor functor

From now on,  $R$  is an integral domain. Denote  $Q := \text{Frac}(R)$ ,  $S := R - \{0\}$  and  $K := Q/R$  (the quotient). These components form an exact sequence:

$$0 \longrightarrow R \longrightarrow Q \longrightarrow K \longrightarrow 0$$

By theorem 100, this SES and the functor  $\mathrm{Tor}_n$  induces a LES:

$$\cdots \longrightarrow \text{Tor}_2(K, A) \longrightarrow \text{Tor}_1(R, A) \longrightarrow \text{Tor}_1(Q, A) \longrightarrow \text{Tor}_1(K, A) \longrightarrow \text{Tor}_0(R, A) \longrightarrow \text{Tor}_0(Q, A) \longrightarrow \text{Tor}_0(K, A) \longrightarrow 0$$

Now, we want to demystify each spot in this long exact sequence:

- (1)  $\forall n \geq 1$ ,  $\text{Tor}_n(R, A) = 0$ , since  $R$  is a free  $R$ -module  $\Rightarrow$  is projective.  
(2)  $\forall n \geq 1$ ,  $\text{Tor}_n(Q, A) = 0$  since  $Q$  is flat. This is because the equivalency of  $(-) \otimes_R Q : R\text{-Mod} \rightarrow_{S^{-1}R} \text{Mod}$  and  $[S^{-1}] : R\text{-Mod} \rightarrow_{S^{-1}R} \text{Mod}$  as functors:

## Localization Tensor

$$[S^{-1}] \xleftarrow{\sim} (-) \otimes_R S^{-1}R$$

exact  $\rightsquigarrow$  exact

$S^{-1}R$  is flat

(3)  $\forall n \geq 2$ ,  $\text{Tor}_n(K, A) = 0$ . This comes from the exactness at  $\text{Tor}_n(K, A)$ .  
The name  $\text{Tor}$  comes from the following reasons. Consider a 'functor'  $(-)_t : {}_R \text{Mod} \rightarrow {}_R \text{Mod}$  that maps an  $R$ -module  $M$  to its torsion submodule  $M_t$ , and an  $R$ -module homomorphism  $f : M \rightarrow N$  to  $f_t : M_t \rightarrow N_t$  with  $f_t \circ f = f$ .

— 1 —

$$H_1(\Gamma^1_{\alpha}, \mu^1_{\alpha}) = 1 - T_{\alpha}(K_{\alpha}) + 1/\alpha \leq 1 - \frac{1}{\alpha} + \frac{1}{\alpha} = 1$$

### Proof:

$\text{Tor}_n$  for PID:

From now on, suppose that  $R$  is a PID and  $M, N$  are finitely generated  $R$ -modules. From the structure theorem for finitely generated modules over PIDs,  $M$  and  $N$  have the following decomposition:

$$M \cong R^s \oplus \bigoplus_{i=1}^d R/I_i \quad N \cong R^t \oplus \bigoplus_{j=1}^e R/J_j$$

By virtue of the fact that  $L_n F$  is [???](#), each  $\text{Tor}_n(M, N)$  can be decomposed into

$$\text{Tor}_n(M, N) = \text{Tor}_n(R^s, R^t) \oplus \bigoplus_{i=1}^d \text{Tor}_n(R/I_i, R^t) \oplus \bigoplus_{j=1}^e \text{Tor}_n(R^s, R/J_j) \oplus \bigoplus_{\substack{1 \leq i \leq d \\ 1 \leq j \leq e}} \text{Tor}_n(R/I_i, R/J_j)$$

Each  $\text{Tor}_n(*, *)$  with  $R^s$  or  $R^t$  appearing at  $*$  vanishes because free implies projective. So, it reduces the calculation of  $\text{Tor}_n(M, N)$  into calculation of  $\text{Tor}_n(R/I, R/J)$  for some  $I, J \trianglelefteq R$ . The outcome is condensed in the following theorem:

### Theorem 6.3: Tor for PID

Let  $R$  be a PID and  $I, J \trianglelefteq R$ . Then,

$$\text{Tor}_n(R/I, R/J) = \begin{cases} R/(I+J) & n = 0 \\ (I \cap J)/IJ & n = 1 \\ 0 & n \geq 2 \end{cases}$$

## 7 Examples for right-derived functors

### 7.1 Ext functor

#### 7.1.1 Applications of Ext 1: Classifying extensions of $R$ -modules

Given two  $R$ -modules, how to nest them into a bigger one? This entails the knowledge of extensions. Let  $A, C$  be two  $R$ -modules ( $R$  is commutative). Then,

#### Definition 7.1: Extension of $R$ -modules

Use the notations above. An  $R$ -module  $E$  is called an extension of  $A$  by  $C \Leftrightarrow$  there is an exact sequence of  $R$ -modules  $\xi$

$$\xi : 0 \longrightarrow A \xrightarrow{f} E \xrightarrow{g} C \longrightarrow 0$$

**Remark** Such an extension  $\xi$  is called **split**  $\Leftrightarrow$  a homomorphism  $h$  such that  $g \circ h = \text{id}_C$ , called **section** of  $g$ .

**Lemma 7.1 (Equivalence of split extensions)** Let  $\xi : 0 \rightarrow A \xrightarrow{f} E \xrightarrow{g} C \rightarrow 0$  be an extension of  $R$ -modules  $A$  by  $C$ ,  $\xi$  is split  $\Leftrightarrow \xi$  is equivalent to the short exact sequence  $0 \rightarrow A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \rightarrow 0$ <sup>3</sup>, where  $\iota : a \mapsto (a, 0)$  and  $\pi : (0, c) \mapsto c$ .

**Proof:**  $\Rightarrow$  If  $\xi$  is split, the goal is to show  $E \cong f(A) \oplus g(C)$ . This is equivalent to see  $f(A) \cap g(C) = \{0\}$  and  $f(A)g(C) = E$ . The second one needs to pick a  $y \in E$  and use the element  $y - h(g(y))$ .

$\Leftarrow$  Suppose  $E \cong A' \oplus C'$  where  $A \cong A'$  and  $C \cong C'$ . The equivalence gives a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} & C \longrightarrow 0 \\ & & \parallel & & \downarrow \varphi & & \parallel \\ 0 & \longrightarrow & A & \xrightarrow{\iota} & A' \oplus C' & \xrightarrow{\pi} & C \longrightarrow 0 \end{array}$$

<sup>3</sup>Here  $\oplus$  is the exterior direct sum.

Explicitly, suppose the isomorphisms are given by  $\alpha : A \rightarrow A'$  and  $\gamma : C \rightarrow C'$ . Then,  $\pi : (a, c) \mapsto \gamma(c)$ . Define  $\tilde{h} : C \rightarrow A' \oplus C'$  by  $c \mapsto (0, \gamma^{-1}(c))$ . It is quick to see that  $\pi \circ \tilde{h} = \text{id}_C$ . Define  $h := \varphi^{-1} \circ \tilde{h}$ . This  $h$  is the desired one because

$$g \circ h = g \circ (\varphi^{-1} \circ \tilde{h}) = \pi \circ \varphi \circ \varphi^{-1} \circ \tilde{h} = \pi \circ \tilde{h} = \text{id}_C$$

Hence,  $\xi$  is a split extension.  $\square$

Next, the notion of equivalence extension is needed. Because every extension keeps  $A$  and  $C$  and merely alters the middle  $E$ , equivalence should be given as

### Definition 7.2: Equivalent extensions of $R$ -modules

Let  $\xi, \xi'$  be two  $R$ -module extensions of  $A$  by  $C$ .  $\xi$  and  $\xi'$  are **equivalent**, denoted  $\xi \sim \xi' \Leftrightarrow \exists$   $R$ -module homomorphism  $\varphi : E \rightarrow E'$  making the following diagram commutes.

$$\begin{array}{ccccccc} \xi : & 0 & \longrightarrow & A & \xrightarrow{f} & E & \xrightarrow{g} C \longrightarrow 0 \\ & & & \text{id}_A \parallel & & \downarrow \varphi & \parallel \text{id}_C \\ \xi' & 0 & \longrightarrow & A & \xrightarrow{f'} & E' & \xrightarrow{g'} C \longrightarrow 0 \end{array}$$

**Remark** The equivalence between two extensions is not barely equivalent to the homomorphism between  $E$  and  $E'$ . Because this seemingly classifies  $E$ . But it in fact classifies the triple  $(E, f, g)$ . The object  $E$  and the morphisms related to  $E$  should be considered as integrity.

$\varphi$  is automatically an isomorphism. It suffices to see that  $\varphi$  is a bijection. •  $\varphi$  is *injective*. First notice that  $\forall x \in \ker \varphi, g(x) = g'(\varphi(x)) = 0$ . So,  $\ker \varphi \subseteq \ker g = \text{im } f$ . For this  $x, \exists y \in A$  such that  $x = f(y)$ . Using the first block,  $f'(y) = \varphi(f(y)) = \varphi(x) = 0$ . Then,  $y \in \ker f'$ . Since  $f'$  is injective,  $y = 0$ . This implies that  $x = 0$ . So,  $\ker \varphi = \{0\}$ . •  $\varphi$  is *surjective*.  $\forall w \in E'$ , we want to find an element  $z \in E$  such that  $w = \varphi(z)$ . But first, consider  $g'(w) \in C$ . Since  $g$  is surjective,  $\exists t \in E$  such that  $g(t) = g'(w)$ . In the meanwhile,  $g(t) = g'(\varphi(t))$ . So,  $w - \varphi(t) \in \ker g' = \text{im } f'$ . So,  $w - \varphi(t) = f'(a)$  for some  $a \in A$ . Notice that  $f'(a) = \varphi(f(a))$ . So,  $w = \varphi(t) + \varphi(f(a)) = \varphi(t + f(a))$ . Let  $z := t + f(a) \in E$ . This  $z$  is desired, showing  $\varphi$  is surjective. Hence, equivalence of two extensions  $\Rightarrow \varphi : E \rightarrow E'$  is an isomorphism. But, the converse is not true as suggested in the following example.

The example gives an isomorphism  $E \rightarrow E'$  but the corresponding extensions are not equivalent:

Consider two short exact sequence  $\xi_1$  and  $\xi_2$ :

$$\xi_1 : 0 \rightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{f_1} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{g} \mathbb{Z}/p\mathbb{Z} \rightarrow 0 \quad \xi_2 : 0 \rightarrow \mathbb{Z}/p\mathbb{Z} \xrightarrow{f_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{g} \mathbb{Z}/p\mathbb{Z} \rightarrow 0$$

where  $f_1 : 1 + p\mathbb{Z} \mapsto p + p^2\mathbb{Z}$  and  $f_2 : 1 + p\mathbb{Z} \mapsto 2p + p^2\mathbb{Z}$ . Suppose there is an isomorphism  $\varphi : \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z}$  making the diagram commutes. This  $\varphi$  determines a mapping  $\bar{\varphi} : p^2\mathbb{Z} \rightarrow p^2\mathbb{Z}$  such that  $\varphi(a + p^2\mathbb{Z}) = \bar{\varphi}(a) + p^2\mathbb{Z}$ .

The first block  $\varphi \circ f_1 = f_2 \circ \text{id}_{\mathbb{Z}/p\mathbb{Z}}$  acting on  $1 + p\mathbb{Z}$  yields  $p \cdot \bar{\varphi}(1) \equiv 2p \pmod{p^2}$ .

The second block  $\text{id}_{\mathbb{Z}/p\mathbb{Z}} \circ g = g \circ \varphi$  acting on  $1 + p\mathbb{Z}$  gives that  $g(\bar{\varphi}(1) + p^2\mathbb{Z}) = g(1 + p^2\mathbb{Z})$ , which implies that  $\bar{\varphi}(1) - 1 \in \ker g \cong \mathbb{Z}/p\mathbb{Z}$ . Hence,  $\bar{\varphi}(1) - 1 \in p\mathbb{Z}$ . This yields  $\bar{\varphi}(1) = 1 + kp$  for some  $k$ .

But,  $p \cdot \bar{\varphi}(1) = p + kp^2 \equiv p \not\equiv 2p \pmod{p^2}$ , contradiction. So, these two extensions are not equivalent.

Let  $[\xi] := \{\xi' : 0 \rightarrow A \rightarrow E \rightarrow C \rightarrow 0 | \xi' \text{ is exact}, \xi' \sim \xi\}$  be an equivalence class of exact sequences which are equivalent to  $\xi$ .

The notation  $e(C, A)$  denotes the collection of all equivalence classes of exact sequences that are extensions of  $A$  by  $C$ .  $e(C, A)$  is characterized by  $\text{Ext}^1(C, A)$ . Why this The map between  $e(C, A)$  and  $\text{Ext}^1(A, C)$  is given by the following process:

- First choose a representative, i.e. a SES  $\xi : 0 \rightarrow A \rightarrow E \rightarrow C \rightarrow 0$  that is an extension of  $A$  by  $C$ , of some equivalence class  $[\xi]$
- Then, pick a projective resolution of  $C, \cdots \rightarrow 0 \rightarrow P_1 \rightarrow P_0 \rightarrow C \rightarrow 0$
- prolonging the left hand side of  $\xi$  by 0s, the identity map on  $C$ ,  $\text{id}_C$ , could be extended into many maps by comparison lemma 5.2:

$$\begin{array}{ccccccc} P_\bullet & \cdots & \longrightarrow & 0 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} P_0 \xrightarrow{d_0} C \longrightarrow 0 \\ & & & \downarrow & & \downarrow \alpha_1 & \downarrow \alpha_0 \downarrow \text{id}_C \\ \xi & \cdots & \longrightarrow & 0 & \longrightarrow & A & \longrightarrow E \longrightarrow C \longrightarrow 0 \end{array}$$

- Then, the map  $\Psi : e(C, A) \rightarrow \text{Ext}^1(C, A)$  is defined to be  $[\xi] \mapsto \alpha_1 + \text{im}Fd_1$ , where  $F = \text{Hom}_R(-, A)$ .

**Theorem 7.1:  $\Psi$**

The map  $\Psi : e(C, A) \rightarrow \text{Ext}^1(C, A)$   $[\xi] \mapsto \alpha_1 + \text{im}Fd_1$  is well-defined.

**Proof:** The definition of  $\Psi$  depends on two choices: one is for  $\alpha_1$  (the extension of  $\text{id}_C$ ), and another is for the representative  $\xi$ .

Suppose that we have another extension of  $\text{id}_C$  at  $P_1 \rightarrow A$ , say  $\alpha'_1$ . By the comparison lemma 5.2,  $\exists$  morphisms  $s_0 : P_0 \rightarrow A$  and  $s_1 : P_1 \rightarrow 0$  such that  $\alpha_1 - \alpha'_1 = 0 \circ s_1 + s_0 \circ d_1 = s_0 \circ d_1$ . Notice that  $\text{im}Fd_1 = \{f \circ d_1 : f \in \text{Hom}_R(P_0, A)\}$ . So,  $\alpha'_1 \in \text{im}Fd_1$ .

Suppose that there is another representative of  $\xi$ ,  $\xi'$ .  $\xi'$  is another extension of  $A$  by  $C$  that is isomorphic to  $\xi$ . Then, we have a composition of morphisms of SESs:

$$\begin{array}{ccccccc} P_\bullet & \cdots \longrightarrow 0 \xrightarrow{d_2} & P_1 \xrightarrow{d_1} & P_0 \xrightarrow{d_0} & C \longrightarrow 0 \\ & \downarrow & \downarrow \alpha_1 & \downarrow \alpha_0 & \downarrow \text{id}_C \\ \xi & \cdots \longrightarrow 0 \longrightarrow A \longrightarrow E \longrightarrow C \longrightarrow 0 \\ & \downarrow & \downarrow \text{id}_A & \downarrow \phi & \downarrow \text{id}_C \\ \xi' & \cdots \longrightarrow 0 \longrightarrow A \longrightarrow E' \longrightarrow C \longrightarrow 0 \end{array}$$

By definition of  $\Psi$ , it sends  $[\xi']$  to the class of morphism from  $P_1$  to  $A$ , which is  $\text{id}_A \circ \alpha_1 + \text{im}Fd_1 = \alpha_1 + \text{im}Fd_1$ , showing that  $\Psi([\xi]) = \Psi([\xi'])$ .  $\square$

The map is used to characterize  $e(C, A)$ , so it should have nice property, being an isomorphism. To show this, we should construct an inverse of  $\Psi$ . Namely, for every  $\alpha_1$ , find an extension of  $A$  by  $C$ .

### 7.1.2 Application of Ext 2: Baer sum

## 7.2 Sheaf cohomology

## 7.3 Group cohomology

Take the functor to be the invariant group functor  $(-)^G : \mathbb{Z}[G]\text{-Mod} \rightarrow \mathbb{Z}\text{-Mod}$ . This functor sends every  $\mathbb{Z}[G]$ -module  $A$  to its invariant submodule under the action of  $G$ ,  $A^G$ . Since  $A^G$  is the part that is independent of the action of  $G$ , then it is viewed as a  $\mathbb{Z}$ -module.  $(-)^G$  also takes every morphism  $f$  to its restriction. Consider an exact sequence of  $\mathbb{Z}[G]$ -modules

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

The functor induces an left-exact sequence

$$0 \longrightarrow A^G \xrightarrow{f|_{A^G}} B^G \xrightarrow{g|_{B^G}} C^G$$

Because  $\ker g|_{B^G} = \ker g \cap B^G = \text{im}f \cap B^G = \text{im}f|_{A^G}$ . The last equality comes from the fact that  $f$  is  $G$ -equivariant and injective. For the sequence not necessarily being exact at  $C$ , here is an example: filling.

A central theme in homological algebra is to remedy the failure of exactness caused by applying a functor, typically by extending the resulting sequence into a long exact sequence. The treatment of the functor  $(-)^G$  is no exception to this principle. However, before we can construct such an extension of the sequence  $0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$ , a shift in perspective is necessary.

There are two perspectives for the invariants:

- (1) The first perspective is 'internal'.  $A^G$  is viewed as something defined inside  $A$ . It is defined by checking whether individual elements  $a \in A$  satisfy a certain property: remaining invariant under the action of every element of  $g \in G$ . This is an 'element-wise' or 'local' viewpoint.
- (2) However, the core philosophy of homological algebra and categories are quite different. The center of study shifts away from the individual elements inside every single object. Instead, an object is understood by studying the morphisms between it and any other objects. This idea draws heavily from the Grothendieck school. Its essence, the so-called *point de vue relatif* (relative point of view), is that an object's identity is characterized by its morphisms with all the other objects. This philosophy inspires us to recast the 'internal property'  $A^G$  in terms of an 'external relationship', expressed as a collection of morphisms. We call this 'external perspective'.

How to make this shift of perspective operational? To talk about morphisms, we need another object  $X$  in addition to  $A$ , allowing us to study  $\text{Hom}(X, A)$ . This object must serve as a universal probe to detect the specific property we are interested in,  $G$ -invariance across all the objects as  $\mathbb{Z}[G]$ -modules.

So, what object best embodies the concept of  $G$ -invariance? The answer is precisely  $\mathbb{Z}$ . This is because  $G$ -invariance signifies the triviality of  $G$ -action ( $G$ -action is ignored), leaving only the  $\mathbb{Z}$ -module structure. Hence, it is natural to think the relationship between  $A^G$  and  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ .

**Lemma 7.2** *Let  $A$  be a  $\mathbb{Z}[G]$ -module and  $\mathbb{Z}$  have the trivial  $G$ -action on it. Then,*

$$A^G \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

**Proof:** Define the map

$$\Psi : A^G \rightarrow \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \quad a \mapsto (f_a : 1 \mapsto a)$$

$\Psi$  is a group homomorphism(hence a  $\mathbb{Z}$ -module homomorphism) because  $\forall x, y, \Psi(x+y) = f_{x+y} = f_x + f_y = \Psi_x + \Psi_y$ . This map is injective because  $f_a$  is uniquely determined by the value assigned to 1.  $\Psi$  is also surjective because  $\forall f \in \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A), \forall g \in G, {}^g f(1) = f({}^g 1) = f(1)$ . The first equality comes from  $G$ -equivariance of  $f$  and the second equality comes from triviality of the action  $G \curvearrowright \mathbb{Z}$ . So,  $f(1) \in A^G$  and  $f = \Psi(f(1))$ .  $\square$

**Remark** Similarly, there is a general version:

$$A \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A)$$

Something deeper underlies here: as a left-exact covariant functor  $(-)^G$ ,  $(-)^G$  can be identified with the functor  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ . We just abuse the notation  $H^n$  and define

$$H^n(G, A) := (R^n(-)^G)(A) \cong (R^n \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -))(A) =: \text{Ext}_{\mathbb{Z}[G]}^n(\mathbb{Z}, A)$$

Especially,  $H^0(G, A) = \text{Ext}_{\mathbb{Z}[G]}^0(\mathbb{Z}, A) \cong A^G$ . From filling, the short exact sequence  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  induces a long exact sequence

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G \rightarrow H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \rightarrow H^2(G, A) \rightarrow \dots$$

Group cohomology was first conceived as a technical mechanism to measure and remedy the non-exactness of the functor  $(-)^G$  only. But, it was quickly realized that these groups were not merely corrective tools. These groups themselves are subtle invariants, revealing profound structural insights and applications that extended far beyond the purely 'corrective' motivations. Consequently, they become a central object in research.

### 7.3.1 Calculation of cohomology groups 1: Choosing resolutions

Cohomology groups are concretely defined to be something derived from some resolution(either injective or projective). So, the standard way to calculate  $H^n(G, A)$  for some group  $G$  and a  $\mathbb{Z}[G]$ -module  $A$  is to choose a  $\mathbb{Z}[G]$ -modules resolution of  $\mathbb{Z}$ . In fact, projective resolutions are simpler filling.

To assign each object and morphism concrete stuff on the following sequence

$$\mathbf{P}_{\mathbb{Z}} : \dots \xrightarrow{d_3} Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$$

and make it a projective resolution. For some certain groups, the projective resolutions are easier to construct. Here are two examples for specific groups. The general construction of  $\mathbf{P}_{\mathbb{Z}}$  follows.

(1) Let  $G = \langle t \rangle$  of infinite order. Then,

$$0 \rightarrow \mathbb{Z}[G] \xrightarrow{\cdot(t-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$$

is a free (hence projective) resolution of  $\mathbb{Z}$ .

Let  $\varphi$  be the map  $\cdot(t-1)$ . Applying  $\epsilon \circ \varphi$  for any element in  $\mathbb{Z}[G]$ ,  $\sum_{n=0}^m b_n t^n$ , where  $m$  is the highest index of non-zero  $b_n$ ,

$$(\epsilon \circ \varphi) \left( \sum_{n=0}^m b_n t^n \right) = \epsilon \left( \sum_{n=0}^m b_n t^{n+1} \right) - \epsilon \left( \sum_{n=0}^m b_n t^n \right) = 0$$

Fix an element  $\sum_n^M a_n t^n$  in  $\ker \epsilon$ , where  $M$  is the highest integer making  $a_n$  non-zero. Hence,  $\sum_{n=0}^M a_n = 0$ . Suppose there is a  $\sum_{n=0}^N b_n t^n$  such that

$$\sum_{n=0}^M a_n t^n = \sum_{n=0}^N b_n t^n (t-1) = -b_0 + \sum_{n=1}^N (b_{n-1} - b_n) t^n + b_N t^{N+1}$$

To equate both sides, first  $M = N+1$ . This equation also gives the coefficients of each  $b_n$ .  $\forall 0 < N, b_n = -\sum_{i=0}^n a_i$ . But, for  $n = N$ , there are two equations for  $b_N$ ,

$$\begin{aligned} b_N &= -\sum_{i=0}^N a_i \\ b_N &= a_{N+1} \end{aligned}$$

But,  $\sum_{i=0}^{N+1} a_i = 0$  guarantees the existence of solutions of two equations by asserting they are equal. Therefore, we find an element  $\sum_n (-\sum_{i=0}^n a_i) t^n$ , showing that  $\ker \epsilon \subseteq \text{im } \varphi$ .

(2) Let  $G = \langle t \rangle$  of finite order  $n$ . Then,

$$\dots \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\beta} \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\beta} \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is a free resolution with  $\alpha(x) = (t-1) \cdot x$  and  $\beta(x) = \left(\sum_{i=0}^{t-1} t^i\right) \cdot x$ .

Just as we did above,  $\ker \epsilon = \text{im } \alpha$ . (Even though the group  $G$  has finite order now, just slightly modify the argument.)

It remains to see that  $\ker \alpha = \text{im } \beta$  and  $\ker \beta = \text{im } \alpha$ .

For any  $x \in \mathbb{Z}[G]$ ,

$$(\alpha \circ \beta)(x) = (t-1) \cdot \left( \sum_{i=0}^{t-1} t^i \right) \cdot x = \left( \sum_{i=0}^{n-1} t^i - \sum_{i=0}^{n-1} t^i \right) \cdot x = 0, \quad (\beta \circ \alpha)(x) = 0$$

For any  $x = \sum_{i=0}^{n-1} a_i t^i \in \ker \alpha$ , this implies that  $\forall i, a_i$  are all equal. Then,  $x = a_0 \cdot (\sum_i t^i) \in \text{im } \beta$ .

(3) Now, let's consider the most general case. We do the following steps: Assume first that  $G$  is a finite group.

• For objects:  $\mathbb{Z}$  can be thought of as a  $\mathbb{Z}[G]$ -module with null basis. Following this idea, the objects in the resolution can be taken to be  $\mathbb{Z}[G]$ -modules with  $G^0, G, G^2$ , etc, as basis. So,  $\forall n \geq 0$ , let  $Q_n$  be the free  $\mathbb{Z}[G]$ -module over the basis  $G^n$ . Due to historical reasons and for the sake of visual clarity, we adopt the notation

$$[x_1 | \dots | x_n] := (x_1, \dots, x_n)$$

Under this notation,  $Q_n$  is actually the free  $\mathbb{Z}[G]$ -module over the basis  $\{[x_1 | \dots | x_n] : x_1, \dots, x_n \in G\}$ . Especially,  $Q_0$  has  $\{[]\}$  as its basis, meaning  $Q_0$  is identical to  $\mathbb{Z}[G]$  or  $\text{rank}_{\mathbb{Z}[G]} Q_0 = 1$ . Similarly,  $\text{rank}_{\mathbb{Z}[G]} Q_n = |G|^n$ .

• For morphisms: First consider  $\epsilon$ , define it to be

$$\epsilon : Q_0 \rightarrow \mathbb{Z} \quad \left( \sum_{g \in G} n_g g \cdot [] \right) \mapsto \sum_{g \in G} n_g$$

This is indeed a  $\mathbb{Z}[G]$ -module homomorphism.

Then, for  $n \geq 1$ , it suffices to define  $d_n$  and operate it on the basis of  $Q_n$  and then extend the map  $\mathbb{Z}[G]$ -linearly to whole  $Q_n$ .  $d_n : Q_n \rightarrow Q_{n-1}$  works elementwise as follows:

$$d_n([x_1 | \dots | x_n]) := x_1[x_2 | \dots | x_n] + \sum_{i=1}^{n-1} (-1)^i [x_1 | \dots | x_{i-1} | x_i x_{i+1} | x_{i+2} | \dots | x_n] + (-1)^n [x_1 | \dots | x_{n-1}]$$

There is no need to check this  $d_n$  is a  $\mathbb{Z}[G]$ -module homomorphism ( $\mathbb{Z}[G]$ -linear) because we specifies the rules on basis and force it to be  $\mathbb{Z}[G]$ -linear on  $Q_n$ .

For lower rank, this map looks milder:

$$\begin{aligned} d_1([x_1]) &= x_1[] - [] \\ d_2([x_1|x_2]) &= x_1[x_2] - [x_1 x_2] + [x_1] \\ d_3([x_1|x_2|x_3]) &= x_1[x_2|x_3] - [x_1 x_2|x_3] + [x_1|x_2 x_3] - [x_1|x_2] \end{aligned}$$

Now the definition work is done and it remains to check that this sequence is indeed a  $\mathbb{Z}[G]$ -module resolution.

### Lemma 7.1: Bar resolution

Let  $Q_n$  and  $d_n$  ( $\epsilon := d_0$ ) be the objects and morphisms defined above. Then,

$$\dots \xrightarrow{d_3} Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is a  $\mathbb{Z}[G]$ -module projective resolution of  $\mathbb{Z}$ .

**Proof:**

To facilitate the discussion below, here is another identification. Objects in the complex (we just showed it is) resulting from the  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$  functor

$$0 \rightarrow \text{Hom}_{\mathbb{Z}[G]}(Q_0, A) \rightarrow \text{Hom}_{\mathbb{Z}[G]}(Q_1, A) \rightarrow \text{Hom}_{\mathbb{Z}[G]}(Q_2, A) \rightarrow \cdots$$

are cumbersome. A natural way to streamline  $\text{Hom}_{\mathbb{Z}[G]}(Q_n, A)$  is to reduce functions to the basis  $G^n$  of  $Q_n$ :

$$\text{Hom}_{\mathbb{Z}[G]}(Q_n, A) \cong \{\text{set-theoretical functions } f : G^n \rightarrow A\}$$

**Lemma 7.3**  $A^{G^n} = \{\text{set-theoretical functions } f : G^n \rightarrow A\}$ .  $A^{G^n}$  can naturally be equipped with a  $\mathbb{Z}[G]$ -module structure. Then,  $\text{Hom}_{\mathbb{Z}[G]}(Q_n, A) \cong_{\mathbb{Z}[G]\text{-Mod}} A^{G_n}$ .

**Proof:** For any  $\mathbb{Z}[G]$ -linear map  $g : Q_n \rightarrow A$ , define  $\Phi : h \mapsto h|_{G^n}$ . Then,  $h|_{G^n}$  is a function  $G^n \rightarrow A$ . From right to left, send each  $f$  to its unique  $\mathbb{Z}[G]$ -linear extension to get the  $\tilde{f} \in \text{Hom}_{\mathbb{Z}[G]}(Q_n, A)$ , i.e. the map defined is  $\Omega : \tilde{f} \mapsto f$ .  $\Omega \circ \Phi(h) = h$  because  $h$  is uniquely determined by its acting on the basis. Hence,  $\Phi$  is a bijection.  $\square$

**Remark** The key advantage of this identification is simplification, in two ways:

First, by focusing on  $A^{G^n}$ , a subset of  $\text{Hom}_{\mathbb{Z}[G]}(Q_n, A)$ , we are dealing with a more constrained (and likely simpler) set. Second, elements of  $A^{G^n}$  are simpler. This allows us to treat them as simpler objects, set-theoretical functions and forget the  $\mathbb{Z}[G]$ -linearity.

### 7.3.2 Calculations of group cohomology 2: formal calculations

Now we are trying to compute some group cohomology groups to feel how it works. The examples at our disposal are cyclic groups with infinite order and finite order, respectively.

Recall that the cohomology groups are independent of choice of resolutions. There are resolutions found previously. So, we shall use the resolution just found to do computations.

(1) First, consider  $G = \langle t \rangle$  with infinite order. One resolution we found is

$$0 \longrightarrow \mathbb{Z}[G] \xrightarrow{\cdot(t-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

The corresponding exact sequence resulting from acting  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$  is

$$0 \longleftarrow \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xleftarrow{\cdot(t-1)^*} \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \longleftarrow 0$$

But this looks cumbersome to compute. One way to simplify this sequence is to exploit the isomorphism in the remark of lemma 7.1,  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$ :

$$\begin{array}{ccccccc} 0 & \xleftarrow{d^{2*}} & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xleftarrow{d^{1*}} & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xleftarrow{d^{0*}} & 0 \\ & & \Phi \downarrow \sim & & \Phi \downarrow \sim & & \\ 0 & \xleftarrow{\tilde{d}^2} & A & \xleftarrow{\tilde{d}^1} & A & \xleftarrow{\tilde{d}^0} & 0 \end{array}$$

Notice that  $\forall n \geq 2$ ,  $H^n(G, A) = 0$ .

For  $H^1(G, A) \cong \ker \tilde{d}^2 / \text{im } \tilde{d}^1$ , we can use the sequence below.  $\ker \tilde{d}^2 = A$ . For  $\text{im } \tilde{d}^1 = \{n \in A : \exists m \in A, \tilde{d}^1(m) = n\}$ , by virtue of the commutativity of the diagram,  $\tilde{d}^1 = \Phi \circ d^{1*} \circ \Phi^{-1}$ . Let's compute  $\tilde{d}^1(m)$ :

$$\tilde{d}^1(m) = \Phi \circ d^{1*} \circ \Phi^{-1}(m) \tag{4}$$

$$= (\Phi \circ d^{1*})(f_m) \quad \text{construction of } \Phi : \Phi^{-1} : m \mapsto (f_m : 1 \mapsto m) \tag{5}$$

$$= \Phi(f_m \circ d^1) \quad \text{definition of } d^{1*}, \text{ where } d^1 = \cdot(t-1) \tag{6}$$

$$= (f_m \circ d^1)(1) \quad \text{construction of } \Phi : \Phi : \theta \mapsto \theta(1) \tag{7}$$

$$= f_m(t-1) \tag{8}$$

$$= (t-1) \cdot m \quad f_m : 1 \mapsto m \tag{9}$$

This shows that  $\text{im } \tilde{d}^1 = \{(t-1) \cdot m : m \in A\}$ . Let  $\delta := (t-1)$ . Then,  $H^1(G, A) \cong A/\delta A = A_G$ .  $A_G$  is the co-invariant of  $A$ , i.e. the largest quotient fixed by  $G$ . <sup>4</sup>

<sup>4</sup>Here is the definition of  $A_G$ . Let  $I_G A := \langle \{(g-1)m : g \in G, m \in A\} \rangle$ . Then,  $A_G := A/I_G A$ . A very important property of  $A_G$  is: It is the largest quotient fixed by  $G(G \curvearrowright A/I_G A)$ , more precisely  $(A/I_G A)^G = A/I_G A$ . 'Largest' means that there is no such submodule  $N$  of  $A$  with  $N \subsetneq I_G A$  such that  $(A/N)^G = A/N$ . Because any such submodule must contain all  $(g-1)m$ ,  $g \in G$  and  $m \in A$ , meaning  $I_G A \subseteq N$ .

In the context of cyclic group  $G$ ,  $I_G A$  gets simplified a lot. Because every  $g$  is of the form  $t^k$ , so  $(t^k - 1)m = (t-1)(t^{k-1} + \dots + 1)m$ . Let  $m' = (t^{k-1} + \dots + 1)m$ .  $(g-1)m$  can still be written in the form  $(t-1)m'$ . So, in the cyclic group case,  $I_G A = \{(t-1)m : m \in A\}$ .

For  $H^0(G, A)$ , it is quick to see  $H^0(G, A) \cong \ker \tilde{d}^1 = \{m \in A : (t-1) \cdot m = \tilde{d}^1(m) = 0\} = \{m \in A : tm = m\} = A^G$ . In short,

$$H^0(G, A) \cong A^G, \quad H^1(G, A) \cong A/\delta A = A_G, \quad H^n(G, A) = 0 \text{ for } n \geq 2$$

(2) Second, consider  $G = \langle t \rangle$  with order  $n$ . The resolution we found is

$$\cdots \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\beta} \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\beta} \mathbb{Z}[G] \xrightarrow{\alpha} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$$

Let  $\delta := (t-1)$  and  $\eta := \sum_{i=0}^{n-1}$ . Again, applying the  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$  functor, we have the sequence:

$$\cdots \xleftarrow{d_\alpha^3} \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xleftarrow{d_\beta^{2^2}} \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xleftarrow{d_\alpha^1} \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xleftarrow{d^0} 0$$

Once more, exploit the isomorphism  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$ ,

$$\begin{array}{ccccccc} \cdots & \xleftarrow{d_\alpha^3} & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xleftarrow{d_\beta^{2^2}} & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xleftarrow{d_\alpha^1} & \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xleftarrow{d^0} 0 \\ & & \Phi \downarrow \sim & & \Phi \downarrow \sim & & \Phi \downarrow \sim \\ \cdots & \xleftarrow{d_\alpha^{2^3}} & A & \xleftarrow{d_\beta^{2^2}} & A & \xleftarrow{d_\alpha^{2^1}} & A \xleftarrow{d^{2^0}} 0 \end{array}$$

The calculations are quite similar to the infinite order case.  $H^0(G, A) = A^G$ .

For  $n \geq 1$ ,  $H^{2n}(G, A) = \ker d_\alpha^{2n+1}/\text{im} d_\beta^{2n}$  and  $H^{2n-1}(G, A) = \ker d_\beta^{2n}/\text{im} d_\alpha^{2n-1}$ .

Notice that  $d_\beta^{2n}(x) = (\Phi \circ d_\beta^{2n} \circ \Phi^{-1})(x) = \eta \cdot x$  and  $d_\alpha^{2n-1}(x) = \delta \cdot x$ . So,

$$\ker d'^{2n+1} = \{x \in A : \delta \cdot x = 0\} = \{x \in A : \forall t \in G, (t-1) \cdot x = 0\} = \{x \in A : \forall t \in G, t \cdot x = x\} = A^G$$

For  $\ker d'^{2n}$ , calculations are same:  $\ker d'^{2n} = \{x \in A : \eta \cdot x = 0\} = \{x \in A : \forall t \in G, \sum_{i=0}^{n-1} t^i \cdot x = 0\} =: A[\eta]$ . Similarly,  $\text{im} d_\beta^{2n} = \{\eta \cdot x : x \in A\} = \eta A$  and  $\text{im} d_\alpha^{2n-1} = \{\delta \cdot x : x \in A\} = \delta A$ .

So, in conclusion,

$$H^0(G, A) \cong A^G, \quad H^{2n-1} \cong A[\eta]/\delta A, \quad H^{2n}(G, A) \cong A^G/\eta A, \text{ for } n \geq 1$$

(3) Some general(independent of groups) results on  $H^n(G, A)$  hold. Now take  $G$  to be an arbitrary group. Still,  $A$  is a  $\mathbb{Z}[G]$ -module. Then,

$$H^0(G, A) \cong A^G$$

To see this, take an arbitrary resolution of  $\mathbb{Z}$ :  $\cdots \rightarrow Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{\epsilon} \mathbb{Z} \rightarrow 0$ . Applying  $\text{Hom}_{\mathbb{Z}[G]}(-, A)$  functor(left-exact contravariant) to it, we obtain a sequence only exact at  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$  and  $\text{Hom}_{\mathbb{Z}[G]}(Q_0, A)$ :

$$\cdots \xleftarrow{d^{2^*}} \text{Hom}_{\mathbb{Z}[G]}(Q_1, A) \xleftarrow{d^{1^*}} \text{Hom}_{\mathbb{Z}[G]}(Q_0, A) \xleftarrow{\epsilon^*} \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \longleftarrow 0$$

The exactness at  $\text{Hom}_{\mathbb{Z}[G]}(Q_0, A)$  and  $\text{Hom}_{\mathbb{Z}[G]}(Q_1, A)$  yields injectivity of  $\epsilon^*$  and  $\ker d^{1^*} = \text{im} \epsilon^* \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ , respectively. While, the calculation of  $H^n(G, A)$  uses the sequence deleting  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$  and keeps the remaining part the same:

$$\cdots \xleftarrow{d^{2^*}} \text{Hom}_{\mathbb{Z}[G]}(Q_1, A) \xleftarrow{d^{1^*}} \text{Hom}_{\mathbb{Z}[G]}(Q_0, A) \longleftarrow 0$$

Lemma 7.1.  $\Rightarrow$  the isomorphism  $\text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong A^G$ . Hence,  $H^0(G, A) = \ker d^{1^*} = \text{im} \epsilon^* \cong \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong A^G$ .

### 7.3.3 Application of group cohomology: Number theory

We now introduce applications of group cohomology to number theory and class field theory. First, let's look at Hilbert's 90.

#### Theorem 7.2: Hilbert's 90

Let  $L/K$  be a finite Galois extension with Galois group  $\text{Gal}(L/K)$ . Then,  $H^1(\text{Gal}(L/K), L^\times) = 0$ .

**Proof:**  $H^1(\text{Gal}(L/K), L^\times) = \ker d^{2*}/\text{im}d^{1*}$ , where  $\text{Hom}_{\mathbb{Z}[G]}(Q_2, L^\times) \xleftarrow{d^{2*}} \text{Hom}_{\mathbb{Z}[G]}(Q_1, L^\times) \xleftarrow{d^{1*}} \text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times)$ . In this calculation, we still adopt the standard bar resolution of  $\mathbb{Z}, \dots \xleftarrow{d_2} Q_1 \xleftarrow{d_1} Q_0 \leftarrow 0$ . For any  $\varphi \in \ker d^{2*}$ ,  $\varphi \in \ker d^{2*} \Leftrightarrow \varphi : Q_1 \rightarrow L^\times$  and  $\varphi \circ d_2 = 1_{L^\times}$ . To decode the condition  $\varphi \circ d_2 = 1_{L^\times}$ , apply it to basis element of  $Q_1$ ,  $\text{Gal}(L/K)$ .  $\forall \tau, \sigma \in \text{Gal}(L/K)$ , we have

$$1_{L^\times} = \varphi \circ d_2([\tau|\sigma]) = \varphi([\tau] - [\sigma] + [\tau]) \quad (10)$$

$$= \varphi([\tau]) \cdot \varphi([\tau\sigma])^{-1} \cdot \varphi([\tau]) \quad \mathbb{Z}[\text{Gal}(L/K)] - \text{linearity of } \varphi, \text{ operation of } L^\times \text{ is } \cdot \quad (11)$$

$$= \varphi([\tau]) \cdot \varphi([\tau\sigma])^{-1} \cdot \varphi([\tau]) \quad {}^\tau[\sigma] := \tau[\sigma] \quad (12)$$

$$= {}^\tau(\varphi([\sigma])) \cdot \varphi([\tau\sigma])^{-1} \cdot \varphi([\tau]) \quad \mathbb{Z}[\text{Gal}(L/K)] - \text{linearity or Gal}(L/K) \text{ equivariance of } \varphi \quad (13)$$

$$= {}^\tau(\varphi(\sigma)) \cdot \varphi(\tau\sigma)^{-1} \cdot \varphi(\tau) \quad [\sigma] = \sigma, [\tau] = \tau, [\tau\sigma] = \tau\sigma \text{ are basis of } Q_1 \quad (14)$$

(14) implicitly uses the above-mentioned identification. Transforming it, we finally have

$$\varphi(\tau\sigma) = {}^\tau(\varphi(\sigma)) \cdot \varphi(\tau) \quad (15)$$

A map  $\psi \in \text{im}d^{1*}$  if and only if  $\exists$  a  $\mathbb{Z}[G]$ -module homomorphism  $\alpha : G^0 = \mathbb{Z}[G] \cdot [] \rightarrow L^\times$  such that  $\psi = \alpha \circ d_1$ . Notice that  $\alpha$  is uniquely determined by the value on the basis  $[]$ . Let  $c := \alpha([])$ . So, the existence of such an  $\alpha$  is equivalent to the existence of such a  $c$ , under this:  $\forall [\tau] \in Q_1$ ,

$$\psi([\tau]) = \alpha \circ d_1([\tau]) = \alpha(\tau[] - []) = \tau(\alpha([])) \cdot \alpha([])^{-1} = \tau(c) \cdot c^{-1}$$

Now the task is transferred to find an element  $c \in L^\times$  such that  $\forall \tau \in \text{Gal}(L/K)$ ,  $\varphi(\tau) = \tau(c) \cdot c^{-1}$ .

Let  $\tilde{\sigma} := \sigma|_{L^\times}$ , where  $\sigma \in \text{Gal}(L/K)$ . Such a  $\tilde{\sigma} : L^\times \rightarrow L^\times$  is a character. By Dedekind's lemma on the independence of characters,  $\exists a \in L^\times$ , such that

$$\sum_{\sigma \in \text{Gal}(L/K)} \varphi(\sigma)\tilde{\sigma}(a) = \sum_{\sigma \in \text{Gal}(L/K)} \varphi(\sigma)\sigma(a) \neq 0$$

Let  $b := \sum_{\sigma \in \text{Gal}(L/K)} \varphi(\sigma)\sigma(a)$ . Applying  $\tau$ ,

$$\tau b = {}^\tau \left( \sum_{\sigma \in \text{Gal}(L/K)} \varphi(\sigma)\sigma(a) \right) \quad (16)$$

$$= \sum_{\sigma \in \text{Gal}(L/K)} {}^\tau \varphi(\sigma) {}^\tau \sigma(a) \quad (17)$$

$$= \sum_{\sigma \in \text{Gal}(L/K)} {}^\tau \varphi(\sigma) \tau \sigma(a) \quad (18)$$

$$= \sum_{\sigma \in \text{Gal}(L/K)} \varphi(\tau\sigma) \varphi(\tau)^{-1} \tau \sigma(a) \quad \text{by (15)} \quad (19)$$

$$= \varphi(\tau)^{-1} \sum_{\eta \in \text{Gal}(L/K)} {}^\tau \varphi(\eta) \eta(a) \quad (20)$$

$$= \varphi(\tau)^{-1} \cdot b \quad (21)$$

Hence,  $\varphi(\tau) = b \cdot (\tau b)^{-1}$ . Let  $c := b^{-1}$ . We have  $\varphi(\tau) = {}^\tau c \cdot c^{-1}$ .  $\square$

**Remark** As previous calculation suggested, elements of  $\ker d^{2*}$  are twisted homomorphism. A function  $f : G \rightarrow L^\times$ <sup>5</sup> is called twisted homomorphism  $\Leftrightarrow \forall \tau, \sigma \in G$ ,

$$f(\tau\sigma) = {}^\tau(f(\sigma)) \cdot f(\tau)$$

Comparing to a homomorphism  $f(\tau\sigma) = f(\tau)f(\sigma)$ , the term  ${}^\tau(f(\sigma))$  is acted by  $\tau$ , called 'twisted'.  $H^1(G, A)$  is the quotient of the collection of twisted homomorphisms by the collection of 'trivial' homomorphisms. In other words, for any group  $G$  with an action on  $L^\times$ ,  $H^1(G, L^\times) = Z^1/B^1 = \ker d^{2*}/\text{im}d^{1*}$  is a collection of classes of twisted homomorphism.

The Hilbert 90 says there is no 'non-trivial' twisted homomorphism  $f : \text{Gal}(L/K) \rightarrow L^\times$ .<sup>6</sup> The word 'trivial' means

<sup>5</sup>Here  $G$  is not necessarily a Galois group, it can be any group has an action on  $L^\times$ .

<sup>6</sup>Here the  $\mathbb{Z}[G]$ -module homomorphism  $\mathbb{Z}[\text{Gal}(L/K)] =: Q_1 \rightarrow L^\times$  is identified with the set-theoretic function  $\text{Gal}(L/K) \rightarrow L^\times$ .

a twisted homomorphism  $f$  is constructable via a simpler element  $\mu \in L^\times$ . More concretely,  $f$  is trivial if there is a  $\mu \in L^\times$  that for every  $\tau \in \text{Gal}(L/K)$ ,

$$f(\tau) = {}^\tau \mu \cdot \mu^{-1}$$

This form comes from

$$\text{im } d^{1*} = \{\varphi \circ d_1 : \varphi \in \text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times)\}$$

Hence,  $\forall [\tau] \in \text{Gal}(L/K)$  (basis of  $Q_1$ ),  $\varphi \circ d_1([\tau]) = {}^\tau \varphi([\ ]) \cdot \varphi([\ ])^{-1}$  ranging over all  $\varphi \in \text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times)$ . Notice that  $\text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times) \cong L^\times$  by  $\varphi \mapsto \varphi([\ ])$ . So,  $\varphi \circ d^{1*}([\tau]) = {}^\tau \mu \mu^{-1}$  for every  $\mu \in L^\times$ . More explicitly,

$$\begin{aligned} \{\varphi \circ d_1([\tau]) : \varphi \in \text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times)\} &= \{{}^\tau \varphi([\ ]) \varphi([\ ])^{-1} : \varphi \in \text{Hom}_{\mathbb{Z}[G]}(Q_0, L^\times)\} \\ &\cong \{{}^\tau \varphi([\ ]) \varphi([\ ])^{-1} : \varphi([\ ]) \in L^\times\} \\ &= \{{}^\tau(\mu) \mu^{-1} : \mu \in L^\times\} \end{aligned}$$

### Corollary 7.1: Normalized elements in a cyclic Galois extension

Let  $L/K$  be a finite cyclic Galois extension with Galois group  $\text{Gal}(L/K) = \langle g \rangle$  of order  $n$ . If  $\lambda \in L^\times$  is an element whose norm to  $K^\times$  equals to 1, i.e.  $\prod_{i=0}^{n-1} g^i(\lambda) = 1$ , then  $\exists \mu \in L^\times$  such that  $\lambda = g(\mu) \cdot \mu^{-1}$ .

**Remark** There are two kinds of additions: one is the addition in  $\mathbb{Z}[G]$ ; another is the 'addition' in a  $\mathbb{Z}[G]$ -module  $A$ . In the following example, the operation (or 'addition') is actually multiplication. So, more attention to the symbol is needed.

**Proof:** When  $G := \text{Gal}(L/K)$  is a finite cyclic group, we can choose the above-mentioned resolution of  $\mathbb{Z}$ . Then, we have  $H^1(\text{Gal}(L/K), L^\times) = A[\eta]/\delta A$ , where  $\eta = \sum_{i=0}^{n-1} g^i$  and  $\delta = g - 1$ . The Hilbert 90 theorem 7.2 asserts that  $H^1(\text{Gal}(L/K), L^\times) = 0$  implying that  $L^\times[\eta] = \delta L^\times$ .

Since

$${}^\eta \lambda = {}^{(1+\mathbb{Z}[G] g + \mathbb{Z}[G] \cdots + \mathbb{Z}[G] g^{n-1})} \lambda \quad +_{\mathbb{Z}[G]} \text{ is the addition in } \mathbb{Z}[G] \quad (22)$$

$$= ({}^1 \lambda) +_{L^\times} ({}^g \lambda) +_{L^\times} \cdots +_{L^\times} ({}^{g^{n-1}} \lambda) \quad +_{L^\times} \text{ is the addition in } L^\times \quad (23)$$

$$= ({}^1 \lambda) \cdot ({}^g \lambda) \cdot \cdots \cdot ({}^{g^{n-1}} \lambda) \quad +_{L^\times} \text{ is actually } \cdot \quad (24)$$

$$= \prod_{i=0}^{n-1} g^i(\lambda) = 1 \quad {}^{g^i} \lambda = g^i(\lambda), \text{ by assumption} \quad (25)$$

$\lambda$  should be an element in the kernel of  $\eta$ , i.e.  $\lambda \in L^\times[\eta] = \delta L^\times$ . So,  $\lambda$  is in the image of  $\delta$ . Hence,  $\exists \mu \in L^\times$ , such that  $\lambda = {}^\delta \mu = {}^{g^{-1}} \mu = {}^g \mu \cdot \mu^{-1} = g(\mu) \cdot \mu^{-1}$ .  $\square$

### Lemma 7.2

Still, let  $L/K$  be a finite Galois extension with Galois group  $\text{Gal}(L/K)$  and  $\mu_n \subseteq K$  ( $K$  contains  $n$  distinct  $n$ -th roots of unity). Then, <sup>a</sup>

$$\frac{(L^\times)^n \cap K^\times}{(K^\times)^n} \cong \text{Hom}(G, \mu_n)$$

---


$${}^a(L^\times)^n = \{x^n : x \in L^\times\}.$$

**Proof:** Notice that  $0 \rightarrow \mu_n \xrightarrow{\iota} L^\times \xrightarrow{x \mapsto x^n} (L^\times)^n \rightarrow 0$  is an exact sequence. Let  $G := \text{Gal}(L/K)$ .

Then, apply the lemma 3.2 and use Hilbert's 90 7.2. We obtain a long exact sequence

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(G, \mu_n) & \longrightarrow & H^0(G, L^\times) & \longrightarrow & H^0(G, L^\times)^n & \longrightarrow & H^1(G, \mu_n) & \longrightarrow & H^1(G, L^\times) & \longrightarrow & \cdots \\ & & \parallel & & \parallel & & \parallel & & \parallel_{G \curvearrowright \mu_n \text{ trivially}} & & \parallel_{\text{Hilbert' 90 7.2}} & & \\ 0 & \longrightarrow & \mu_n^G & \longrightarrow & (L^\times)^G & \longrightarrow & (L^\times)^n G & \longrightarrow & \text{Hom}(G, \mu_n) & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \parallel_{\mu_n \subseteq K} & & \parallel & & \parallel & & \parallel & & \parallel & & \\ 0 & \longrightarrow & \mu_n & \longrightarrow & L^\times \cap K = K^\times & \longrightarrow & (L^\times)^n \cap K^\times & \longrightarrow & \text{Hom}(G, \mu_n) & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

The exactness at  $(L^\times)^n \cap K^\times$  yields the desired formula.  $\square$

**Remark** The isomorphism in this lemma has an explicit form:

$$\varphi : \frac{(L^\times)^n \cap K^\times}{(K^\times)^n} \cong \text{Hom}(G, \mu_n) \quad \bar{\lambda} \mapsto \left( \sigma \mapsto \frac{\sigma t}{t} \right)$$

where  $t^n = \lambda$ .

### Corollary 7.2

If  $L/K$  is a finite cyclic Galois extension of order  $n$ , then  $(L^\times)^n \cap K^\times / (K^\times)^n = \langle \bar{\alpha}^n \rangle$  is a cyclic group of order  $n$  for some  $\alpha \in L^\times$  with  $\alpha^n \in K^\times$ . Moreover,  $L = K(\alpha)$ .

**Proof:**  $\text{Gal}(L/K) = \langle \sigma \rangle$  is cyclic  $\Rightarrow$  the character group  $\text{Hom}(\text{Gal}(L/K), \mu_n)$  is cyclic. Because all elements of  $\text{Hom}(\text{Gal}(L/K), \mu_n)$  are  $\delta_i : \sigma \mapsto \xi^i$  where  $\xi$  is a primitive  $n$ -th root of unity (non-canonical). All  $\delta_i$  can be generated by the function  $\delta_1$ .

Tracing the isomorphism from corollary 7.1 gives a  $\lambda \in (L^\times)^n \cap K^\times$  corresponding to this  $\delta_1$ . Namely,  $\varphi : \bar{\lambda} \mapsto (\delta_1 : \sigma \mapsto \xi)$ . This  $\lambda$  also determines an  $\alpha$  such that  $\delta_1 \mapsto \sigma \alpha / \alpha$  and  $\alpha^n = \lambda$ . Equating both sides,  $\xi = \sigma \alpha / \alpha$ .

Also,  $\text{Gal}(L/K)$  is cyclic  $\Rightarrow \forall \sigma \neq \text{id}_L, \sigma \alpha \neq \alpha$ . Hence,  $|\text{Stab}_{\text{Gal}(L/K)}(\alpha)| = 1$ . Notice that  $\text{Stab}_{\text{Gal}(L/K)}(\alpha) = \text{Gal}(L/K(\alpha))$ . The Galois correspondence gives

$$[K(\alpha) : K] = [\text{Gal}(L/K) : \text{Gal}(L/K(\alpha))] = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/K(\alpha))|} = n$$

Hence,  $K(\alpha) = L$ . □

This corollary lies in a broader background, an equivalence which is the main part of Kummer's theory. It is sort of dual to the *point de vue relatif*: To classify cyclic extensions  $L/K$  of  $K$  of order  $n$ , the following theorem converts the perspective into  $K$  itself rather than looking outwards.

### Theorem 7.3: Correspondence between cyclic extensions and cyclic groups

Let  $K$  be a field with  $\mu_n \subseteq K$ . Then, there is a bijection

$$\begin{aligned} \{ \langle \bar{\alpha} \rangle \leq K^\times / (K^\times)^n : |\alpha| = n \} &\longleftrightarrow \{ L/K : L/K \text{ cyclic, } [L : K] = n \} \\ \langle \bar{\alpha} \rangle &\mapsto K(\sqrt[n]{\alpha}) \end{aligned}$$

In a more explicit word description,

$$\{ \text{cyclic subgroups of } K^\times / (K^\times)^n \text{ of order } n \} \longleftrightarrow \{ \text{cyclic extensions of } K \text{ of order } n \}$$

**Remark** This is a very excellent example of classification. The question is to classify all cyclic extensions  $L/K$  over  $K$  of order  $n$ . It is hard and cumbersome to know what  $L$  is. One might need to construct some  $L$ , to look at the minimal polynomial. Even though a candidate of  $L$  is constructed, there is no guarantee that all compliant  $L$ 's are obtained. Instead of staring at the outsides, this equivalence turns to the internal information in terms of  $K$ , which is known a priori.

#### 7.3.4 Application of group cohomology: Group extension

The case of group extension is similar to the case of  $R$ -module extensions. To utilize the language of modules, if there are some group actions, it can be made into  $\mathbb{Z}[G]$ -modules. This bridge the gap between groups and  $R$ -modules. But, category of group is not an abelian category. Let  $A, C, E$  be groups. The notion of extensions of  $A$  by  $C$  is almost the same as in  $R$ -modules:

### Definition 7.3: Extensions of groups

A group  $E$  is an extension of  $A$  by  $C \Leftrightarrow$  there is an exact sequence of groups  $\xi$

$$\xi : 0 \longrightarrow A \xrightarrow{f} E \xrightarrow{g} C \longrightarrow 0$$

Now for this short exact sequence of groups  $\xi : 0 \longrightarrow A \xrightarrow{f} E \xrightarrow{g} C \longrightarrow 0$ , we try to see something. The first observation is  $A \cong f(A) = \ker g$ , so  $f(A) \trianglelefteq E$ . This fact implies that  $\forall h \in C, hf(A)h^{-1} = f(A)$ . (Also true for  $E$ . But, the goal is to see all structures of  $E$  jointed by  $A$  and  $C$ .) For an arbitrary element  $h \in C$ , take a lift  $\tilde{h} \in E$  of  $g$ , i.e.  $g(\tilde{h}) = h$ . So, every lift of  $h$ ,  $\tilde{h}$ , induces an automorphism of  $f(A)$ :

$$\psi_{\tilde{h}} : f(A) \rightarrow f(A) \quad f(a) \mapsto \tilde{h}f(a)\tilde{h}^{-1}$$

Indeed, this equivalent to an automorphism of  $A$  by pulling the elements back.  $A \rightarrow A \quad a \mapsto f^{-1}(\tilde{h}f(a)\tilde{h}^{-1})$ . It seems natural to define an action  $C \curvearrowright A$ . Notice that this is only for lifted elements of  $C$  in  $E$ . One more gap is between this and an action of  $C$  on  $A$ : If both  $\tilde{h}_1$  and  $\tilde{h}_2$  are lifts of  $h$  in  $E$ , then

$$\psi_{\tilde{h}_1} : f(a) \mapsto \tilde{h}_1 f(a) \tilde{h}_1^{-1} \quad \psi_{\tilde{h}_2} : f(a) \mapsto \tilde{h}_2 f(a) \tilde{h}_2^{-1}$$

Since  $g(\tilde{h}_1) = g(\tilde{h}_2) = g$ ,  $\tilde{h}_1 \tilde{h}_2^{-1} \in \ker g$ . So,  $\exists k \in f(A), \tilde{h}_2 = \tilde{h}_1 k$ .

In this case,  $\psi_{\tilde{h}_2} : f(a) \mapsto \tilde{h}_1(kf(a)k^{-1})\tilde{h}_1^{-1}$ .  $\psi_{\tilde{h}_2} \circ \psi_{\tilde{h}_1}^{-1} \in \text{Inn}(f(A))$ . This implies that  $C$  barely induces a map

$$G \rightarrow \text{Out}(f(A)) = \text{Aut}(f(A))/\text{Inn}(f(A))$$

Further, it also induces a map  $C \rightarrow \text{Out}(A)$ . But  $\text{Out}(A)$  usually has complex structures beyond a module. But, the case gets simplified if  $A$  is abelian. When  $A$  is commutative,  $kf(a)k^{-1} = f(a)$  or  $\text{Inn}(f(A)) = \{1\}$ . The  $\text{Out}(A)$  structure is beyond the scope of our study here. To make the question simpler to get started with, the condition  $A$  is abelian is put.

So, from now on,  $\xi : 0 \rightarrow A \rightarrow E \rightarrow C \rightarrow 0$  is a short exact sequence with  $A$  being abelian and  $C$  being arbitrary.

The notion of equivalence is the same as in the module case.

Once an extension is given, there is a well-defined group action  $C \curvearrowright A$  or  $C \curvearrowright f(A)$ :  $\theta : G \rightarrow \text{Aut}(f(A))$ . The well-definedness is just from the argument above. Thus,  $\theta$  equip  $A$  with a  $C$ -module structure, which can be extended linearly and uniquely to a  $\mathbb{Z}[C]$ -module structure on  $A$ . The  $\mathbb{Z}[C]$  structure allows the discussion to fit into the frame of Ext functors and group cohomology. not quite clear.

#### Theorem 7.4: Classification of group extensions

Let  $A$  be an abelian group and  $C$  be an arbitrary group. Given an action  $\theta : C \rightarrow \text{Aut}(A)$ ,  $H^2(C, A_\theta)$  classifies all equivalence classes of group extensions of  $A$  by  $C$  under the action  $\theta$ . Then, the trivial element  $0 \in H^2(C, A_\theta)$  corresponds to the trivial class of extension, the semi-direct product  $A \rtimes_\theta C$ .

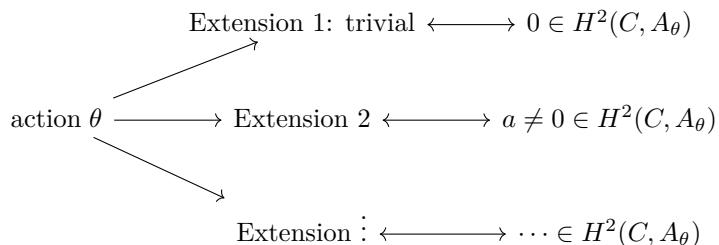
If  $H^2(C, A_\theta) = \{0\}$ , then any extension of  $A$  by  $C$  is a semi-direct product and the complement of  $A$  in  $E$  is classified by  $H^1(C, A_\theta)$ .

**Remark** The reason why we write the cohomology group as  $H^2(C, A_\theta)$  (sometimes  $H_\theta^2(C, A)$ ) is from

$$H^2(C, A_\theta) = \text{Ext}_{\mathbb{Z}[C]}^2(\mathbf{P}_\mathbb{Z}, A)$$

where the Ext functor depends on the  $\mathbb{Z}[C]$ -module structure of  $A$ . The structure of  $\mathbb{Z}[C]$  is always the same for a fixed  $C$ , because it merely depends on  $C$ . While, different actions  $C \curvearrowright A$  give different  $C$ -module structure of  $A$ . (Equivalently, different  $\mathbb{Z}[C]$ -module structure of  $A$ ). So, each time we talk about  $H^2(C, A_\theta)$ , an action  $\theta : C \rightarrow \text{Aut}(A)$  is already fixed beforehand.

After an action  $\theta$  being fixed, this theorem suggests that there are possibly many extensions of  $A$  by  $C$  corresponds to this action. Each action has at least one extension corresponds to an action. This is shown in the following diagram:



In the above-mentioned diagram, an 'extension' means an equivalent class of extension actually.

**Proof:**

□

The complete picture of classification entails all actions  $\theta$  and all extensions corresponds to a specific action. It is illustrated as follows:

$$\text{All extensions of } A \text{ by } C = \underbrace{\text{Actions } \theta : C \rightarrow \text{Aut}(A)}_{\text{representation theory}} + \underbrace{\text{Extensions corresponding to } \theta}_{\text{Theorem 7.4, using } H^2(C, A_\theta)}$$

So, representation theory tells us how many actions are there up to isomorphism(equivalence). For each action get in previous step, calculation of  $H^2(C, A_\theta)$  tells the number of extensions for this action. Combining these two steps together, we finally obtain all possible extensions of  $A$  by  $C$  up to equivalence.

**Lemma 7.4** If  $|A| = n$ , then  $\forall i \geq 0$ ,  $n \cdot H^i(C, A) = 0$ . If  $|G| = m$ , then  $\forall i \geq 1$ ,  $m \cdot H^i(C, A) = 0$

**Proof:** Fact: a group homomorphism  $\varphi : A \rightarrow B$  induces another group homomorphism  $\varphi^{i,*} : H^i(G, A) \rightarrow H^i(G, B)$  by  $[f] \mapsto [\varphi \circ f]$ .

$[n] : A \rightarrow A$  is also a group homomorphism by  $x \mapsto n \cdot x$ . So, it induces a homomorphism  $[n]^{i,*} : H^i(G, A) \rightarrow H^i(G, A)$ . Since  $|A| = n$ ,  $[n] \circ f = 0$ . This implies that  $[n]^{i,*}$  is a zero map. Hence,  $n \cdot H^i(G, A) = 0$  for all  $i \geq 0$ .

For the second case, a detour occurs. unfinished

### Corollary 7.3: Schur-Zassenhaus theorem

Let  $E$  be a finite group with an abelian subgroup  $A \trianglelefteq E$  (normal abelian) such that  $(|A|, |E/A|) = 1$ . Then,  $H^2(E/A, A) = \{0\}$ . Hence,  $E = A \rtimes E/A$  and complements of  $A$  in  $E$  are conjugate.

**Proof:** By the previous lemma,  $\forall n \geq 1$ ,  $|A| \cdot H^n(E/A, A) = 0$  and  $|E/A| \cdot H^n(E/A, A) = 0$  simultaneously.  $(|A|, |E/A|) = 1$  implies that  $\exists a, b \in \mathbb{Z}$ ,  $a|A| + b|E/A| = 1$ . Hence,  $\forall n \geq 1$ ,  $H^n(E/A, A) = \{0\}$ .  $n = 2$  is desired. Because  $0 \rightarrow A \rightarrow E \rightarrow E/A \rightarrow 0$  is an extension of  $A$  by  $E/A$ . Theorem 7.4 asserts  $E \cong A \rtimes E/A$ .

The conjugacy classes are classified by  $H^1(E/A, A) = \{0\}$ . □

**Example** (1) Consider the alternating group  $A_4$  and its Klein subgroup  $K = \{(1), (12)(34), (13)(24), (14)(23)\}$ . Notice  $K \trianglelefteq A_4$  and  $K$  is abelian (normal abelian).  $|A_4| = 12$ ,  $|K| = 4$  and  $|A_4/K| = 3$ . So, the corollary 7.3 implies that  $H^2(A_4/K, K) = 0$  and  $A_4$  is the semi-direct product of  $K$  and its complement in  $A_4$ , i.e. of the form  $K \rtimes H$  with  $H \leq A_4$  and  $|H| = 3$ . ( $H$  can be taken as  $\langle (123) \rangle$  for example.) The corollary also states that any two choices of  $H$  (two complements of  $K$ ) are conjugate. Even though two '3-cycle' elements are not conjugate in  $A_4$  ( $(123)$  and  $(132)$  are not conjugate in  $A_4$ ), the subgroups generated by each of them are conjugate. So, this theorem provides an alignment on the subgroup level.

(2) Consider a group  $E$  of order  $|E| = 11^2 \cdot 3 \cdot 5$ .

By Sylow's theorem, the Sylow 11 subgroup  $G_{11}$  of  $E$  is normal in  $E$ .  $|G_{11}| = 11^2$ , so  $G_{11}$  is an abelian group. The quotient  $E/G_{11}$  has order 15. Thus, we can apply the corollary 7.3 to get  $H^2(E/G_{11}, G_{11}) = 0$  and  $E \cong G_{11} \rtimes E/G_{11}$ . Since the order of  $E/G_{11}$  is of the type  $pq$  and  $p \nmid (q-1)$ ,  $E/G_{11}$  is cyclic hence  $\cong \mathbb{Z}/15\mathbb{Z}$ . Hence, every group of order  $11^2 \cdot 3 \cdot 5$  is an extension of  $G_{11}$  by  $\mathbb{Z}/15\mathbb{Z}$ :

$$0 \rightarrow G_{11} \rightarrow E \rightarrow \mathbb{Z}/15\mathbb{Z} \rightarrow 0$$

and  $E \cong G_{11} \rtimes_{\theta} \mathbb{Z}/15\mathbb{Z}$

By fundamental theorem of abelian groups, the possibilities of  $G_{11}$  are either  $\cong \mathbb{Z}/11^2\mathbb{Z}$  or  $\cong (\mathbb{Z}/11\mathbb{Z})^2$ :

Case 1:  $G_{11} \cong \mathbb{Z}/121\mathbb{Z}$  (cyclic).  $\text{Aut}(\mathbb{Z}/121\mathbb{Z})$  is determined by where the generators go. So,  $|\text{Aut}(\mathbb{Z}/121\mathbb{Z})| = |\varphi(121)| = 110$ . Let  $B$  be a subgroup of  $\mathbb{Z}/15\mathbb{Z}$  of order 3. Restrict  $\theta$  to  $\theta|_B$ .  $|\text{im } \theta|_B| = [B : \ker \theta|_B]$ , so  $|\text{im } \theta|_B| \mid 3$ .

Simultaneously,  $|\text{im } \theta|_B| \mid 110$ . So, the action  $\theta|_B$  is trivial, implying  $B \subseteq \ker \theta$ . Hence,  $B \trianglelefteq \mathbb{Z}/15\mathbb{Z}$ .

This complement  $\mathbb{Z}/15\mathbb{Z}$  of  $G_{11}$  can be intrinsically recovered from  $E$ : Let  $P_3$  be an arbitrary Sylow-3 group of  $E$ ,  $P_3 \trianglelefteq E$ . Take any Sylow-5 subgroup of  $E$ ,  $P_5$ . Consider the internal direct product  $P_3 P_5$ , which is a group because  $P_3 \trianglelefteq E$ .  $|P_3 P_5| = |P_3||P_5|/|P_3 \cap P_5| = 15$ . It is a complement of  $A$ . Further calculation yields  $G_{11} \cap (P_3 P_5) = \{1\}$  and they consist a group of order  $11^2 \cdot 3 \cdot 5$ .

Case 2:  $G_{11} \cong (\mathbb{Z}/11\mathbb{Z})^2 \cong \mathbb{F}_{11}^2$  (non-cyclic).  $\text{Aut}((\mathbb{Z}/11\mathbb{Z})^2) \cong \text{GL}_2(\mathbb{Z}/11\mathbb{Z}) = \text{GL}_2(\mathbb{F}_{11})$ .  $|\text{Aut}(\mathbb{Z}/11\mathbb{Z})| = (11^2 - 1)(11^2 - 11)$ .<sup>7</sup>

<sup>7</sup>This is from counting elements of  $\text{GL}_n(F)$  over a finite field  $F$ . As in  $\text{GL}_2$ , finding elements of  $\text{GL}_2(F)$  is equivalent to find all possible combinations of two non-zero linear independent vectors  $(x, y)^\top$  with  $x, y \in F$ . For the first column, one can pick all vectors except  $(0, 0)^\top$ . For the second column, by fixing the first column one can pick all vectors besides the subspace generated by the first column. This subspace is of 11 elements including  $(0, 0)^\top$ . So, there are  $11^2 - 11$  choices of elements for the second column.

## 8 Introduction to spectral sequences

## References

- [Rot09] Joseph J. Rotman. “Homology”. In: *An Introduction to Homological Algebra*. New York, NY: Springer New York, 2009, pp. 1–81. ISBN: 978-0-387-68324-9. DOI: [10.1007/978-0-387-68324-9\\_6](https://doi.org/10.1007/978-0-387-68324-9_6). URL: [https://doi.org/10.1007/978-0-387-68324-9\\_6](https://doi.org/10.1007/978-0-387-68324-9_6).