

Part A
Homological Algebra

MATH 101B: ALGEBRA II
PART A: HOMOLOGICAL ALGEBRA

These are notes for our first unit on the algebraic side of homological algebra. While this is the last topic (Chap XX) in the book, it makes sense to do this first so that grad students will be more familiar with the ideas when they are applied to algebraic topology (in 121b). At the same time, it is not my intention to cover the same material twice. The topics are

CONTENTS

1. Additive categories	1
2. Abelian categories	2
2.1. some definitions	2
2.2. definition of abelian category	3
2.3. examples	4
3. Projective and injective objects	5
4. Injective modules	7
4.1. dual module	7
4.2. constructing injective modules	8
4.3. proof of lemmas	9
4.4. Examples	12
5. Divisible groups	15
Injective envelope	17
6. Projective resolutions	17
6.1. Definitions	17
6.2. Modules of a PID	18
6.3. Chain complexes	20
6.4. Homotopy uniqueness of projective resolutions	23
6.5. Derived functors	26
6.6. Left derived functors	31

1. ADDITIVE CATEGORIES

On the first day I talked about additive categories.

Definition 1.1. An additive category is a category \mathcal{C} for which every hom set $\text{Hom}_{\mathcal{C}}(X, Y)$ is an additive group and

- (1) composition is biadditive, i.e., $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$ and $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$.
- (2) The category has finite direct sums.

I should have gone over the precise definition of direct sum:

Definition 1.2. The direct sum $\bigoplus_{i=1}^n A_i$ is an object X together with morphisms $j_i : A_i \rightarrow X, p_i : X \rightarrow A_i$ so that

- (1) $p_i \circ j_i = \text{id} : A_i \rightarrow A_i$
- (2) $p_i \circ j_j = 0$ if $i \neq j$.
- (3) $\sum j_i \circ p_i = \text{id}_X : X \rightarrow X$.

Theorem 1.3. $\bigoplus A_i$ is both the product and coproduct of the A_i

Proof. Suppose that $f_i : Y \rightarrow A_i$ are morphisms. Then there is a morphism

$$f = \sum j_i \circ f_i : Y \rightarrow \bigoplus A_i$$

which has the property that $p_i \circ f = p_i j_i f_i = f_i$. Conversely, given any morphism $g : Y \rightarrow \bigoplus A_i$ satisfying $p_i \circ g = f_i$ for all i , then we have:

$$f = \sum j_i f_i = \sum j_i p_i g = \text{id}_X \circ g = g$$

So, f is unique and $\bigoplus A_i$ is the product of the A_i . By an analogous argument, it is also the coproduct. □

The converse is also true:

Proposition 1.4. *Suppose that $X = \prod A_i = \coprod A_i$ and the composition of the inclusion $j_i : A_i \rightarrow X$ with $p_j : X \rightarrow A_j$ is*

$$p_j \circ j_i = \delta_{ij} : A_i \rightarrow A_j$$

I.e., it is the identity on A_i for $i = j$ and it is zero for $i \neq j$. Then

$$\sum j_i \circ p_i = id_X$$

Proof. Let $f = \sum j_i \circ p_i : X \rightarrow X$. Then

$$p_j \circ f = \sum_i p_j \circ j_i \circ p_i = \sum_i \delta_{ij} p_i = p_j$$

So, $f = id_X$ by the universal property of a product. \square

In class I pointed out the sum of no objects is the zero object 0 which is both initial and terminal. Also, I asked you to prove the following.

Problem. Show that a morphism $f : A \rightarrow B$ is zero if and only if it factors through the zero object.

2. ABELIAN CATEGORIES

2.1. some definitions. First I explained the abstract definition of kernel, monomorphism, cokernel and epimorphism.

Definition 2.1. *A morphism $f : A \rightarrow B$ in an additive category \mathcal{C} is a monomorphism if, for any object X and any morphism $g : X \rightarrow A$, $f \circ g = 0$ if and only if $g = 0$. (g acts like an “element” of A . It goes to zero in B iff it is zero.)*

Another way to say this is that $f : A \rightarrow B$ is a monomorphism and write $0 \rightarrow A \rightarrow B$ if

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(X, A) \xrightarrow{f_{\sharp}} \text{Hom}_{\mathcal{C}}(X, B)$$

is exact, i.e., f_{\sharp} is a monomorphism of abelian groups. The lower sharp means composition on the left or “post-composition.” The lower sharp is order preserving:

$$(f \circ g)_{\sharp} = f_{\sharp} \circ g_{\sharp}$$

Epimorphisms are defined analogously: $f : B \rightarrow C$ is an *epimorphism* if for any object Y we get a monomorphism of abelian groups:

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(C, Y) \xrightarrow{f^{\sharp}} \text{Hom}_{\mathcal{C}}(B, Y)$$

An abelian category is an additive category which has kernels and cokernels satisfying all the properties that one would expect which can be stated categorically. First, I explained the categorical definition of kernel and cokernel.

Definition 2.2. *The kernel of a morphism $f : A \rightarrow B$ is an object K with a morphism $j : K \rightarrow A$ so that*

- (1) $f \circ j = 0 : K \rightarrow B$
- (2) *For any other object X and morphism $g : X \rightarrow A$ so that $f \circ g = 0$ there exists a unique $h : X \rightarrow K$ so that $g = j \circ h$.*

Since this is a universal property, the kernel is unique if it exists.

Theorem 2.3. *A is the kernel of $f : B \rightarrow C$ if and only if*

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(X, A) \rightarrow \text{Hom}_{\mathcal{C}}(X, B) \rightarrow \text{Hom}_{\mathcal{C}}(X, C)$$

is exact for any object X . In particular, $j : \ker f \rightarrow B$ is a monomorphism.

If you replace A with 0 in this theorem you get the following statement.

Corollary 2.4. *A morphism is a monomorphism if and only if 0 is its kernel.*

Cokernel is defined analogously and satisfies the following theorem which can be used as the definition.

Theorem 2.5. *The cokernel of $f : A \rightarrow B$ is an object C with a morphism $B \rightarrow C$ so that*

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(C, Y) \rightarrow \text{Hom}_{\mathcal{C}}(B, Y) \rightarrow \text{Hom}_{\mathcal{C}}(A, Y)$$

is exact for any object Y .

Again, letting $C = 0$ we get the statement:

Corollary 2.6. *A morphism is an epimorphism if and only if 0 is its cokernel.*

These two theorems can be summarized by the following statement.

Corollary 2.7. *For any additive category \mathcal{C} , $\text{Hom}_{\mathcal{C}}$ is left exact in each coordinate.*

2.2. definition of abelian category.

Definition 2.8. *An abelian category is an additive category \mathcal{C} so that*

- (1) *Every morphism has a kernel and a cokernel.*
- (2) *Every monomorphism is the kernel of its cokernel.*

- (3) Every epimorphism is the cokernel of its kernel.
- (4) Every morphism $f : A \rightarrow B$ can be factored as the composition of an epimorphism $A \rightarrow I$ and a monomorphism $I \hookrightarrow B$.
- (5) A morphism $f : A \rightarrow B$ is an isomorphism if and only if it is both mono and epi.

Proposition 2.9. *The last condition follows from the first four conditions.*

Proof. First of all, isomorphisms are always both mono and epi. The definition of an isomorphism is that it has an inverse $g : B \rightarrow A$ so that $f \circ g = id_B$ and $g \circ f = id_A$. The second condition implies that f is mono since

$$(g \circ f)_{\#} = g_{\#} \circ f_{\#} = id_{\#} = id$$

which implies that $f_{\#}$ is mono and f is mono. Similarly, $f \circ g = id_B$ implies that f is epi.

Conversely, suppose that $f : A \rightarrow B$ is both mono and epi. Then, by (2), it is the kernel of its cokernel which is $B \rightarrow 0$. So, by left exactness of Hom we get:

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(B, A) \rightarrow \text{Hom}_{\mathcal{C}}(B, B) \rightarrow \text{Hom}_{\mathcal{C}}(B, 0)$$

In other words, $f_{\#} : \text{Hom}_{\mathcal{C}}(B, A) \cong \text{Hom}_{\mathcal{C}}(B, B)$. So, there is a unique element $g : B \rightarrow A$ so that $f \circ g = id_B$. Similarly, by (3), there is a unique $h : B \rightarrow A$ so that $h \circ f = id_A$. If we can show that $g = h$ then it will be the inverse of f making f invertible and thus an isomorphism. But this is easy:

$$h = h \circ id_B = h \circ f \circ g = id_A \circ g = g$$

□

2.3. examples. The following are abelian categories:

- (1) The category of abelian groups and homomorphisms.
- (2) The category of finite abelian groups. This is an abelian category since any homomorphism of finite abelian groups has a finite kernel and cokernel and a finite direct sum of finite abelian groups is also finite.
- (3) $R\text{-mod}$ = the category of all left R -modules and homomorphisms
- (4) $R\text{-Mod}$ = the category of finitely generated (f.g.) left R -modules is an abelian category assuming that R is left Noetherian (all submodules of f.g. left R -modules are f.g.)
- (5) $\text{mod-}R$ =the category of all right R -modules and homomorphisms
- (6) $\text{Mod-}R$ =the category of f.g. right R -modules is abelian if R is right Noetherian.

The following are examples of additive categories which are not abelian.

- (1) Free abelian groups. (This category does not have cokernels)
- (2) Let R be a non-Noetherian ring, for example a polynomial ring in infinitely many variables:

$$R = k[X_1, X_2, \dots]$$

Then $R\text{-Mod}$, the category of f.g. R -modules is not abelian since it does not have kernels. E.g., the kernel of the augmentation map

$$R \rightarrow k$$

is infinitely generated.

3. PROJECTIVE AND INJECTIVE OBJECTS

At the end of the second lecture we discussed the definition of injective and projective objects in any additive category. And it was easy to show that the category of R -modules has sufficiently many projectives.

Definition 3.1. *An object P of an additive category \mathcal{C} is called projective if for any epimorphism $f : A \rightarrow B$ and any morphism $g : P \rightarrow B$ there exists a morphism $\tilde{g} : P \rightarrow A$ so that $f \circ \tilde{g} = g$. The map \tilde{g} is called a lifting of g to A .*

Theorem 3.2. *P is projective if and only if $\text{Hom}_{\mathcal{C}}(P, -)$ is an exact functor.*

Proof. If $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact then, by left exactness of Hom we get an exact sequence:

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(P, A) \rightarrow \text{Hom}_{\mathcal{C}}(P, B) \rightarrow \text{Hom}_{\mathcal{C}}(P, C)$$

By definition, P is projective if and only if the last map is always an epimorphism, i.e., iff we get a short exact sequence

$$0 \rightarrow \text{Hom}_{\mathcal{C}}(P, A) \rightarrow \text{Hom}_{\mathcal{C}}(P, B) \rightarrow \text{Hom}_{\mathcal{C}}(P, C) \rightarrow 0$$

□

Theorem 3.3. *Any free R -module is projective.*

Proof. Suppose that F is free with generators x_{α} . Then every element of F can be written uniquely as $\sum r_{\alpha}x_{\alpha}$ where the coefficients $r_{\alpha} \in R$ are almost all zero (only finitely many are nonzero). Suppose that $g : F \rightarrow B$ is a homomorphism. Then, for every index α , the element

$g(x_\alpha)$ comes from some element $y_\alpha \in A$. I.e., $g(x_\alpha) = f(y_\alpha)$. Then a lifting \tilde{g} of g is given by

$$\tilde{g}\left(\sum r_\alpha x_\alpha\right) = \sum r_\alpha y_\alpha$$

The verification that this is a lifting is “straightforward” or I would say “obvious” but it would go like this: The claim is that, first, $\tilde{g} : F \rightarrow A$ is a homomorphism of R -modules and, second, it is a lifting: $f \circ \tilde{g} = g$. The second statement is easy:

$$f \circ \tilde{g}\left(\sum r_\alpha x_\alpha\right) = f\left(\sum r_\alpha y_\alpha\right) = \sum r_\alpha f(y_\alpha) = \sum r_\alpha g(x_\alpha) = g\left(\sum r_\alpha x_\alpha\right)$$

The first claim says that \tilde{g} is additive:

$$\begin{aligned} \tilde{g}\left(\sum r_\alpha x_\alpha + \sum s_\alpha x_\alpha\right) &= \tilde{g}\left(\sum (r_\alpha + s_\alpha)x_\alpha\right) \\ &= \sum (r_\alpha + s_\alpha)y_\alpha = \tilde{g}\left(\sum r_\alpha x_\alpha\right) + \tilde{g}\left(\sum s_\alpha x_\alpha\right) \end{aligned}$$

and \tilde{g} commutes with the action of R :

$$\begin{aligned} \tilde{g}\left(r \sum r_\alpha x_\alpha\right) &= \tilde{g}\left(\sum r r_\alpha x_\alpha\right) \\ &= \sum r r_\alpha y_\alpha = r \sum r_\alpha x_\alpha = r \tilde{g}\left(\sum r_\alpha x_\alpha\right) \end{aligned}$$

□

For every R -module M there is a free R -module which maps onto M , namely the free module F generated by symbols $[x]$ for all $x \in M$ and with projection map $p : F \rightarrow M$ given by

$$p\left(\sum r_\alpha [x_\alpha]\right) = \sum r_\alpha x_\alpha$$

The notation $[x]$ is used to distinguish between the element $x \in M$ and the corresponding generator $[x] \in F$. The homomorphism p is actually just defined by the equation $p[x] = x$.

Corollary 3.4. *The category of R -modules has sufficiently many projectives, i.e., for every R -module M there is a projective R -module which maps onto M .*

This implies that every R -module M has a *projective resolution*

$$0 \leftarrow M \leftarrow P_0 \leftarrow P_1 \leftarrow P_2 \leftarrow \dots$$

This is an exact sequence in which every P_i is projective. The projective modules are constructed inductively as follows. First, P_0 is any projective which maps onto M . This gives an exact sequence:

$$P_0 \rightarrow M \rightarrow 0$$

By induction, we get an exact sequence

$$P_n \rightarrow P_{n-1} \rightarrow P_{n-2} \rightarrow \cdots \rightarrow P_0 \rightarrow M \rightarrow 0$$

Let K_n be the kernel of $d_n : P_n \rightarrow P_{n-1}$. Since there are enough projectives, there is a projective module P_{n+1} which maps onto K_n . The composition $P_{n+1} \rightarrow K_n \hookrightarrow P_n$ is the map $d_{n+1} : P_{n+1} \rightarrow P_n$ which extends the exact sequence one more step.

Definition 3.5. *An object Q of \mathcal{C} is injective if, for any monomorphism $A \rightarrow B$, any morphism $A \rightarrow Q$ extends to B . I.e., iff*

$$\text{Hom}_{\mathcal{C}}(B, Q) \rightarrow \text{Hom}_{\mathcal{C}}(A, Q) \rightarrow 0$$

As before this is equivalent to:

Theorem 3.6. *Q is injective if and only if $\text{Hom}_{\mathcal{C}}(-, Q)$ is an exact functor.*

The difficult theorem we need to prove is the following:

Theorem 3.7. *The category of R -modules has sufficiently many injectives. I.e., every R -module embeds in an injective R -module.*

As in the case of projective modules this theorem will tell us that every R -module M has an *injective co-resolution* which is an exact sequence:

$$0 \rightarrow M \rightarrow Q_0 \rightarrow Q_1 \rightarrow Q_2 \rightarrow \cdots$$

where each Q_i is injective.

4. INJECTIVE MODULES

I will go over Lang's proof that every R -module M embeds in an injective module Q . Lang uses the dual of the module.

4.1. dual module.

Definition 4.1. *The dual of a left R -module M is defined to be the right R -module*

$$M^\wedge := \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$

with right R -action given by

$$\phi r(x) = \phi(rx)$$

for all $\phi \in M^\wedge, r \in R$.

Proposition 4.2. *Duality is a left exact functor*

$$(\)^\wedge : R\text{-mod} \rightarrow \text{mod-}R$$

which is additive and takes sums to products:

$$(\oplus M_\alpha)^\wedge \cong \prod M_\alpha^\wedge$$

Proof. We already saw that the hom functor $\text{Hom}_{\mathbb{Z}}(-, X)$ is left exact for any abelian group X . It is also obviously *additive* which means that $(f + g)^\sharp = f^\sharp + g^\sharp$ for all $f, g : N \rightarrow M$. I.e., the duality functor induces a homomorphism (of abelian groups):

$$\text{Hom}_R(N, M) \rightarrow \text{Hom}_{\mathbb{Z}}(M^\wedge, N^\wedge)$$

Duality also takes sums to products since a homomorphism

$$f : \oplus M_\alpha \rightarrow X$$

is given uniquely by its restriction to each summand: $f_\alpha : M_\alpha \rightarrow X$ and the f_α can all be nonzero. (So, it is the product not the sum.) \square

4.2. constructing injective modules. In order to get an injective left R -module we need to start with a right R -module.

Theorem 4.3. *Suppose F is a free right R -module. (I.e., $F = \oplus R_R$ is a direct sum of copies of R considered as a right R -module). Then F^\wedge is an injective left R -module.*

This theorem follows from the following lemma.

Lemma 4.4. (1) *A product of injective modules is injective.*
 (2) $\text{Hom}_R(M, R_R^\wedge) \cong \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$
 (3) \mathbb{Q}/\mathbb{Z} *is an injective \mathbb{Z} -module.*

Proof of the theorem. Lemma (3) implies that $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is an exact functor. (2) implies that $\text{Hom}_R(-, R_R^\wedge)$ is an exact functor. Therefore, R_R^\wedge is an injective R -module. Since duality takes sums to products, (1) implies that F^\wedge is injective for any F with is a sum of R_R 's, i.e. F is a free right R -module. \square

We need one more lemma to prove the main theorem. Then we have to prove the lemmas.

Lemma 4.5. *Any left R -module is naturally embedded in its double dual:*

$$M \subseteq M^{\wedge\wedge}$$

Assume this 4th fact for a moment.

Theorem 4.6. *Every left R -module M can be embedded in an injective left R -module.*

Proof. Let F be a free right R -module which maps onto M^\wedge :

$$F \rightarrow M^\wedge \rightarrow 0$$

Since duality is left exact we get:

$$0 \rightarrow M^{\wedge\wedge} \rightarrow F^\wedge$$

By the last lemma we have $M \subseteq M^{\wedge\wedge} \subseteq F^\wedge$. So, M embeds in the injective module F^\wedge . \square

4.3. proof of lemmas. There are four lemmas to prove. Suppose for a moment that $T = \mathbb{Q}/\mathbb{Z}$ is injective then the other three lemmas are easy:

Proof of Lemma 4.5. A natural embedding $M \rightarrow M^{\wedge\wedge}$ is given by the evaluation map ev which sends $x \in M$ to $ev_x : M^\wedge \rightarrow T$ which is *evaluation at x* :

$$ev_x(\phi) = \phi(x)$$

Evaluation is additive:

$$ev_{x+y}(\phi) = \phi(x+y) = \phi(x) + \phi(y) = ev_x(\phi) + ev_y(\phi) = (ev_x + ev_y)(\phi)$$

Evaluation is an R -module homomorphism:

$$ev_{rx}(\phi) = \phi(rx) = (\phi r)(x) = ev_x(\phi r) = (rev_x)(\phi)$$

Finally, we need to show that ev is a monomorphism. In other words, for every nonzero element $x \in M$ we need to find some additive map $\phi : M \rightarrow T$ so that $ev_x(\phi) = \phi(x) \neq 0$. To do this take the cyclic group C generated by x

$$C = \{kx \mid k \in \mathbb{Z}\}$$

This is either \mathbb{Z} or \mathbb{Z}/n . In the second case let $f : C \rightarrow T$ be given by

$$f(kx) = \frac{k}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$$

This is nonzero on x since $1/n$ is not an integer. If $C \cong \mathbb{Z}$ then let $f : C \rightarrow T$ be given by

$$f(kx) = \frac{k}{2} + \mathbb{Z}$$

Then again, $f(x)$ is nonzero. Since T is \mathbb{Z} -injective, f extends to an additive map $\phi : M \rightarrow T$. So, ev_x is nonzero and $ev : M \rightarrow M^{\wedge\wedge}$ is a monomorphism. \square

Proof that products of injectives are injective. Suppose that J_α are injective. Then we want to show that $Q = \prod J_\alpha$ is injective. Let $p_\alpha : Q \rightarrow J_\alpha$ be the projection map. Suppose that $f : A \rightarrow B$ is a monomorphism and $g : A \rightarrow Q$ is any morphism. Then we want to extend g to B .

Since each J_α is injective each composition $p_\alpha \circ g : A \rightarrow J_\alpha$ extends to a morphism $g_\alpha : B \rightarrow J_\alpha$. I.e., $g_\alpha \circ f = p_\alpha \circ g$ for all α . By definition of the product there exists a unique morphism $\bar{g} : B \rightarrow Q = \prod J_\alpha$ so that $p_\alpha \circ \bar{g} = g_\alpha$ for each α . So,

$$p_\alpha \circ \bar{g} \circ f = g_\alpha \circ f = p_\alpha \circ g : A \rightarrow J_\alpha$$

The uniquely induced map $A \rightarrow \prod J_\alpha$ is $\bar{g} \circ f = g$. Therefore, \bar{g} is an extension of g to B as required. \square

Finally, we need to prove that

$$\text{Hom}_R(M, R_R^\wedge) \cong \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$

To do this we will give a 1-1 correspondence and show that it (the correspondence) is additive.

If $f \in \text{Hom}_R(M, R_R^\wedge)$ then f is a homomorphism $f : M \rightarrow R_R^\wedge$ which means that for each $x \in M$ we get a homomorphism $f(x) : R \rightarrow \mathbb{Q}/\mathbb{Z}$. In particular we can evaluate this at $1 \in R$. This gives $\phi(f) : M \rightarrow \mathbb{Q}/\mathbb{Z}$ by the formula

$$\phi(f)(x) = f(x)(1)$$

This defines a mapping

$$\phi : \text{Hom}_R(M, R_R^\wedge) \rightarrow \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$$

We need to know that this is additive. I used “know” instead of “show” since this is one of those steps that you should normally skip. However, you need to know what it is that you are skipping. The fact that we need to know is that

$$\phi(f + g) = \phi(f) + \phi(g)$$

This is an easy calculation which follows from the way that $f + g$ is defined, namely, addition of function is defined “pointwise” which means that $(f + g)(x) = f(x) + g(x)$ by definition. So, $\forall x \in M$,

$$\begin{aligned} \phi(f + g)(x) &= (f + g)(x)(1) = [f(x) + g(x)](1) = f(x)(1) + g(x)(1) \\ &= \phi(f)(x) + \phi(g)(x) = [\phi(f) + \phi(g)](x) \end{aligned}$$

Finally we need to show that ϕ is a bijection. To do this we find the inverse $\phi^{-1} = \psi$. For any homomorphism $g : M \rightarrow \mathbb{Q}/\mathbb{Z}$ let $\psi(g) : M \rightarrow R_R^\wedge$ be given by

$$\psi(g)(x)(r) = g(rx)$$

Since this is additive in all three variables, ψ is additive and $\psi(g)$ is additive. We also need to check that $\psi(g)$ is a homomorphism of left R -modules, i.e., that $\psi(g)(rx) = r\psi(g)(x)$. This is an easy calculation:

$$\begin{aligned} \psi(g)(rx)(s) &= g(s(rx)) = g((sr)x) \\ [r\psi(g)(x)](s) &= [\psi(g)(x)](sr) = g((sr)x) \end{aligned}$$

The verification that ψ is the inverse of ϕ is also straightforward: For all $f \in \text{Hom}_R(M, R_R^\wedge)$ we have

$$\psi(\phi(f))(x)(r) = \phi(f)(rx) = f(rx)(1) = [rf(x)](1) = f(x)(1r) = f(x)(r)$$

So, $\psi(\phi(f)) = f$. Similarly, for all $g \in \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ we have:

$$\phi(\psi(g))(x) = \psi(g)(x)(1) = g(1x) = g(x)$$

So, $\phi(\psi(g)) = g$.

I will do the last lemma (injectivity of \mathbb{Q}/\mathbb{Z}) tomorrow.

4.4. Examples. I prepared 3 examples but I only got to two of them in class.

4.4.1. polynomial ring. Let $R = \mathbb{Z}[t]$, the integer polynomial ring in one generator. This is a commutative Noetherian ring. It has dimension 2 since a maximal tower of prime ideal is given by

$$0 \subset (t) \subset (t, 2)$$

These ideals are prime since the quotient of R by these ideals are domains (i.e., have no zero divisors):

$$R/0 = \mathbb{Z}[t], \quad R/(t) = \mathbb{Z}$$

are domains and

$$R/(t, 2) = \mathbb{Z}/(2) = \mathbb{Z}/2\mathbb{Z}$$

is a field, making $(2, t)$ into a maximal ideal.

Proposition 4.7. *A $\mathbb{Z}[t]$ module M is the same as an abelian group together with an endomorphism $M \rightarrow M$ given by the action of t . A homomorphism of $\mathbb{Z}[t]$ -modules $f : M \rightarrow N$ is an additive homomorphism which commutes with the action of t .*

Proof. I will use the fact that the structure of an R -module on an additive group M is the same as a homomorphism of rings $\phi : R \rightarrow \text{End}(M)$. When $R = \mathbb{Z}[t]$, this homomorphism is given by its value on t since $\phi(f(t)) = f(\phi(t))$. For example, if $f(t) = 2t^2 + 3$ then

$$\phi(f(t)) = \phi(2t^2 + 3) = 2\phi(t) \circ \phi(t) + 3id_M = f(\phi(t))$$

Therefore, ϕ is determined by $\phi(t) \in \text{End}_{\mathbb{Z}}(M)$ which is arbitrary. \square

What do the injective R -modules look like? We know that $Q = R_R^\wedge$ is injective. What does that look like?

$$Q = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[t], \mathbb{Q}/\mathbb{Z})$$

But $\mathbb{Z}[t]$ is a free abelian group on the generators $1, t, t^2, t^3, \dots$. Therefore, an element $f \in Q$, $f : \mathbb{Z}[t] \rightarrow \mathbb{Q}/\mathbb{Z}$ is given uniquely by the sequence

$$f(1), f(t), f(t^2), f(t^3), \dots \in \mathbb{Q}/\mathbb{Z}$$

Multiplication by t shifts this sequence to the left since $tf(t^i) - f(t^i t) = f(t^{i+1})$. This proves the following.

Theorem 4.8. *The injective module $Q = \mathbb{Z}[t]^\wedge$ is isomorphic to the additive group of all sequences (a_0, a_1, a_2, \dots) of elements $a_i \in \mathbb{Q}/\mathbb{Z}$ with the action of t given by shifting to the left and dropping the first coordinate. I.e.,*

$$t(a_0, a_1, a_2, \dots) = (a_1, a_2, \dots)$$

The word “isomorphism” is correct here because these are not the same set.

4.4.2. *fields.* Suppose that $R = k$ is a field. Then I claim that all k -modules are both projective and injective.

First note that a k -module is the same as a vector space over the field k . Since every vector space has a basis, all k -modules are free. Therefore, all k -modules are projective. Then I went through a round about argument to show that all k -modules are injective and I only managed to show that finitely generated k -modules are injective. (More on this later.)

Finally, I started over and used the following theorem.

Theorem 4.9. *Suppose that R is any ring. Then the following are equivalent (tfae).*

- (1) *All left R -modules are projective.*
- (2) *All left R -modules are injective.*
- (3) *Every short exact sequence of R -modules splits.*

First I recalled the definition of a splitting of a short exact exact sequence.

Proposition 4.10. *Given a short exact sequence of left R -modules*

$$(4.1) \quad 0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

Tfae.

- (1) *$B = f(A) \oplus D$ for some submodule $D \subseteq B$.*
- (2) *f has a retraction, i.e., a morphism $r : B \rightarrow A$ s.t. $r \circ f = id_A$.*
- (3) *g has a section, i.e., a morphism $s : C \rightarrow B$ s.t. $g \circ s = id_C$.*

Proof. This is a standard fact that most people know very well. For example, (1) \Rightarrow (2) because a retraction r is given by projection to the first coordinate followed by the inverse of the isomorphism $f : A \rightarrow f(A)$. (2) \Rightarrow (1) by letting $D = \ker r$. [You need to verify that $B = f(A) \oplus D$ which is in two steps: $D \cap f(A) = 0$ and $D + f(A) = B$. For example, $\forall x \in B, x = fr(x) + (x - fr(x)) \in f(A) + D.$] \square

Proof of Theorem . (1) \Rightarrow (3): In the short exact sequence (4.1), C is projective (since all modules are assumed projective). Therefore, the identity map $C \rightarrow C$ lifts to B and the sequence splits.

(3) \Rightarrow (1): Since any epimorphism $g : B \rightarrow C$ has a section s , any morphism $f : X \rightarrow C$ has a lifting $\tilde{f} = s \circ f : X \rightarrow B$.

The equivalence (2) \iff (3) is similar. □

5. DIVISIBLE GROUPS

\mathbb{Z} -modules are the same as abelian groups. And we will see that injective \mathbb{Z} -modules are the same as divisible groups.

Definition 5.1. *An abelian group D is called divisible if for any $x \in D$ and any positive integer n there exists $y \in D$ so that $ny = x$. (We say that x is divisible by n .)*

For example, \mathbb{Q} is divisible. 0 is divisible. A finite groups is divisible if and only if it is 0 .

Proposition 5.2. *Any quotient of a divisible group is divisible.*

Proof. Suppose D is divisible and K is a subgroup. Then any element of the quotient D/K has the form $x + K$ where $x \in D$. This is divisible by any positive n since, if $ny = x$ then

$$n(y + K) = ny + K = x + K$$

Therefore D/K is divisible. □

Theorem 5.3. *The following are equivalent (tfae) for any abelian group D :*

- (1) D is divisible.
- (2) If A is a subgroup of a cyclic group B then any homomorphism $A \rightarrow D$ extends to B .
- (3) D is an injective \mathbb{Z} -module.

Proof. It is easy to see that the first two conditions are equivalent. Suppose that $x \in D$ and $n \geq 0$. Then, $A = n\mathbb{Z}$ is a subgroup of the cyclic group $B = \mathbb{Z}$ and $f : n\mathbb{Z} \rightarrow D$ can be given by sending the generator n to x . The homomorphism $f : n\mathbb{Z} \rightarrow D$ can be extended to \mathbb{Z} if and only if D is divisible. Thus (2) implies (1) and (1) implies (2) in the case $B = \mathbb{Z}$. The argument for any cyclic group is the same.

It follows from the definition of injectivity that (3) \Rightarrow (2). So, we need to show that (1) and (2) imply (3).

So, suppose that D is divisible. Then we will use Zorn's lemma to prove that it is injective. Suppose that A is a submodule of B and $f : A \rightarrow D$ is a homomorphism. Then we want to extend f to all of B . To use Zorn's lemma we take the set of all pairs (C, g) where $A \subseteq C \subseteq B$ and g is an extension of f (i.e., $f = g|_A$). This set is partially ordered in an obvious way: $(C, g) < (C', g')$ if $C \subseteq C'$ and $g = g'|_C$. It also satisfies the hypothesis of Zorn's lemma. Namely, any totally ordered subset (C_α, g_α) has an upper bound: $(\cup C_\alpha, \cup g_\alpha)$. Zorn's lemma tells us that this set has a maximal element, say, (M, g) . We just need to show that $M = B$. We show this by contradiction.

If $M \neq B$ then there is at least one element $x \in B$ which is not in M . Let $\mathbb{Z}x = \{kx \mid k \in \mathbb{Z}\}$ be the subgroup of B generated by x . Then $M + \mathbb{Z}x$ is strictly bigger than M . So, if we can find an extension $\bar{g} : M + \mathbb{Z}x \rightarrow D$ of g then we have a contradiction proving the theorem. There are two cases.

Case 1. $M \cap \mathbb{Z}x = 0$. In this case, let $\bar{g} = (g, 0)$. I.e. $\bar{g}(a, kx) = g(a)$.

Case 2. $M \cap \mathbb{Z}x = n\mathbb{Z}x$. (n is the smallest positive integer so that $nx \in M$.) Since D is divisible, there is an element $y \in D$ so that $ny = g(nx)$. Let $\bar{g} : M + \mathbb{Z}x \rightarrow D$ be defined by $\bar{g}(a + kx) = g(a) + ky$. This is well defined by the following lemma since, for any $a = knx$

$$g(a) = g(knx) = kg(nx) = kny$$

□

Lemma 5.4. *Suppose that A, B are submodules of an R -module C and $f : A \rightarrow X, g : B \rightarrow X$ are homomorphisms of R -modules which agree on $A \cap B$. Then we get a well-defined homomorphism $f + g : A + B \rightarrow X$ by the formula*

$$(f + g)(a + b) = f(a) + g(b)$$

Proof. Well-defined means that, if the input is written in two different ways, the output is still the same. So suppose that $a + b = a' + b'$. Then $a - a' = b' - b \in A \cap B$. So,

$$f(a - a') = f(a) - f(a') = g(b' - b) = g(b') - g(b)$$

by assumption. Rearranging the terms, we get $f(a) + g(b) = f(a') + g(b')$ as desired. □

INJECTIVE ENVELOPE

There is one other very important fact about injective modules which was not covered in class for lack of time and which is also not covered in the book. This is the fact that every R -module M embeds in a minimal injective module which is called the *injective envelope* of M . This is from Jacobson’s Basic Algebra II.

Definition 5.5. *An embedding $A \hookrightarrow B$ is called essential if every nonzero submodule of B meets A . I.e., $C \subseteq B, C \neq 0 \Rightarrow A \cap C \neq 0$.*

For example, $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is essential because, if a subgroup of \mathbb{Q} contains a/b , then it contains $a \in \mathbb{Z}$. Also, every isomorphism is essential.

Exercise 5.6. *Show that the composition of essential maps is essential.*

Lemma 5.7. *Suppose $A \subseteq B$. Then*

- (1) $\exists X \subseteq B$ s.t. $A \cap X = 0$ and $A \hookrightarrow B/X$ is essential.
- (2) $\exists C \subseteq B$ maximal so that $A \subseteq C$ is essential.

Proof. For (1) the set of all $X \subseteq B$ s.t. $A \cap X = 0$ has a maximal element by Zorn’s lemma. Then $A \hookrightarrow B/X$ must be essential, otherwise there would be a disjoint submodule of the form Y/X and $X \subset Y, A \cap Y = 0$ contradicting the maximality of Y . For (2), C exists by Zorn’s lemma. □

Lemma 5.8. *Q is injective iff every short exact sequence*

$$0 \rightarrow Q \rightarrow M \rightarrow N \rightarrow 0$$

splits.

Proof. If Q is injective then the identity map $Q \rightarrow Q$ extends to a retraction $r : M \rightarrow Q$ giving a splitting of the sequence. Conversely, suppose that every sequence as above splits. Then for any monomorphism $i : A \hookrightarrow B$ and any morphism $f : A \rightarrow Q$ we can form the pushout M in the following diagram

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ f \downarrow & & \downarrow f' \\ Q & \xrightarrow{j} & M \end{array}$$

As you worked out in your homework, these morphisms form an exact sequence:

$$A \xrightarrow{\begin{pmatrix} f \\ i \end{pmatrix}} Q \oplus B \xrightarrow{(j, -f')} M \rightarrow 0$$

Since i is a monomorphism by assumption, A is the kernel of $(j, -f')$. Therefore (again using your homework) A is the pull-back in the above diagram. This implies that j is a monomorphism. [Any morphism $g : X \rightarrow Q$ which goes to zero in M , i.e., so that $j \circ g = 0$, will give a morphism $(g, 0) : X \rightarrow Q \oplus B$ which goes to zero in M and therefore lifts uniquely to $h : X \rightarrow A$ so that

$$\begin{pmatrix} f \\ i \end{pmatrix} \circ h = \begin{pmatrix} f \circ h \\ i \circ h \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix}$$

But i is a monomorphism. So, $i \circ h = 0$ implies $h = 0$ which in turn implies that $f \circ h = g = 0$. So, j is a monomorphism.]

Since j is a monomorphism there is a short exact sequence

$$0 \rightarrow Q \xrightarrow{j} M \rightarrow \text{coker } j \rightarrow 0$$

We are assuming that all such sequences split. So, there is a retraction $r : M \rightarrow Q$. ($r \circ j = id_Q$) Then it is easy to see that $r \circ f' : B \rightarrow Q$ is the desired extension of $f : A \rightarrow Q$:

$$r \circ f' \circ i = r \circ j \circ f = id_Q \circ f = f$$

So, Q is injective. □

Lemma 5.9. *Q is injective if and only if every essential embedding $Q \hookrightarrow M$ is an isomorphism.*

Proof. (\Rightarrow) Suppose Q is injective and $Q \hookrightarrow M$ is essential. Then the identity map $Q \rightarrow Q$ extends to a retraction $r : M \rightarrow Q$ whose kernel is disjoint from Q and therefore must be zero making $M \cong Q$.

(\Leftarrow) Now suppose that every essential embedding of Q is an isomorphism. We want to show that Q is injective. By the previous lemma it suffices to show that every short exact sequence

$$0 \rightarrow Q \xrightarrow{j} M \rightarrow N \rightarrow 0$$

splits. By Lemma 5.7 there is a submodule $X \subseteq M$ so that $jQ \cap X = 0$ and $Q \hookrightarrow M/X$ is essential. Then, by assumption, this map must be an isomorphism. So, $M \cong Q \oplus X$ and the sequence splits proving that Q is injective. □

Theorem 5.10. *For any R -module M there exists an essential embedding $M \hookrightarrow Q$ with Q injective. Furthermore, Q is unique up to isomorphism under M .*

Proof. We know that there is an embedding $M \hookrightarrow Q_0$ where Q_0 is injective. By Lemma 5.7 we can find Q maximal with $M \hookrightarrow Q \hookrightarrow Q_0$ so that $M \hookrightarrow Q$ is essential.

Claim: Q is injective.

If not, there exists an essential $Q \hookrightarrow N$. Since Q_0 is injective, there exists $f : N \rightarrow Q_0$ extending the embedding $Q \hookrightarrow Q_0$. Since f is an embedding on Q , $\ker f \cap Q = 0$. This forces $\ker f = 0$ since $Q \hookrightarrow N$ is essential. So, $f : N \rightarrow Q_0$ is a monomorphism. This contradicts the maximality of Q since the image of N is an essential extension of M in Q_0 which is larger than Q .

It remains to show that Q is unique up to isomorphism. So, suppose $M \hookrightarrow Q'$ is another essential embedding of M into an injective Q' . Then the inclusion $M \hookrightarrow Q'$ extends to a map $g : Q \rightarrow Q'$ which must be a monomorphism since its kernel is disjoint from M . Also, g must be onto since $g(Q)$ is injective making the inclusion $g(Q) \hookrightarrow Q'$ split which contradicting the assumption that $M \hookrightarrow Q'$ is essential unless $g(Q) = Q'$. \square

6. PROJECTIVE RESOLUTIONS

We talked for a week about projective resolutions.

- (1) Definitions
- (2) Modules over a PID
- (3) Chain complexes, maps and homotopies
- (4) Homotopy uniqueness of projective resolutions
- (5) Examples

6.1. Definitions. Suppose that M is an R -module (or, more generally, an object of any abelian category with enough projectives) then a *projective resolution* of M is defined to be a long exact sequence of the form

$$\cdots \rightarrow P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \rightarrow \cdots \rightarrow P_0 \xrightarrow{\epsilon} M \rightarrow 0$$

where P_i are all projective.

The (left) *projective dimension* of M is the smallest integer $n \geq 0$ so that there is a projective resolution of the form

$$0 \rightarrow P_n \rightarrow P_{n-1} \rightarrow \cdots \rightarrow P_0 \xrightarrow{\epsilon} M \rightarrow 0$$

We write $pd(M) = n$. If there is no finite projective resolution then the $pd(M) = \infty$.

The (left) *global dimension* of the ring R written $gl\ dim(R)$ is the maximum projective dimension of any module.

Example 6.1. (0) R has global dimension 0 if and only if it is semi-simple (e.g., any field).

- (1) Any principal ideal domain (PID) has global dimension ≤ 1 since every submodule of a free module is free and every module (over any ring) is (isomorphic to) the quotient of a free module.

An *injective coresolution* of a module M is an exact sequence of the form

$$0 \rightarrow M \rightarrow Q_0 \rightarrow Q_1 \rightarrow \cdots$$

where all of the Q_i are injective. If an abelian category has enough injectives then every object has an injective resolution. We went to a lot of trouble to show this holds for the category of R -modules.

The *injective dimension* $id(M)$ is the smallest integer n so that there is an injective resolution of the form

$$0 \rightarrow M \rightarrow Q_0 \rightarrow Q_1 \rightarrow \cdots \rightarrow Q_n \rightarrow 0$$

We will see later that the maximum injective dimension is equal to the maximum projective dimension.

6.2. Modules of a PID. At this point I decided to go through Lang's proof of the following well-known theorem that I already mentioned several times.

Theorem 6.2. *Suppose that R is a PID and E is a free R -module. Then every submodule of E is free.*

Proof. (This proof is given on page 880 as an example of Zorn's lemma.) Suppose that E is free with basis I and let F be a arbitrary submodule of E . Then we consider the set P of all pairs (J, w) where $J \subseteq I$ and w is a basis for $F_J := F \cap E_J$ where E_J is the submodule of E generated by J . In other words, F_J is the set of all elements of F which are linear combinations of elements of the subset J of the given basis of E .

For example, suppose that $I = \{i, j, k\}$ and $J = \{i, j\}$. If $F \subset E$ is the submodule given by

$$F = \{(x, y, z) \mid x + y + z = 0\}$$

then $F_J = \{(x, -x, 0)\}$.

The set $P = \{(J, w)\}$ is partially ordered in the usual way: $(J, w) \leq (J', w')$ if $J \subseteq J'$ and $w \subseteq w'$. To apply Zorn's lemma we need to check that every tower has an upper bound. So, suppose that $\{(J_\alpha, w_\alpha)\}$ is a tower. Then the upper bound is given in the usual way by

$$(J, w) = (\cup_\alpha J_\alpha, \cup_\alpha w_\alpha)$$

This clearly has the property that $(J_\alpha, w_\alpha) \leq (J, w)$ for all α . We need to verify that (J, w) is an element of the poset P . Certainly, $J = \cup J_\alpha$ is a subset of I . So, it remains to check that

- (1) w is linearly independent.
- (2) w spans F_J , i.e., $w \subset F_J$ and every element of F_J is a linear combination of elements of w .

The first point is easy since any linear dependence among elements of w involves only a finite number of elements of w which must all belong to some w_α (if $x_1, \dots, x_n \in w$ then each x_i is contained in some w_{α_i} . Let α be the largest α_i . Then w_α contains all the x_i . Since w_α is a basis for F_{J_α} , these elements are linearly independent.

The second point is also easy. $w_\alpha \subset F_{J_\alpha} \subseteq F_J$. So, the union $w = \cup w_\alpha$ is contained in F_J . Any element $x \in F_J$ has only a finite number of nonzero coordinates which all lie in some J_α . So $x \in F_{J_\alpha}$ which is spanned by w_α .

This verifies the hypothesis of Zorn's lemma. Therefore, the conclusion holds and our poset P has a maximal element (J, w) . We claim that $J = I$. This would mean that $F_J = F_I = F$ and w would be a basis for F and we would be done.

To prove that $J = I$ suppose J is strictly smaller. Then there exists an element k of I which is not in J . Let $J' = J \cup \{k\}$. Then we want to find a basis w' for $F_{J'}$ so that $(J, w) < (J', w')$, i.e., the basis w' needs to contain w . In that case we get a contradiction to the maximality of (J, w) . There are two cases.

Case 1. $F_{J'} = F_J$. In that case take $w' = w$ and we are done.

Case 2. $F_{J'} \neq F_J$. This means that there is at least one element of $F_{J'}$ whose k -coordinate is nonzero. Let A be the set of all elements of R which appear as k -coordinates of elements of $F_{J'}$. This is the image of the k -coordinate projection map

$$F_{J'} \subseteq E_{J'} \xrightarrow{p_k} R$$

So, A is an ideal in R . So, $A = Rs$ for some $s \in R$. Let $x \in F_{J'}$ so that $p_k(x) = s$. Then I claim that $w' = w \cup \{x\}$ is a basis for $F_{J'}$. First, w' is clearly linearly independent since any linear combination which involves x will have nonzero k -coordinate so cannot be zero. And any linear combination not involving x cannot be zero since w is linearly independent. Finally, w' spans $F_{J'}$. Given any $z \in F_{J'}$ we must have $p_k(z) \in A = Rs$. So $p_k(z) = rs$ and $p_k(z - rx) = 0$. This implies that $z - rx \in F_J$ which is spanned by w . So z is rx plus a linear combination of elements of w . So, w' spans $F_{J'}$ and we are done. \square

Since \mathbb{Z} is a PID we get the following.

Corollary 6.3. *Every subgroup of a free abelian group is free.*

6.3. Chain complexes. At this point I decided to review the basic definitions for chain complexes, chain maps and chain homotopies.

Suppose that \mathcal{A} is an abelian category. Then a *chain complex* over \mathcal{A} is an infinite sequence of objects and morphisms (called *boundary maps*):

$$\cdots \rightarrow C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} \cdots \rightarrow C_1 \xrightarrow{d_1} C_0$$

so that the composition of any two arrows is zero:

$$d_{n-1} \circ d_n = 0$$

The chain complex is denoted either C_* or (C_*, d_*) .

Given two chain complexes C_*, D_* a *chain map* $f_* : C_* \rightarrow D_*$ is a sequence of morphisms $f_n : C_n \rightarrow D_n$ so that $d_n^D \circ f_n = f_{n-1} \circ d_n^C$ where the superscripts are to keep track of which chain complex the boundary maps d_n are in. These morphisms form a big commuting diagram in the shape of a ladder.

6.3.1. *category of chain complexes.*

Proposition 6.4. *If \mathcal{A} is abelian let $C_*(\mathcal{A})$ be the category of chain complexes over \mathcal{A} and chain maps. Then $C_*(\mathcal{A})$ is also abelian.*

I didn't give a detailed proof but I pointed out how direct sums, kernels and cokernels are constructed. First the *direct sum*: $C_* \oplus D_*$ is the chain complex with objects $C_n \oplus D_n$ and boundary maps

$$d_n^{C \oplus D} = d_n^C \oplus d_n^D : C_n \oplus D_n \rightarrow C_{n+1} \oplus D_{n+1}$$

Then the *kernel* of a chain map $f_* : C_* \rightarrow D_*$ is defined to be the chain complex with n th term $\ker f_n$ and boundary map

$$d'_n : \ker f_n \rightarrow \ker f_{n-1}$$

induced by the morphism $d_n^C : C_n \rightarrow C_{n-1}$. (Since $f_{n-1} \circ d_n^C = d_n^D \circ f_n = 0$ on $\ker f_n$, we get this induced map.) The *cokernel* complex is given similarly by

$$\cdots \rightarrow \operatorname{coker} f_n \xrightarrow{\bar{d}_n} \operatorname{coker} f_{n-1} \rightarrow \cdots$$

where \bar{d}_n is the morphism induced by d_n^D .

A *cochain complex* over an abelian category \mathcal{A} is a sequence of objects and morphisms (called *coboundary maps*)

$$C^0 \xrightarrow{d_0} C^1 \xrightarrow{d_1} \cdots$$

so that $d_{n+1} \circ d_n = 0$. A morphism of cochain complexes $C^* \rightarrow D^*$ is a sequence of morphisms $f^n : C^n \rightarrow D^n$ which form a commuting ladder diagram. It is convenient to use the fact that this is the same as a chain complex over the opposite category \mathcal{A}^{op} which is also abelian.

If the category of cochain complexes over \mathcal{A} is denoted $\mathcal{C}^*(\mathcal{A})$ then this duality can be written as

$$\mathcal{C}^*(\mathcal{A})^{op} \cong \mathcal{C}(\mathcal{A}^{op})$$

6.3.2. *homology.* The *homology* of a chain complex C_* is defined to be the sequence of objects:

$$H_n(C_*) := \frac{\ker d_n}{\text{im } d_{n+1}}$$

In theory these are defined only up to isomorphism. So, they are not true functors. However, in practice, they can almost always be explicitly constructed. The construction does not have to be particularly elegant or simple. But it avoids set theoretic headaches since the Axiom of Choice does not apply to categories: We are not allowed to “choose” an object $H_n(C_*)$ for every chain complex C_* only for a *set* of chain complexes.

Homology is a *functor* in the sense that any chain map $f_* : C_* \rightarrow D_*$ induces a morphism in homology $H_n(f) : H_n(C_*) \rightarrow H_n(D_*)$. This is because commutativity of the “ladder” implies that $\ker d_n^C$ maps to $\ker d_n^D$ and $\text{im } d_{n+1}^C$ maps to $\text{im } d_{n+1}^D$. This functor is *additive* in the sense that $H_n(f_* + g_*) = H_n(f_*) + H_n(g_*)$. In other words, H_n gives a homomorphism

$$H_n : \text{Hom}_{\mathcal{C}_*(\mathcal{A})}(C_*, D_*) \rightarrow \text{Hom}_{\mathcal{A}}(H_n(C_*), H_n(D_*))$$

Additivity follows from the shape of the diagram in a way that I will explain later.

6.3.3. *chain homotopy.* Two chain maps $f_*, g_* : C_* \rightarrow D_*$ are called *chain homotopic* if there is a sequence of morphisms

$$h_n : C_n \rightarrow D_{n+1}$$

so that

$$d_{n+1}^D \circ h_n + h_{n-1} \circ d_n^C = g_n - f_n$$

for all $n \geq 0$ where $h_{-1} = 0$. We call h_* a *homotopy* from f_* to g_* and we write

$$h_* : f_* \simeq g_*$$

Theorem 6.5. *Homotopic chain maps induce the same map in homology.*

Proof. This follows from the fact that H_n is additive:

$$\begin{aligned} H_n(g_*) - H_n(f_*) &= H_n(g_* - f_*) = H_n(d_*^D \circ h_* + h_* \circ d_*^C) \\ &= H_n(d_*^D \circ h_*) + H_n(h_* \circ d_*^C) \end{aligned}$$

But both of these are zero since $d_*^D \circ h_*$ maps to the image of d_*^D and therefore to zero in $H_*(D_*)$ and $h_* \circ d_*^C$ is zero on $\ker d_*^C$. \square

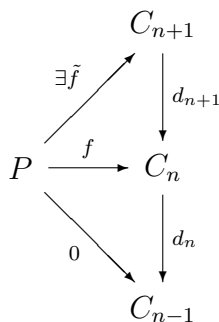
6.3.4. *homotopy equivalence.* Two chain complexes C_*, D_* are called *(chain) homotopy equivalent* and we write $C_* \simeq D_*$ if there exist chain maps $f_* : C_* \rightarrow D_*$ and $g_* : D_* \rightarrow C_*$ so that $f_* \circ g_* \simeq id_D$ and $g_* \circ f_* \simeq id_C$. The chain maps f_*, g_* are called *(chain) homotopy equivalences* and we write $f_* : C_* \simeq D_*$.

Corollary 6.6. *Any chain homotopy equivalence induces an isomorphism in homology.*

Proof. Theorem 6.5 implies that $H_n(f_*) \circ H_n(g_*) = H_n(id_D) = id_{H_n(D)}$ and similarly the other way. So, $H_n(f_*)$ is an isomorphism with inverse $H_n(g_*)$. \square

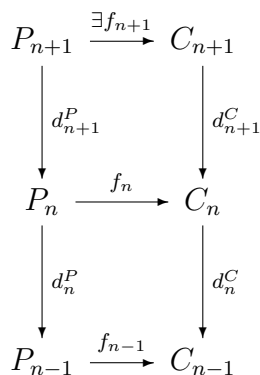
6.4. Homotopy uniqueness of projective resolutions. Here I proved that the projective resolution of any R -module (or any object of an abelian category with enough projectives) is unique up to chain homotopy. I used diagrams and the (equivalent) equation. First I wrote down the *understood standard interpretation* of a diagram.

Lemma 6.7. *Given that the solid arrows (in below) form a commuting diagram, there exists a dotted arrow (the arrow labeled $\exists \tilde{f}$ is supposed to be dotted) as indicates making the entire diagram commute. [This is the understood meaning of this kind of diagram.] The dotted arrow is not necessarily uniquely determined (it is labeled \exists and not $\exists!$) The assumptions are that P is projective and $g : A \rightarrow B$ is onto.*



Proof. By definition of kernel, f lifts uniquely to $\ker d_n$. But C_{n+1} maps onto $\ker d_n$. So, by definition of P being projective, f lifts to C_{n+1} . \square

Lemma 6.8. *With standard wording as above. The additional assumptions are that the right hand column is exact (i.e., $\text{im } d_{n+1}^C = \ker d_n^C$), P_{n+1} is projective and the left hand column is a chain complex (i.e. $d_n^P \circ d_{n+1}^P = 0$).*



Proof. The assumptions implies $d_n^C \circ (f_n \circ d_{n+1}^P) = 0$. By the previous lemma this implies that $f_n \circ d_{n+1}^P$ lifts to C_{n+1} . \square

Theorem 6.9. *Suppose $P_* \rightarrow M \rightarrow 0$ is a projective chain complex (augmented) over M and $C_* \rightarrow N \rightarrow 0$ is a resolution of N (i.e., an exact sequence). Suppose $f : M \rightarrow N$ is any morphism. Then*

- (1) *There exists a chain map $f_* : P_* \rightarrow C_*$ over f . I.e., the following diagram commutes:*

$$\begin{array}{ccc} P_* & \xrightarrow{f_*} & C_* \\ \epsilon \downarrow & & \downarrow \epsilon \\ M & \xrightarrow{f} & N \end{array}$$

- (2) *f_* is unique up to chain homotopy.*

Proof. (1) Since $\epsilon : C_0 \rightarrow N$ is an epimorphism and P_0 is projective, the map $f \circ \epsilon : P_0 \rightarrow N$ lifts to a map $f_0 : P_0 \rightarrow C_0$. The rest is by induction using lemma we just proved.

(2) To prove the existence of the homotopy, I first restated Lemma 6.7 as an equation. It says that for any homomorphism $f : P \rightarrow C_n$ so that $d_n \circ f = 0$, there exists a homomorphism $\tilde{f} : P \rightarrow C^{n+1}$ so that $d_{n+1} \circ \tilde{f} = f$.

We want to show that f_* is unique up to homotopy. So, suppose f_*, g_* are two chain maps over $f : M \rightarrow N$. Then we want to show that there exists a sequence of morphisms $h_n : P_n \rightarrow C_{n+1}$ so that

$$d_{n+1}^C \circ h_n + h_{n-1} \circ d_n^P = g_n - f_n$$

We set $h_{-1} = 0$ by definition. So, for $n = 0$ we get:

$$d_1 \circ h_0 = g_0 - f_0$$

First, h_0 exists because $\epsilon(g_0 - f_0) = (f - f)\epsilon = 0$. If h_0, \dots, h_{n-1} exist satisfying the above equation then in particular we have:

$$(6.1) \quad d_n \circ h_{n-1} + h_{n-2} \circ d_{n-1} = g_{n-1} - f_{n-1}$$

We want to show that h_n exists satisfying the equation

$$d_{n+1}^C \circ h_n = g_n - f_n - h_{n-1} \circ d_n^P$$

The right hand side is the f of Lemma 6.7 and the map that we want (h_n) is the \tilde{f} in Lemma 6.7. So, all we need to do is show that $d_n^C \circ f = 0$.

$$\begin{aligned} d_n(g_n - f_n - h_{n-1} \circ d_n) &= d_n \circ g_n - d_n \circ f_n - d_n \circ h_{n-1} \circ d_n \\ &= g_{n-1} \circ d_n - f_{n-1} \circ d_n - d_n \circ h_{n-1} \circ d_n \end{aligned}$$

Factoring out the d_n and using Equation (6.1) we get:

$$= (g_{n-1} - f_{n-1} - d_n \circ h_{n-1})d_n = h_{n-2} \circ d_{n-1} \circ d_n = 0$$

This is 0 since $d_{n-1} \circ d_n = 0$. Thus h_n exists and $f_* \simeq g_*$. \square

This gives us the statement that we really want:

Corollary 6.10. *In any abelian category with enough projectives, any object A has a projective resolution $P_* \rightarrow A$. Furthermore, any two projective resolutions of A are homotopy equivalent.*

Proof. If there are two projective resolutions P_*, P'_* then the first part of the theorem above tells us that there are chain maps $f_* : P_* \rightarrow P'_*$ and $g_* : P'_* \rightarrow P_*$ which cover the identity map on A . Since $g_* \circ f_*$ and the identity map are both chain maps $P_* \rightarrow P_*$ over the identity of A , the second part of the theorem tells us that

$$f_* \circ g_* \simeq id_{P_*}$$

and similarly $g_* \circ f_* \simeq id_{P'_*}$. So, $P_* \simeq P'_*$. □

The dual argument gives us the following. [In general you should state the dual theorem but not prove it.]

Theorem 6.11. *In any abelian category with enough injectives, any object B has an injective coresolution. Furthermore, any two injective coresolutions of B are homotopy equivalent.*

Following this rule, I should also give the statement of the dual of the previous theorem:

Theorem 6.12. *Suppose $0 \rightarrow M \rightarrow Q_*$ is an injective cochain complex under M and $0 \rightarrow N \rightarrow C_*$ is a coresolution of N (i.e., a long exact sequence). Suppose $f : N \rightarrow M$ is any morphism. Then*

- (1) *There exists a cochain map $f^* : C_* \rightarrow Q_*$ under f . I.e., the following diagram commutes:*

$$\begin{array}{ccc} C_* & \xrightarrow{f^*} & Q_* \\ \uparrow & & \uparrow \\ N & \xrightarrow{f} & M \end{array}$$

- (2) *f^* is unique up to chain homotopy.*

6.5. Derived functors.

Definition 6.13. Suppose that \mathcal{A}, \mathcal{B} are abelian categories where \mathcal{A} has enough injectives and $F : \mathcal{A} \rightarrow \mathcal{B}$ is a left exact (additive) functor. Then the right derived functors $R^i F$ are defined as follows. For any object B of \mathcal{A} choose an injective coresolution $B \rightarrow Q_*$ and let $R^i F(B)$ be the i th cohomology of the cochain complex $F(Q_*)$:

$$0 \rightarrow F(Q_0) \rightarrow F(Q_1) \rightarrow F(Q_2) \rightarrow \cdots$$

In the case $F = \text{Hom}_R(A, -)$, the right derived functors are the Ext functors:

$$\text{Ext}_R^i(A, B) := R^i F(B) = H^i(\text{Hom}_R(A, Q_*))$$

Note that the derived functors are only well-defined up to isomorphism. If there is another choice of injective coresolutions Q'_* then $Q_* \simeq Q'_*$ which implies that $F(Q_*) \simeq F(Q'_*)$ which implies that

$$H^i(F(Q_*)) \cong H^i(F(Q'_*))$$

I pointed out later that, for R -modules, there is a canonical minimal injective coresolution for any module.

By definition of $F(Q_*)$ we take only the injective objects. The term $F(B)$ is deliberately excluded. But F is left exact by assumption. So we have an exact sequence

$$0 \rightarrow F(B) \rightarrow F(Q_0) \rightarrow F(Q_1)$$

Thus

Theorem 6.14. The zero-th derived functor $R^0 F$ is canonically isomorphic to F . In particular,

$$\text{Ext}_R^0(A, B) \cong \text{Hom}_R(A, B)$$

At this point we tried to do an example: Compute $\text{Ext}_{\mathbb{Z}}^1(\mathbb{Z}/3, \mathbb{Z}/2)$. We took an injective coresolution of $\mathbb{Z}/2$

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Q}/2\mathbb{Z} \xrightarrow{j} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

We used that fact that any quotient of a divisible group is divisible. We took $\text{Hom}(\mathbb{Z}/3, -)$ into the injective part:

$$j_* : \text{Hom}(\mathbb{Z}/3, \mathbb{Q}/2\mathbb{Z}) \rightarrow \text{Hom}(\mathbb{Z}/3, \mathbb{Q}/\mathbb{Z})$$

Then I claimed that this map is an isomorphism. Here is a simple-minded proof. A homomorphism $\mathbb{Z}/3 \rightarrow \mathbb{Q}/\mathbb{Z}$ is given by its value on the generator $1 + 3\mathbb{Z}$ of $\mathbb{Z}/3\mathbb{Z}$. This must be a coset $a/b + \mathbb{Z}$ so that $3a/b \in \mathbb{Z}$. In other words $b = 3$ and $a = 0, 1$ or 2 . Similarly, a homomorphism $\mathbb{Z}/3 \rightarrow \mathbb{Q}/2\mathbb{Z}$ sends the generator of $\mathbb{Z}/3$ to a coset

$a/b + 2\mathbb{Z}$ so that $3a/b \in 2\mathbb{Z}$. So, $b = 3$ and $a = 0, 2$ or 4 . So, both of these groups have exactly three elements and a simple calculation shows that j_* is a bijection.

6.5.1. *delta operator.* One of the basic properties of the derived functors is that they fit into an a long exact sequence.

Theorem 6.15. *Given any short exact sequence*

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

there is a sequence of homomorphisms

$$\delta_n : R^n F(C) \rightarrow R^{n+1} F(A)$$

making the following sequence exact:

$$0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C) \xrightarrow{\delta_0} R^1 F(A) \rightarrow R^1 F(B) \rightarrow R^1 F(C) \xrightarrow{\delta_1} R^2 F(A) \rightarrow R^2 F(B) \rightarrow R^2 F(C) \xrightarrow{\delta_2} R^3 F(A) \rightarrow \dots$$

Furthermore, δ_n is natural in the sense that, given any commuting diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C & \longrightarrow & 0 \end{array}$$

we get a commuting square:

$$\begin{array}{ccc} R^n F(C) & \xrightarrow{\delta_n} & R^{n+1} F(A) \\ h_* \downarrow & & \downarrow f_* \\ R^n F(C') & \xrightarrow{\delta_n} & R^{n+1} F(A') \end{array}$$

I gave the following construction of these δ operators. First I needed the following lemmas, the first being obvious.

Lemma 6.16. *If Q is injective then $R^n F(Q) = 0$ for all $n \geq 1$.*

Lemma 6.17. *If $0 \rightarrow A \rightarrow Q \rightarrow K \rightarrow 0$ is a short exact sequence where Q is injective, then we have an exact sequence*

$$0 \rightarrow F(A) \rightarrow F(Q) \rightarrow F(K) \rightarrow R^1 F(A) \rightarrow 0$$

and

$$R^n F(K) \cong R^{n+1} F(A)$$

for all $n \geq 1$.

Proof. We can use $Q = Q_0$ as the beginning of an injective coresolution of A :

$$0 \rightarrow A \xrightarrow{j} Q_0 \xrightarrow{j_0} Q_1 \xrightarrow{j_1} Q_2 \xrightarrow{j_2} Q_3 \rightarrow \dots$$

Since $\text{coker } j \cong \text{im } j_0 \cong \ker j_1 \cong K$, we can break this up into two exact sequences:

$$\begin{aligned} 0 \rightarrow A \xrightarrow{j} Q_0 \rightarrow K \rightarrow 0 \\ 0 \rightarrow K \rightarrow Q_1 \xrightarrow{j_1} Q_2 \xrightarrow{j_2} Q_3 \rightarrow \dots \end{aligned}$$

The second exact sequence shows that the injective coresolution of K is the same as that for A but shifted to the left with the first term deleted. So,

$$R^n F(K) \cong R^{n+1} F(A)$$

for all $n \geq 1$.

When $n = 0$ we have, by left exactness of F , the following exact sequence:

$$0 \rightarrow F(K) \rightarrow F(Q_1) \xrightarrow{(j_1)_*} F(Q_2)$$

In other words, $F(K) \cong \ker(j_1)_*$. The image of $(j_0)_* : F(Q_0) \rightarrow F(Q_1)$ lands in $F(K) = \ker(j_1)_*$. The cokernel is by definition the first cohomology of the cochain complex $F(Q_*)$ which is equal to $R^1 F(A)$. So, we get the exact sequence

$$F(Q_0) \rightarrow F(K) \rightarrow R^1 F(A) \rightarrow 0$$

We already know that the kernel of $F(Q_0) \rightarrow F(K)$ is $F(A)$ so this proves the lemma. \square

My construction of the delta operator proceeded as follows. Start with any short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$. Then choose an injective coresolution of A :

$$0 \rightarrow A \xrightarrow{j} Q_0 \xrightarrow{j_0} Q_1 \xrightarrow{j_1} Q_2 \xrightarrow{j_2} Q_3 \rightarrow \dots$$

Let $K = \ker j_1 = \text{im } j_0 = \text{coker } j$. Since Q_0 is injective, the map $A \rightarrow Q_0$ extends to B and cokernels map to cokernels giving a commuting diagram:

$$(6.2) \quad \begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C \longrightarrow 0 \\ & & \downarrow id_A & & \downarrow f & & \downarrow g \\ 0 & \longrightarrow & A & \xrightarrow{j} & Q_0 & \xrightarrow{p} & K \longrightarrow 0 \end{array}$$

The map $g : C \rightarrow K$ induces a map $g_* : R^n F(C) \rightarrow R^n F(K)$ and I defined the connecting homomorphism δ_n for $n \geq 1$ to be the composition:

$$\delta_n : R^n F(C) \xrightarrow{g_*} R^n F(K) \cong R^{n+1} F(A)$$

I showed that this is independent of the choice of $g : C \rightarrow K$ since, for any other choice g' , the difference $g - g'$ lifts to Q_0 since $f - f' : B \rightarrow Q_0$ is zero on A and therefore factors through C . So, $g_* - g'_* = R^n F(g - g')$ factors through $R^n F(Q_0) = 0$ so $g_* = g'_*$. To show independence from the choice of Q_0 I said that there was a canonical choice for Q_0 called the *injective envelope* of A and I promised to write up the proof of that.

What about $n = 0$? In this case, Lemma 6.17 gives us a 4 term exact sequence:

$$0 \rightarrow F(A) \rightarrow F(Q_0) \rightarrow F(K) \rightarrow R^1 F(A) \rightarrow 0$$

So, we can define $\delta_0 : F(C) \rightarrow R^1 F(A)$ to be the composition

$$\delta_0 : F(C) \xrightarrow{g_*} F(K) \rightarrow R^1 F(A)$$

Again, for any other choice $g' : C \rightarrow K$, the difference $g - g'$ factors through Q_0 . This time $F(Q_0) \neq 0$. But that is OK since $F(Q_0)$ is in the kernel of the next map $F(K) \rightarrow R^1 F(A)$ by the 4 term exact sequence.

6.5.2. *Proof of Theorem 6.15.* From your homework you might remember that the sequence (6.2) gives a short exact sequence:

$$0 \rightarrow B \xrightarrow{\begin{pmatrix} f \\ \beta \end{pmatrix}} Q_0 \oplus C \xrightarrow{(-p, g)} K \rightarrow 0$$

Since $R^n F(Q_0) = 0$ the top row in the following sequence is supposed to be exact:

$$\begin{array}{ccccccccc} \longrightarrow & R^{n-1}F(K) & \xrightarrow{\delta_{n-1}} & R^n F(B) & \xrightarrow{\beta_*} & R^n F(C) & \xrightarrow{g_*} & R^n F(K) & \longrightarrow \\ & \downarrow \cong & & \downarrow = & & \downarrow = & & \downarrow \cong & \\ \longrightarrow & R^n F(A) & \xrightarrow{\alpha_*} & R^n F(B) & \xrightarrow{\beta_*} & R^n F(C) & \xrightarrow{\delta_n} & R^{n+1}F(A) & \longrightarrow \end{array}$$

In the top sequence $R^n F(C)$ occurs in position $3n - 1$ and in the bottom sequence it occurs in position $3n$. Therefore, exactness of the bottom sequence for all $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ at position $k - 1$ implies the exactness of the top sequence at position $k - 1$ which implies the exactness of the bottom sequence at position k . So, it is exact everywhere, proving theorem.

We just need to check that the diagram commutes. (Actually it doesn't. But that's OK.) The middle square obviously commutes. The right hand square commutes by definition of δ_n . The left square anti-commutes (i.e., going one way is negative the other way). But that is good enough for the argument to work. This will follow from the way that α_* and δ_{n-1} are defined.

The morphism $\alpha : A \rightarrow B$ induces a cochain map of injective coresolutions:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{j} & Q_0 & \longrightarrow & Q_1 & \longrightarrow & Q_2 & \longrightarrow & \cdots \\ & & \downarrow \alpha & & \downarrow \alpha^0 & & \downarrow \alpha^1 & & \downarrow \alpha^2 & & \\ 0 & \longrightarrow & B & \xrightarrow{j^B} & Q_0^B & \longrightarrow & Q_1^B & \longrightarrow & Q_2^B & \longrightarrow & \cdots \end{array}$$

The cochain map α^* induces the cochain map $\alpha_* : F(Q_*) \rightarrow F(Q_*^B)$. The induced map in cohomology is $\alpha_* : R^n F(A) \rightarrow R^n F(B)$ by definition. If the cokernels of j, j^B are K, L we get the commuting diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{j} & Q_0 & \xrightarrow{p} & K & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \alpha^0 & & \downarrow \bar{\alpha} & & \\ 0 & \longrightarrow & B & \xrightarrow{j^B} & Q_0^B & \xrightarrow{p^B} & L & \longrightarrow & 0 \\ & & & & & & & & \\ 0 & \longrightarrow & K & \longrightarrow & Q_1 & \longrightarrow & Q_2 & \longrightarrow & \cdots \\ & & \downarrow \bar{\alpha} & & \downarrow \alpha^1 & & \downarrow \alpha^2 & & \\ 0 & \longrightarrow & L & \longrightarrow & Q_1^B & \longrightarrow & Q_2^B & \longrightarrow & \cdots \end{array}$$

Just as we had $R^n F(K) \cong R^{n+1} F(A)$ we also have $R^n F(L) \cong R^{n+1} F(B)$ and the above diagrams show that the maps of injective coresolutions induced by $\alpha : A \rightarrow B$ and $\bar{\alpha} : K \rightarrow L$ are the same but shifted. In other words, $\alpha_* : R^n F(A) \rightarrow R^n F(B)$ is the same as the map $\bar{\alpha}_* : R^{n-1} F(K) \rightarrow R^{n-1} F(L)$.

We need one more commuting diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{\begin{pmatrix} f \\ \beta \end{pmatrix}} & Q_0 \oplus C & \xrightarrow{(-p, g)} & K & \longrightarrow & 0 \\ & & \downarrow = & & \downarrow (\alpha^0, -h) & & \downarrow -\bar{\alpha} & & \\ 0 & \longrightarrow & B & \xrightarrow{j^B} & Q_0^B & \xrightarrow{p^B} & L & \longrightarrow & 0 \end{array}$$

Here $h : C \rightarrow Q_0^B$ is the morphism needed to make the diagram commute, i.e., the maps $\alpha^0 \circ f, j^B : B \rightarrow Q_0^B$ are not equal. But they agree on A . So their difference factors through C . I.e. $\exists h : C \rightarrow Q_0^B$ so that

$$h \circ \beta = \alpha^0 \circ f - j^B$$

The coboundary map $\delta_{n-1} : R^{n-1} F(K) \rightarrow R^n F(B)$ is given by the composition

$$\delta_{n-1} : R^{n-1} F(K) \xrightarrow{-\bar{\alpha}_*} R^{n-1} F(L) \cong R^n F(B)$$

By what I said in the last paragraph, this is the same as $-\alpha_* : R^n F(A) \rightarrow R^n F(B)$ proving the theorem. (The $n = 1$ case is slightly different.) \square

6.6. Left derived functors. There are two cases when we use projective resolutions instead of injective coresolutions:

- (1) When the functor is left exact but contravariant, e.g., $F = \text{Hom}_R(-, B)$.
- (2) When the functor is right exact and covariant, e.g., $F = - \otimes_R B$.

In both cases we take a projective resolution $P_* \rightarrow A \rightarrow 0$ and define the left derived functors to be $L^n F(A) = H^n(F(P_*))$ in the first case and $L^n F(A) = H_n(F(P_*))$ in the second case.

Definition 6.18. *The left derived functors of $F(A) = A \otimes_R B$ are called $L^n F(A) = \text{Tor}_n^R(A, B)$*

6.6.1. *review of tensor product.* Following Lang, I will take tensor products only over commutative rings. The advantage is that $A \otimes_R B$ will be an R -module. The tensor product is defined by a universal condition.

Definition 6.19. *Suppose that A, B are modules over a commutative ring R . Then a map*

$$g : A \times B \rightarrow C$$

from the Cartesian product $A \times B$ to a third R -module C is called R -bilinear if it is an R -homomorphism in each variable. I.e., for each $a \in A$, the mapping $b \mapsto g(a, b)$ is a homomorphism $B \rightarrow C$ and similarly $g(-, b) \in \text{Hom}_R(A, C)$ for all $a \in A$. $A \otimes_R B$ is defined to be the R -module which is the target of the universal R -bilinear map

$$f : A \times B \rightarrow A \otimes B$$

When I say that f is universal I mean that for any other R -bilinear map $g : A \times B \rightarrow C$ there is a unique R -homomorphism $h : A \otimes B \rightarrow C$ so that $g = h \circ f$.

The universal property tells us that $A \otimes_R B$ is unique if it exists. To prove existence we need to construct it. But this easy. You just take $A \otimes_R B$ to be the free R -module generated by all symbols $a \otimes b$ where $a \in A, b \in B$ modulo the relations that are required, namely:

- (1) $(ra) \otimes b = r(a \otimes b)$
- (2) $(a + a') \otimes b = a \otimes b + a' \otimes b$
- (3) $a \otimes rb = r(a \otimes b)$
- (4) $a \otimes (b + b') = a \otimes b + a \otimes b'$

I pointed out that the universal property can be expressed as an isomorphism

$$\text{Hom}_R(A \otimes B, C) \cong \text{BiLin}_R(A \times B, C)$$

And the definition of R -bilinear can be expressed as the isomorphisms $BiLin_R(A \times B, C) \cong \text{Hom}_R(A, \text{Hom}_R(B, C)) \cong \text{Hom}_R(B, \text{Hom}_R(A, C))$

So, we conclude that

$$\text{Hom}_R(A \otimes B, C) \cong \text{Hom}_R(A, \text{Hom}_R(B, C))$$

This is a special case of:

$$\text{Hom}_R(F(A), C) \cong \text{Hom}_R(A, G(C))$$

with $F = \otimes B$ and $G = \text{Hom}_R(B, \)$. When we have this kind of isomorphism, F is called the *left adjoint* and G is called the *right adjoint* and F, G are called *adjoint functors*.

Lemma 6.20. *Any left adjoint functor is right exact. In particular, tensor product is right exact. Also, any right adjoint functor is left exact.*

Proof. In the first case, suppose that F is a left adjoint functor and

$$(6.3) \quad 0 \rightarrow A \xrightarrow{\alpha} A' \xrightarrow{\beta} A'' \rightarrow 0$$

is a short exact sequence. Then for any C , the left exactness of $\text{Hom}_R(-, G(C))$ gives an exact sequence

$$0 \rightarrow \text{Hom}_R(A'', G(C)) \rightarrow \text{Hom}_R(A', G(C)) \rightarrow \text{Hom}_R(A, G(C))$$

By adjunction, this is equivalent to an exact sequence

$$0 \rightarrow \text{Hom}_R(F(A''), C) \rightarrow \text{Hom}_R(F(A'), C) \rightarrow \text{Hom}_R(F(A), C)$$

The exactness of this sequence for all C is equivalent to the exactness of the following sequence by definition of $\text{coker } F(\alpha)$:

$$F(A) \xrightarrow{F(\alpha)} F(A') \rightarrow F(A'') \rightarrow 0$$

The left exactness of G is analogous. (Also, the proof uses the left exactness of Hom so the second case is dumb.) \square

Take the sequence (6.3) and suppose that it splits. I.e., $A' \cong A \oplus A''$ and there is a retraction $r : A' \rightarrow A$ so that $r \circ \alpha = id_A$. Then, in the exact sequence

$$F(A) \xrightarrow{F(\alpha)} F(A') \rightarrow F(A'') \rightarrow 0$$

$F(\alpha)$ is a monomorphism since $F(r) \circ F(\alpha) = F(r \circ \alpha) = id_{F(A)}$. So, we get a short exact sequence which furthermore splits. This proves the following.

Lemma 6.21. *If F is any right (or left) exact functor then $F(A \oplus A'') \cong F(A) \oplus F(A'')$. In particular,*

$$(A \oplus A'') \otimes_R B \cong (A \otimes_R B) \oplus (A'' \otimes_R B)$$

Another important lemma was the following.

Lemma 6.22. *$R \otimes_R B$ is isomorphic to B as R -modules.*

Proof. I showed that B satisfies the universal property. Let

$$f : R \times B \rightarrow B$$

be the map $f(r, b) = rb$. This is R -bilinear when R is commutative. Suppose that $g : R \times B \rightarrow C$ is another R -bilinear map. Then we can define $h : B \rightarrow C$ by $h(b) = g(1, b)$. This is R -linear since g is R -bilinear. The required diagram commutes since

$$h \circ f(r, b) = h(rb) = g(1, rb) = rg(1, b) = g(r, b)$$

Furthermore, h is unique since it has no choice but to send b to $g(1, b)$. Since B satisfies the universal property, $B \cong R \otimes B$. Also the proof gives the isomorphism. $r \otimes b \in R \otimes B$ corresponds to $rb \in B$. \square

There was one other lemma that I didn't prove because it was "obvious."

Lemma 6.23. $A \otimes B \cong B \otimes A$

6.6.2. *computations.* With these lemmas, I did some computations. Suppose that $R = \mathbb{Z}$ and $A = \mathbb{Z}/n$. Then a projective resolution of A is given by

$$0 \rightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \rightarrow \mathbb{Z}/n \rightarrow 0$$

Since this sequence is exact it gives the following right exact sequence for any abelian group B :

$$\mathbb{Z} \otimes B \xrightarrow{n} \mathbb{Z} \otimes B \rightarrow \mathbb{Z}/n \otimes B \rightarrow 0$$

Using the lemma that $R \otimes_R B \cong B$ this becomes:

$$B \xrightarrow{n} B \rightarrow \mathbb{Z}/n \otimes B \rightarrow 0$$

So, we conclude that

$$\mathbb{Z}/n \otimes B \cong B/nB$$

More generally, if A is any finitely generated abelian group then

$$A \cong \mathbb{Z}^r \oplus \mathbb{Z}/t_1 \oplus \mathbb{Z}/t_2 \oplus \cdots \oplus \mathbb{Z}/t_n$$

and, since tensor product distributes over direct sum we get:

$$A \otimes_{\mathbb{Z}} B = B^r \oplus B/t_1 B \oplus B/t_2 B \oplus \cdots \oplus B/j_n B$$

The derived functor $\text{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n, B)$ is by definition the kernel of the map

$$\mathbb{Z} \otimes B \xrightarrow{n} \mathbb{Z} \otimes B$$

Since $\mathbb{Z} \otimes B = B$ this is just the map $B \rightarrow B$ given by multiplication by n . So,

$$\text{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n, B) = \{b \in B \mid nb = 0\}$$

It is the subgroup of B consisting of all elements whose order divides n . It is the “ n -torsion” subgroup of B . Maybe that is why it is called Tor.

6.6.3. *extension of scalars.* Suppose that R is a subring of S (e.g., $\mathbb{Z} \subset \mathbb{R}$). A homomorphism of free R -modules

$$R^n \xrightarrow{f} R^m$$

is given by a matrix $M(f) = (a_{ij})$ as follows. If the basis elements of R^n are e_j and the basis elements of R^m are e_i then

$$f(e_j) = \sum_{i=1}^m a_{ij} e_i$$

for some $a_{ij} \in R$. These numbers determine f since, for an arbitrary element $x = \sum x_j e_j \in R^n$ we have

$$f(x) = f\left(\sum_j x_j e_j\right) = \sum_{i,j} x_j a_{ij} e_i = \sum_{i,j} a_{ij} x_j e_i$$

since R is commutative. (Take free right R -modules when R is not commutative and this will still work.) This can be written in matrix form:

$$f \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum a_{1j} x_j \\ \sum a_{2j} x_j \\ \dots \\ \sum a_{mj} x_j \end{pmatrix} = (a_{ij}) \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$$

When you tensor with S you get $R^n \otimes_R S = (R \otimes_R S)^n = S^n$

$$R^n \otimes_R S = S^n \xrightarrow{f \otimes id_S} R^m \otimes_R S = S^m$$

The claim is that $M(f \otimes id_S) = M(f)$. So, $f_* = f \otimes id_S$ is obtained from f by “extending scalars” to S . If you have an integer matrix, you just take the same matrix and consider it as a real matrix.

6.6.4. *two definitions of Ext.* The last thing I did was to prove that the two definitions of $\text{Ext}_R^n(A, B)$ that we now had were equivalent.

Theorem 6.24. *If $P_* \rightarrow A$ is a projective resolution of A and $B \rightarrow Q_*$ is an injective resolution of B then*

$$H^n(\text{Hom}(P_*, B)) \cong H^n(\text{Hom}(A, Q_*))$$

So, either formula gives $\text{Ext}_R^n(A, B)$.

Proof. The theorem is true in the case when $n = 0$ because both sides are isomorphic to $\text{Hom}_R(A, B)$. So, suppose $n \geq 1$. I gave the proof in the case $n = 2$.

I want to construct a homomorphism

$$H^n(\text{Hom}(A, Q_*)) \rightarrow H^n(\text{Hom}(P_*, B))$$

So, take an element $[f] \in H^n(\text{Hom}(P_*, B))$. The notation means

$$f \in \ker((j_2)_* : \text{Hom}_R(A, Q_2) \rightarrow \text{Hom}_R(A, Q_3))$$

$$[f] = f + \text{im}((j_1)_* : \text{Hom}_R(A, Q_1) \rightarrow \text{Hom}_R(A, Q_2))$$

This gives the following diagram

$$(6.4) \quad \begin{array}{ccccccccccc} P_3 & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & A & \longrightarrow & 0 \\ \downarrow f_3 & \searrow 0 & \downarrow f_2 & & \downarrow f_1 & & \downarrow f_0 & & \downarrow f & \searrow 0 & \downarrow \\ 0 & \longrightarrow & B & \longrightarrow & Q_0 & \xrightarrow{j_0} & Q_1 & \xrightarrow{j_1} & Q_2 & \xrightarrow{j_2} & Q_3 \end{array}$$

Since $j_2 \circ f = 0$, f maps to the kernel K of j_2 . But P_* is a projective resolution of A and $B \rightarrow Q_0 \rightarrow \dots \rightarrow Q_{n-1} \rightarrow K$ is a resolution of K . So, we proved that there is a chain map from P_* to this resolution of K which is unique up to chain homotopy. This gives the maps f_0, f_1 , etc in the diagram. Note that $f_2 \circ d_3 = 0 \circ f_3 = 0$. So,

$$f_2 \in \ker((d_3)^* : \text{Hom}_R(P_2, B) \rightarrow \text{Hom}_R(P_3, B))$$

But f_2 is only well defined up to homotopy $h : P_1 \rightarrow B$. So, we could get $f'_2 = f_2 + h \circ d + d \circ h$. But the second term must be zero since it goes through 0 and the first term

$$h \circ d_2 \in \text{im}((d_2)^* : \text{Hom}_R(P_1, B) \rightarrow \text{Hom}_R(P_2, B))$$

This means that

$$[f_2] = f_2 + \text{im}(d_2)^*$$

is a well defined element of $H^2(\text{Hom}(P_*, B))$ and we have a homomorphism:

$$\text{Hom}_R(A, \ker j_2) \rightarrow H^2(\text{Hom}(P_*, B))$$

But this homomorphism is zero on the image of $(j_1)_* : \text{Hom}(A, Q_1) \rightarrow \text{Hom}(A, Q_2)$ because, if $f = j_1 \circ g$ then we can take $f_0 = g \circ d_0$ and $f_1 = 0 = f_2$. Therefore, we have a well defined map

$$H^2(\text{Hom}(A, Q_*)) \rightarrow H^2(\text{Hom}(P_*, B))$$

which sends $[f]$ to $[f_2]$.

This is enough! The reason is that the diagram (6.4) is symmetrical. We can use the dual argument to define a map

$$H^2(\text{Hom}(P_*, B)) \rightarrow H^2(\text{Hom}(A, Q_*))$$

which will send $[f_2]$ back to $[f]$. So, the two maps are inverse to each other making them isomorphisms. \square

By the way, this gives a symmetrical definition of Ext^n , namely it is the group of homotopy classes of chain maps from the chain complex $P_* \rightarrow A \rightarrow 0$ to the cochain complex $0 \rightarrow B \rightarrow Q_*$ shifted by n . Elements of $\text{Ext}_R^n(A, B)$ are represented by vertical maps as in Equation (6.4).