Contents

Chapter 14
Homological Algebra

Homological algebra begins with the notion of a *differential object,* that is, an object with an endomorphism $A \stackrel{d}{\to} A$ such that $d^2 = 0$. This equation leads to the obvious inclusion $\mathrm{Im}(d) \subset \ker(d)$, but the inclusion generally is not equality. We will find that the difference between $\ker(d)$ and $\mathrm{Im}(d)$, called the *homology,* is a highly useful variant of a differential object: its first basic property is that if an exact sequence

$$0 \to A' \to A \to A'' \to 0$$

of differential objects is given, the homology of A is related to that of A', A'' through a long exact sequence. The basic example, and the one we shall focus on, is where A is a chain complex, and d the usual differential. In this case, homology simply measures the failure of a complex to be exact.

After introducing these preliminaries, we develop the theory of *derived functors.* Given a functor that is only left or right-exact, derived functors allow for an extension of a partially exact sequence to a long exact sequence. The most important examples to us, Tor and Ext, provide characterizations of flatness, projectivity, and injectivity.

§1 Complexes

1.1 Chain complexes

The chain complex is the most fundamental construction in homological algebra.

Definition 1.1 Let R be a ring. A **chain complex** is a collection of R-modules $\{C_i\}$ (for $i \in \mathbb{Z}$) together with boundary operators $\partial_i : C_i \to C_{i-1}$ such that $\partial_{i-1}\partial_i = 0$. The boundary map is also called the **differential.** Often, notation is abused and the indices for the boundary map are dropped.

A chain complex is often simply denoted C_*.

In practice, one often has that $C_i = 0$ for $i < 0$.

Example 1.2 All exact sequences are chain complexes.

Example 1.3 Any sequence of abelian groups $\{C_i\}_{i\in\mathbb{Z}}$ with the boundary operators identically zero forms a chain complex.

We will see plenty of more examples in due time.

At each stage, elements in the image of the boundary $C_{i+1} \to C_i$ lie in the kernel of $\partial_i : C_i \to C_{i-1}$. Let us recall that a chain complex is *exact* if the kernel and the image coincide. In general, a chain complex need not be exact, and this failure of exactness is measured by its homology.

Definition 1.4 Let C_* The submodule of cycles $Z_i \subset C_i$ is the kernel $\ker(\partial_i)$. The submodule of boundaries $B_i \subset C_i$ is the image $Im(\partial_{i+1})$. Thus homology is said to be "cycles mod boundaries," i.e. Z_i/B_i.

To further simplify notation, often all differentials regardless of what chain complex they are part of are denoted ∂, thus the commutativity relation on chain maps is $f\partial = \partial f$ with indices and distinction between the boundary operators dropped.

Definition 1.5 Let C_* be a chain complex with boundary map ∂_i. We define the **homology** of the complex C_* via $H_i(C_*) = \ker(\partial_i)/Im(\partial_{i+1})$.

Example 1.6 In a chain complex C_* where all the boundary maps are trivial, $H_i(C_*) = C_i$.

Often we will bundle all the modules C_i of a chain complex together to form a graded module $C_* = \bigoplus_i C_i$. In this case, the boundary operator is a endomorphism that takes elements from degree i to degree $i - 1$. Similarly, we often bundle together all the homology modules to give a graded homology module $H_*(C_*) = \bigoplus_i H_i(C_*)$.

Definition 1.7 A **differential module** is a module M together with a morphism $d : M \to M$ such that $d^2 = 0$.

Thus, given a chain complex C_*, the module $\bigoplus C_i$ is a differential module with the direct sum of all the differentials ∂_i. A chain complex is just a special kind of differential module, one where the objects are graded and the differential drops the grading by one.

1.2 Functoriality

We have defined chain complexes now, but we have no notion of a morphism between chain complexes. We do this next; it turns out that chain complexes form a category when morphisms are appropriately defined.

Definition 1.8 A **morphism** of chain complexes $f : C_* \to D_*$, or a **chain map**, is a sequence of maps $f_i : C_i \to D_i$ such that $f\partial = \partial' f$ where ∂ is the boundary map of C_* and ∂' of D_* (again we are abusing notation and dropping indices).

There is thus a *category* of chain complexes where the morphisms are chain maps.

One can make a similar definition for differential modules. If (M, d) and (N, d') are differential modules, then a *morphism of differential modules* $(M, d) \to (N, d')$ is a morphism of modules $M \to N$ such that the diagram

$$\begin{array}{ccc} M & \xrightarrow{d} & M \\ \downarrow & & \downarrow \\ N & \xrightarrow{d'} & N \end{array}$$

commutes. There is therefore a category of differential modules, and the map $C_* \to \bigoplus C_i$ gives a functor from the category of chain complexes to that of differential modules.

Proposition 1.9 *A chain map $C_* \to D_*$ induces a map in homology $H_i(C) \to H_i(D)$ for each i; thus homology is a covariant functor from the category of chain complexes to the category of graded modules.*

More precisely, each H_i is a functor from chain complexes to modules.

Proof. Let $f : C_* \to D_*$ be a chain map. Let ∂ and ∂' be the differentials for C_* and D_* respectively. Then we have a commutative diagram:

$$\begin{array}{ccccc} C_{i+1} & \xrightarrow{\partial_{i+1}} & C_i & \xrightarrow[\partial_i]{} & C_{i-1} \\ \downarrow f_{i+1} & & \downarrow f_i & & \downarrow f_{i-1} \\ D_{i+1} & \xrightarrow{\partial'_{i+1}} & D_i & \xrightarrow[\partial'_i]{} & D_{i-1} \end{array} \tag{14.1}$$

Now, in order to check that a chain map f induces a map f_* on homology, we need to check that $f_*(Im(\partial)) \subset Im(\partial')$ and $f_*(\ker(\partial)) \subset \ker(\partial)$. We first check the condition on images: we want to look at $f_i(Im(\partial_{i+1}))$. By commutativity of f and the boundary maps, this is equal to $\partial'_{i+1}(Im(f_{i+1})$. Hence we have $f_i(Im(\partial_{i+1})) \subset Im(\partial'_{i+1})$. For the condition on kernels, let $x \in \ker(\partial_i)$. Then by commutativity, $\partial'_i(f_i(x)) = f_{i-1}\partial_i(x) = 0$. Thus we have that f induces for each i a homomorphism $f_i : H_i(C_*) \to H_i(D_*)$ and hence it induces a homomorphism on homology as a graded module. ▲

Exercise 14.1 Define the *homology* $H(M)$ of a differential module (M, d) via $\ker d / \operatorname{Im} d$. Show that $M \mapsto H(M)$ is a functor from differential modules to modules.

1.3 Long exact sequences

TO BE ADDED: OMG! We have all this and not the most basic theorem of them all.

Definition 1.10 If M is a complex then for any integer k, we define a new complex $M[k]$ by shifting indices, i.e. $(M[k])^i := M^{i+k}$.

Definition 1.11 If $f : M \to N$ is a map of complexes, we define a complex $\operatorname{Cone}(f) := \{N^i \oplus M^{i+1}\}$ with differential

$$d(n^i, m^{i+1}) := (d_N^i(n_i) + (-1)^i \cdot f(m^{i+1}, d_M^{i+1}(m^{i+1}))$$

Remark: This is a special case of the total complex construction to be seen later.

Proposition 1.12 *A map $f : M \to N$ is a quasi-isomorphism if and only if* $\operatorname{Cone}(f)$ *is acyclic.*

Proposition 1.13 *Note that by definition we have a short exact sequence of complexes*

$$0 \to N \to \operatorname{Cone}(f) \to M[1] \to 0$$

so by Proposition 2.1, we have a long exact sequence

$$\dots \to H^{i-1}(\operatorname{Cone}(f)) \to H^i(M) \to H^i(N) \to H^i(\operatorname{Cone}(f)) \to \dots$$

so by exactness, we see that $H^i(M) \simeq H^i(N)$ if and only if $H^{i-1}(\operatorname{Cone}(f)) = 0$ and $H^i(\operatorname{Cone}(f)) = 0$. Since this is the case for all i, the claim follows. ■

1.4 Cochain complexes

Cochain complexes are much like chain complexes except the arrows point in the opposite direction.

Definition 1.14 A **cochain complex** is a sequence of modules C^i for $i \in \mathbb{Z}$ with **coboundary operators**, also called **differentials**, $\partial^i : C^i \to C^{i+1}$ such that $\partial^{i+1}\partial^i = 0$.

The theory of cochain complexes is entirely dual to that of chain complexes, and we shall not spell it out in detail. For instance, we can form a category of cochain complexes and **chain maps** (families of morphisms commuting with the differential). Moreover, given a cochain complex C^*, we define the **cohomology objects** to be $h^i(C^*) = \ker(\partial^i)/Im(\partial^{i-1})$; one obtains cohomology functors.

It should be noted that the long exact sequence in cohomology runs in the opposite direction. If $0 \to C'_* \to C_* \to C''_* \to 0$ is a short exact sequence of cochain complexes, we get a long exact sequence

$$\dots \to H^i(C') \to H^i(C) \to H^i(C'') \to H^{i+1}(C') \to H^{i+1}(C) \to \dots.$$

Similarly, we can also turn cochain complexes and cohomology modules into a graded module.

Let us now give a standard example of a cochain complex.

Example 1.15 (The de Rham complex) Readers unfamiliar with differential forms may omit this example. Let M be a smooth manifold. For each p, let $C^p(M)$ be the $\mathbb{R}$-vector space of smooth p-forms on M. We can make the $\{C^p(M)\}$ into a complex by defining the maps

$$C^p(M) \to C^{p+1}(M)$$

via $\omega \to d\omega$, for d the exterior derivative. (Note that $d^2 = 0$.) This complex is called the **de Rham complex** of M, and its cohomology is called the **de Rham cohomology.** It is known that the de Rham cohomology is isomorphic to singular cohomology with real coefficients.

It is a theorem, which we do not prove, that the de Rham cohomology is isomorphic to the singular cohomology of M with coefficients in $\mathbb{R}$.

1.5 Long exact sequence

1.6 Chain Homotopies

In general, two maps of complexes $C_* \rightrightarrows D_*$ need not be equal to induce the same morphisms in homology. It is thus of interest to determine conditions when they do. One important condition is given by chain homotopy: chain homotopic maps are indistinguishable in homology. In algebraic topology, this fact is used to show that singular homology is a homotopy invariant. We will find it useful in showing that the construction (to be given later) of a projective resolution is essentially unique.

Definition 1.16 Let C_*, D_* be chain complexes with differentials d_i. A chain homotopy between two chain maps $f, g : C_* \to D_*$ is a series of homomorphisms $h^i : C^i \to D^{i-1}$ satisfying $f^i - g^i = dh^i + h^{n+1}d$. Again often notation is abused and the condition is written $f - g = dh + hd$.

Proposition 1.17 *If two morphisms of complexes $f, g : C_* \to D_*$ are chain homotopic, they are taken to the same induced map after applying the homology functor.*

Proof. Write $\{d_i\}$ for the various differentials (in both complexes). Let $m \in Z_i(C)$, the group of i-cycles. Suppose there is a chain homotopy h between f, g (that is, a set of morphisms $C_i \to D_{i-1}$). Then

$$f^i(m) - g^i(m) = h^{i+1} \circ d^i(m) + d^{i-1} \circ h^i(m) = d^{i-1} \circ H^i(m) \in \Im(d^{i-1})$$

which is zero in the cohomology $H^i(D)$. ▲

Corollary 1.18 *If two chain complexes are chain homotopically equivalent (there are maps $f : C_* \to D_*$ and $g : D_* \to C_*$ such that both fg and gf are chain homotopic to the identity), they have isomorphic homology.*

Proof. Clear. ▲

Example 1.19 Not every quasi-isomorphism is a homotopy equivalence. Consider the complex

$$\cdots \to 0 \to \mathbb{Z}/\cdot 2 \to \mathbb{Z} \to 0 \to 0 \to \dots$$

so $H^0 = \mathbb{Z}/2\mathbb{Z}$ and all cohomologies are 0. We have a quasi-isomorphism from the above complex to the complex

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

but no inverse can be defined (no map from $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$).

Proposition 1.20 *Additive functors preserve chain homotopies*

Proof. Since an additive functor F is a homomorphism on $Hom(-,-)$, the chain homotopy condition will be preserved; in particular, if t is a chain homotopy, then $F(t)$ is a chain homotopy. ▲

In more sophisticated homological theory, one often makes the definition of the "homotopy category of chain complexes."

Definition 1.21 The homotopy category of chain complexes is the category $hKom(R)$ where objects are chain complexes of R-modules and morphisms are chain maps modulo chain homotopy.

1.7 Topological remarks

TO BE ADDED: add more detail The first homology theory to be developed was simplicial homology - the study of homology of simplicial complexes. To be simple, we will not develop the general theory and instead motivate our definitions with a few basic examples.

Example 1.22 Suppose our simplicial complex has one line segment with both ends identified at one point p. Call the line segment a. The n-th homology group of this space roughly counts how many "different ways" there are of finding n dimensional sub-simplices that have no boundary that aren't the boundary of any $n+1$ dimensional simplex. For the circle, notice that for each integer, we can find such a way (namely the simplex that wraps counter clockwise that integer number of times). The way we compute this is we look at the free abelian group generated by 0 simplices, and 1 simplices (there are no simplices of dimension 2 or higher so we can ignore that). We call these groups C_0 and C_1 respectively. There is a boundary map $\partial_1 : C_1 \to C_0$. This boundary map takes a 1-simplex and associates to it its end vertex minus its starting vertex (considered as an element in the free abelian group on vertices of our simplex). In the case of the circle, since there is only one 1-simplex and one 0-simplex, this map is trivial. We then get our homology group by looking at $\ker(\partial_1)$. In the case that there is a nontrivial boundary map $\partial_2 : C_2 \to C_1$ (which can only happen when our simplex is at least 2-dimensional), we have to take the quotient $\ker(\partial_1)/\ker(\partial_2)$. This motivates us to define homology in a general setting.

Originally homology was intended to be a homotopy invariant meaning that space with the same homotopy type would have isomorphic homology modules. In fact, any homotopy induces what is now known as a chain homotopy on the simplicial chain complexes.

Exercise 14.2 (Singular homology) Let X be a topological space and let S^n be the set of all continuous maps $\Delta^n \to X$ where Δ^n is the convex hull of n distinct points and the origin with orientation given by an ordering of the n vertices. Define C_n to be the free abelian group generated by elements of S^n. Define $\Delta^n_{\hat{i}}$ to be the face of Δ^n obtained by omitting the i-th vertex from the simplex. We can then construct a boundary map $\partial_n : C_n \to C_{n-1}$ to take a map $\sigma^n : \Delta^n \to X$ to $\sum_{i=0}^n (-1)^i \sigma^n|_{\Delta^n_{\hat{i}}}$. Verify that $\partial^2 = 0$ (hence making C_* into a chain complex known as the "singular chain complex of X". Its homology groups are the "singular homology groups".

Exercise 14.3 Compute the singular homology groups of a point.

§2 Derived functors

2.1 Projective resolutions

Fix a ring R. Let us recall (Definition 2.5) that an R-module P is called *projective* if the functor $N \to \mathrm{Hom}_R(P, N)$ (which is always left-exact) is exact.

Projective objects are useful in defining chain exact sequences known as "projective resolutions." In the theory of derived functors, the projective resolution of a module M is in some sense a replacement for M: thus, we want it to satisfy some uniqueness and existence properties. The uniqueness is not quite true, but it is true modulo chain equivalence.

Definition 2.1 Let M be an arbitrary module, a projective resolution of M is an exact sequence

$$\dots \to P_i \to P_{i-1} \to P_{i-2} \dots \to P_1 \to P_0 \to M \tag{14.2}$$

where the P_i are projective modules.

Proposition 2.2 *Any module admits a projective resolution.*

The proof will even show that we can take a *free* resolution.

Proof. We construct the resolution inductively. First, we take a projective module P_0 with $P_0 \twoheadrightarrow N$ surjective by the previous part. Given a portion of the resolution

$$P_n \to P_{n-1} \to \dots \to P_0 \twoheadrightarrow N \to 0$$

for $n \geq 0$, which is exact at each step, we consider $K = \ker(P_n \to P_{n-1})$. The sequence

$$0 \to K \to P_n \to P_{n-1} \to \dots \to P_0 \twoheadrightarrow N \to 0$$

is exact. So if P_{n+1} is chosen such that it is projective and there is an epimorphism $P_{n+1} \twoheadrightarrow K$, (which we can construct by Proposition 6.6), then

$$P_{n+1} \to P_n \to \dots$$

is exact at every new step by construction. We can repeat this inductively and get a full projective resolution. ▲

Here is a useful observation:

Proposition 2.3 *If R is noetherian, and M is finitely generated, then we can choose a projective resolution where each P_i is finitely generated.*

We can even take a resolution consisting of finitely generated free modules.

Proof. To say that M is finitely generated is to say that it is a quotient of a free module on finitely many generators, so we can take P_0 free and finitely generated. The kernel of $P_0 \to M$ is finitely generated by noetherianness, and we can proceed as before, at each step choosing a finitely generated object. ▲

Example 2.4 The abelian group $\mathbb{Z}/2$ has the free resolution $0 \to \dots 0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2$. Similarly, since any finitely generated abelian group can be decomposed into the direct sum of torsion subgroups and free subgroups, all finitely generated abelian groups admit a free resolution of length two.

Actually, over a principal ideal domain R (e.g. $R = \mathbb{Z}$), *every* module admits a free resolution of length two. The reason is that if $F \twoheadrightarrow M$ is a surjection with F free, then the kernel $F' \subset F$ is free by a general fact (**TO BE ADDED:** citation needed) that a submodule of a free module is free (if one works over a PID). So we get a free resolution of the type

$$0 \to F' \to F \to M \to 0.$$

In general, projective resolutions are not at all unique. Nonetheless, they *are* unique up to chain homotopy. Thus a projective resolution is a rather good "replacement" for the initial module.

Proposition 2.5 *Let M, N be modules and let $P_* \to M, P'_* \to N$ be projective resolutions. Let $f : M \to N$ be a morphism. Then there is a morphism*

$$P_* \to P'_*$$

such that the following diagram commutes:

$$\begin{CD}
\cdots @>>> P_1 @>>> P_0 @>>> M \\
@. @VVV @VVV @VV{f}V \\
\cdots @>>> P'_1 @>>> P'_0 @>>> N
\end{CD}$$

This morphism is unique up to chain homotopy.

Proof. Let $P_* \to M$ and $P'_* \to N$ be projective resolutions. We will define a morphism of complexes $P_* \to P'_*$ such that the diagram commutes. Let the boundary maps in P_*, P'_* be denoted d (by abuse of notation). We have an exact diagram

$$\begin{CD}
\cdots @>>> P_n @>{d}>> P_{n-1} @>{d}>> \cdots @>{d}>> P_0 @>>> M @>>> 0 \\
@. @. @. @. @. @VV{f}V \\
\cdots @>>> P'_n @>{d}>> P'_{n-1} @>>> \cdots @>{d}>> P'_0 @>>> N @>>> 0
\end{CD}$$

Since $P'_0 \twoheadrightarrow N$ is an epimorphism, the map $P_0 \to M \to N$ lifts to a map $P_0 \to P'_0$ making the diagram

$$\begin{CD}
P_0 @>>> M \\
@VVV @VV{f}V \\
P'_0 @>>> N
\end{CD}$$

commute. Suppose we have defined maps $P_i \to P'_i$ for $i \leq n$ such that the following diagram commutes:

$$\begin{CD}
P_n @>{d}>> P_{n-1} @>{d}>> \cdots @>{d}>> P_0 @>>> M @>>> 0 \\
@VVV @VVV @. @VVV @VV{f}V \\
P'_n @>{d}>> P'_{n-1} @>>> \cdots @>{d}>> P'_0 @>>> N @>>> 0
\end{CD}$$

Then we will define $P_{n+1} \to P'_{n+1}$, after which induction will prove the existence of a map. To do this, note that the map

$$P_{n+1} \to P_n \to P'_n \to P'_{n-1}$$

is zero, because this is the same as $P_{n+1} \to P_n \to P_{n-1} \to P'_{n-1}$ (by induction, the diagrams before n commute), and this is zero because two P-differentials were composed one after another. In particular, in the diagram

$$\begin{CD}
P_{n+1} @>>> P_n \;, \\
@. @VVV \\
P'_{n+1} @>>> P'_n
\end{CD}$$

the image in P'_n of P_{n+1} lies in the kernel of $P'_n \to P'_{n-1}$, i.e. in the image I of P'_{n+1}. The exact diagram

$$\begin{array}{ccccc} & & P_{n+1} & & \\ & & \downarrow & & \\ P'_{n+1} & \longrightarrow & I & \longrightarrow & 0 \end{array}$$

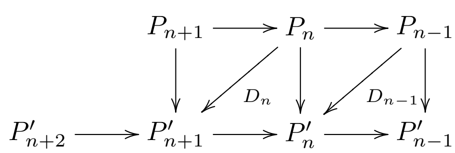
shows that we can lift $P_{n+1} \to I$ to $P_{n+1} \to P'_{n+1}$ (by projectivity). This implies that we can continue the diagram further and get a morphism $P_* \to P'_*$ of complexes.

Suppose $f, g : P_* \to P'_*$ are two morphisms of the projective resolutions making

$$\begin{array}{ccc} P_0 & \longrightarrow & M \\ \downarrow & & \downarrow \\ P'_0 & \longrightarrow & N \end{array}$$

commute. We will show that f, g are chain homotopic.

For this, we start by defining $D_0 : P_0 \to P'_1$ such that $dD_0 = f - g : P_0 \to P'_0$. This we can do because $f - g$ sends P_0 into $\ker(P'_0 \to N)$, i.e. into the image of $P'_1 \to P'_0$, and P_0 is projective. Suppose we have defined chain-homotopies $D_i : P_i \to P_{i+1}$ for $i \leq n$ such that $dD_i + D_{i-1}d = f - g$ for $i \leq n$. We will define D_{n+1}. There is a diagram



where the squares commute regardless of whether you take the vertical maps to be f or g (provided that the choice is consistent).

We would like to define $D_{n+1} : P_n \to P'_{n+1}$. The key condition we need satisfied is that

$$dD_{n+1} = f - g - D_n d.$$

However, we know that, by the inductive hypothesis on the D's

$$d(f - g - D_n d) = fd - gd - dD_n d = fd - gd - (f - g)d + D_n dd = 0.$$ ▲

In particular, $f - g - D_n d$ lies in the image of $P'_{n+1} \to P'_n$. The projectivity of P_n ensures that we can define D_{n+1} satisfying the necessary condition.

Corollary 2.6 *Let $P_* \to M, P'_* \to M$ be projective resolutions of M. Then there are maps $P_* \to P'_*, P'_* \to P_*$ under M such that the compositions are chain homotopic to the identity.*

Proof. Immediate. ▲

2.2 Injective resolutions

One can dualize all this to injective resolutions. **TO BE ADDED:** do this

2.3 Definition

Often in homological algebra, we see that "short exact sequences induce long exact sequences." Using the theory of derived functors, we can make this formal.

Let us work in the category of modules over a ring R. Fix two such categories. Recall that a right-exact functor F (from the category of modules over a ring to the category of modules over another ring) is an additive functor such that for every short exact sequence $0 \to A \to B \to C \to 0$, we get a exact sequence $F(A) \to F(B) \to F(C) \to 0$.

We want a natural way to continue this exact sequence to the left; one way of doing this is to define the left derived functors.

Definition 2.7 Let F be a right-exact functor and $P_* \to M$ are projective resolution. We can form a chain complex $F(P_*)$ whose object in degree i is $F(P_i)$ with boundary maps $F(\partial)$. The homology of this chain complex denoted L_iF are the left derived functors.

For this definition to be useful, it is important to verify that deriving a functor yields functors independent on choice of resolution. This is clear by **??**.

Theorem 2.8 *The following properties characterize derived functors:*

1. $L_0F(-) = F(-)$
2. *Suppose* $0 \to A \to B \to C \to 0$ *is an exact sequence and* F *a right-exact functor; the left derived functors fit into the following exact sequence:*

$$\cdots L_iF(A) \to L_iF(B) \to L_iF(C) \to L_{i-1}F(A) \cdots \to L_1(C) \to L_0F(A) \to L_0F(B) \to L_0F(C) \to 0 \tag{14.3}$$

Proof. The second property is the hardest to prove, but it is by far the most useful; it is essentially an application of the snake lemma. ▲

One can define right derived functors analogously; if one has a left exact functor (an additive functor that takes an exact sequence $0 \to A \to B \to C \to 0$ to $0 \to F(A) \to F(B) \to F(C)$), we can pick an injective resolution instead (the injective criterion is simply the projective criterion with arrows reversed). If $M \to I^*$ is a injective resolution then the cohomology of the chain complex $F(I^*)$ gives the right derived functors. However, variance must also be taken into consideration so the choice of whether or not to use a projective or injective resolution is of importance (in all of the above, functors were assumed to be covariant). In the following, we see an example of when right derived functors can be computed using projective resolutions.

2.4 Ext **functors**

Definition 2.9 The right derived functors of $Hom(-, N)$ are called the *Ext*-modules denoted $Ext^i_R(-, N)$.

We now look at the specific construction:

Let M, M' be R-modules. Choose a projective resolution

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0$$

and consider what happens when you hom this resolution into N. Namely, we can consider $\mathrm{Hom}_R(M, N)$, which is the kernel of $\mathrm{Hom}(P_0, M) \to \mathrm{Hom}(P_1, M)$ by exactness of the sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N).$$

You might try to continue this with the sequence

$$0 \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(P_0, N) \to \mathrm{Hom}_R(P_1, N) \to \mathrm{Hom}_R(P_2, N) \to \dots.$$

In general, it won't be exact, because Hom_R is only left-exact. But it is a chain complex. You can thus consider the homologies.

Definition 2.10 The homology of the complex $\{\mathrm{Hom}_R(P_i, N)\}$ is denoted $\mathrm{Ext}^i_R(M, N)$. By definition, this is $\ker(\mathrm{Hom}(P_i, N) \to \mathrm{Hom}(P_{i+1}, N))/\mathrm{Im}(\mathrm{Hom}(P_{i-1}, N) \to \mathrm{Hom}(P_i, N))$. This is an R-module, and is called the ith ext group.

Let us list some properties (some of these properties are just case-specific examples of general properties of derived functors)

Proposition 2.11 $\mathrm{Ext}^0_R(M, N) = \mathrm{Hom}_R(M, N)$.

Proof. This is obvious from the left-exactness of $\mathrm{Hom}(-, N)$. (We discussed this.) ▲

Proposition 2.12 $\mathrm{Ext}^i(M, N)$ *is a functor of* N.

Proof. Obvious from the definition. ▲

Here is a harder statement.

Proposition 2.13 $\mathrm{Ext}^i(M, N)$ *is well-defined, independent of the projective resolution* $P_* \to M$, *and is in fact a contravariant additive functor of* M.[1]

Proof. Omitted. We won't really need this, though; it requires more theory about chain complexes. ▲

Proposition 2.14 *If* M *is annihilated by some ideal* $I \subset R$, *then so is* $\mathrm{Ext}^i(M, N)$ *for each* i.

Proof. This is a consequence of the functoriality in M. If $x \in I$,then $x : M \to M$ is the zero map, so it induces the zero map on $\mathrm{Ext}^i(M, N)$.

Proposition 2.15 $\mathrm{Ext}^i(M, N) = 0$ *if* M *projective and* $i > 0$.

Proof. In that case, one can use the projective resolution

$$0 \to M \to M \to 0.$$

Computing Ext via this gives the result. ▲

Proposition 2.16 *If there is an exact sequence*

$$0 \to N' \to N \to N'' \to 0,$$

there is a long exact sequence of Ext *groups*

$$0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'') \to \mathrm{Ext}^1(M, N') \to \mathrm{Ext}^1(M, N) \to \dots$$

[1]I.e. a map $M \to M'$ induces $\mathrm{Ext}^i(M', N) \to \mathrm{Ext}^i(M, N)$.

Proof. This proof will assume a little homological algebra. Choose a projective resolution $P_* \to M$. (The notation P_* means the chain complex $\dots \to P_2 \to P_1 \to P_0$.) In general, homming out of M is not exact, but homming out of a projective module is exact. For each i, we get an exact sequence

$$0 \to \mathrm{Hom}_R(P_i, N') \to \mathrm{Hom}_R(P_i, N) \to \mathrm{Hom}_R(P_i, N'') \to 0,$$

which leads to an exact sequence of *chain complexes*

$$0 \to \mathrm{Hom}_R(P_*, N') \to \mathrm{Hom}_R(P_*, N) \to \mathrm{Hom}_R(P_*, N'') \to 0.$$

Taking the long exact sequence in homology gives the result. ▲

Much less obvious is:

Proposition 2.17 *There is a long exact sequence in the M variable. That is, a short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

leads a long exact sequence

$$0 \to \mathrm{Hom}_R(M'', N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N) \to \mathrm{Ext}^1(M'', N) \to \mathrm{Ext}^1(M, N) \to \dots .$$

Proof. Omitted. ▲

We now can characterize projectivity:

Corollary 2.18 *TFAE:*

1. *M is projective.*
2. *$\mathrm{Ext}^i(M, N) = 0$ for all R-modules N and $i > 0$.*
3. *$\mathrm{Ext}^1(M, N) = 0$ for all N.*

Proof. We have seen that 1 implies 2 because projective modules have simple projective resolutions. 2 obviously implies 3. Let's show that 3 implies 1.Choose a projective module P and a surjection $P \twoheadrightarrow M$ with kernel K. There is a short exact sequence $0 \to K \to P \to M \to 0$. The sequence

$$0 \to \mathrm{Hom}(M, K) \to \mathrm{Hom}(P, K) \to \mathrm{Hom}(K, K) \to \mathrm{Ext}^1(M, K) = 0$$

shows that there is a map $P \to K$ which restricts to the identity $K \to K$. The sequence $0 \to K \to P \to M \to 0$ thus splits, so M is a direct summand in a projective module, so is projective. ▲

Finally, we note that there is another way of constructing Ext. We constructed them by choosing a projective resolution of M. But you can also do this by resolving N by *injective* modules.

Definition 2.19 An R-module Q is **injective** if $\mathrm{Hom}_R(-, Q)$ is an exact (or, equivalently, right-exact) functor. That is, if $M_0 \subset M$ is an inclusion of R-modules, then any map $M_0 \to Q$ can be extended to $M \to Q$.

If we are given M, N, and an injective resolution $N \to Q_*$, we can look at the chain complex $\{\mathrm{Hom}(M, Q_i)\}$, i.e. the chain complex

$$0 \to \mathrm{Hom}(M, Q^0) \to \mathrm{Hom}(M, Q^1) \to \dots$$

and we can consider the cohomologies.

Definition 2.20 We call these cohomologies

$$\mathrm{Ext}^i_R(M,N)' = \ker(\mathrm{Hom}(M,Q^i) \to \mathrm{Hom}(M,Q^{i+1}))/\operatorname{Im}(\mathrm{Hom}(M,Q^{i-1}) \to \mathrm{Hom}(M,Q^i)).$$

This is dual to the previous definitions, and it is easy to check that the properties that we couldn't verify for the previous Exts are true for the Ext′'s.

Nonetheless:

Theorem 2.21 *There are canonical isomorphisms:*

$$\mathrm{Ext}^i(M,N)' \simeq \mathrm{Ext}^i(M,N).$$

In particular, to compute Ext groups, you are free either to take a projective resolution of M, or an injective resolution of N.

Proof (Idea of proof). In general, it might be a good idea to construct a third more complex construction that resembles both. Given M, N construct a projective resolution $P_* \to M$ and an injective resolution $N \to Q^*$. Having made these choices, we get a *double complex*

$$\mathrm{Hom}_R(P_i, Q^j)$$

of a whole lot of R-modules. The claim is that in such a situation, where you have a double complex C_{ij}, you can form an ordinary chain complex C' by adding along the diagonals. Namely, the nth term is $C'_n = \bigoplus_{i+j=n} C_{ij}$. This *total complex* will receive a map from the chain complex used to compute the Ext groups and a chain complex used to compute the Ext′ groups. There are maps on cohomology,

$$\mathrm{Ext}^i(M,N) \to H^i(C'_*), \quad \mathrm{Ext}^i(M,N)' \to H^i(C'_*).$$

The claim is that isomorphisms on cohomology will be induced in each case. That will prove the result, but we shall not prove the claim. ▲

Last time we were talking about Ext groups over commutative rings. For R a commutative ring and M, N R-modules, we defined an R-module $\mathrm{Ext}^i(M,N)$ for each i, and proved various properties. We forgot to mention one.

Proposition 2.22 *If R noetherian, and M, N are finitely generated,* $\mathrm{Ext}^i(M,N)$ *is also finitely generated.*

Proof. We can take a projective resolution P_* of M by finitely generated free modules, R being noetherian. Consequently the complex $\mathrm{Hom}(P_*, N)$ consists of finitely generated modules. Thus the cohomology is finitely generated, and this cohomology consists of the Ext groups. ▲

2.5 Application: Modules over DVRs

Definition 2.23 Let M be a module over a domain A. We say that M is torsion-free, if for any nonzero $a \in A$, $a : M \to M$ is injective. We say that M is torsion if for any $m \in M$, there is nonzero $a \in A$ such that $am = 0$.

Lemma 2.24 *For any module finitely generated module M over a Noetherian domain A, there is a short exact sequence*

$$0 \to M_{tors} \to M \to M_{tors-free} \to 0$$

where M_{tors} is killed by an element of A and $M_{tors-free}$ is torsion-free.

Proof. This is because we may take M_{tors} to be all the elements which are killed by a non-zero element of A. Then this is clearly a sub-module. Since A is Noetherian, it is finitely generated, which means that it can be killed by one element of A (take the product of the elements that kill the generators). Then it is easy to check that the quotient M/M_{tors} is torsion-free. ▲

Lemma 2.25 *For R a PID, a module M over R is flat if and only if it is torsion-free.*

Proof. This is the content of Problem 2 on the Midterm. ▲

Using this, we will classify modules over DVRs.

Proposition 2.26 *let M be a finitely generated module over a DVR R. Then*

$$M = M_{tors} \oplus R^{\oplus n},$$

i.e, where M_{tors} can be annihilated by π^n for some n.

Proof. Set $M_{tors} \subset M$ be as in Lemma 2.24 so that M/M_{tors} is torsion-free. Therefore, by Corollary **??** and Lemma 2.25 we see that it is flat. But it is over a local ring, so that means that it is free. So we have $M/M_{tors} = R^{\oplus n}$ for some n. Furthermore, since $R^{\oplus n}$ is free, it is additionally projective, so the above sequence splits, so

$$M = M_{tors} \oplus R^{\oplus n}$$

as desired. ▲

There is nothing more to say about the free part, so let us discuss the torsion part in more detail.

Lemma 2.27 *Any finitely generated torsion module over a DVR is*

$$\bigoplus R/\pi^n R.$$

Before we prove this, let us give two examples:

1. Take $R = k[[t]]$, which is a DVR with maximal ideal (t). Thus, by the lemma, for a finitely generated torsion module M, $t : M \to M$ is a nilpotent operator. However, $k[[t]]/t^n$ is a Jordan block so we are exactly saying that linear transformations can be written in Jordan block form.
2. Let $R = \mathbb{Z}_p$. Here the lemma implies that finitely generated torsion modules over $\mathbb{Z}_p$ can be written as a direct sum of p-groups.

Now let us proceed with the proof of the lemma.

Proof (Proof of Lemma 2.27). Let n be the minimal integer such that π^n kills M. This means that M is a module over $R_n = R/\pi^n R$, and also there is an element $m \in M$, and an injective map $R_n \hookrightarrow M$, because we may choose m to be an element which is not annihilated by π^{n-1}, and then take the map to be $1 \mapsto m$.

Proceeding by induction, it suffices to show that the above map $R_n \hookrightarrow M$ splits. But for this it suffices that R_n is an injective module over itself. This property of rings is called the Frobenius property, and it is very rare. We will write this as a lemma.

Lemma 2.28 *R_n is injective as a module over itself.*

Proof (Proof of Lemma 2.28). Note that a module M over a ring R is injective if and only if for any ideal $I \subset R$, $\mathrm{Ext}^1(R/I, M) = 0$. This was shown on Problem Set 8, Problem 2a.

Thus we wish to show that for any ideal I, $\mathrm{Ext}^1_{R_n}(R_n/I, R_n) = 0$. Note that since R is a DVR, we know that it is a PID, and also any element has the form $r = \pi^k r_0$ for some $k \geq 0$ and some r_0 invertible. Then all ideals in R are of the form (π^k) for some k, so all ideals in R_n are also of this form. Therefore, $R_n/I = R_m$ for some $m \leq n$, so it suffices to show that for $m \leq n$, $\mathrm{Ext}^1_{R_n}(R_m, R_n) = 0$.

But note that we have short exact sequence

$$0 \to R_{n-m} \to^{\pi^m \cdot} R_n \to R_m \to 0$$

which gives a corresponding long exact sequence of Exts

$$0 \to \mathrm{Hom}_{R_n}(R_m, R_n) \to \mathrm{Hom}_{R_n}(R_n, R_n) \to^{\heartsuit} \mathrm{Hom}_{R_n}(R_{n-m}, R_n)$$

$$\to \mathrm{Ext}^1_{R_n}(R_m, R_n) \to \mathrm{Ext}^1_{R_n}(R_n, R_n) \to \cdots$$

But note that any map of R_n modules, $R_{n-m} \to R_n$, must map $1 \in R_{n-m}$ to an element which is killed by π^{n-m}, which means it must be a multiple of π^m, so say is is $\pi^m a$. Then the map is

$$r \mapsto \pi^m ar,$$

which is the image of the map

$$[r \mapsto ar] \in \mathrm{Hom}_{R_n}(R_n, R_n).$$

Thus, $\heartsuit$ is surjective. Also note that R_n is projective over itself, so $\mathrm{Ext}^1_{R_n}(R_n, R_n) = 0$. This, along with the surjectivity of $\heartsuit$ shows that

$$\mathrm{Ext}^1_{R_n}(R_m, R_n) = 0$$

as desired. ▲

As mentioned earlier, this lemma concludes our proof of Lemma 2.27 as well. ▲

CRing Project contents

CRing Project bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In *Analysis and topology on singular spaces, I (Luminy, 1981)*, volume 100 of *Astérisque*, pages 5–171. Soc. Math. France, Paris, 1982.

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Cam88] Oscar Campoli. A principal ideal domain that is not a euclidean domain. *American Mathematical Monthly*, 95(9):868–871, 1988.

[CF86] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*, London, 1986. Academic Press Inc. [Harcourt Brace Jovanovich Publishers]. Reprint of the 1967 original.

[Cla11] Pete L. Clark. Factorization in euclidean domains. 2011. Available at `http://math.uga.edu/~pete/factorization2010.pdf`.

[dJea10] Aise Johan de Jong et al. *Stacks Project*. Open source project, available at `http://www.math.columbia.edu/algebraic_geometry/stacks-git/`, 2010.

[Eis95] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[For91] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.

[GD] Alexander Grothendieck and Jean Dieudonné. *Élements de géometrie algébrique*. Publications Mathématiques de l'IHÉS.

[Ger] Anton Geraschenko (mathoverflow.net/users/1). Is there an example of a formally smooth morphism which is not smooth? MathOverflow. `http://mathoverflow.net/questions/200` (version: 2009-10-08).

[Gil70] Robert Gilmer. An existence theorem for non-Noetherian rings. *The American Mathematical Monthly*, 77(6):621–623, 1970.

[Gre97] John Greene. Principal ideal domains are almost euclidean. *The American Mathematical Monthly*, 104(2):154–156, 1997.

[Gro57] Alexander Grothendieck. Sur quelques points d'algèbre homologique. *Tôhoku Math. J. (2)*, 9:119–221, 1957.

[Har77] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Hat02] Allen Hatcher. *Algebraic topology.* Cambridge University Press, Cambridge, 2002. Available at `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`.

[Hov07] Mark Hovey. *Model Categories.* American Mathematical Society, 2007.

[KS06] Masaki Kashiwara and Pierre Schapira. *Categories and sheaves*, volume 332 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 2006.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[LR08] T. Y. Lam and Manuel L. Reyes. A prime ideal principle in commutative algebra. *J. Algebra*, 319(7):3006–3027, 2008.

[Mar02] David Marker. *Model theory*, volume 217 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2002. An introduction.

[Mat80] Hideyuki Matsumura. *Commutative algebra*, volume 56 of *Mathematics Lecture Note Series.* Benjamin/Cummings Publishing Co., Inc., Reading, Mass., second edition, 1980.

[McC76] John McCabe. A note on Zariski's lemma. *The American Mathematical Monthly*, 83(7):560–561, 1976.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, Princeton, N.J., 1980.

[ML98] Saunders Mac Lane. *Categories for the working mathematician*, volume 5 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1998.

[Per04] Hervé Perdry. An elementary proof of Krull's intersection theorem. *The American Mathematical Monthly*, 111(4):356–357, 2004.

[Qui] Daniel Quillen. Homology of commutative rings. Mimeographed notes.

[Ray70] Michel Raynaud. *Anneaux locaux henséliens.* Lecture Notes in Mathematics, Vol. 169. Springer-Verlag, Berlin, 1970.

[RG71] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. *Invent. Math.*, 13:1–89, 1971.

[Ser65] Jean-Pierre Serre. *Algèbre locale. Multiplicités*, volume 11 of *Cours au Collège de France, 1957–1958, rédigé par Pierre Gabriel. Seconde édition, 1965. Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1965.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser09] Jean-Pierre Serre. How to use finite fields for problems concerning infinite fields. 2009. arXiv:0903.0517v2.

[SGA72] *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos.* Lecture Notes in Mathematics, Vol. 269. Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat.

[SGA03] *Revêtements étales et groupe fondamental (SGA 1).* Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 3. Société Mathématique de France, Paris, 2003. Séminaire de géométrie algébrique du Bois Marie 1960–61. [Algebraic Geometry Seminar of Bois Marie 1960-61], Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin; MR0354651 (50 #7129)].

[Tam94] Günter Tamme. *Introduction to étale cohomology.* Universitext. Springer-Verlag, Berlin, 1994. Translated from the German by Manfred Kolster.

[Vis08] Angelo Vistoli. Notes on Grothendieck topologies, fibered categories, and descent theory. *Published in* FGA Explained, 2008. arXiv:math/0412512v4.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, 1994.