Math 559: Commutative Algebra

Wolmer V. Vasconcelos

Set 3: Homological Algebra Tools

Fall 2009

Outline

Intro to Homological Algebra

Let R be a ring. We are going to examine some of the objects of the category $M(R)$ of left R-modules and their homomorphisms.

We have studied very few classes of modules–with two notable exceptions:

- Modules over PIDs or Dedekind domins
- Modules over semisimple rings

Even for these modules, we have yet to examine in some detail the morphisms between these modules.

Big Picture

We will focus on rings such as $R = k[x_1, \ldots, x_d]$, rings of polynomials in $d > 1$ indeterminates over a field k.

The following modules will me significant:

- Modules of syzygies: Those that occur as modules of relations
$$0 \to M \longrightarrow R^n \longrightarrow E \to 0$$

- Graded modules: Modules with a decomposition as k-vector spaces
$$M = \bigoplus_{n \in \mathbb{Z}} M_n, \quad x_i \cdot M_n \subset M_{n+1}$$
They have interesting numerical functions attached (the Hilbert function of M) $H_M(n) := \dim_k M_n$

Free modules

Definition

A free module F is a module $F = \bigoplus_\alpha R_\alpha$, $R_\alpha \simeq R$. In other words, there is a set $\{e_\alpha\}$ of elements in F such that every $v \in F$ has a unique representation $v = r_{\alpha_1} e_{\alpha_1} + \cdots + r_n e_{\alpha_n}$, $r_i \in R$.

They are characterized by the following:

Proposition

Given any mapping $\varphi : \{e_\alpha\} \to A$, where A is an R-module, there exists a unique homomorphism $\mathbf{f} : F \to A$ such that $\mathbf{f}(e_\alpha) = \varphi(e_\alpha)$.

Proof. Set $\mathbf{f}(\sum_\alpha r_\alpha e_\alpha) = \sum_\alpha r_\alpha \varphi(e_\alpha)$.

Homomorphisms

Let $\mathbf{f} : A \to B$ be a homomorphism of R-modules. Recall

$$\begin{aligned}\ker(\mathbf{f}) &= \{x \in A : \mathbf{f}(x) = 0\}\\ \operatorname{image}\mathbf{f} &= \{\mathbf{f}(x) : x \in A\}\\ \operatorname{coker}(\mathbf{f}) &= B/\operatorname{image}\mathbf{f}\end{aligned}$$

A complex of R-modules is a sequence of R-modules and homomorphisms

$$\mathbb{F} : \quad \cdots \longrightarrow F_n \xrightarrow{\mathbf{f}_n} F_{n-1} \xrightarrow{\mathbf{f}_{n-1}} F_{n-2} \longrightarrow \cdots$$

such that $\mathbf{f}_{n-1} \circ \mathbf{f}_n = 0$ for each n. This condition means that $\operatorname{image}\mathbf{f}_n \subset \ker(\mathbf{f}_{n-1})$ for each n. If one has equality, the complex is said to be exact. (A variation of terminology is *acyclic*, which we will clarify later.)

Short Exact Sequences

SES are the exact complexes of the form

$$0 \to A \xrightarrow{\mathbf{f}} B \xrightarrow{\mathbf{g}} C \to 0$$

f is 1-1, **g** is onto and Image $\mathbf{f} = \ker \mathbf{g}$. They are the basic components of longer exact complexes: The exact complex

$$0 \to A \xrightarrow{\mathbf{f}} B \xrightarrow{\mathbf{g}} C \xrightarrow{\mathbf{h}} D \to 0$$

is a concatenation of the two SES

$$0 \to A \xrightarrow{\mathbf{f}} B \longrightarrow \text{image}\,\mathbf{g} \to 0, \quad 0 \to \ker(\mathbf{h}) \longrightarrow C \xrightarrow{\mathbf{h}} D \to 0$$

glued by the equality $\text{image}\,\mathbf{g} = \ker \mathbf{h}$.

Syzygies

Let A be an R-module and $\{m_\alpha\}$ a set of elements of A–possibly a set of generators. Using the same index set, let F be a free R-module with a basis $\{e_\alpha\}$. Define a mapping $\mathbf{f} : F \to A$ by setting $\mathbf{f}(e_\alpha) = m_\alpha \in A$.

Definition

An element $\sum_\alpha r_\alpha e_\alpha$ is called a relation or a syzygy of the m_α if $\sum_\alpha r_\alpha m_\alpha = 0$. The set of all these relations is a submodule of F, the kernel of $\mathbf{f}$.

Free presentation

Let E be an R-module generated by the set $\{u_i\}$, $1 \leq i \leq n$. Let F be a free module with basis $\{e_i\}$, $1 \leq i \leq n$. Let L be the module of syzygies $\{v = (r_1 e_1 + \cdots + r_n e_n)\}$. If $v_1, \ldots, v_m$ is a set of generators of L, we have a complex

$$R^m \xrightarrow{\mathbf{A}} R^n \longrightarrow E \to 0,$$

where $\mathbf{A}$ is an $m \times n$ matrix

$$\mathbf{A} = \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mn} \end{bmatrix},$$

whose rows are the coordinates of the v_j. E is coded by $\mathbf{A}$. Can the properties of E be derived directly from $\mathbf{A}$?

Projective modules

Definition

An R-module P is projective if P a direct summand of a free R-module F, $F \simeq P \oplus Q$.

1. Let $R = \mathbb{Z} \times \mathbb{Z}$ and $P = \mathbb{Z} \oplus (O)$ and $Q = (O) \oplus \mathbb{Z}$.
2. $R \simeq P \oplus Q$
3. Note that P is not R-free

Properties

- If P_α is a family of projective modules, then $P = \bigoplus_\alpha P_\alpha$ is projective: For each α there is $P_\alpha \oplus Q_\alpha \simeq F_\alpha$, a free R-module. Setting $Q = \bigoplus_\alpha Q_\alpha$ we have

$$P \oplus Q \simeq \bigoplus_\alpha F_\alpha.$$

- If P is projective, there is a free R-module G such that $P \oplus G \simeq G$: Setting

$$G = Q \oplus P \oplus Q \oplus P \oplus \cdots \simeq F \oplus F \oplus \cdots$$

gives $P \oplus G \simeq G$

Characterization of projective modules

Proposition

An R-module E is projective iff whenever there is a surjection $\mathbf{f} : M \longrightarrow E \to 0$, there exists a homomorphism $\mathbf{h} : E \longrightarrow M$ such that the composite $\mathbf{f} \circ \mathbf{h}$ is the identity $\mathbf{I}$ of E.

Proof.

- Suppose $E \oplus Q \simeq F = \bigoplus Re_\alpha$, $Re_\alpha \simeq R$. Note that each $e_\alpha = p_\alpha + q_\alpha$, $p_\alpha \in E$, $q_\alpha \in Q$.
- Since $\mathbf{f}$ is surjective, for each p_α there is $m_\alpha \in M$ such that $\mathbf{f}(m_\alpha) = p_\alpha$.
- Because F is free, we can define a map $\mathbf{g} : F \longrightarrow M$ such that $\mathbf{g}(e_\alpha) = m_\alpha$.
- If we let $\mathbf{h}$ be the restriction of $\mathbf{g}$ to its submodule E, we have the forward implication.

For the converse, pick a surjection $\mathbf{f} : F \longrightarrow E \to 0$, where F is a free R-module. The existence of $\mathbf{h} : E \longrightarrow F$ such that $\mathbf{f} \circ \mathbf{h} = \mathbf{I}_E$ easily shows that if we set $P = \mathbf{h}(E)$ and $Q = \ker(\mathbf{f})$, then

- $P \simeq E$, as $\mathbf{h}$ is one-one onto
- $F = P + Q$
- $P \cap Q = (O)$
- Therefore $F = P \oplus Q \simeq E \oplus Q$

3-Sphere

$$R = \mathbb{R}[x,y,z]/(x^2+y^2+z^2-1) = \mathbb{R}[u,v,w], \quad u^2+v^2+w^2 = 1$$
$$\mathbf{f} : R^3 \longrightarrow R, \quad \mathbf{f}(a,b,c) = au+bv+cw$$

- $\mathbf{f}(u,v,w) = u^2+v^2+w^2 = 1$, so **f** is surjective
- Since R is free, sequence splits, that is $R^3 \simeq R \oplus \ker(\mathbf{f})$
- $T = \ker(\mathbf{f})$ consists of the elements $(a,b,c) \in R^3$ such that $au+bv+cw = 0$, i.e. of the *vectors* (a,b,c) perpendicular to (u,v,w)
- Discuss the picture!

Dedekind domains

Let R be an integral domain of field of fractions **K**. The ideals of R are part of an important class of R-submodules of **K**:

Definition

A submodule L of **K** is fractionary if there is $0 \neq d \in R$ such that $dL \subset R$.

1. This means that $L = d^{-1}Q$, where Q is an ideal of R.
2. **K** is not fractionary, unless $R = \mathbf{K}$.

The sum and the product of fractionary ideals is fractionary. Another operation is

Definition

The quotient of two fractionary ideals is

$$L_1 : L_2 = \{x \in \mathbf{K} : xL_2 \subset L_1\}.$$

In particular

$$R : L = \{x \in \mathbf{K} : xL \subset R\}.$$

L_1 is said to be invertible if there is a fractionary ideal L_2 such that $L_1 \cdot L_2 = R$.

Invertible Ideals

Proposition

If L is an invertible ideal of R, then L is a finitely generated R-module.

Proof.

The equality $L \cdot L' = R$ means that there are $x_i \in L$, $y_i \in L'$, $1 \leq i \leq n$, such that

$$1 = x_1 y_1 + \cdots + x_n y_n.$$

Thus for any $x \in L$,

$$x = (xy_1)x_1 + \cdots + (xy_n)x_n$$

which shows that $L_1 = (x_1, \ldots, x_n)$ since all $xy_i \in R$. □

Proposition

Let R be an integral domain and L an invertible ideal. Then L is a projective R-module.

Proof.

Let $L = (x_1, \ldots, x_n)$ and $L' = (y_1, \ldots, y_n)$ with $L \cdot L' = R$ and $x_1 y_1 + \cdots + x_n y_n = 1$. We use this data to show that L is a direct summand of a free R-module. Define the maps

$$\varphi : R^n \to L, \varphi(e_i) = x_i,$$

$$\phi : L \to R^n, \quad \phi(x) = xy_1 e_1 + \cdots + xy_n e_n, \quad x \in L$$

Observe: $\varphi \circ \phi : L \to L$ is the identity of L. □

Circle ring

Let $R = \mathbb{R}[\cos t, \sin t]$, the ring of trigonometric polynomials.

$$\begin{aligned} &(1-\cos t, \sin t)\cdot(1+\cos t, \sin t) \\ &= (1-\cos^2 t, (1-\cos t)\sin t, (1+\cos t)\sin t, \sin^2 t) \\ &= \sin t(\sin t, 1-\cos t, 1+\cos t, \sin t) \\ &= (\sin t) \end{aligned}$$

Thus $(1-\cos t, \sin t)$ is invertible, hence projective.
In fact every ideal of R is invertible.

When are projective modules free

We already know that projective $\mathbb{Z}$-modules are free.

Theorem

Let $\mathbf{R}$ *be a local ring of maximal ideal* $\mathfrak{m}$*. Then any projective* $\mathbf{R}$*-module* P *is free.*

Proof. This theorem holds true for all projective $\mathbf{R}$-modules [Kaplansky]. Here we only deal with the easy case, when P is finitely generated.

- Consider the finite dimensional $\mathbf{R}/\mathfrak{m}$-vector space $P/\mathfrak{m}P$. That is $P = (x_1, \ldots, x_n, \mathfrak{m}P)$ where the classes of x_i generate a basis of $P/\mathfrak{m}P$.

- By Nakayama Lemma, $P = (x_1, \ldots, x_n)$. Therefore there is a surjection
$$0 \to L \longrightarrow \mathbf{R}^n \longrightarrow P \to 0.$$
- Since P is projective, this sequence splits,
$$\mathbf{R}^n \simeq P \oplus L,$$
so reduction modulo $\mathfrak{m}$ gives
$$\mathbf{R}^n/\mathfrak{m}\mathbf{R}^n \simeq P/\mathfrak{m}P \oplus L/\mathfrak{m}L$$
- Therefore $L/\mathfrak{m}L = 0$, and by Nakayama Lemma $L = 0$ since it is finitely generated. Thus $P \simeq \mathbf{R}^n$.

Graded modules

Theorem

Let $(\mathbf{R}, \mathfrak{m})$ be a local ring and $\mathbf{A}$ a positively graded finitely generated $\mathbf{R}$-algebra,

$$\mathbf{A} = A_0(= \mathbf{R}) + A_1 + A_2 + \cdots .$$

If $\mathbf{M}$ is a finitely generated, graded, projective $\mathbf{A}$-module then $\mathbf{M}$ is a free $\mathbf{A}$-module.

The proof is similar. Pass to the $\mathbf{R}/\mathfrak{m}$-vector space

$$\mathbf{M}/(\mathfrak{m}, \mathbf{A}_+)\mathbf{M}, \quad \mathbf{A}_+ = A_1 + A_2 + \cdots$$

Theorem (Quillen-Suslin)

If k is a field, projective modules over rings of polynomials $\mathbf{R} = k[x_1, \ldots, x_d]$ are free.

Projective Modules and Vector Bundles

Let $\mathbf{R}$ be a commutative ring and P a finitely generated projective module.

- Let $\mathfrak{p}$ be a prime ideal. $P_{\mathfrak{p}}$ is a free $\mathbf{R}_{\mathfrak{p}}$-module. Let $x_1, \ldots, x_n$ be elements of P such that their images in $P_{\mathfrak{p}}$ form a basis. [Why?]
- Map $\mathbf{R}^n$ into P, $\varphi : e_i \to x_i$. This gives rise to a exact sequence

$$0 \to K \longrightarrow \mathbf{R}^n \xrightarrow{\varphi} P \longrightarrow C \to 0.$$

- Localizing at $\mathfrak{p}$ gives $K_{\mathfrak{p}} = C_{\mathfrak{p}} = 0$, since $\varphi_{\mathfrak{p}}$ is an isomorphism. It follows that here is $f \notin \mathfrak{p}$ such that $K_f = C_f = 0$.

Vector Bundles

Theorem

Let $\mathbf{R}$ be a commutative ring and P a finitely presented $\mathbf{R}$-module. P is projective iff P is locally free on $\mathrm{Spec}(\mathbf{R})$, that is for each prime ideal $\mathfrak{p}$ there is $f \notin \mathfrak{p}$ such that P_f is a free $\mathbf{R}_f$-module.

Injective modules

Definition

An R-module E is injective if for any diagram of modules and homomorphims

$$\begin{array}{ccc} A & \xrightarrow[\mathbf{g}]{} & B \\ {\scriptstyle \mathbf{f}}\big\downarrow & & \\ E & & \end{array}$$

with $\mathbf{g}$ injective, there is a homomorphism $\mathbf{h} : B \to E$ such $\mathbf{f} = \mathbf{h} \circ \mathbf{g}$.

Note that this says that “homomorphisms into E can be extended.”

It is hard to test. The next results cuts down on the task.

Baer Test

Theorem

An R-module E is injective if for any diagram of modules and homomorphims

$$\begin{array}{ccc} I & \xrightarrow[\mathbf{g}]{} & R \\ {\scriptstyle \mathbf{f}}\downarrow & & \\ E & & \end{array}$$

with $\mathbf{g}$ *injective, there is a homomorphism* $\mathbf{h} : R \to E$ *such* $\mathbf{f} = \mathbf{h} \circ \mathbf{g}$.

Proof. Suppose we have a mapping $\mathbf{f} : A \to E$ from the submodule $A \hookrightarrow B$ we seek to extend it to a mapping $\mathbf{h} : B \to E$. The assumption is that this is possibe whenever A is as ideal of $B = R$.

Proof cond'd

- We are going to argue that if $A \neq B$, we can extend $\mathbf{f} : A \to E$ to a larger submodule $A \subsetneq A' \subseteq B$, $\mathbf{f}' : A' \to E$.
- Then we use a simple application of Zorn's Lemma to build an extension $\mathbf{g} : B \to E$.
- Let $b \in B \setminus A$ and let $I = \{r \in R : rb \in A\}$. I is a left ideal of R.
- Let use see how $\mathbf{f}$ induces a homomorphism $\varphi : I \to E$. For $r \in I$, define
$$\varphi(r) = \mathbf{f}(rb)$$

- Let φ' be an extension of $\varphi : I \to E$ to $\varphi' : R \to E$. Note that for any $r \in I$, $\varphi(r) = \varphi'(r \cdot 1) = r\varphi'(1)$.
- Define $\mathbf{f}' : A + Rb \to E$ by

$$\mathbf{f}'(a + sb) \quad = \quad \mathbf{f}(a) + s\varphi'(1)$$

- We claim that $\mathbf{f}'$ is well defined: If $x = a + sb = a' + s'b$ we must show the value $\mathbf{f}'(x)$ is independent of the representation.
- The equality gives $(s - s')b = a' - a \in A$ so $s - s' \in I$ and the assertion follows.
- Zorn's: Consider the set of pairs $(C, \mathbf{f}')$ where $\mathbf{f}' : C \to E$ where $\mathbf{f}'$ extends $\mathbf{f}$. This set is partially ordered. etc

$\mathbb{Z}$-modules

Theorem

Any injective $\mathbb{Z}$-module E is divisible (and conversely).

Proof.

1. Recall that an abelian group E is **divisible** if for $x \in E$ and $0 \neq n$ there is $y \in E$ with $x = ny$.
2. Let E be an injective $\mathbb{Z}$-module. If $x \in E$, for any integer n there is a group homomorphism $\mathbf{f} : (n) \to E$ with $\mathbf{f}(n) = x$.
3. Denote by $\mathbf{g} : (n) \to \mathbb{Z}$ the natural inclusion
4. Since E is injective, let $\mathbf{h} : \mathbb{Z} \to E$ such that $\mathbf{f} = \mathbf{h} \circ \mathbf{g}$
5. $x = \mathbf{f}(n) = \mathbf{h}(\mathbf{g}(n)) = \mathbf{h}(n \cdot 1) = n\mathbf{h}(1)$, that is $x = n\mathbf{h}(1)$

Corollary

A $\mathbb{Z}$-module is injective iff it is divisible.

The ring of dual numbers

Let k be a field and $R = k[x]/(x^2)$. R is a ring which is a k-vector space of dimension two, with basis which we denote 1 and u, with $u^2 = 0$.

Let us show that as a module over itself, R is injective.

- We are going to use Baer Test. Observe that R has only 3 ideals: $(0), (x)$ and R. Given a morphism from one of them, $\mathbf{f} : I \to R$, we must show it can be extended to a morphism $\mathbf{g} : R \to R$.
- If $I = 0$ or $I = R$, there is nothing to do, so we assume $I = (x)$. If $\mathbf{f} = 0$, there is nothing to do.
- If $\mathbf{f} \neq 0$, the image of $\mathbf{f} : (x) \to R$ is also (x), so $\mathbf{f}(x) = rx$, $r \in k$.
- This shows that $\mathbf{g}$ can be taken as multiplcation by r

Outline

The Hom Functor

Let R be a ring with 1. We denote by $\mathrm{mod}(R)$ the category of left R-modules. In most cases we assume R commutative.

- Let E be a left R-module. If A is an R-module we set $\mathrm{Hom}_R(E, A)$ for the abelian group of all R-homomorphisms $\mathbf{f} : E \to A$. (If R is commutative, $\mathrm{Hom}_R(E, A)$ is an R-module.)
- For example, if $E = R$, $\mathrm{Hom}_R(R, A) \simeq A$,
- $\mathrm{Hom}_R(E, A \oplus B) \simeq \mathrm{Hom}_R(E, A) \oplus \mathrm{Hom}_R(E, B)$.
- Many properties of this construction mimic what is done with vector spaces. **Achtung:** $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2), \mathbb{Z}) = 0$

Properties of Hom

- If $\varphi : A \to B$, there is a group homomorphism

$$\varphi_* : \mathrm{Hom}_R(E, A) \to \mathrm{Hom}_R(E, B), \quad \varphi_*(\mathbf{f}) = \varphi \circ \mathbf{f}$$

- We also write $\varphi_* = \mathrm{Hom}(\varphi)$
- $\varphi_*(\mathbf{f}_1 + \mathbf{f}_2) = \varphi_*(\mathbf{f}_1) + \varphi_*(\mathbf{f}_2)$
- If φ is the identity of A, $\mathbf{I} : A \to A$, then φ_* is identity of $\mathrm{Hom}_R(E, A)$
- If $A \xrightarrow{\varphi} B \xrightarrow{\phi} C$ then $(\phi \circ \varphi)_* = \varphi_* \circ \phi_*$

Exactness and Hom

Proposition

Let R be a ring and E an R-module.

1. *Then E is projective iff the functor $\mathrm{Hom}_R(E, \cdot)$ is exact, that is for any SES of R-modules*

$$0 \to A \longrightarrow B \longrightarrow C \to 0,$$

   the complex

$$0 \to \mathrm{Hom}_R(E, A) \longrightarrow \mathrm{Hom}_R(E, B) \longrightarrow \mathrm{Hom}_R(E, C) \to 0$$

   is exact.

2. *Similarly, E is injective if the complex*

$$0 \to \mathrm{Hom}_R(C, E) \longrightarrow \mathrm{Hom}_R(B, E) \longrightarrow \mathrm{Hom}_R(A, E) \to 0$$

   is exact.

Exactness and Hom

Proposition

Let R be a ring and E an R-module.

1. *Then E is projective iff for each surjection $B \longrightarrow C \to 0$, the induced mapping*

$$\mathrm{Hom}_R(E, B) \longrightarrow \mathrm{Hom}_R(E, C) \to 0$$

   is also a surjection.

2. *Similarly, E is injective iff for each injection $0 \to A \longrightarrow B$, the induced mapping*

$$\mathrm{Hom}_R(B, E) \longrightarrow \mathrm{Hom}_R(A, E) \to 0$$

   is a surjection.

Exactness and Hom cont'd

Proposition

Let R be a ring and E an R-module.

1. *Then E is projective iff the functor $\mathrm{Hom}_R(E, \cdot)$ is exact, that is for any SES of R-modules*

$$0 \to A \longrightarrow B \longrightarrow C \to 0,$$

the complex

$$0 \to \mathrm{Hom}_R(E, A) \longrightarrow \mathrm{Hom}_R(E, B) \longrightarrow \mathrm{Hom}_R(E, C) \to 0$$

is exact.

2. *Similarly, E is injective if the complex*

$$0 \to \mathrm{Hom}_R(C, E) \longrightarrow \mathrm{Hom}_R(B, E) \longrightarrow \mathrm{Hom}_R(A, E) \to 0$$

is exact.

Adjointness

Let us briefly discuss a tool that produces injective modules galore. It has many other uses that will be left untouched.

Let A be an R-module [say right R-module]. A being an abelian group, then for any abelian group E we may consider $\mathrm{Hom}_{\mathbb{Z}}(A, E)$. We make some observations about this abelian group:

- $\mathrm{Hom}_{\mathbb{Z}}(A, E)$ has a natural structure of a left R-module: For $r \in R$ and $\mathbf{f} \in \mathrm{Hom}_{\mathbb{Z}}(A, E)$ define

$$(r \cdot \mathbf{f})(a) = \mathbf{f}(ar)$$

- For any left R-module B,

$$\mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(R, E)) = \mathrm{Hom}_{\mathbb{Z}}(B, E)$$

Proposition

Let E be an injective $\mathbb{Z}$-module. Then $\mathrm{Hom}_{\mathbb{Z}}(R, E)$ is a left [and right] injective R-module.

Proof. According to the observation above,

$$\mathrm{Hom}_R(B, \mathrm{Hom}_{\mathbb{Z}}(R, E)) = \mathrm{Hom}_{\mathbb{Z}}(B, E)$$

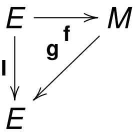
Since E is an injective $\mathbb{Z}$-module, the $\mathbb{Z}$-functor $\mathrm{Hom}_{\mathbb{Z}}(\cdot, E)$ is exact, so the R-functor $\mathrm{Hom}_R(\cdot, \mathrm{Hom}_{\mathbb{Z}}(R, E))$ is exact, hence the assertion.

Characterization of injective modules

Proposition

An R-module E is injective iff whenever there is an embedding $\mathbf{f} : E \longrightarrow M$, there exists a homomorphism $\mathbf{h} : M \longrightarrow E$ such that the composite $\mathbf{h} \circ \mathbf{f}$ is the identity $\mathbf{I}$ of E.

This is represented by the commutative diagram



This is a special case of the definition of injective module. To prove the converse one first shows

Theorem

Every R-module A embeds into an injective module $A \hookrightarrow E$.

We first prove a very special case:

Theorem

Every abelian group A can be embedded into a divisible abelian group.

Proof. Let $F = \bigoplus \mathbb{Z} e_\alpha$ be a free abelian group mapping onto A, so $A \simeq F/L$. Next embed F into the $\mathbb{Q}$-vector space $G = \bigoplus \mathbb{Q} e_\alpha$.

G is a divisible group and so is its homomorphic image G/L. But we have

$$A \simeq F/L \hookrightarrow G/L.$$

Theorem

Every R-module A embeds into an injective module $A \hookrightarrow E$.

Proof.

- First, embed A into a divisible abelian group, $\varphi : A \hookrightarrow D$.
- We claim that A embeds into $\mathrm{Hom}_{\mathbb{Z}}(R, D)$, which by the adjointness observation is an injective R-module.
- For each $x \in A$ define $\mathbf{f}(x) \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$ by the rule $\mathbf{f}(x)(r) = \varphi(rx)$.
- It is clear that $\mathbf{f}$ is an R-module homomorphism and is 1-1 (as $\mathbf{f}(x)(1) = \varphi(x)$).

Injective Resolution

We can iterate the process of embedding a module into an injective module:

- Let A be an R-module, and $0 \to A \xrightarrow{\mathbf{f}_0} E_0$ an embedding with E_0 injective.
- Set $A_1 = E_0/\mathbf{f}_0(A)$ and let $0 \to A_1 \xrightarrow{\mathbf{f}_1} E_1$ an embedding with E_1 injective.
- Iteration leads to the exact complex

  $$0 \to A \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \cdots ,$$

  called an injective resolution of A.
- If $R = \mathbb{Z}$, after the first embedding $0 \to A \xrightarrow{\mathbf{f}_0} E_0$, we already have an injective resolution since A_1 is a divisible abelian group.

Sums and Products of Injectives

Let R be a ring and $\{E_\alpha\}$ is be a collection of injective modules:

- $E = \prod E_\alpha$ is injective:
  This clear since a map $f : A \to E$ is defined by a collection $f_\alpha : A \to E_\alpha$,
  $$f(x) = (f_\alpha(x))$$
  Therefore given an inclusion $A \subset B$ and a map f from A to E, to extend it to a map from B to E, it suffices to extend each of the components f_α mentioned above.
- The situation is very different if we replace $\prod E_\alpha$ by $\bigoplus E_\alpha$

Characterizing Noetherianess with injectives(Bass)

Theorem

The ring R is Noetherian iff the direct sum of a collection of injective modules is injective.

Proof.

- Suppose R is Noetherian and $\{E_\alpha\}$ is a collection of injectives. To prove that $E = \bigoplus E_\alpha$ is injective, we apply Baer's Test: If $f : I \to E$ is a map from the ideal I, we argue that it can be extended to a map $f' : R \to E$.

  Since I is finitely generated, its image actually lies in the summand $E' = E_{\alpha_1} \oplus \cdots \oplus E_{\alpha_n}$ of E. E' being a direct product of injectives, f can be extended to $f' : R \to E' \subset E$.

- To prove the converse, suppose R is not Noetherian. There is then a chain of distinct ideals

$$(x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, \ldots, x_n) \subset \ldots$$

- Set $I_n = (x_1, \ldots, x_n)$ and $I = \bigcup I_n$. For each n let $g_n : I/I_n \to E_n$ be an embedding into the injective module E_n.
- Define a map $g : I \to \bigoplus E_n$ as $g(x) = (g_n(x))$. Note that for each $x \in I$, $g_n(x) = 0$ for almost all n, so this effectively defines a map from I into the direct sum.
- Note that g cannot be extended into a map $g' : R \to \bigoplus E_n$ since $g'(R)$ is contained in a finite direct sum of E_n, while $g(I)$ is not.

Outline

Projective Resolution

Let R be a ring and M an R-module. One of the most fruitful way to study M is to build the following structure:

$$O \to K \xrightarrow{\alpha} F = R^n \xrightarrow{\varphi} M \to 0, \quad K = \ker(\varphi)$$

with F a free (projective) module. This complex is called a free (projective) presentation of M.
We can build a free presentation of K itself

$$O \to L \longrightarrow G = R^m \xrightarrow{\beta} K \to 0, \quad K = \ker(\beta)$$

and composing $\mathbf{f} = \alpha \circ \beta$ get the acyclic complex where $\mathbf{f}$ can be represented by a $n \times m$ matrix with entries in R

$$R^m \xrightarrow{\mathbf{f}} R^n \longrightarrow M \to 0$$

Example

Let $R = k[x, y]$, k a field, and $M = (x, y)$, the ideal generated by x, y. A free presentation consists of the mapping

$$R^2 \to (x, y), \quad (a, b) \to ax + by, \quad a, b \in R$$

- The kernel K consists of $\{(a, b) : ax + by = 0\}$ or $ax = -by$,
- This implies that $a = yc$ and $b = xd$ and therefore $c = -d$ because x and y are prime elements
- Thus the kernel consists of elements $c(y, -x)$, $c \in R$ and therefore

$$O \to R \xrightarrow{\mathbf{f}} R^2 \longrightarrow (x, y) \to O, \quad \mathbf{f}(1) = (y, -x)$$

Example

A more interesting example is $M = (x, y, z) \subset R = k[x, y, z]$. The full free presentation (meaning what) of M is the complex

$$0 \to R \xrightarrow{\mathbf{f}_2} R^3 \xrightarrow{\mathbf{f}_1} R^3 \xrightarrow{\varphi} M \to 0,$$

with maps (represented by matrices)

$$\mathbf{f}_1 = \begin{bmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{bmatrix}, \quad \mathbf{f}_2 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$$

This is another instance of a complex known as the Koszul complex

Example

Another kind of resolution is illustrated by the example:
$M = (xy, xz, yz) \subset R = k[x, y, z]$

$$0 \longrightarrow R^2 \xrightarrow{\mathbf{f}} R^3 \xrightarrow{\varphi} M \longrightarrow 0$$

where

$$\mathbf{f} = \begin{bmatrix} z & 0 \\ -y & y \\ 0 & -x \end{bmatrix}$$

This is an instance of a complex known as the Hilbert-Burch complex

Complexes from matrices

Many complexes of free modules are associated to matrices **A** with entries in a ring R. Let us discuss one that goes back to Hilbert.

Let R be an integral domain [think a polynomial ring] and let **A** be an $(n-1)\times n$ matrix with entries in R [for convenience we make $n = 3$]:
Let Δ_1, Δ_2 and Δ_3 be the minors (with signs) of the columns.
For instance, $\Delta_1 = a_{12}a_{23} - a_{13}a_{22}$.

We are going to find some of the syzygies of $\Delta_1, \Delta_2, \Delta_3$:
$b_1\Delta_1 + b_2\Delta_2 + b_3\Delta_3 = 0$

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = a_{11}\Delta_1 + a_{12}\Delta_2 + a_{12}\Delta_3 = 0$$

Thus the column vectors of the transpose of

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

are syzygies of $(\Delta_1, \Delta_2, \Delta_3)$.

Let **B** be the column matrix of the Δ's.

With the matrices **A** and **B** [note that $\mathbf{B}\mathbf{A}^t = 0$], we form the complex:

$$0 \to R^2 \xrightarrow{\mathbf{A}^t} R^3 \xrightarrow{\mathbf{B}} R \longrightarrow R/(\Delta_1, \Delta_2, \Delta_3) \to 0$$

Theorem

If R is a UFD this complex is exact iff $\gcd(\Delta_1, \Delta_2, \Delta_3) = 1$.

Hilbert-Burch

Theorem

Let $R = k[x, y]$. Then for any ideal $I = (a_1, \dots, a_n)$ with $\gcd(I) = 1$ there exists an $(n-1) \times n$ matrix $\mathbf{A}$ with entries in R such that its maximal minors $\Delta_i = a_i$.

This means that if we map the free R-module R^n onto $(a_1, \dots, a_n)$

$$Re_1 \oplus \cdots Re_n \xrightarrow{\varphi} I, \quad \varphi(e_i) = a_i,$$

the kernel of φ is generated by $n-1$ vectors, $v_i = (d_{1,i}, \dots, d_{n-1,i})$ and the a_i are the cofactors of the matrix $\mathbf{A} = [d_{ij}]$.

Return to an important example

Example

Let $\mathbf{V}$ be a finite dimensional vector space over the field k, and let

$$\varphi : \mathbf{V} \longrightarrow \mathbf{V}$$

be a linear transformation. Define a $k[\mathbf{x}]$-module structure $\mathbf{M}$ by declaring

$$x \cdot v = \varphi(v), \quad \forall v \in \mathbf{V}.$$

More generally, for a polynomial $\mathbf{f}(\mathbf{x})$, define

$$\mathbf{f}(\mathbf{x})v = \mathbf{f}(\varphi)(v).$$

We denote this module by $\mathbf{V}_\varphi$.

The Syzygies of $\mathbf{V}_\varphi$

Pick a k-basis $u_1, \ldots, u_n$ for $\mathbf{V}$, so that $\varphi = [c_{ij}]$. Let us determine a free presentation for $\mathbf{V}_\varphi$

$$0 \longrightarrow K \longrightarrow Re_1 \oplus \cdots \oplus Re_n \longrightarrow \mathbf{V}_\varphi \to 0, \quad e_i \to u_i.$$

Let us determine the module K. If

$$v = (\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}_n(\mathbf{x})),$$

$$\sum_{i=1}^{n} \mathbf{f}_i(\varphi)(u_i) = 0.$$

For instance, from

$$\varphi(u_i) = \mathbf{x}u_i = \sum c_{ij}u_j,$$

we have that the rows of the matrix lie in K

$$[c_{ij}] - \mathbf{x}\mathbf{I} = \begin{bmatrix} c_{11} - \mathbf{x} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} - \mathbf{x} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} - \mathbf{x} \end{bmatrix}$$

Proposition

K is generated by the rows of $\varphi - \mathbf{x}\mathbf{I}$.

Proof. Let $v = (\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}_n(\mathbf{x})) \in L$. We argue that v is a linear combination (with coefficients in R) of the rows of $\varphi - \mathbf{x}\mathbf{I}$.

- If all the $\mathbf{f}_i(\mathbf{x})$ constants, $\sum_i \mathbf{f}_i u_i = 0$ means that $\mathbf{f}_i = 0$, since the u_i are k-linearly independent.
- We induct on $\sup\{\deg(\mathbf{f}_i)\}$ and on the number of components of this degree. Say $\deg(\mathbf{f}_1) = \sup\{\deg(\mathbf{f}_i)\}$. Divide $\mathbf{f}_1$ by $c_{11} - \mathbf{x}$, $\mathbf{f}_1 = \mathbf{q}(c_{11} - \mathbf{x}) + r$,

$$(\mathbf{f}_1, \ldots, \mathbf{f}_n) - \mathbf{q}(c_{11} - \mathbf{x}, \ldots, c_{1n}) = (\mathbf{g}_1, \ldots, \mathbf{g}_n) = u.$$

  Note that u has fewer terms, if any, of degree $\geq \deg(\mathbf{f}_1)$.

Proposition

If k is a field and $\varphi : V \simeq k^n \to V$ is a linear transformation, the $R = k[\mathbf{x}]$-module V_φ has for a matrix representation $\mathbf{f}$, a free $k[\mathbf{x}]$-resolution

$$O \to R^n \xrightarrow{\mathbf{f}} R^n \longrightarrow V_\varphi \to O,$$

where $\mathbf{f} = \varphi - \mathbf{x}\mathbf{I}_n$.

Projective/Free Resolutions

Definition

Let R be a ring and M an R-module. A free resolution of M is an acyclic complex

$$\cdots \to F_n \to F_{n-1} \to \cdots \to F_1 \to F_0 \to M \to 0,$$

where the F_i are free R-modules. If we replace free by projective, we call the complex a projective resolution of M.

Example: Let $R = \mathbb{Z}/(4)$ and $M = R/(2) = \mathbb{Z}/(2)$. The free resolution of M is the infinite complex

$$\cdots R \to \cdots \to R \to R \to M \to 0$$

where all maps $R \to R$ are multiplication by 2.

Examples

- If $R = k$, a field, then any k-module M is a vector space, so its free resolution is ($n = \dim_k M$)

$$0 \to R^n \longrightarrow M \to 0$$

- $R = \mathbb{Z}$, for abelian group M,

$$0 \to R^m \longrightarrow R^n \longrightarrow M \to 0,$$

  m and n appropriate cardinals.
- $R = k[x, y]$ and $M = R/(x, y)$

$$0 \to R \longrightarrow R^2 \longrightarrow R \longrightarrow M \to 0$$

Projective Resolutions

We would like to use the length of these complexes as a form of **dimension** for the module. It is more convenient to consider the case of acyclic complexes

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

where P_i is projective for $i < n$. To make sense, we must compare it to another complex

$$0 \to Q_n \to Q_{n-1} \to \cdots \to Q_1 \to Q_0 \to M \to 0,$$

where Q_i is projective for $i < n$.

Question: How are P_n and Q_n related? We will focus on the case $n = 1$.

Fibre Products

Definition

Let $\mathbf{f} : A \to C$ and $\mathbf{g} : B \to C$ be homomorphims of R-modules. The fiber product of $\mathbf{f}$ and $\mathbf{g}$ is the submodule of $A \times B$

$$A \times_C B = \{(x, y) : \mathbf{f}(x) = \mathbf{g}(y)\}.$$

Schanuel Lemma

Proposition

Let M be an R-module and

$$0 \to K \longrightarrow P \xrightarrow{\mathbf{f}} M \to 0, \quad 0 \to L \longrightarrow Q \xrightarrow{\mathbf{g}} M \to 0$$

be projective presentations of M. Then

$$K \oplus Q \simeq L \oplus P.$$

Proof. Consider the projection $\varphi : P \times_M Q \to P$ into the first component. For each $x \in P$ there is $y \in Q$ such that $\mathbf{f}(x) = \mathbf{g}(y)$ since both maps $\mathbf{f}$ and $\mathbf{g}$ are surjective. This implies that φ is also surjective. Note that $(x, y) \in \ker(\varphi) \simeq L : x = 0$ and thus $\mathbf{f}(x) = \mathbf{g}(y) = 0$.

Since P is projective, φ will split:

$$P \otimes_M Q \simeq P \oplus L$$

Corollary

Let

$$0 \to K \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

$$0 \to L \to Q_{n-1} \to \cdots \to Q_1 \to Q_0 \to M \to 0,$$

be acyclic complexes with P_i, Q_i projective modules for $i < n$. Then

$$K \oplus Q_{n-1} \oplus P_{n-2} \oplus Q_{n-3} \oplus \cdots \simeq L \oplus P_{n-1} \oplus Q_{n-2} \oplus P_{n-} \oplus \cdots .$$

In particular, if K is projective, then L is projective as well.

Class discussion

Consider the injective analogue of Schanuel's Lemma:

Proposition

Let A be an R-module and

$$0 \to A \longrightarrow E \xrightarrow{\mathbf{f}} B \to 0, \quad 0 \to A \longrightarrow E' \xrightarrow{\mathbf{g}} B' \to 0$$

be injective presentations of A. Then

$$B \oplus E' \simeq B' \oplus E.$$

Proof. (A volunteer please!)

Projective dimension

Definition

The projective dimension of an R-module M is the length n of the shortest acyclic complex

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to M \to 0,$$

with $0 \neq P_i$ projective for all i, or ∞. It is written $\mathrm{proj.\ dim.}_R M$.

Modules of Polynomials

Let R be a commutative ring and M an R-module. We define the module of polynomials with coefficients in M:

$$M[x] = \bigoplus_{n \geq 0} M_n, \quad M_n = M$$

made into an $R[x]$-module by the rule

$$x \cdot M_n \subset M_{n+1}.$$

It is convenient to write $M_n = M \otimes x^n$. We make this construction into a functor from the category $\mathcal{M}(R)$ to the category $\mathcal{M}(R[x])$ as follows: If $\mathbf{f} : M \to N$

$$\mathbf{f}' : M[x] \to N[x], \quad \mathbf{f}'(m \otimes x^n) = \mathbf{f}(m) \otimes x^n$$

Properties

Proposition

The functor $\mathbf{T} : M \to M[x]$ *has the following properties:*

1. *If* M *is a projective* R*-module, then* $\mathbf{T}(M) = M[x]$ *is a projective* $R[x]$*-module.*
2. *If* $0 \to A \longrightarrow B \longrightarrow C \to 0$ *is a SES of* R*-modules, then*

$$0 \to \mathbf{T}(A) \longrightarrow \mathbf{T}(B) \longrightarrow \mathbf{T}(C) \to 0$$

is a SES of $R[x]$*-modules.*

Achtung: If E is an injective R-module, $\mathbf{T}(E)$ is not an injective $R[x]$-module. It is not divisible by x, for one.

Exercises

- Let $R = k[x, y]$. For each integer n, find the free resolution of the ideal $I = (x, y)^n$.
- Write a brief essay on: If E is an injective R-module, what is an injective resolution of the $R[x]$-module $E[x]$ like?

Exercises

- $R = k[x, y]$, the polynomial ring in 2 indeterminates over the field k. Prove that different powers of (x, y) cannot be isomorphic. Prove also that (x, y) cannot be isomorphic to $(x, y - 1)$.

  You may need

  Lemma: Let I, J be two ideals of the integral domain R of field of fractions $\mathbf{K}$. Then

$$\mathrm{Hom}_R(I, J) = \{q \in \mathbf{K} : qI \subset J\}.$$

Graphs and Ideals

Let $G = \{V, E\}$ be a graph of vertex set $V = \{v_1, \ldots, v_n\}$ and edge set E. We will associate to G a graded algebra.

- Let $R = k[x_1, \ldots, x_n]$, one indeterminate to each vertex. To the edge $\{v_i, v_j\}$, we associate the monomial $x_i x_j$. The edge ideal of G is the ideal $I(G)$ generated by all $x_i x_j$'s.
- $I(G)$ is a homogeneous ideal. One expects the graded algebra $R/I(G)$ to reflect properties of the graph. For example, describe the minimal primes of $I(G)$ in graph theoretic info.

Outline

Multilinear functions

What is this? We have studied linear functions on vector spaces/modules

$$\mathbf{T} : \mathbf{V} \to \mathbf{W},$$

$$\mathbf{T}(au + bv) = a\mathbf{T}(u) + b\mathbf{T}(v).$$

A bilinear function is an extension of the product operation

$$(\mathbf{x}, \mathbf{y}) \to \mathbf{xy}.$$

Note that it is additive in ‘each variable’, e.g.

$$\mathbf{x}(\mathbf{y}_1 + \mathbf{y}_2) = \mathbf{xy}_1 + \mathbf{xy}_2$$

$$(\mathbf{x}_1 + \mathbf{x}_2)\mathbf{y} = \mathbf{x}_1\mathbf{y} + \mathbf{x}_2\mathbf{y}$$

We want to examine functions like these whose sources and targets are vector spaces/modules. For example, the function $\mathbf{B}$ is bilinear if

$$\mathbf{B} : \mathbf{V} \times \mathbf{V} \to \mathbf{W},$$

is linear in each variable

$$\mathbf{B}(u_1 + u_2, v) = \mathbf{B}(u_1, v) + \mathbf{B}(u_2, v), \quad \mathbf{B}(au, v) = a\mathbf{B}(u, v)$$

$$\mathbf{B}(u, v_1 + v_2) = \mathbf{B}(u, v_1) + \mathbf{B}(u, v_2), \quad \mathbf{B}(u, av) = a\mathbf{B}(u, v)$$

You can define trilinear, and generally multilinear in the same manner: $\mathbf{B}(v_1, v_2, \ldots, v_n)$, linear in each variable.

Let us begin with a beautiful example: Let $\mathbf{V} = \mathbf{F}^2$ be a plane. For every pair of vectors $u = (a, b), v = (c, d)$, define

$$\mathbf{B}(u, v) = ad - bc.$$

You can check easily that $\mathbf{B}$ is a bilinear function from $\mathbf{F}^2$ into $\mathbf{F}$. For example, $\mathbf{B}(u, v_1 + v_2) = \mathbf{B}(u, v_1) + \mathbf{B}(u, v_2)$.

This particular function is called **the 2-by-2 determinant**: $\det(u, v)$ It has many uses in Mathematics.

Another example, on this same space, is

$$\mathbf{C}(u, v) = ac + bd.$$

This one is called a **dot or scalar product.**

$\mathbf{B}(u, v)$ and $\mathbf{C}(u, v)$ read different info about the pair of vectors u, v as we shall see.

Another well-known bilinear transformation $\mathbf{F}^3 \times \mathbf{F}^3 \to \mathbf{F}^3$ is the following: For $u = (a, b, c)$, $v = (d, e, f)$,

$$(u, v) \to u \wedge v = (bf - ce, -af + cd, ae - bd)$$

This function is called the **exterior**, or **vector** product of $\mathbf{F}^3$.

When $\mathbf{F} = \mathbb{R}$, it has many useful properties geometric used in Physics [in Mechanics, Electricity, Magnetism]. Partly this arises because

$$u \wedge v \perp u \quad \& \perp v$$

and its magnitude says something about the parallelogram defined by u and v.

There are two main classes of multilinear functions. Say **B** is *n*-linear, that is it has *n* input cells and is linear in each separately: $\mathbf{B}(v_1, \ldots, v_n)$.
B is **symmetric**: If you exchange the contents of two cells

$$\mathbf{B}(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = \mathbf{B}(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n)$$

causes no change. Like the dot product above.

B is **skew-symmetric** or **alternating**: If

$$\mathbf{B}(v_1, \ldots, v_i = v, \ldots, v_j = v, \ldots, v_n) = 0$$

whenever two cells have the same content. Like the determinant above.

Let $\mathbf{M}_n(\mathbf{F})$ be the vector space of all $n \times n$ matrices over the field **F**. Consider the **trace** function on $\mathbf{A} \in \mathbf{M}_n(\mathbf{F})$, $\mathbf{A} = [a_{ij}]$:

$$\mathbf{trace}([a_{ij}]) = \sum_{i=1}^{n} a_{ii}$$

Now define the function

$$\mathbf{T}(\mathbf{A}, \mathbf{B}) = \mathbf{trace}(\mathbf{AB})$$

T is clearly a bilinear function. It is a good exercise (do it) to show that

$$\mathbf{trace}(\mathbf{AB}) = \mathbf{trace}(\mathbf{BA})$$

so **T** is **symmetric**

Here is a variation that will appear later

$$\mathbf{T}(\mathbf{A}, \mathbf{B}) = \textbf{trace}(\mathbf{A}\mathbf{B}^t),$$

where $\mathbf{B}^t$ denotes the **transpose** of **B.**

Question: On the same space $\mathbf{M}_n(\mathbf{F})$, define

$$\mathbf{total}([a_{ij}]) = \sum_{i,j} a_{ij}$$

It is clear that

$$\mathbf{S}(\mathbf{A}, \mathbf{B}) = \mathbf{total}(\mathbf{AB})$$

is a bilinear function.

Is it **symmetric**?

Proposition

If $\mathbf{B}$ *is an alternating multilinear function, then*

$$\mathbf{B}(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -\mathbf{B}(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n),$$

that is, switching two variables changes the sign of the function.

Proof.

For convenience we assume $\mathbf{B}(u, v)$ has two variables. We must show that $\mathbf{B}(v, u) = -\mathbf{B}(u, v)$. By definition, we have

$$\begin{aligned} \mathbf{B}(u+v, u+v) &= 0, \quad \text{which we expand} \\ &= \mathbf{B}(u, u) + \mathbf{B}(u, v) + \mathbf{B}(v, u) + \mathbf{B}(v, v) \end{aligned}$$

Notice that the first and fourth summands are zero. Thus $\mathbf{B}(u, v) + \mathbf{B}(v, u) = 0$, as desired. □

Here are some additional properties.

Proposition

The set **M** *of all n–linear functions on the vector space* **V** *with values in* **W** *is a vector space. The subsets* **S** *and* **K** *of symmetric and alternating functions are subspaces.*

Proof.

If $\mathbf{B}_1$ and $\mathbf{B}_2$ are (say) symmetric bilinear functions,

$$\begin{aligned} (c_1\mathbf{B}_1 + c_2\mathbf{B}_2)(u, v) &= c_1\mathbf{B}_1(u, v) + c_2\mathbf{B}_2(u, v) \\ &= c_1\mathbf{B}_1(v, u) + c_2\mathbf{B}_2(v, u), \end{aligned}$$

which shows that any linear combination of $\mathbf{B}_1$ and $\mathbf{B}_2$ is symmetric. The argument is similar for alternating functions. □

If **B** is bilinear and $2 \neq 0$, we could do as in an early exercise:

$$\mathbf{B}(u, v) = \frac{\mathbf{B}(u, v) + \mathbf{B}(v, u)}{2} + \frac{\mathbf{B}(u, v) - \mathbf{B}(v, u)}{2}$$

that shows that every bilinear function is a [unique] sum of a symmetric and an alternating bilinear function.

It is very easy to create multilinear functions, at least general functions and symmetric ones. Here are a couple of approaches:

- Let $\mathbf{f}_1, \mathbf{f}_2$ and $\mathbf{f}_3$ be linear functions on $\mathbf{V} = \mathbf{F}^3$. Now define

$$\mathbf{T} : \mathbf{V}^3 \to \mathbf{F}, \quad \mathbf{T}(v_1, v_2, v_3) := \mathbf{f}_1(v_1)\mathbf{f}_2(v_2)\mathbf{f}_3(v_3).$$

  $\mathbf{T}$ is clearly trilinear

- Let $\mathbf{T}$ be a trilinear function on $\mathbf{F}^3$. We get a symmetric function $\mathbf{S}$ by 'mixing up' [symmetrizing] $\mathbf{T}$:

$$\begin{aligned}\mathbf{S}(v_1, v_2, v_3) \quad &:= \quad \mathbf{T}(v_1, v_2, v_3) + \mathbf{T}(v_2, v_1, v_3) + \mathbf{T}(v_1, v_3, v_2) \\ &+ \quad \mathbf{T}(v_3, v_1, v_2) + \mathbf{T}(v_2, v_3, v_1) + \mathbf{T}(v_3, v_2, v_1)\end{aligned}$$

  If $\mathbf{T}$ is already symmetric, $\mathbf{S} = 6\mathbf{T}$.

Let us begin to see what makes the **determinant** important:

Proposition

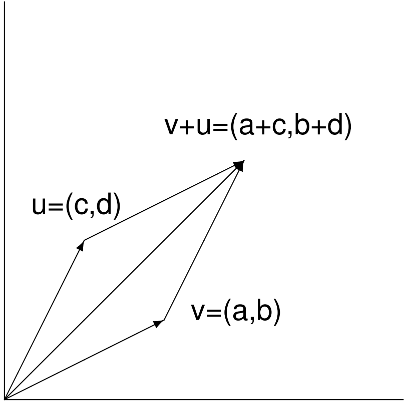
The vector space $\mathbf{K}$ *of all skew-symmetric bilinear functions on* $\mathbf{F}^2$ *with values in* $\mathbf{F}$ *has a basis which is the 2-by-2 determinant function.*

Proof.

1. Let $e_1 = (1, 0)$, $e_2 = (0, 1)$ be the standard basis of $\mathbf{F}^2$.
2. Given any two vectors $u, v \in \mathbf{F}^2$, we can write $u = ae_1 + be_2$, $v = ce_1 + de_2$.
3. If $\mathbf{B} \in \mathbf{K}$, expand $\mathbf{B}(u, v) = \mathbf{B}(ae_1 + be_2, ce_1 + de_2)$:

$$ac\mathbf{B}(e_1, e_1) + ad\mathbf{B}(e_1, e_2) + bc\mathbf{B}(e_2, e_1) + bd\mathbf{B}(e_2, e_2)$$

4. Note that the first and fourth terms are zero and $\mathbf{B}(e_1, e_2) = -\mathbf{B}(e_2, e_1)$. It gives
5. $\mathbf{B}(u, v) = (ad - bc)\mathbf{B}(e_1, e_2) = \mathbf{B}(e_1, e_2)\det(u, v)$



Area of parallelogram defined by u and v is $\det(v, u) = ad - bc$

Exercise 1: Prove that the space of all symmetric bilinear functions of $\mathbf{F}^2$ has dimension 3. Note that the space of linear functions

$$\mathbf{T} : \mathbf{F}^2 \times \mathbf{F}^2 \to \mathbf{F}$$

has dimension 4. [This is the dual space of $\mathbf{F}^2 \times \mathbf{F}^2 = \mathbf{F}^4$]. Since bilinear functions are **linear**, the space of symmetric bilinear functions is a subspace and therefore has dimension at most 4. You must show that it has a basis of 3 functions.

Exercise 2:

If $\mathbf{V}$ is a vector space of dimension n, and $\mathbf{S}$ and $\mathbf{K}$ are the spaces of symmetric and skew-symmetric bilinear functions, prove that

$$\begin{aligned} \dim \mathbf{S} &= \binom{n+1}{2} \\ \dim \mathbf{K} &= \binom{n}{2} \end{aligned}$$

Important Observation

A quick way to get new multilinear functions from old ones is the following:

If $\mathbf{B} : \mathbf{V} \times \mathbf{V} \to \mathbf{W}$ is a bilinear transformation, and $\mathbf{T} : \mathbf{W} \to \mathbf{Z}$ is a linear transformation, the composite

$$\mathbf{T} \circ \mathbf{B} : \mathbf{V} \times \mathbf{V} \to \mathbf{Z}$$

$$\mathbf{T} \circ \mathbf{B}(u, v) = \mathbf{T}(\mathbf{B}(u, v))$$

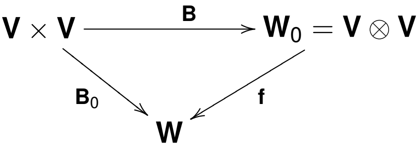
is a bilinear transformation. We want to argue that there is a bilinear map

$$\mathbf{B}_0 : \mathbf{V} \times \mathbf{V} \to \mathbf{W}_0$$

such that for any bilinear map $\mathbf{B} : \mathbf{V} \times \mathbf{V} \to \mathbf{W}$ there is a a unique linear map $\mathbf{f} : \mathbf{W}_0 \to \mathbf{W}$ such that

$$\mathbf{B} = \mathbf{f} \circ \mathbf{B}_0$$

Universal



The most famous bilinear (multi also) is called the **tensor product**,

$$\mathbf{B} : \mathbf{V} \times \mathbf{V} \to \mathbf{V} \otimes \mathbf{V},$$

$$(u, v) \to u \otimes v$$

We will develop this in greater generality.

Outline

Tensor Products of Modules

Definition

Let R be a ring. If A is a right R-module, B a left R-module, and M an abelian group, then an R-bilinear mapping is a function $\mathbf{f} : A \times B \to M$ such that for all $a, a' \in A$, $b, b' \in B$, and $r \in R$

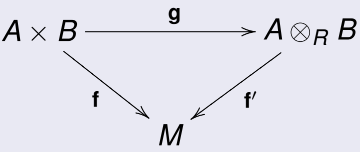
$$\begin{aligned} \mathbf{f}(a + a', b) &= \mathbf{f}(a, b) + \mathbf{f}(a', b) \\ \mathbf{f}(a, b + b') &= \mathbf{f}(a, b) + \mathbf{f}(a, b') \\ \mathbf{f}(ar, b) &= \mathbf{f}(a, rb) \end{aligned}$$

An example is the multiplication in the ring R.

If we follow up a bilinear mapping $\mathbf{f} : A \times B \to C$ with a linear mapping $\mathbf{g} : C \to D$, we get a bilinear mapping $\mathbf{g} \circ \mathbf{f} : A \times B \to D$.

Definition

The tensor product of A and B (as above) is an abelian group $A \otimes_R B$ and a R–bilinear function $\mathbf{g} : A \times B \to A \otimes_R B$ that solves the following universal problem



Universal means that given the bilinear mapping $\mathbf{f}$ there exists a unique additive mapping $\mathbf{f}'$ such that $\mathbf{f} = \mathbf{f}' \circ \mathbf{g}$.

The elements of $A \otimes_R B$ are written $\sum_{i=1}^{n} a_i \otimes b_i$

Examples

- $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x] = \mathbb{C}[x]$
- Let $A = k[x]$ and $B = k[y]$ and consider the bilinear mapping
$$k[x] \times k[y] \to k[x, y]$$
$$(\mathbf{f}(x), \mathbf{g}(y)) \to \mathbf{f}(x)\mathbf{g}(y)$$
It gives rise to a surjection (actually an isomorphism of algebras)
$$k[x] \otimes_k k[y] \to k[x, y]$$
- More generally:
$$k[x_1, \ldots, x_n] \otimes_k k[y_1, \ldots, y_m] = k[x_1, \ldots, x_n, y_1, \ldots, y_m]$$

Existence of Tensor Products

Theorem

The tensor product of a right R-module A and a left R-module B exists.

Proof. Let F be the free abelian group with basis $A \times B$, and let L be the subgroup generated the all $(ar, b) - (a, rb)$ (if R is commutative, we add the relations $r(a, b) - (ra, b)$)

$$(a, b + b') - (a, b) - (a, b'), \quad (a + a', b) - (a, b) - (a', b)$$

Set $A \otimes_R B = F/L$, and denote by $\mathbf{g} : A \times B \to A \otimes_R B$ the natural mapping $\mathbf{g}(a, b) = (a, b) + L$. It is easy to verify that:

1. $\mathbf{g}$ is a bilinear mapping
2. Given a bilinear mapping $\mathbf{h} : A \times B \to M$ it defines a linear mapping $\mathbf{f} : F \to M$. Since $\mathbf{g}$ is a bilinear mapping, $\mathbf{f}$ vanishes on the generators of L, so defines the bilinear mapping $\mathbf{g} : F/L \to M$, and universality is met.

Remark

Proposition

Let $x_i \in A$, $y_i \in B$ be such that $\sum x_i \otimes y_i = 0$ in $A \otimes B$. Then there exist f.g. submodules A_0 of A and B_0 of B, containing x_i and y_i respectively, such that $\sum x_i \otimes y_i = 0$ in $A_0 \otimes B_0$.

Proof. If $\sum x_i \otimes y_i = 0$, in $A \otimes B$, then $\sum (x_i, y_i) \in L$, and therefore $\sum (x_i, y_i)$ is a finite sum of generators of L like

$$(a, b + b') - (a, b) - (a, b'), \quad (a + a', b) - (a, b) - (a', b), \quad r(a, b) -$$

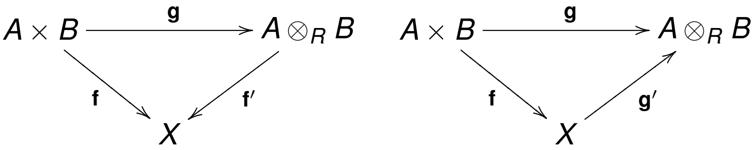
Let A_0 be the submodule of A generated by the x_i and all the first coordinates in these generators of L, and define B_0 similarly. Then $\sum x_i \otimes y_i = 0$ as an element of $A_0 \otimes B_0$.

Uniqueness of tensor products

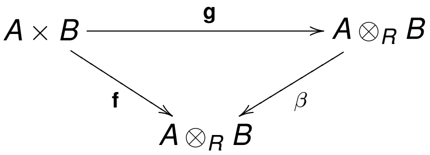
Theorem

Any two tensor products of A and B are isomorphic.

Suppose there is another group X and a map $\mathbf{f} : A \times B \to X$ is a tensor product of A and B. This gives two diagrams



Now set $\phi = \mathbf{f}' \circ \mathbf{g}'$ and consider the diagram



where β works with either $\mathbf{I}$ or ϕ. By the universality, $\mathbf{I} = \phi$.

The Functor $\otimes$

Theorem

Let $\mathbf{f} : A \to A'$ *and* $\mathbf{g} : B \to B'$ *be* R*-maps of right and left* R*-modules, resp. There is a unique homomorphism* $A \otimes_R B \to A' \otimes_R B'$ *with* $a \otimes b \to \mathbf{f}(a) \otimes \mathbf{g}(b)$.

Proof.

The function $A \times B \to A \otimes_R B$ defined by $(a, b) \to \mathbf{f}(a) \otimes \mathbf{g}(b)$ is clearly bilinear. Use universality to finish. □

This map is denoted $\mathbf{f} \otimes \mathbf{g}$: the tensor product of $\mathbf{f}$ and $\mathbf{g}$

Right exactness

Theorem

Let

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

be an exact sequence of left R-modules. Then for any right R-module M, the following sequence of abelian groups is exact [right exact]

$$M \otimes_R A \xrightarrow{\mathbf{I} \otimes \mathbf{f}} M \otimes_R B \xrightarrow{\mathbf{I} \otimes \mathbf{g}} M \otimes_R C \longrightarrow 0.$$

Examples

To make things simpler, we assume that R is a commutative ring. In this case $A \otimes_R B$ acquires also the structure of an R-module by defining $r(a \otimes b) = ra \otimes b$ $(= a \otimes rb)$.

- $R \otimes A \simeq A$
- $A \otimes (B \oplus C) \simeq (A \otimes B) \oplus (A \otimes C)$
- If R is a commutative ring, then $A \otimes B \simeq B \otimes A$
  $\mathbb{Z}/(a) \otimes_R \mathbb{Z}/(b) \simeq \mathbb{Z}/(\mathrm{gcd}(a, b))$
  See next result.

Useful tool

Proposition

If I is an ideal and M an R-module, then $R/I \otimes M \simeq M/IM$.

Proof. Consider the natural SES $0 \to I \to R \to R/I \to 0$. Tensoring with M we obtain the acyclic complex

$$I \otimes M \xrightarrow{\varphi} R \otimes M \to R/I \otimes M \to 0$$

We make use of the isomorphism $R \otimes M \simeq M$ so that the image of φ is the submodule IM of M. By the right exactness, $M/IM \simeq R/I \otimes M$.

Illustrate how to use this to calculate the tensor product $M \otimes N$ of any two f.g. modules over a PID.

Flat Modules

Let $\mathbf{R}$ be a ring and N a left $\mathbf{R}$-module. The functor $\mathbf{T} : M \to M \otimes_{\mathbf{R}} N$ on the category $mod(\mathbf{R})$ is not exact in general. If $\mathbf{T}$ is exact, then N is said to be a flat module.

Proposition

For an $\mathbf{R}$*-module N, TFAE:*

1. *N is flat.*
2. *If* $0 \to M \to M \to M'' \to 0$ *is an exact sequence, the tensored sequence* $0 \to M \otimes N \to M \otimes N \to M'' \otimes N \to 0$ *is an exact is exact.*
3. *If* $f : M' \to M$ *is injective, then* $f \otimes 1 : M' \otimes N \to M \otimes N$ *is injective.*
4. *If* $f : M' \to M$ *is injective and* M', M *are finitely generated, then* $f \otimes 1 : M' \otimes N \to M \otimes N$ *is injective.*

Proof

- (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftarrow$ (4): clear
- (4) $\Leftarrow$ (3): Let $f : M' \to M$ be injective and let $u = \sum x_i \otimes y_i \in \ker(f \otimes 1)$ so that $\sum f(x_i) \otimes y_i = 0$ in $M \otimes N$.
- Let M'_0 be the submodule of M' generated by the x_i and let $u_0 = \sum x_i \otimes y_i \in M'_0 \otimes N$. By the construction of tensor products, there exists a finitely generated submodule M_0 of M containing $f(M'_0)$ and such that $\sum f(x_i) \otimes y_i = 0$ as an element of $M_0 \otimes N$.
- If $f_0 : M'_0 \to M_0$ is the restriction of f, this means $f \otimes 1$ is injective. Since $(f_0 \otimes 1)(u_0) = 0$, this means $u_0 = 0$ and therefore $u = 0$.

Outline

Tensor Power of a Module

Theorem

Given an R-module A, and R-algebra S, and a homomorphim $\mathbf{f} : A \to S$ *there is a unique R-algebra homomorphim* $\mathbf{g} : T(A) \to S$ *such that the restriction of* $\mathbf{g}$ *to* $T_1(A)$ *coincides with* $\mathbf{f}$*.*

Proof.

For each $n \in \mathbb{N}$, there is n-linear mapping

$$(a_1, \ldots, a_n) \to \mathbf{f}(a_1) \cdots \mathbf{f}(a_n) \in S, \quad a_i \in A$$

which we extend to a homomorphism

$$\mathbf{g}_n : T_n(A) = \underbrace{A \otimes \cdots \otimes A}_{n} \to S$$

Functorial Property

Theorem

Let $\mathbf{f} : A \to B$ be a homomorphism of modules over the commutative ring R. Then there is a natural (meaning what?) ring homomorphism $T(\mathbf{f}) : T(A) \to T(B)$ of their tensor algebras.

Proof. It is enough to consider the commutative diagram (explain)

$$\begin{array}{ccc} A & \xrightarrow{\mathbf{f}} & B \\ \downarrow & & \downarrow \\ T(A) & \xrightarrow[T(\mathbf{f})]{} & T(B) \end{array}$$

$$T(\mathbf{f})(a_1 \otimes \cdots \otimes a_n) = \mathbf{f}(a_1) \otimes \cdots \otimes \mathbf{f}(a_n)$$

If **V** is the k-vector space k^n, then

$$T(\mathbf{V}) = k\langle x_1, \ldots, x_n \rangle$$

Its elements are linear combinations with coefficients in k of the words

$$w = y_1 y_2 \cdots y_m$$

where the y_i are symbols from the alphabet $\{x_1, \ldots, x_n\}$.
Multiplication of words is by concatenation.
Note that $T(\mathbf{V})$ is a graded algebra.

Super algebra

- Let $R = k\langle x, y\rangle$. This is a graded algebra, $R = \oplus_{n\geq 0} R_n$.
- Let I be the two-sided ideal generated by the element $xy - yx - 1$. Because this element is not homogeneous, $\mathbf{W} = R/I$ is not a graded algebra.
- However we can organize R as $R = R_{\text{even}} \oplus R_{\text{odd}}$, and these components behave as homogeneous ones, for example $R_{\text{even}} \cdot R_{\text{odd}} \subset R_{\text{odd}}$.
- For this 'grading' of R, $xy - yx - 1$ is even (so homogeneouus). The algebra R/I is the (a) Weyl algebra.
- Discuss why it is remarkable.

Symmetric algebra of a module

- Let R be a commutative ring, A an R-module, S a commutative R-algebra and $\mathbf{f} : A \to S$ a homomorphism of R-modules. According to the preceding theorem, there is a homomorphism of R-algebras

$$\mathbf{g} : T(A) \to S$$

  that extends $\mathbf{f}$ (Recall that $T(A)_1 = A$).
- Since S is commutative,

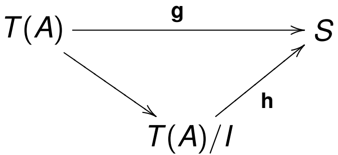
$$\mathbf{g}(a \otimes b) = \mathbf{f}(a)\mathbf{f}(b) = \mathbf{f}(b)\mathbf{f}(a) = \mathbf{g}(b \otimes a)$$

  so all tensors $a \otimes b - b \otimes a$ lie in the kernel of $\mathbf{g}$.

Let I be the two-sided ideal of $T(A)$ generated by all $a \otimes b - b\otimes$, $a, b \in A$. Note that I is a graded $T(A)$-ideal

$$I = I_0(=0) + I_1(=0) + I_2 + I_3 + \cdots + I_n + \cdots$$

$I_n \subset T(A)_n$.



Note that **h** is universally defined.

Definition

The algebra $T(A)/I$ is called the symmetric algebra of A and denoted $S_R(A)$. Since $I = \oplus I_n$,

$$S_R(A) = \bigoplus S_n(A) = \bigoplus T_n(A)/I_n.$$

The component $S_n(A)$ is called the nth symmetric power of A.

Example: Let $\mathbf{V}$ be the k-vector space k^n. Then $S_k(\mathbf{V}) = k[x_1, \ldots, x_n]$.

Functorial Property

Theorem

Let $\mathbf{f} : A \to B$ be a homomorphism of modules over the commutative ring R. Then there is a natural (meaning what?) ring homomorphism $S(\mathbf{f}) : S(A) \to S(B)$ of their symmetric algebras.

Proof. It is enough to consider the commutative diagram (explain)

$$\begin{array}{ccc} A & \xrightarrow{\mathbf{f}} & B \\ \downarrow & & \downarrow \\ S(A) & \xrightarrow[S(\mathbf{f})]{} & S(B) \end{array}$$

$$S(\mathbf{f})(a_1 \cdots a_n) = \mathbf{f}(a_1) \cdots \mathbf{f}(a_n)$$

Exterior algebra of a module

Let A be an R-module and let $T(A)$ be its tensor algebra. Let I be the ideal of $T(A)$ generated by all elements of the form $a \otimes a$.

- I is a homogeneous ideal of $T(A)$: $I_0 = I_1 = 0$, I_2 is the submodule of $A \otimes A$ generated by all $a \otimes a$, $a \in A$.
- $I_3 = T_1 \cdot I_2 + I_2 \cdot T_1$
- $I_n = \sum_{r \leq n-2} T_r \cdot I_2 \cdot T_{n-r-2}$

Definition

Let A be an R-module. The exterior algebra of A is

$$\bigwedge_R(A) = \bigoplus_{n\geq 0} \bigwedge^n(A) = \bigoplus T(A)/I.$$

- $\wedge^0(A) = R$ and $\wedge^1(A) = A$
- $\wedge^n(A)$ is called the nth exterior power of A.
- Its elements are linear combinations of $v_1 \wedge v_2 \cdots \wedge v_n$.

Properties

Proposition

If A generated by n elements, then $\bigwedge^n(A)$ is a cyclic module (possibly O), and $\bigwedge^m(A) = 0$ for $m > n$.

Proof. Suppose $A = (x_1, \ldots, x_n)$. Then any element of A is a linear combination

$$v = \sum_i r_i x_i$$

$$v_1 \wedge v_2 \wedge \cdots \wedge v_m =$$

$$\sum_i r_{1i} x_i \wedge \sum_i r_{2i} \wedge \cdots \wedge \sum_i r_{mi} x_i =$$

$$\sum r_{1i_1} r_{2i_2} \cdots r_{mi_m} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_m}$$

In the expression

$$\sum r_{1i_1} r_{2i_2} \cdots r_{mi_m} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_m}$$

- If $m > n$, at least two of the x_i are equal, so the wedge product is zero.
- If $m = n$ and the x_{i_j} are distinct, the products are all equal to $\pm x_1 \wedge x_2 \wedge \cdots \wedge x_n$. Collecting the signs we have

  $$v_1 \wedge \cdots \wedge v_n = \det(\mathbf{A}) x_1 \wedge \cdots \wedge x_n$$

  where $\mathbf{A}$ is the matrix $\mathbf{A} = [r_{ij}]$.

Functorial Property

Theorem

Let $\mathbf{f} : A \to B$ *be a homomorphism of modules over the commutative ring* R*. Then there is a natural (meaning what?) ring homomorphism* $\bigwedge(\mathbf{f}) : \bigwedge(A) \to \bigwedge(B)$ *of their exterior algebras.*

Proof. It is enough to consider the commutative diagram (explain)

$$\begin{array}{ccc} A & \xrightarrow{\mathbf{f}} & B \\ \downarrow & & \downarrow \\ \bigwedge(A) & \xrightarrow[\bigwedge(\mathbf{f})]{} & \bigwedge(B) \end{array}$$

$$\bigwedge(\mathbf{f})(a_1 \wedge \cdots \wedge a_n) = \mathbf{f}(a_1) \wedge \cdots \wedge \mathbf{f}(a_n)$$

One consequence:

$$\bigwedge(\mathbf{f}\circ\mathbf{g}) = \bigwedge\mathbf{f}\circ\bigwedge\mathbf{g}$$

For example, if $\mathbf{f} : R^n \to R^n$, then $\wedge^n\mathbf{f} = \det\mathbf{f}$.

The formula above asserts

$$\det(\mathbf{f}\circ\mathbf{g}) = \det\mathbf{f}\cdot\det\mathbf{g}$$

Exercise

- Let R be a (commutative) local ring of maximal ideal $\mathfrak{m}$. If A and B are finitely generated R–modules, prove that

  $$\nu(A \otimes_R B) = \nu(A) \cdot \nu(B),$$

  where $\nu(\cdot)$ is the numerical function that gives the minimal number of generators of modules.

Outline

Syzygy Theorems

Let **R** be a ring and *mod*(**R**) the category of **R**-modules. A syzygy theorem is a statement about the projective dimensions of the modules in a subset/subcategory of *mod*(**R**). Each of these has shed light on the structure of **R**.

Here are some versions:

- The supremum of all $\mathrm{proj\ dim}_{\mathbf{R}} M$ for all **R**-modules
- The supremum of all $\mathrm{proj\ dim}_{\mathbf{R}} M$ for all cyclic **R**-modules
- The supremum of all $\mathrm{proj\ dim}_{\mathbf{R}} M$ for all **R**-modules of finite projective dimension
- The supremum of all $\mathrm{proj\ dim}_{\mathbf{R}} M$ for all finitely generated **R**-modules of finite projective dimension

Let us borrow some results from future notes to illustrate properties of these numbers.

McCoy's Theorem

The following result describes how a finite free resolution is anchored on its left end.

Theorem (McCoy Theorem)

Let R be a commutative ring and $\varphi\colon R^m \to R^n$ be a homomorphism of free R–modules. Denote by I the ideal generated by the $m \times m$ minors of a matrix representation of φ. Then φ is injective if and only if $0\colon I = 0$. In particular, if $(R, \mathfrak{m})$ is a local ring, $0 : \mathfrak{m} \neq 0$, and all entries of φ lie in $\mathfrak{m}$, then φ is not injective.

Proof. If $v = (a_1, \ldots, a_m)$ is a nonzero vector in the kernel of φ, by Cramer rule it follows that I is annihilated by a_i for each i.

Proof of McCoy's Theorem

For the converse, denote by $I_t(\varphi)$ the ideal generated by the $t \times t$ minors of φ. We may assume that for some $t \leq m$, $0 \colon I_{t-1}(\varphi) = 0$ and $0 \colon I_t(\varphi) \neq 0$. If $t = 1$, for any annihilator r of $I_1(\varphi)$, we have $\varphi(rR^m) = 0$, so we may take $t \geq 2$.

Consider the system of linear equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= 0 \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nm}x_m &= 0. \end{aligned}$$

Let $0 \neq r \in 0 \colon I_t(\varphi)$; we may assume that r does not annihilate one minor of size $t-1$, say the upper-left minor of size $t-1$.

A nonzero solution can be now obtained: set $x_{t+1} = \cdots = x_m = 0$, and let x_i, for $i \leq t$, be the minor defined by the ith column of the upper-left $(t-1) \times t$ submatrix. Then $r \cdot (x_1, \ldots, x_m)$ solves the first $t-1$ equations by Cramer rule, and the remaining equations because $r \cdot I_t(\varphi) = 0$. □

Example

Let **R** be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated **R**-module of projective dimension 1. We can then arrange a resolution of M,

$$0 \to \mathbf{R}^m \xrightarrow{\varphi} \mathbf{R}^n \longrightarrow M \to 0$$

where n is the minimal number of generators of M, which implies that the entries of a matrix representation of φ lie in $\mathfrak{m}$.

Corollary

If $0 : \mathfrak{m} \neq 0$ $m = 0$*. In particular, there are no finitely generated non-free modules of finite projective dimension.*

A special case is that of local Artinian ring when $\mathfrak{m}$ is nilpotent. Actually, for these rings there is no restriction on the generation type.

Example

Example

Let $R = \mathbb{Z}/(4)$ and $M = R/(2) = \mathbb{Z}/(2)$. The free resolution of M is the infinite complex

$$\cdots R \to \cdots \to R \to R \to M \to 0$$

where all maps $R \to R$ are multiplication by 2.

Example

Let $\mathbf{R}$ be a ring and x a non-nilpotent, non-unit element of $\mathbf{R}$. Let $M = \mathbf{R}_x$ be the ring of fractions. M is not a finitely generated $\mathbf{R}$. It is generated by the fractions $\{1/x^n, n \geq 0\}$. A free resolution of M is given as follows. Let F be a countably generated free $\mathbf{R}$-module on the basis $\{e_n, n \geq 0\}$. Mapping $e_n \to 1/x^n$, the set of elements $\{f_n = xe_{n+1} - e_n, n \geq 0\}$ is a generating set for the module of syzygies [check] and thus M has a free resolution

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

Hilbert Syzygy Theorem

Theorem

If $R = k[x_1, \ldots, x_n]$, then the module $M = R/(x_1, \ldots, x_n)$ has projective dimension n. Moreover, every R-module has projective dimension at most n.

- This result opened the way to lots of mathematics. It became a driver for Homological Algebra and Algebraic Geometry, later to Computational Algebra.
- We make a short study if the subject.

Glodal dimension

Definition

The *global dimension* of the ring R is

$$\text{global dim } R = d(R) = \max\{ \text{ proj dim}_R M, \ \text{ for all } R\text{–modules}\}.$$

- $d(\mathbb{Z}) = 1$, $d(k) = 0$, for k a field.
- If $d(R)$ is finite, we say that R is *regular*. As a measure of size, $d(R)$ is too strict. For most rings, $d(R) = \infty$ simply because some module has infinite projective dimension. For this reason, it is often necessary to consider in the definition above only those modules with finite projective resolutions.

Hilbert Syzygy Theorem

Theorem

Let $R[x]$ denote the ring of polynomials in one indeterminate over R. Then

$$\boxed{d(R[x]) = d(R) + 1.} \tag{1}$$

In particular, for a field k, the ring of polynomials $k[x_1, \ldots, x_n]$ has global dimension n, while the ring $\mathbb{Z}[x_1, \ldots, x_n]$ has global dimension $n + 1$.

Some Properties of Modules of Finite Projective Dimension

Proposition

Given a short exact sequence of **R**-*modules*

$$0 \to A \to B \to C \to 0,$$

there is an exact sequence of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F} & \longrightarrow & \mathbb{G} & \longrightarrow & \mathbb{H} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

such that $\mathbb{F} \to A$, $\mathbb{G} \to B$ *and* $\mathbb{H} \to C$ *are projective resolutions.*

Proof

The construction starts by choosing projective presentations of A and C

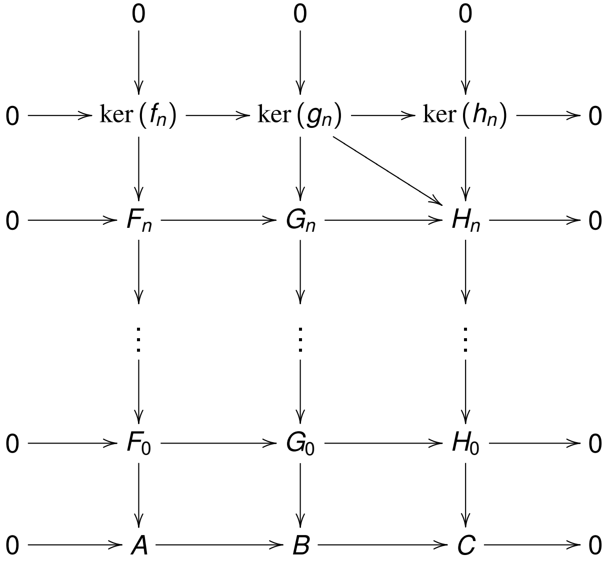
$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_0 & \longrightarrow & G_0 = F_0 \oplus H_0 & \longrightarrow & H_0 & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle f_0} & & & & \Big\downarrow{\scriptstyle h_0} & & \\ 0 & \longrightarrow & A & \xrightarrow[\varphi]{} & B & \xrightarrow[\psi]{} & C & \longrightarrow & 0 \end{array}$$

Since H_0 is projective and ψ is surjective, there is $h'_0 : H_0 \to B$ such that $h'_0\psi = h_0$.

Now define $g_0 : F_0 \oplus H_0 \to B$ by $g_0(x, y) = f_0(x) + h'_0(y)$. The resulting diagram is commutative.

By the snake lemma, we have a SES to restart the construction

$$0 \to \ker(f_0) \to \ker(g_0) \to \ker(h_0) \to 0.$$


0 0 0
0 ker (f_n) ker (g_n) ker (h_n) 0
0 F_n G_n H_n 0
0 F_0 G_0 H_0 0
0 A B C 0

SES

Corollary

Given a short exact sequence of **R***-modules*

$$0 \to A \to B \to C \to 0,$$

if two of the modules have finite projective dimensions, so will the third. More precisely,

$$\begin{aligned} \text{proj. dim. } B &\leq \max\{\text{proj. dim. } A, \text{proj. dim. } C\} \\ \text{proj. dim. } A &\leq \max\{\text{proj. dim. } B, \text{proj. dim. } C - 1\} \\ \text{proj. dim. } C &\leq \max\{\text{proj. dim. } A + 1, \text{proj. dim. } B\} \end{aligned}$$

Proof of HST

We begin with a useful observation. For a given $R[x]$–module M consider the sequence

$$0 \longrightarrow R[x] \otimes_R M \xrightarrow{\psi} R[x] \otimes_R M \xrightarrow{\varphi} M \longrightarrow 0,$$

where

$$\begin{aligned} \psi(x^n \otimes e) &= x^n \otimes xe - x^{n+1} \otimes e, \\ \varphi(x^n \otimes e) &= x^n \cdot e. \end{aligned}$$

It is a straightforward verification that this sequence of $R[x]$–modules and homomorphisms is exact.

- Let M be an R–module and let

$$0 \to P_r \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \to 0$$

  be a projective resolution. Since $R[x]$ is R-free, tensoring–**Explain**–the complex with $R[x]$ yields an $R[x]$–projective resolution of $R[x] \otimes_R M$, and $\mathrm{proj\ dim}_{R[x]}\,(R[x] \otimes_R M) \leq \mathrm{proj\ dim}_R\, M$.
- Suppose now that M is an $R[x]$–module, view it as an R–module and use it in the sequence: by elementary considerations we obtain,

$$\mathrm{proj\ dim}_{R[x]}\, M \leq 1 + \mathrm{proj\ dim}_{R[x]}\,(R[x] \otimes_R M) \leq 1 + \mathrm{proj\ dim}_R\, M,$$

  which shows that

$$d(R[x]) \leq d(R) + 1.$$

- For the reverse inequality, we argue as follows. Any R–module M can be made into an $R[x]$–module by defining $f(x)e = f(0)e$, for $e \in M$. With this structure, we claim that

$$\mathrm{proj}\ \mathrm{dim}_{R[x]} M = \mathrm{proj}\ \mathrm{dim}_R M + 1.$$

- From the observation above, we already have that the left hand side cannot exceed the right hand side of the expression. To prove equality, we use induction on $n = \mathrm{proj}\ \mathrm{dim}_R M$.

- If $n = 0$, that is, if M is R–projective, then M cannot be $R[x]$–projective, since it is annihilated by x, which is a regular element of $R[x]$.
- If $n > 0$, map a free R–module F onto M,

$$0 \to K \longrightarrow F \longrightarrow M \to 0,$$

$\operatorname{proj\,dim}_R K = n - 1$ and by induction $\operatorname{proj\,dim}_{R[x]} K = n$. Since $\operatorname{proj\,dim}_{R[x]} F = 1$, by the preceding case, $\operatorname{proj\,dim}_{R[x]} M = n + 1$, unless, possibly, $n = 1$.

To deal with this last case, map a free $R[x]$–module G over M with kernel L. The assumption to be contradicted is that L is $R[x]$–projective. Since $xM = 0$, $xG \subset L$, and the exact sequence

$$0 \to L/xG \to G/xG \longrightarrow M \to 0$$

says that L/xG is R-projective. But we also have the exact sequence

$$0 \to xG/xL \longrightarrow L/xL \longrightarrow L/xG \to 0,$$

and therefore xG/xL is R–projective. Since $xG/xL \simeq G/L \simeq M$, we get the desired contradiction.

Exercises

- Prove that any ideal I of a Dedekind domain can be generated by 1.5 elements, that is $I = (a, b)$, with a being any nonzero element.
- Let R be a commutative ring. If $\mathbf{f} : R^n \to R^m$ is an isomorphism of R-modules, prove that $m = n$.
- Let $I = (x, y)$ be an invertible ideal of the integral domain R. Prove that I^2 can be generated by x^2 and y^2 (i.e. no need to use xy). Can you generalize (any invertible ideal and any power)?

- Let R be a commutative ring and let $f(x)$ and $g(x)$ be nonzero polynomials (elements of $R[x]$) such that $f(x)g(x) = 0$. Prove that there is a nonzero element $r \in R$ such that $rf(x) = 0$.
- Show that $\mathbb{Q}[x]$ and $\mathbb{Q}[x, y]$ are isomorphic as abelian groups but not as rings.
- Let R be a commutative ring and assume the ideal I is contained in the set theoretic union of 3 prime ideals

$$I \subset P \cup Q \cup M.$$

Show that I must be contained in one of them.

Outline

Chain Complexes

Let R be a ring. A chain complex of R-modules is a sequence of R-modules E_i and module homomorphisms $f_i : E_i \to E_{i+1}$ $\mathcal{E} = \{E_i, f_i\}$, with $f_{i+1} \circ f_i = 0$:

$$\cdots \longrightarrow E_{i+1} \xrightarrow{f_{i+1}} E_i \xrightarrow{f_i} E_{i-1} \xrightarrow{f_{i-1}} \cdots$$

- The submodule $Z_i(\mathcal{E}) = \ker(f_i)$ is the module of i-cycles;
- The submodule $B_i(\mathcal{E}) = f_{i+1}(E_{i+1})$ is the module of i-boundaries;
- The module $H_i(\mathcal{E}) = Z_i(\mathcal{E})/B_i(\mathcal{E})$ is the i^{th} homology module of $\mathcal{E}$. If $H_i(\mathcal{E}) = 0 \; \forall i$, the chain complex is said to be exact.

Hilbert-Burch complex

Many complexes of free modules are associated to matrices $\mathbf{A}$ with entries in a ring R. Let us discuss one that goes back to Hilbert.

Let R be an integral domain [think a polynomial ring] and let $\mathbf{A}$ be an $(n-1) \times n$ matrix with entries in R [for convenience we make $n = 3$]:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix}$$

Let Δ_1, Δ_2 and Δ_3 be the minors (with signs) of the columns. For instance, $\Delta_1 = a_{12}a_{23} - a_{13}a_{22}$.

$$\det \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} = a_{11}\Delta_1 + a_{12}\Delta_2 + a_{12}\Delta_3 = 0$$

Thus the row vectors of **A** are syzygies of $(\Delta_1, \Delta_2, \Delta_3)$.
Let **B** be the column matrix of the Δ's.
With the matrices **A** and **B** [note that $\mathbf{BA} = 0$], we form the complex:

$$0 \to R^2 \xrightarrow{\mathbf{A}} R^3 \xrightarrow{\mathbf{B}} R \longrightarrow R/(\Delta_1, \Delta_2, \Delta_3) \to 0$$

Theorem

If R is a UFD this complex is exact iff $\gcd(\Delta_1, \Delta_2, \Delta_3) = 1$.

Co-Chain Complexes/Shifts

Chain Maps

Let $\mathcal{E} = \{E_i, \partial_i\}$ and $\mathcal{F} = \{F_i, \partial'\}$ be chain complexes. A chain mapping

$$\mathbf{f} : \mathcal{E} \longrightarrow \mathcal{F}$$

is collection $\mathbf{f} = \{f_i\}$ of module homomorphisms such that the diagrams

$$\begin{array}{ccc} E_{i+1} & \xrightarrow{\partial_i} & E_i \\ \downarrow{\scriptstyle f_{i+1}} & & \downarrow{\scriptstyle f_i} \\ F_{i+1} & \xrightarrow[\partial'_i]{} & F_i \end{array}$$

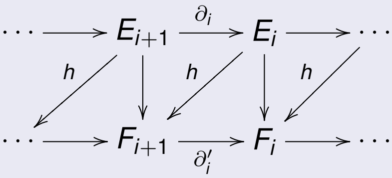
commute. That is

$$\partial'_i \circ f_{i+1} = f_i \circ \partial_i, \quad \forall i$$

Homotopy equivalent chain maps

Definition

Two chain maps $\mathbf{f}, \mathbf{g} : \mathcal{E} \to \mathcal{F}$ are homotopy equivalent if there is a mapping $\mathbf{h} = (h_i) : \mathcal{E} \to \mathcal{F}$



such that

$$\mathbf{f} - \mathbf{g} = \partial' \mathbf{h} + \mathbf{h} \partial.$$

Proposition

If two chain maps $\mathbf{f}, \mathbf{g} : \mathcal{E} \to \mathcal{F}$ *are homotopy equivalent, they induce the same map in homology*

$$H(\mathbf{f}) = H(\mathbf{g}) : H_*(\mathcal{E}) \to H_*(\mathcal{E}).$$

Proof.

ETS that the chain map $\mathbf{f} - \mathbf{g}$ induces the zero mapping in homology. We can replace $\mathbf{f}$ by $\mathbf{f} - \mathbf{g}$ and $\mathbf{g}$ by the zero chain mapping.

Let $\mathbf{h}$ be a homotopy equivalence between $\mathbf{f}$ and 0. Let x be a cycle of $\mathcal{E}$; we argue that $\mathbf{f}(x)$ is a boundary of $\mathcal{F}$:

$$\mathbf{f}(x) = \partial'(h(x)) + h(\partial(x)) = \partial'(h(x)).$$

□

Proposition

Let $\mathcal{F}$ and $\mathcal{G}$ be two complexes

$$\cdots \longrightarrow F_i \xrightarrow{\varphi_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0$$

$$\cdots \longrightarrow G_i \xrightarrow{\psi_i} G_{i-1} \longrightarrow \cdots \longrightarrow G_1 \xrightarrow{\psi_1} G_0$$

and let $M = \operatorname{coker} \varphi_1 = H_0(\mathcal{F})$ and $N = \operatorname{coker} \psi_1 = H_0(\mathcal{G})$. If the modules F_i are projective and $\mathcal{G}$ is acyclic, then any map $\beta : M \to N$ is the map induced be a chain map $\alpha : \mathcal{F} \to \mathcal{G}$, and α is determined by β up to homotopy.

Proof

$$\begin{array}{ccccc} F_1 & \xrightarrow{\varphi_1} & F_0 & \xrightarrow{\varphi_0} & M \\ & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \beta} \\ G_1 & \xrightarrow{\psi_1} & G_0 & \xrightarrow{\psi_0} & N \end{array}$$

- The existence and homotopy uniqueness of α are proved by induction.
- The existence of α: Since G_0 maps onto N, the composite $F_0 \to M \to N$ may be lifted to a map $\alpha_0 : F_0 \to G_0$.
- Note that $\alpha_0\varphi_1$ maps F_1 to $\ker \psi_0 : G_0 \to N$, so $\alpha_0\varphi_1$ has a lifting $\alpha_1 : F_1 \to G_1$. Continue to get the full chain map α

- Homotopy uniqueness: If α and α' are two lifts, it is enough to show that the trivial lifting $\alpha - \alpha'$ of 0 is homotopically trivial. We change notation, assume $\beta = 0$.
- We claim that $\alpha_i = h_{i-1}\varphi_i + \psi_{i+1}h_i$ for maps $h_i : F_i \to G_{i+1}$. Since α_0 induces 0: $\operatorname{coker}\varphi_1 \to \operatorname{coker}\psi_1$, it takes F_0 into image ψ_1.
- Thus there is a lifting $h_0 : F_0 \to G_1$ such that $\psi_1 h_0 = \alpha_0$. Now

  $$\psi_1(h_0\varphi_1 - \alpha_1) = \alpha_0\varphi_1 - \psi_1\alpha_1 = 0$$

  so $h_0\varphi_1 - \alpha_1$ maps into $\ker\psi_1 = \operatorname{im}\psi_2$. Since F_1 is projective, we can lift this to a map $h_1 : F_1 \to G_2$. And so on...

Properties of chain maps

Here are some observations:

- $f_i(Z_i(\mathcal{E})) \subset Z_i(\mathcal{F})$
- $f_i(B_i(\mathcal{E})) \subset B_i(\mathcal{F})$
- Consequently **f** defines a sequence

$$H(f_i) : H_i(\mathcal{E}) \longrightarrow H_i(\mathcal{F})$$

This construction is functorial (Explain).

Exact Sequence of Chain Complexes

Consider the diagram where the columns are chain complexes and the rows are short exact sequences and the squares are commutative:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A_{i+1} & \xrightarrow{f_{i+1}} & B_{i+1} & \xrightarrow{g_{i+1}} & C_{i+1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_{i+1}} & & \downarrow{\scriptstyle \partial'_{i+1}} & & \downarrow{\scriptstyle \partial''_{i+1}} & & \\
0 & \longrightarrow & A_i & \xrightarrow{f_i} & B_i & \xrightarrow{g_i} & C_i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_i} & & \downarrow{\scriptstyle \partial'_i} & & \downarrow{\scriptstyle \partial''_i} & & \\
0 & \longrightarrow & A_{i-1} & \xrightarrow{f_{i-1}} & B_{i-1} & \xrightarrow{g_{i-1}} & C_{i-1} & \longrightarrow & 0
\end{array}
$$

We are going to make some observations. We already know that there are collections of maps

$$H_*(\mathcal{A}) \longrightarrow H_*(\mathcal{B}) \longrightarrow H_*(\mathcal{C})$$

Connecting Homomorphism

We are going to extract from this diagram, a sequence of homomorphisms

$$\mathbf{h}_i : H_i(\mathcal{C}) \to H_{i-1}(\mathcal{A})$$

called the connecting homomorphism.

- Let z be a cycle in C_i, $\partial''(z) = 0$. Since g_i is surjective, there is $b \in B_i$ with $g_i(b) = z$.
- The commutativity of the squares implies that $0 = \partial''(z) = \partial''(g_i(b)) = g_{i-1}(\partial'(b))$.
- Thus $\partial'(b) = f_{i-1}(a)$ for some $a \in A_{i-1}$.
- To sum: For $i \geq 1$ $\mathbf{h}_i : H_i(\mathcal{C}) \to H_{i-1}(\mathcal{A})$

Homology Exact Sequence

Theorem

Let

$$0 \longrightarrow \mathcal{E} \xrightarrow{\mathbf{f}} \mathcal{F} \xrightarrow{\mathbf{g}} \mathcal{G} \longrightarrow 0$$

be a short exact sequence of chain complexes and chain mappings. Then there is an exact sequence

$$H_i(\mathcal{E}) \stackrel{H_i(\mathbf{f})}{\rightarrow} H_i(\mathcal{F}) \stackrel{H_i(\mathbf{g})}{\rightarrow} H_i(\mathcal{G}) \stackrel{\mathbf{h}_i}{\rightarrow} H_{i-1}(\mathcal{E}) \stackrel{H_{i-1}(\mathbf{f})}{\rightarrow} H_{i-1}(\mathcal{F}) \stackrel{H_{i-1}(\mathbf{g})}{\rightarrow} H_{i-1}(\mathcal{G})$$

where the $\mathbf{h}_i$ *are the connecting homomorphisms.*

Example: Class discussion

Proposition

Consider the commutative diagram with exact rows

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

There is an exact sequence

$$0 \to \ker(f) \to \ker(g) \to \ker(h) \to \operatorname{coker}(f) \to \operatorname{coker}(g) \to \operatorname{coker}(h) \to 0.$$

Exercise

Exercise

Let $A \xrightarrow{f} B \xrightarrow{g} C$ be module homomorphisms. Show that there is an exact sequence

$$0 \to \ker(f) \to \ker(gf) \to \ker(g) \to \operatorname{coker}(f) \to \operatorname{coker}(gf) \to \operatorname{coker}(g) \to 0.$$

Outline

Derived Functors

We are going to define the derived functors of $\otimes$ and Hom.

Let M be an **R**-module. Given a short exact sequence of **R**-modules,

$$0 \to A \to B \to C \to 0,$$

tensoring with M, or applying $\mathrm{Hom}_{\mathbf{R}}(M, \cdot)$, gives rise to complexes

$$A \otimes M \to B \otimes M \to C \otimes M \to 0,$$

$$0 \to \mathrm{Hom}(M, A) \to \mathrm{Hom}(M, B) \to \mathrm{Hom}(M, C),$$

which we seek to extend.

Derived Functors

Proposition

Given a short exact sequence of **R***-modules*

$$0 \to A \to B \to C \to 0,$$

there is an exact sequence of complexes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{F} & \longrightarrow & \mathbb{G} & \longrightarrow & \mathbb{H} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

such that $\mathbb{F} \to A$*,* $\mathbb{G} \to B$ *and* $\mathbb{H} \to C$ *are projective resolutions.*

Derived Functors

The construction starts by choosing projective presentations of A and C

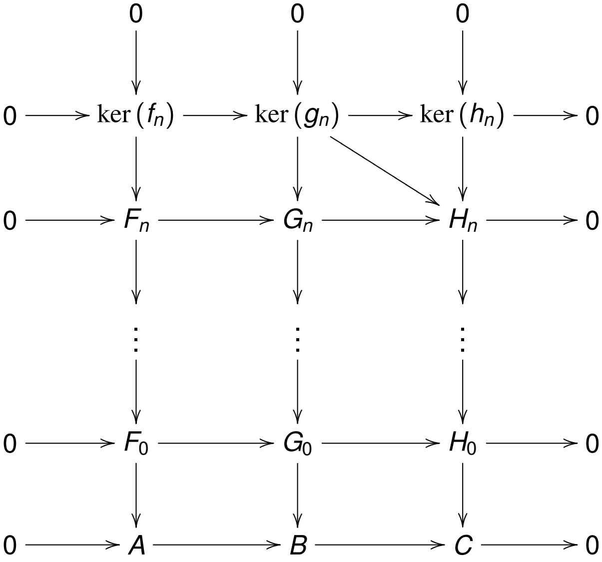
$$\begin{array}{ccccccccc}
0 & \longrightarrow & F_0 & \longrightarrow & G_0 = F_0 \oplus H_0 & \longrightarrow & H_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_0} & & & & \downarrow{\scriptstyle h_0} & & \\
0 & \longrightarrow & A & \xrightarrow[\varphi]{} & B & \xrightarrow[\psi]{} & C & \longrightarrow & 0
\end{array}$$

Since H_0 is projective and ψ is surjective, there is $h_0' : H_0 \to B$ such that $h_0'\psi = h_0$.

Now define $g_0 : F_0 \oplus H_0 \to B$ by $g_0(x, y) = f_0(x) + h_0'(y)$. The resulting diagram is commutative.

By the snake lemma, we have a SES to restart the construction

$$0 \to \ker(f_0) \to \ker(g_0) \to \ker(h_0) \to 0.$$


0 0 0
0 ker (f_n) ker (g_n) ker (h_n) 0
0 F_n G_n H_n 0
0 F_0 G_0 H_0 0
0 A B C 0

Derived Functors

Corollary

Given a short exact sequence of $\mathbf{R}$*-modules*

$$0 \to A \to B \to C \to 0,$$

if two of the modules have finite projective dimensions, so will the third. More precisely,

$$\begin{aligned}
\text{proj. dim. } B &\leq \max\{\text{proj. dim. } A, \text{proj. dim. } C\} \\
\text{proj. dim. } A &\leq \max\{\text{proj. dim. } B, \text{proj. dim. } C - 1\} \\
\text{proj. dim. } C &\leq \max\{\text{proj. dim. } A + 1, \text{proj. dim. } B\}
\end{aligned}$$

Derived Functors

Definition of Left-Derived Functors

Definition

Suppose F is a right–exact functor on the category of R–modules. If A is an R–module, let

$$P : \cdots \longrightarrow P_i \xrightarrow{\varphi_i} P_{i-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\varphi_1} P_0$$

be a projective resolution of A, and define the *ith left–derived functor* of F to be $L_iF(A) = H_iFP$, where FP is the complex

$$FP : \cdots \longrightarrow FP_i \xrightarrow{F\varphi_i} FP_{i-1} \longrightarrow \cdots \longrightarrow FP_1 \xrightarrow{F\varphi_1} FP_0,$$

the result of applying F to P.

Properties of Derived Functors

Proposition

The left–derived functors of F are independent of the choice of resolution and have the following properties :

(a) $L_0 F = F$.

(b) *If A is a projective module, then $L_i F(A) = 0$ for all $i > 0$.*

(c) *For every short exact sequence*

$$0 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C \longrightarrow 0,$$

there is a long exact sequence as shown:

Long homology sequence of left-derived functors

$$\cdots \to L_{i+1}FC \to L_iFA \to L_iFB \to L_iFC \to \cdots$$

$$\cdots \to L_1FC \to L_0FA \to L_0FB \to L_0FC \to 0$$

Proposition

(d) *The connecting homomorphisms δ_i in the long exact sequence are natural : That is if*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

is a commutative diagram with exact rows, then the diagrams

$$\begin{array}{ccc} L_{i+1}FC & \xrightarrow{\delta_{i+1}} & L_iFA \\ {\scriptstyle L_{i+1}F\gamma}\downarrow & & \downarrow{\scriptstyle L_iF\alpha} \\ L_{i+1}FC' & \xrightarrow[\delta_i]{} & L_iFA' \end{array}$$

(a) To show that $L_0 FA = F(A)$, just use the right–exactness of F: From the definition

$$L_0 FA = H_0(\cdots \to FP_1 \to FP_0),$$

we get $L_0 FA = \mathrm{coker}\,(FP_1 \to FP_0) = FA$.

(b) This is immediate from the independence of resolution, since if A is projective then we may take as projective resolution the complex

$$\cdots 0 \to 0 \to A.$$

(c) This is immediate from the construction of projective resolutions for SES and the long homology sequence.

(d) Form the projective resolutions of each of the two short exact sequences as seen. The maps α, β, and γ lift to comparison maps betwen these resolutions. If we use these maps of resolutions to define the maps $L_iF(\alpha)$ and $L_iF(\beta)$, then the verification of the commutativity of the diagram in part (d) is easy. $\square$

Definition of Right-Derived Functors

If F is a left-exact functor, we define the right-derived functors R^iF of F: If A is a module, we let

$$Q: \quad Q_0 \to Q_{-1} \to \cdots$$

be an injective resolution of A, and set

$$R^iF(A) = H_{-i}(FQ),$$

where FQ is the complex

$$FQ: \quad 0 \to FQ_0 \to FQ_{-1} \to \cdots .$$

Tor

Definition

Let M be an $\mathbf{R}$-module. The left-derived functors of the functor $F(\cdot) = M \otimes_{\mathbf{R}} (\cdot)$ are denoted

$$L_i F(A) = \mathrm{Tor}_i^{\mathbf{R}}(M, A).$$

Ext

Definition

Let M be an $\mathbf{R}$-module. The right-derived functors of the functor $F(\cdot) = \mathrm{Hom}_{\mathbf{R}}(M, \cdot)$ are denoted

$$R^i F(A) = \mathrm{Ext}^i{}_{\mathbf{R}}(M, A).$$

There are also derived functors for the contravariant functor $\mathrm{Hom}_{\mathbf{R}}(\cdot, N)$. They are denoted by $\mathrm{Ext}^i{}_{\mathbf{R}}(A, N)$.
The red Ext and the black Ext are naturally isomorphic:

Theorem

If M and N are $\mathbf{R}$-modules, there is a canonical isomorphism

$$\mathrm{Ext}^i{}_{\mathbf{R}}(M, N) \simeq \mathrm{Ext}^i{}_{\mathbf{R}}(M, N).$$

Outline

Finiteness

Theorem

If $\mathbf{R}$ *is a Noetherian ring and* M, N *are finitely generated* $\mathbf{R}$*-modules, then for all* i*,* $\mathrm{Ext}^i_{\mathbf{R}}(M, N)$ *and* $\mathrm{Tor}_i^{\mathbf{R}}(M, N)$ *are finitely generated* $\mathbf{R}$*-modules.*

Proof. Let $\mathbb{P} = \{P_n\} \to M$ be a projective resolution of M using f.g. projective modules [use Noetherianess]. The homology modules of the complexes of f.g. modules

$$\begin{aligned} \mathbb{P} \otimes N &= \{P_n \otimes N\} \\ \mathrm{Hom}(\mathbb{P}, N) &= \{\mathrm{Hom}(P_n, N)\} \end{aligned}$$

are finitely generated.

Vanishing

Theorem

Let $\mathbf{R}$ *be a Noetherian ring.*

1. *A f.g.* $\mathbf{R}$*-module* M *has projective dimension* $\leq r$ *iff* $\mathrm{Tor}^{\mathbf{R}}_{r+1}(M, N) = 0$ *for all f.g. generated [or cyclic]* $\mathbf{R}$*-modules* N*.*
2. *Moreover, if* $(\mathbf{R}, \mathfrak{m})$ *is a local ring, it sufices that* $\mathrm{Tor}^{\mathbf{R}}_{r+1}(M, \mathbf{R}/\mathfrak{m}) = 0$*.*
3. *An* $\mathbf{R}$*-module* M *has projective dimension* $\leq r$ *iff* $\mathrm{Ext}^{r+1}_{\mathbf{R}}(M, N) = 0$ *for all* $\mathbf{R}$*-modules* N*. If* M *is f.g. it suffices to take* N *f.g., and if* $\mathbf{R}$ *is a local ring it suffices to take* $N = \mathbf{R}/\mathfrak{m}$*.*
4. *An* $\mathbf{R}$*-module* N *has injective dimension* $\leq r$ *iff* $\mathrm{Ext}^{r+1}_{\mathbf{R}}(M, N) = 0$ *for all cyclic* $\mathbf{R}$*-modules* M*.*

Let us prove that $\mathrm{Tor}_{r+1}(\mathbf{R}/\mathfrak{m}, M) = 0$ implies $\mathrm{proj\ dim}\, M \leq r$:

- A minimal presentation of M is a SES $0 \to K \to \mathbf{R}^m \to M \to 0$, where $K \subset \mathfrak{m}\mathbf{R}^m$. Use Nakayama lemma to get it: $m = \dim M/\mathfrak{m}M$.
- A minimal free resolution of M is a projective resolution $\mathbb{F}$

$$\cdots \to F_n \xrightarrow{f_n} F_{n-1} \to \cdots \to F_0 \to M \to 0$$

where all entries of matrix f_n lie in $\mathfrak{m}$.

- Tensoring $\mathbb{F}$ with $\mathbf{R}/\mathfrak{m}$ gives a complex where all maps are trivial, so $\mathrm{Tor}_n(\mathbf{R}/\mathfrak{m}, M) = F_n \otimes \mathbf{R}/m$.

Finiteness

Theorem

Let $\mathbf{R}$ *be a Noetherian local ring and* M *a finitely generated* $\mathbf{R}$*-module. If* $x \in \mathfrak{m}$ *is* M*-regular, then*

$$\text{proj dim } M/xM = 1 + \text{proj. dim } M.$$

Proof. Consider the exact sequence $0 \to M \xrightarrow{x} M \to M/xM \to 0$. For a finitely generated $\mathbf{R}$-module N, we write the long homology exact sequence of $\mathrm{Hom}(\cdot, N)$:

$$\mathrm{Ext}^r_{\mathbf{R}}(M/xM, N) \to \mathrm{Ext}^r_{\mathbf{R}}(M, N) \xrightarrow{x} \mathrm{Ext}^r_{\mathbf{R}}(M, N) \to \mathrm{Ext}^{r+1}_{\mathbf{R}}(M/xM, N) \to \mathrm{Ext}^{r+1}_{\mathbf{R}}($$

If $\text{proj dim } M = r$, $\mathrm{Ext}^{r+1}_{\mathbf{R}}(M, N) = 0$ for all N but $\mathrm{Ext}^r_{\mathbf{R}}(M, N) \neq 0$ for some f.g. module N.

The exact sequence above implies that there is an embedding

$$\mathrm{Ext}^r_{\mathbf{R}}(M, N)/x\mathrm{Ext}^r_{\mathbf{R}}(M, N) \hookrightarrow \mathrm{Ext}^{r+1}_{\mathbf{R}}(M/xM, N).$$

By Nakayama Lemma the submodule cannot be zero, and thus $\mathrm{Ext}^{r+1}_{\mathbf{R}}(M/xM, N) \neq 0$.

The rest of the proof is clear.

Finiteness

The situation is distinct for the injective dimension:

Theorem

Let **R** *be a Noetherian local ring and* M *a finitely generated* **R***-module. If* $x \in \mathfrak{m}$ *is* M*-regular, then*

$$\text{inj dim } M/xM = \text{inj. dim } M.$$

Proof. Consider the exact sequence $0 \to M \xrightarrow{x} M \to M/xM \to 0$. For a finitely generated **R**-module N, we write the long homology exact sequence of $\text{Hom}(N, \cdot)$:

$$\text{Ext}^r_{\mathbf{R}}(N, M) \xrightarrow{x} \text{Ext}^r_{\mathbf{R}}(N, M) \to \text{Ext}^r_{\mathbf{R}}(N, M/xM) \to \text{Ext}^{r+1}_{\mathbf{R}}(N, M)$$

If $\text{inj dim } M = r$, $\text{Ext}^{r+1}_{\mathbf{R}}(N, M) = 0$ for all N but $\text{Ext}^r_{\mathbf{R}}(M, N) \neq 0$ for some f.g. module N.

The exact sequence above implies that there is an embedding $\mathrm{Ext}^r_{\mathbf{R}}(M, N)/x\mathrm{Ext}^r_{\mathbf{R}}(M, N) \hookrightarrow \mathrm{Ext}^r_{\mathbf{R}}(M/xM, N)$. By Nakayama Lemma the submodule cannot be zero, and thus
$\mathrm{Ext}^{r+1}_{\mathbf{R}}(M/xM, N) \neq 0$.
The rest of the proof is clear.

Achtung: This suggests that all nonzero f.g. modules of finite injective dimnsion have the same injective dimension...

Ext and Depth

Definition

Let M be a finitely generated module and I a proper ideal such that $M/IM \neq 0$ [automatic if $\mathbf{R}$ is a local ring]. The I-depth of M is the length of the longest M-regular sequence contained in I

Proposition

Let M be a finitely generated module and I a proper ideal such that $M/IM \neq 0$ [automatic if $\mathbf{R}$ is a local ring]. Then

$$I\text{-depth of } M = \inf\{i : \mathrm{Ext}^i_{\mathbf{R}}(\mathbf{R}/I, M) \neq 0.\}$$

Ext and Depth: Proof

- If I consists of zero divisors of M, I is contained in one element in $\mathrm{Ass}\,(M)$, say $\mathfrak{p}$. As $\mathbf{R}/\mathfrak{p} \hookrightarrow M$, and there is a surjection $\mathbf{R}/I \to \mathbf{R}/\mathfrak{p}$. there is a nonzero homomorphism

$$\mathbf{R}/I \to \mathbf{R}/\mathfrak{p} \to M$$

  that is, $\mathrm{Hom}_{\mathbf{R}}(\mathbf{R}/I, M) \neq 0$.
- Conversely, the non-vanishing of this module of homomorphisms implies that $Im = 0$ for some $0 \neq m \in M$.
- Suppose $x \in I$ is M-regular. We apply the functor $\mathrm{Hom}(R/I, \cdot)$ to the SES

$$0 \to M \xrightarrow{x} M \to \overline{M} = M/xM \to 0$$

- First observe that multiplication by x defines the null mapping on all $\mathrm{Ext}^i(\mathbf{R}/I, \cdot)$.
- The homology sequence of derived functors gives SES of the type

$$0 \to \mathrm{Hom}(\mathbf{R}/I, M) \to \mathrm{Hom}(\mathbf{R}/I, \overline{M}) \to \mathrm{Ext}^1(\mathbf{R}/I, M) \to 0$$

$$0 \to \mathrm{Ext}^1(\mathbf{R}/I, M) \to \mathrm{Ext}^1(\mathbf{R}/I, \overline{M}) \to \mathrm{Ext}^2(\mathbf{R}/I, M) \to 0$$

- The assertion follows by induction.

Important Properties

Corollary

If $x \in I$ is M-regular, then

$$I\text{-depth of } M = 1 + I\text{-depth of } M/xM.$$

Corollary

If $M/IM \neq 0$ all maximal regular M-sequences in I have the same length.

Depth of a Module

Definition

Let $(\mathbf{R}, \mathfrak{m})$ be a Noetherian local ring. For any f.g. $\mathbf{R}$-mdule M, the depth of M is the length of the longest regular M-sequence contained in $\mathfrak{m}$.

Proposition

Let M be a finitely generated module of the local ring $(\mathbf{R}, \mathfrak{m})$. Then

$$\operatorname{depth} M = \inf\{r : \operatorname{Ext}^r_{\mathbf{R}}(\mathbf{R}/\mathfrak{m}, M) \neq 0\}.$$

Change of Rings: Rees Theorems

Theorem

Let $\mathbf{R}$ *be a commutative ring and* x *be a regular element of* $\mathbf{R}$*. Set* $\overline{\mathbf{R}} = \mathbf{R}/(x)$*. If* x *is regular on the module* A *and* $xB = 0$*, then*

1. $\mathrm{Ext}^n_{\mathbf{R}}(B, A) \simeq \mathrm{Ext}^{n-1}_{\overline{\mathbf{R}}}(B, A/xA)$;
2. $\mathrm{Ext}^n_{\mathbf{R}}(A, B) \simeq \mathrm{Ext}^n_{\overline{\mathbf{R}}}(A/xA, B)$.

Outline

Koszul Complexes

We give here a discussion of what is likely the most useful complex in commutative algebra. It permits the introduction of various measures of size for ideals and modules.

Exterior algebra of a module

Let A be an R-module and let $T(A)$ be its tensor algebra. Let I be the ideal of $T(A)$ generated by all elements of the form $a \otimes a$.

- I is a homogeneous ideal of $T(A)$: $I_0 = I_1 = 0$, I_2 is the submodule of $A \otimes A$ generated by all $a \otimes a$, $a \in A$.
- $I_3 = T_1 \cdot I_2 + I_2 \cdot T_1$
- $I_n = \sum_{r \leq n-2} T_r \cdot I_2 \cdot T_{n-r-2}$

Definition

Let A be an R-module. The exterior algebra of A is

$$\bigwedge_R(A) = \bigoplus_{n\geq 0} \bigwedge^n(A) = \bigoplus T(A)/I.$$

- $\wedge^0(A) = R$ and $\wedge^1(A) = A$
- $\wedge^n(A)$ is called the nth exterior power of A.
- Its elements are linear combinations of $v_1 \wedge v_2 \cdots \wedge v_n$.

Properties

Proposition

If A generated by n elements, then $\bigwedge^n(A)$ is a cyclic module (possibly O), and $\bigwedge^m(A) = 0$ for $m > n$.

Proof. Suppose $A = (x_1, \ldots, x_n)$. Then any element of A is a linear combination

$$v = \sum_i r_i x_i$$

$$v_1 \wedge v_2 \wedge \cdots \wedge v_m =$$

$$\sum_i r_{1i} x_i \wedge \sum_i r_{2i} \wedge \cdots \wedge \sum_i r_{mi} x_i =$$

$$\sum r_{1i_1} r_{2i_2} \cdots r_{mi_m} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_m}$$

In the expression

$$\sum r_{1i_1} r_{2i_2} \cdots r_{mi_m} x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_m}$$

- If $m > n$, at least two of the x_i are equal, so the wedge product is zero.
- If $m = n$ and the x_{i_j} are distinct, the products are all equal to $\pm x_1 \wedge x_2 \wedge \cdots \wedge x_n$. Collecting the signs we have

$$v_1 \wedge \cdots \wedge v_n = \det(\mathbf{A}) x_1 \wedge \cdots \wedge x_n$$

where $\mathbf{A}$ is the matrix $\mathbf{A} = [r_{ij}]$.

Functorial Property

Theorem

Let $\mathbf{f} : A \rightarrow B$ *be a homomorphism of modules over the commutative ring* R*. Then there is a natural (meaning what?) ring homomorphism* $\bigwedge(\mathbf{f}) : \bigwedge(A) \rightarrow \bigwedge(B)$ *of their exterior algebras.*

Proof. It is enough to consider the commutative diagram (explain)

$$\begin{array}{ccc} A & \xrightarrow{\mathbf{f}} & B \\ \downarrow & & \downarrow \\ \bigwedge(A) & \xrightarrow[\bigwedge(\mathbf{f})]{} & \bigwedge(B) \end{array}$$

$$\bigwedge(\mathbf{f})(a_1 \wedge \cdots \wedge a_n) = \mathbf{f}(a_1) \wedge \cdots \wedge \mathbf{f}(a_n)$$

One consequence:

$$\bigwedge(\mathbf{f} \circ \mathbf{g}) = \bigwedge \mathbf{f} \circ \bigwedge \mathbf{g}$$

For example, if $\mathbf{f} : R^n \to R^n$, then $\wedge^n \mathbf{f} = \det \mathbf{f}$.

The formula above asserts

$$\det(\mathbf{f} \circ \mathbf{g}) = \det \mathbf{f} \cdot \det \mathbf{g}$$

Tensor Product of Complexes

Let $\mathcal{E} = \{E_i, \mathbf{f}_i, i \geq 0\}$ and $\mathcal{F} = \{F_i, \mathbf{g}_i, i \geq 0\}$ be two complexes. Their tensor product is the complex $\mathcal{G} = \{G_i, \mathbf{h}_i, i \geq 0\}$,

$$G_{i+1} = \bigoplus_{j+k=i+1} E_j \otimes F_k \xrightarrow{\mathbf{h}_{i+1}} G_i = \bigoplus_{j+k=i} E_j \otimes F_k$$

$$\mathbf{h}_{i+1}(x_j \otimes y_k) = \mathbf{f}_j(x_j) \otimes y_k + (-1)^k x_j \otimes \mathbf{g}_k(y_k)$$

Suppose $E_1 \xrightarrow{\mathbf{f}} E_0$ and $F_1 \xrightarrow{\mathbf{g}} F_0$ are complexes. Then their tensor product is

$$E_1 \otimes F_1 \to E_1 \otimes F_0 \oplus E_0 \otimes F_1 \to E_0 \otimes F_0$$

with the map above.

Koszul Complex

Let E be an R–module and denote by $\bigwedge(E)$ the exterior algebra of E. Given an element $\varphi \in \mathrm{Hom}_R(E, R)$, one defines a mapping ∂ on $\bigwedge(E)$, given in degree r by

$$\partial(e_1 \wedge \cdots \wedge e_r) = \sum_{i=1}^{r} (-1)^{i-1} \varphi(e_i)(e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_r).$$

∂ sends $\wedge^r E$ to $\wedge^{r-1} E$, and it is easy to see that $\partial^2 = 0$.

We will refer to the complex

$$\mathbb{K} = \mathbb{K}(E, \varphi) = \{\bigwedge(E), \partial\}$$

as the *Koszul complex* associated to E and φ. For an R–module M, we can attach coefficients to $\mathbb{K}(E, \varphi)$ by forming the chain complex $\mathbb{K}(E, \varphi; M) = \mathbb{K}(E, \varphi) \otimes_R M$.
A consequence of the definition of ∂ is that, if ω and ω' are homogeneous elements of $\bigwedge(E)$, of degrees p and q, respectively, then

$$\partial(\omega \wedge \omega') \quad = \quad \partial(\omega) \wedge \omega' + (-1)^p \omega \wedge \partial(\omega').$$

This implies that the cycles $Z(\mathbb{K})$ form a subalgebra of $\mathbb{K}$, and that the boundaries $B(\mathbb{K})$ form a two–sided ideal of $Z(\mathbb{K})$. Thus the homology of the complex, $H(\mathbb{K})$, inherits a structure of R–algebra.

Proposition

$H(\mathbb{K}(E, \varphi; M))$ is annihilated by the ideal $\varphi(E)$.

Proof. If $M \simeq R$, it suffices to note that if $e \in E$ and $\omega \in Z_r(\mathbb{K})$, then $\partial(e \wedge \omega) = \varphi(e)\omega$. The same argument holds when coefficients are attached. □

Since $H_0(\mathbb{K}(E, \varphi; M)) = M/\varphi(E)M$, the main problem of the elementary theory of these complexes is to find criteria for the vanishing of the higher homology modules. The most satisfying setting is the case when E is a free R–module, $E \simeq R^n = Re_1 \oplus \cdots \oplus Re_n$: Setting $x_i = \varphi(e_i)$

$$0 \to R = K_n \xrightarrow{f_n} K_{n-1} \to \cdots \to K_1 \to K_0 = R \to R/\varphi(R^n) \to 0$$

$$f_n(e_1 \wedge \cdots \wedge e_n) = \sum_{i=1}^{n} (-1)^{i-1} x_i (e_1 \wedge \cdots \wedge \widehat{e_i} \wedge \cdots \wedge e_n)$$

Such complexes are more interesting when $\varphi(R^n)$ is a proper ideal of R. It is convenient to consider the elements $x_i = \varphi(e_i)$ and view $\mathbb{K}(R^n, \varphi)$ as the (graded) tensor product of n Koszul complexes associated to maps of the kind $R \stackrel{x}{\longrightarrow} R$. That is, if we denote such a complex by $\mathbb{K}(x)$, we have

$$\mathbb{K}(R^n, \varphi) = \mathbb{K}(x_1) \otimes \cdots \otimes \mathbb{K}(x_n).$$

We will denote such complex by $\mathbb{K}(x_1, \ldots, x_n)$, or $\mathbb{K}(\mathbf{x})$, with $\mathbf{x} = \{x_1, \ldots, x_n\}$.

The complex for $n = 3$:

$$\mathbb{K}(x, y, z) = \mathbb{K}(x) \otimes \mathbb{K}(y) \otimes \mathbb{K}(z)$$

$$0 \to R \xrightarrow{f_3} R^3 \xrightarrow{f_2} R^3 \xrightarrow{f_1} R \to 0$$

$$f_1 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad f_2 = \begin{bmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{bmatrix}, \quad f_3 = \begin{bmatrix} x & y & z \end{bmatrix}$$

Some of the homology modules:

$$H_0(\mathbb{K}) = R/(x, y, z), \quad H_3(\mathbb{K}) = \operatorname{ann}(x, y, z)$$

The complex for $n = 3$ with coeficients in a module M

$$\mathbb{K} = \mathbb{K}(x, y, z; M) = \mathbb{K}(x) \otimes \mathbb{K}(y) \otimes \mathbb{K}(z) \otimes M$$

$$0 \to R \otimes M \xrightarrow{f_3} R^3 \otimes M \xrightarrow{f_2} R^3 \otimes M \xrightarrow{f_1} R \otimes M \to 0$$

$$f_1 = \begin{bmatrix} x \\ y \\ z \end{bmatrix}, \quad f_2 = \begin{bmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{bmatrix}, \quad f_3 = \begin{bmatrix} x & y & z \end{bmatrix}$$

Some of the homology modules:

$$H_0(\mathbb{K}) = M/(x, y, z)M, \quad H_3(\mathbb{K}) = \operatorname{ann}_M(x, y, z) = \{m \in M : (x, y, z)m = 0\}$$

Vanishing of Koszul homology

The vanishing of the homology modules of $\mathbb{K}(\mathbf{x}; M)$ has the following module theoretic explanation.

Proposition (Grade–Sensitivity of Koszul Complexes)

Let R be a Noetherian ring, and let $\mathbf{x} = \{x_1, \ldots, x_n\}$ be a sequence of elements generating the ideal I. Let M be a finitely generated R–module with $M \neq IM$, $\mathbb{K}(\mathbf{x}; M)$ be the corresponding Koszul complex and let q be the largest integer for which $H_q(\mathbb{K}(\mathbf{x}; M)) \neq 0$. Then all maximal M–regular sequences in I have length equal to $n - q$.

Proof. Note that since $H_0(\mathbb{K}(\mathbf{x}; M)) = M/IM$, and the complex $\mathbb{K}(\mathbf{x}; M)$ has length n, $0 \leq q \leq n$.

We use descending induction on q. From the definition of $\mathbb{K}(\mathbf{x}; M)$, $H_n(\mathbb{K}(\mathbf{x}; M))$ consists of the elements of M which are annihilated by I. If this module is nonzero we are done. If not, that is $q < n$, the ideal I is not contained in any associated prime of M and therefore there is $a \in I$ which is a regular element on M.

Consider the short exact sequence induced by multiplication by a,

$$0 \to M \xrightarrow{a} M \longrightarrow M/aM \to 0.$$

Tensoring it with the complex of free modules $\mathbb{K}(\mathbf{x})$, we get the exact sequence of Koszul complexes,

$$0 \to \mathbb{K}(\mathbf{x}; M) \xrightarrow{a} \mathbb{K}(\mathbf{x}; M) \longrightarrow \mathbb{K}(\mathbf{x}; M/aM) \to 0.$$

In homology we get the long exact sequence,

$$H_{q+1}(\mathbb{K}(\mathbf{x}; M)) \to H_{q+1}(\mathbb{K}(\mathbf{x}; M/aM)) \to H_q(\mathbb{K}(\mathbf{x}; M)) \xrightarrow{a} H_q(\mathbb{K}(\mathbf{x}; M)).$$

From the definition of q, we obtain $H_i(\mathbb{K}(\mathbf{x}; M/aM)) = 0$ for $i > q + 1$. We have seen that $H_q(\mathbb{K}(\mathbf{x}; M))$ is annihilated by I, and thus $aH_q(\mathbb{K}(\mathbf{x}; M)) = 0$. Taken together we have

$$H_{q+1}(\mathbb{K}(\mathbf{x}; M/aM)) \simeq H_q(\mathbb{K}(\mathbf{x}; M)),$$

from which an easy induction suffices to complete the proof. $\square$

The last equality in the proof shows also:

Corollary

If $\mathbf{a} = a_1, \ldots, a_{n-q}$ *is a maximal regular sequence on* M *contained in* I*, then*

$$H_q(\mathbb{K}(\mathbf{x}; M)) = (\mathbf{a}M \colon I)/\mathbf{a}M.$$

Depth

Definition

Let I be an ideal of a Noetherian ring R, and let M be a finitely generated R–module. The *I–depth* of M is the length of a maximal regular sequence on M contained in I. If R is a local ring and I is the maximal ideal (in which case the condition $M/IM \neq 0$ is automatically satisfied by Nakayama lemma), the I–depth of M is called the depth of M. If $M = R$, the I–depth of R is called the *grade* of I, and denoted $\mathrm{grade}\, I$.

Heuristically, $\mathrm{grade}\, I$ is a measure of the number of independent 'indeterminates' that may be found in I.

Corollary

Let I be an ideal contained in the Jacobson radical of the Noetherian ring R, and let

$$0 \to E \longrightarrow F \longrightarrow G \to 0$$

be an exact sequence of finitely generated R–modules. Then

$$\begin{array}{lcl} \textit{If } I\text{–depth } F & < & I\text{–depth } G, \ \textit{then } I\text{–depth } E = I\text{–depth } F; \\ \textit{If } I\text{–depth } F & > & I\text{–depth } G, \ \textit{then } I\text{–depth } E = I\text{–depth } G + 1; \\ \textit{If } I\text{–depth } F & = & I\text{–depth } G, \ \textit{then } I\text{–depth } E \geq I\text{–depth } G. \end{array}$$

Proof. Let $\mathbb{K}(\mathbf{x})$ be the Koszul complex on a set $\mathbf{x}$ of generators of I. Tensoring the exact sequence of modules with $\mathbb{K}(\mathbf{x})$ gives the exact sequence of chain complexes,

$$0 \to \mathbb{K}(\mathbf{x}; E) \longrightarrow \mathbb{K}(\mathbf{x}; F) \longrightarrow \mathbb{K}(\mathbf{x}; G) \to 0.$$

The assertions will follow from a scan of the long homology exact sequence and the interpretation of depth given in the previous proposition. $\square$

The next result is the basis for several inductive arguments with ordinary Koszul complexes.

Proposition

Let $\mathbb{C}$ be a chain complex and let $\mathbb{F} = \{F_1, F_0\}$ be a chain complex of free modules concentrated in degrees 1 and 0. Then for each integer $q \geq 0$ there is an exact sequence

$$0 \to H_0(H_q(\mathbb{C}) \otimes \mathbb{F}) \longrightarrow H_q(\mathbb{C} \otimes \mathbb{F}) \longrightarrow H_1(H_{q-1}(\mathbb{C}) \otimes \mathbb{F}) \to 0.$$

Proof. Construct the exact sequence of chain complexes

$$0 \to \widehat{\mathbb{F}_0} \xrightarrow{f} \mathbb{F} \xrightarrow{g} \widehat{\mathbb{F}_1} \to 0,$$

$$\begin{aligned} (\widehat{\mathbb{F}_0})_0 &= F_0 \\ (\widehat{\mathbb{F}_0})_1 &= 0 \\ (\widehat{\mathbb{F}_1})_0 &= 0 \\ (\widehat{\mathbb{F}_1})_1 &= F_1, \end{aligned}$$

and f and g are the obvious injection and surjection mappings.

Tensoring with $\mathbb{C}$ and writing the homology exact sequence, we get

$$H_{q+1}(\mathbb{C}\otimes\widehat{\mathbb{F}_1}) \xrightarrow{\partial} H_q(\mathbb{C}\otimes\widehat{\mathbb{F}_0}) \to H_q(\mathbb{C}\otimes\mathbb{F}) \to H_q(\mathbb{C}\otimes\widehat{\mathbb{F}_1}) \xrightarrow{\partial} H_{q-1}(\mathbb{C}\otimes\widehat{\mathbb{F}_0}),$$

where the connecting homomorphism ∂ is up to a sign the differentiation of $\mathbb{F}$ tensored with $H_q(\mathbb{C})$. Noting that $H_{q+1}(\mathbb{C} \otimes \widehat{\mathbb{F}_1}) = H_q(\mathbb{C}) \otimes F_1$, and $H_q(\mathbb{C} \otimes \widehat{\mathbb{F}_0}) = H_q(\mathbb{C}) \otimes F_0$, we obtain the desired exact sequence. $\square$

Rigidity

Theorem (Rigidity of the Koszul Complex)

Let $\mathbf{x} = \{x_1, \ldots, x_n\}$ be a sequence of elements contained in the Jacobson radical of R, and let M be a finitely generated module. If $H_q(\mathbb{K}(\mathbf{x}; M)) = 0$, then $H_i(\mathbb{K}(\mathbf{x}; M)) = 0$ for $i \geq q$.

Rigidity–Proof

Proof. Denote $\mathbf{y} = \{x_1, \ldots, x_{n-1}\}$, and $a = x_n$. In previous Proposition, set $\mathbb{C} = \mathbb{K}(\mathbf{y}; M)$, $\mathbb{F} = \mathbb{K}(a)$, so that $\mathbb{C} \otimes \mathbb{F} = \mathbb{K}(\mathbf{x}; M)$. For each $i \geq 0$, we have the exact sequence

$$0 \to H_0(H_i(\mathbb{K}(\mathbf{y}; M)) \otimes \mathbb{K}(a)) \to H_i(\mathbb{K}(\mathbf{x}; M)) \to H_1(H_{i-1}(\mathbb{K}(\mathbf{y}; M)) \otimes \mathbb{K}(a)) \to 0$$

If $H_q(\mathbb{K}(\mathbf{x}; M)) = 0$, then

$$H_0(H_q(\mathbb{K}(\mathbf{y}; M)) \otimes \mathbb{K}(a)) = H_q(\mathbb{K}(\mathbf{y}; M))/aH_q(\mathbb{K}(\mathbf{y}; M)) = 0,$$

which by Nakayama lemma implies $H_q(\mathbb{K}(\mathbf{y}; M)) = 0$. Inducting on n, we get

$$H_i(\mathbb{K}(\mathbf{y}; M)) = 0 \quad \text{for } i \geq q.$$

Taking this into the exact sequence gives that $H_i(\mathbb{K}(\mathbf{x}; M)) = 0$ for $i \geq q$. □

Koszul complex and Hilbert syzygy theorem

Let k be a ring and $\mathbf{R} = k[x_1, \ldots, x_n]$ and let M be an $\mathbf{R}$-module that is k-projective. Let us describe a canonical $\mathbf{R}$-projective resolution of M.

Let $S = \mathbf{R} \otimes_k \mathbf{R} \simeq k[x_1, \ldots, x_n; y_1, \ldots, y_n]$; note that we can see S as an $\mathbf{R}$-algebra in two different ways: left or right multiplication.

The polynomials $\mathbf{z} = z_1 = x_1 - y_1, \ldots, z_n = x_n - y_n$, of S form a S-regular sequence and $S/(z_1, \ldots, z_n) = \mathbf{R}$. Therefore $\mathbb{K}(\mathbf{z}; S)$ is a S-projective resolution of $\mathbf{R}$

$$0 \to \wedge^n S^n \to \cdots \to \wedge^1 S^n \to S \to \mathbf{R} \to 0$$

This complex can be seen as a complex of free **R**-modules (on the right or on the left) that splits completely, on either side. Using the right structure, tensoring it with M over **R** gives an exact sequence

$$0 \to \wedge^n S^n \otimes_{\mathbf{R}} M \to \cdots \to \wedge^1 S^n \otimes_{\mathbf{R}} M \to S \otimes_{\mathbf{R}} M \to \mathbf{R} \otimes_{\mathbf{R}} M = M \to 0$$

Observe that the i^{th} component of the complex is

$$\wedge^i S^n \otimes_{\mathbf{R}} M = (S \otimes_{\mathbf{R}} M)^{\binom{n}{i}} = (\mathbf{R} \otimes_k \mathbf{R} \otimes_{\mathbf{R}} M)^{\binom{n}{i}} = (\mathbf{R} \otimes_k M)^{\binom{n}{i}}$$

which is a projective **R**-module, since M is k-projective.

Theorem (HST, proof number 17)

If $\mathbf{R} = k[x_1, \ldots, x_n]$, $S = \mathbf{R} \otimes_k \mathbf{R}$ and M is an $\mathbf{R}$-module that is projective over k, then the Koszul complex

$$\mathbb{K}(\mathbf{z}; S) \otimes_{\mathbf{R}} M$$

is a projective $\mathbf{R}$-resolution of M.

Application

Let k be a field, $\mathbf{R} = k[x_1, \ldots, x_n]$ and set $\mathbb{K} = \mathbb{K}(\mathbf{z}; S)$.

Corollary

Let $\mathbb{P}$

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

be an exact complex of $\mathbf{R}$*-modules. Then*

$$\cdots \to P_r \otimes \mathbb{K} \to \cdots \to P_1 \otimes \mathbb{K} \to P_0 \otimes \mathbb{K} \to M \otimes \mathbb{K} \to 0$$

is a projective resolution of the complex $\mathbb{P}$*.*