Math 552: Abstract Algebra II

Wolmer V. Vasconcelos

Set 5

Spring 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

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

$\mathbf{f}$ is 1-1, $\mathbf{g}$ 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 $\mathbf{f}$ 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 $\mathbf{K}$. The ideals of R are part of an important class of R-submodules of $\mathbf{K}$:

Definition

A submodule L of $\mathbf{K}$ 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. $\mathbf{K}$ is not fractionary, unless $R = \mathbf{K}$.

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

Definition

The quotient of two fractional 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 fractional 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 $L = (x_1, \dots, x_n)$ and $L' = (y_1, \dots, y_n)$ 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.

Injective modules

Definition

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

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

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* $\mathbf{h} : B \to E$ *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

Assignment #18

Do one of the two problems.

- Prove that for any nonzero integer n, the ring $R = \mathbb{Z}/(n)$ is injective as an R-module. (We refer to this property by saying that R is self-injective.)
- Let R be an integral domain and E an injective R-module. Prove that the torsion submodule T of E is also injective.

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,

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

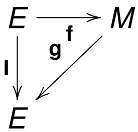
Since E is an injective $\mathbb{Z}$-module, the $\mathbb{Z}$-functor $\mathrm{Hom}_{\mathbb{Z}}(\cdot, E)$ is exact, so the R-functor $\mathrm{Hom}_R(\cdot, \mathrm{Hom}_{\mathbb{Z}}(R, E))$ is exact, hence the assertion.

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.

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 $n = 3$]:

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

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

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 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 $\gcd(\Delta_1, \Delta_2, \Delta_3) = 1$.

Hilbert-Burch

Theorem

Let $R = k[x, y]$. Then for any ideal $I = (a_1, \ldots, a_n)$ 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 $(a_1, \ldots, a_n)$

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

the kernel of φ is generated by $n-1$ vectors, $v_i = (d_{1,i}, \ldots, d_{n-1,i})$ 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

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

Proposition

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

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 $\varphi - \mathbf{x}I$.

- 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.

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.

Outline

Assignment #19

Do one problem.

- 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?

Outline

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 $n + 1$.

Proof

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

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

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 $\operatorname{proj\,dim}_{R[x]} (R[x] \otimes_R M) \leq \operatorname{proj\,dim}_R M$.

- 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,

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

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

$$\operatorname{proj}\dim_{R[x]} M = \operatorname{proj}\dim_R M + 1.$$

- 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 $n = \operatorname{proj}\dim_R M$.

- 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.

Outline

Assignment #20

- $R = k[x, y]$, 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 **K**. Then

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

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 $\mathbf{F}$. 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

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

$\mathbf{T}$ is clearly a bilinear function. It is a good exercise (do it) to show that

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

so $\mathbf{T}$ is **symmetric**

Here is a variation that will appear later

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

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

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

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

It is clear that

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

is a bilinear function.

Is it **symmetric**?

Proposition

If **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 $\mathbf{M}$ *of all n–linear functions on the vector space* $\mathbf{V}$ *with values in* $\mathbf{W}$ *is a vector space. The subsets* $\mathbf{S}$ *and* $\mathbf{K}$ *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 $\mathbf{B}$ 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

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

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

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

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

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

Proposition

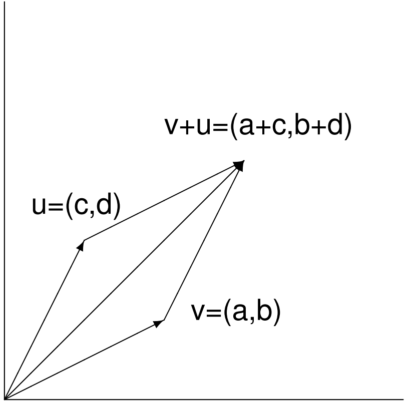
The vector space $\mathbf{K}$ *of all skew-symmetric bilinear functions on* $\mathbf{F}^2$ *with values in* $\mathbf{F}$ *has a basis which is the 2-by-2 determinant function.*

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 **V** is a vector space of dimension n, and **S** and **K** are the spaces of symmetric and skew-symmetric bilinear functions, prove that

$$\dim \mathbf{S} = \binom{n+1}{2}$$

$$\dim \mathbf{K} = \binom{n}{2}$$

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

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

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

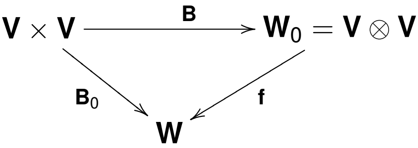
is a bilinear transformation. We want to argue that there is a bilinear map

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

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 $r \in R$

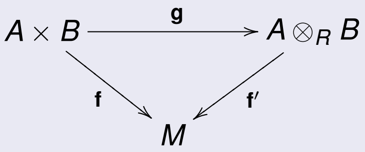
$$\begin{aligned} \mathbf{f}(a + a', b) &= \mathbf{f}(a, b) + \mathbf{f}(a', b) \\ \mathbf{f}(a, b + b') &= \mathbf{f}(a, b) + \mathbf{f}(a, b') \\ \mathbf{f}(ar, b) &= \mathbf{f}(a, rb) \end{aligned}$$

An example is the multiplication in the ring R.

If we followup 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:

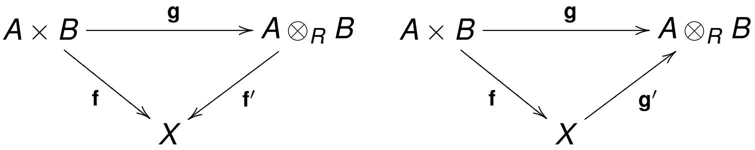
1. $\mathbf{g}$ is a bilinear mapping
2. Given a bilinear mapping $\mathbf{h} : A \times B \to M$ it defines a linear mapping $\mathbf{f} : F \to M$. Since $\mathbf{g}$ is a bilinear mapping, $\mathbf{f}$ vanishes on the generators of L, so defines the bilinear mapping $\mathbf{g} : F/L \to M$. It follows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

Uniqueness of tensor products

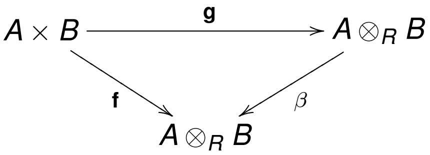
Theorem

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, $\mathbf{I} = \phi$.

$\otimes$ as a functor

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 $A \otimes B \simeq B \otimes A$
  $\mathbb{Z}/(a) \otimes_R \mathbb{Z}/(b) \simeq \mathbb{Z}/(\gcd(a, b))$
  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.

The tensor algebra

Let R be a commutative ring and A an R-module. Now we are going to introduce the tensor algebra of A. First a number of quick observations:

- If A, B and C are R-modules, there is a canonical isomorphism

$$A \otimes (B \otimes C) \quad \simeq \quad (A \otimes B) \otimes C$$

  One way to prove this is first define $A \otimes B \otimes B$ (no parentheses) as a universal target for trilinear maps from $A \times B \times C$ by generators and relations. Then show that both $A \otimes (B \otimes C)$ and $(A \otimes B) \otimes C$ satisfy the universal condition.

Tensor algebra of a module

Let A be an R-module and set

$$T_n(A) = \underbrace{A \otimes \cdots \otimes A}_{\text{n factors}}$$

Set $T_0(A) = R$ and

$$T(A) = \bigoplus_{n \geq 0} T_n(A)$$

It is clear to define a product that endows $T(A)$ with an algebra structure:

$$(a_1 \otimes \cdots \otimes a_m) \cdot (b_1 \otimes \cdots \otimes b_n) = a_1 \otimes \cdots \otimes a_m \otimes b_1 \cdots \otimes b_n$$

This is the tensor algebra of A.

Algebras

Definition

Let R be a commutative ring and A a ring not necessarily with 1 nor commutative. A is an R-algebra if A a R-bimodule and $ra = ar$ for all $r \in R$, $a \in A$.

- Any ring A is naturally a $\mathbb{Z}$-algebra
- The tensor algebra $T(A)$ of an R-module is one of the core examples.
- We will consider two kinds of algebras: commutative and skew-commutative: algebras with the property that $a^2 = 0$ for all $a \in A$. This condition implies–but it is not always equivalent–that $ab = -ba$ for $a, b \in A$:

$$0 = (a+b)(a+b) = a^2 + ab + ba + b^2$$

Graded algebra

Let R be a ring and A an R-algebra. We say that A is a graded R-algebra if

$$A = \bigoplus_{n \in \mathbb{Z}} A_n, \quad A_m \cdot A_n \subset A_{m+n}$$

- Polynomials rings $R[x_1, \ldots, x_n]$ are major examples.
- The elements $x \in A_n$ are called n-forms or homogeneous of degree n.
- We usually assume $A_n = 0$ if $n < 0$. A notable exception is $A = k[x, x^{-1}]$, the ring of Laurent polynomials.

Homogeneous ideals

Definition

An ideal I of a graded algebra is said to be homogeneous if $I = \bigoplus_{n\in\mathbb{Z}} I_n$, $I_n \subset A_n$.

They are handy way to produce new graded algebras:

$$A/I = \bigoplus_n A_n/I_n$$

Proposition

An ideal I of a graded algebra A is homogeneous iff I s generated by a set $\{\mathbf{f}_\alpha\}$ of homogeneous forms $\mathbf{f}_\alpha$.

Proof. Left to reader/listener.

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.

Basic property of the tensor algebra

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

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

which we extend to a homomorphism

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

The $\mathbf{g}_n$ patch into the homomorphism $\mathbf{g}$.

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,

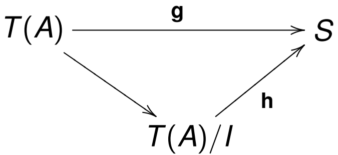
$$\mathbf{g}(a \otimes b) = \mathbf{f}(a)\mathbf{f}(b) = \mathbf{f}(b)\mathbf{f}(a) = \mathbf{g}(b \otimes a)$$

  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

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

Outline

Assignment #21

- 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

Graded modules

- Let $R = k[x_1, \ldots, x_d]$ be the ring of polynomials over the field k. We denote by R_n the vector space of homogeneous polynomials of degree n.
- A graded R-module M is a module with a decomposition $M = \bigoplus_{n\in\mathbb{Z}} M_n$ such that $R_m M_n \subset M_{m+n}$.
- The premier example is R itself. Others are the ideals generated by homogeneous elements.
- This is a very fruitful setting: explain

Proposition

Let $R = k[x_1, \ldots, x_d]$, k a field, and let M be a graded R-module. A submodule $E \subset M$ is graded iff E is generated by homogeneous elements.

Concretely, if $z_1, \ldots, z_m$ are homogeneous elements of $M = \bigoplus M_i$, with z_j of degree d_j, that is $z_j \in M_{d_j}$, they generate the module $E = \bigoplus E_n$, whose elements of degree n are the linear combinations

$$x = r_1 z_1 + \cdots + r_m z_m, \quad r_i \in R_{n-d_i}$$

For example, if $I = (x^2 + y^2, x^3 + x^2 y)$, then

$$I_n = \{a \cdot (x^2 + y^2) + b \cdot (x^3 + x^2 y)\}$$

where a and b homogeneous of degrees $n - 2$ and $n - 3$, resp.

Properties

For the remainder of this discussion, $R = k[x_1, \ldots, x_d]$.

Proposition

If M is a finitely generated graded R-module then each component M_n is a k-vector space of finite dimension.

Proof.

- First consider the case $M = R$. Then M_n is the vector space of all homogeneous polynomials of degree n. A basis for this space is the set of monomials

  $$x_1^{e_1} \cdot x_2^{e_2} \cdots x_d^{e_d}, \quad e_1 + e_2 + \cdots + e_d = n.$$

  The cardinality of this set is

  $$\binom{d+n-1}{d-1.}$$

- If M is a module generated by the homogeneous elements $z_1, \ldots, z_m$, with $\deg(z_i) = d_i$, then M_n is given by the linear combinations

$$r_1 z_1 + \cdots + r_m z_m, \quad r_i \in R_{n-d_i}.$$

- Since each R_j is a finite dimensional vector space, it follows that $\dim_k M_n < \infty$.

Question: Is this fact a gift?

Homogeneous homomorphisms

Definition

Let $R = k[x_1, \ldots, x_d]$ and let $\mathbf{f} : M \to N$ be a homomorphism of graded modules. We say that $\mathbf{f}$ is homogeneous of degree r if

$$\mathbf{f} : M_n \to N_{n+r}, \quad \forall n.$$

If $\mathbf{a}$ is a homogeneous polynomial of degree r, then multiplication by $\mathbf{a}$ defines a homogeneous homomorphism of degree r,

$$R \to R, \quad u \to \mathbf{a}u$$

If $\mathbf{f} : M \to N$ is homogeneous (of degree r), then $K = \ker \mathbf{f}$ and coker $\mathbf{f} = N/\mathbf{f}(M) = C$ are graded.

In each degree there is an exact sequence of vector spaces

$$0 \to K_{n-r} \to M_{n-r} \to N_n \to C_n \to 0$$

Hilbert function of a graded module

Definition

Let M be a finitely generated graded R-module. The function

$$H_M(n) = \dim_k M_n$$

is the Hilbert function of M.

$$H_R(n) = \binom{d+n-1}{d-1}$$

Let $I = (x)$; then $I_n = \{f \cdot x : f \in R_{n-1}\}$. Thus $I_n \simeq R_{n-1}$, and so

$$H_I(n) = \binom{d+n-2}{d-1}$$

Definition

Let M be a finitely generated graded R-module. The formal Laurent power series

$$P_M(\mathbf{t}) = \sum_{n\in\mathbb{Z}} \dim_k M_n \mathbf{t}^n$$

is the Hilbert-Poincaré series of M. It is also called the generating series of M.

$$P_R(\mathbf{t}) = \sum_{n\in\mathbb{Z}} \binom{d+n-1}{d-1} \mathbf{t}^n = \frac{1}{(1-\mathbf{t})^d}$$

- If $R = k$ (0 variables), $M = \bigoplus_n M_n$ is a finite dimensional graded vector space. So $H_M(n) = 0$ for $n \gg 0$, and $P_M(\mathbf{t})$ is a polynomial.
- If $z_1, \ldots, z_m$ are the homogeneous generators of M, since

$$M_n = \{\sum_i r_i z_i, \quad \deg(r_i) + \deg(z_i) = n\},$$

$M_n = 0$ for $n < \inf\{\deg(z_i)\}$. Thus $H_M(n) = 0$ for $0 \gg n$, and $P_M(\mathbf{t})$ has only finitely many terms in negative degrees.

Example

- Let $R = k[x, y, z]$ and $I = (xy, yz, zx)$ and set $M = R/I$. Let us determine the Hilbert-Poincaré series of M.
- Consider the homogeneous homomorphism of M induced by multiplication by x. This gives rise, in each degree, to the exact sequence of vector spaces

$$0 \to K_{n-1} \longrightarrow M_{n-1} \to M_n \longrightarrow C_n \to 0,$$

  where K is the kernel and C is the cokernel of the multiplication by x.
- $C = R/(x, I) = k[y, z]/(yz)$ and $K = (I : x)/I = (y, z)/I$.

Example cont'd

This gives the exact sequence

$$0 \to R/I/(y,z)/I = R/(y,z)[-1] = k[x][-1] \to R/I \to k[y,z]/(yz) \to 0$$

- This gives the equality of Hilbert series

$$P_{R/I}(\mathbf{t}) = P_{k[x][-1]}(\mathbf{t}) + P_{k[y,z]/(yz)}(\mathbf{t}).$$

- $P_{k[x]}(\mathbf{t}) = \frac{1}{1-\mathbf{t}}$ and $P_{k[x][-1]}(\mathbf{t}) = \frac{\mathbf{t}}{1-\mathbf{t}}$
- $P_{k[y,z]/(yz)} = \frac{1-\mathbf{t}^2}{(1-\mathbf{t})^2} = \frac{1+\mathbf{t}}{1-\mathbf{t}}$.
- $P_{R/I}(\mathbf{t}) = \frac{1+2\mathbf{t}}{1-\mathbf{t}}$.

Example

- We denote $\dim M_n = m_n$, etc, so we have the equality $k_{n-1} - m_{n-1} + m_n - c_n = 0$.
-

Big theorem

Theorem

Let M be a finitely generated graded R-module. Then

1. *There exists a polynomial $\mathcal{H}(\mathbf{x})$ such that*

$$H_M(n) = \mathcal{H}(n), \quad n \gg 0.$$

2. *$P_M(\mathbf{t})$ is a rational function of the form*

$$P_M(\mathbf{t}) = \frac{\mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})}{(1-\mathbf{t})^d},$$

where $\mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})$ is a polynomial with integer coefficients.

Proof. The proof is long but instructive. We will introduce various notions along the way.

Let us recall:

Proposition

Let k be a field and

$$0 \to V_n \longrightarrow V_{n-1} \longrightarrow \cdots \longrightarrow V_2 \longrightarrow V_1 \to 0$$

be an exact complex of finite dimensional vector spaces. Then

$$\sum_{i=1}^{n} (-1)^i \dim V_i = 0.$$

Proof. This is a direct consequence of the case $n = 3$: If

$$0 \to V_3 \longrightarrow V_2 \longrightarrow V_1 \to 0$$

is exact, then $\dim V_2 = \dim V_1 + \dim V_3$.

Proof

- The proof will be by induction on the number of d of variables of $R = k[x_1, \ldots, x_d]$. If $d = 0$, $M_n = 0$ for $n \gg 0$, so that $H_M(n) = 0$ and $P_M(\mathbf{t}) = \mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})$ for some polynomial $\mathbf{h}$.
- For the induction step, consider the following sequence defined by multiplication by x_d:

$$0 \to K \longrightarrow M \xrightarrow{\varphi} M \longrightarrow C = M/x_d M \to 0, \quad \varphi(z) = x_d z.$$

- φ maps M_{n-1} to M_n. Its kernel is a graded submodule of M,

$$K = \{z \in M : x_d z = 0\}$$

- Observe that K and C are annihilated by x_d, so they are (graded) modules over $k[x_1, \ldots, x_{d-1}]$.

- Consider the exact sequence of vector spaces

$$0 \to K_{n-1} \longrightarrow M_{n-1} \longrightarrow M_n \longrightarrow C_n \to 0.$$

- By the usual property,

$$\dim K_{n-1} - \dim M_{n-1} + \dim M_n - \dim C_n = 0$$

- We denote the dimensions by small numbers so that

$$k_{n-1} - m_{n-1} + m_n - c_n = 0$$

multiply by $\mathbf{t}^n$ and add the formal power series to get

$$\sum_n k_{n-1}\mathbf{t}^n - \sum_n m_{n-1}\mathbf{t}^n + \sum_n m_n\mathbf{t}^n - \sum_n c_n\mathbf{t}^n = 0$$

That is

$$\mathbf{t}P_K(\mathbf{t}) - \mathbf{t}P_M(\mathbf{t}) + P_M(\mathbf{t}) - P_C(\mathbf{t}) = 0$$

so that

$$P_M(\mathbf{t}) = \frac{P_C(\mathbf{t}) - \mathbf{t}P_K(\mathbf{t})}{1 - \mathbf{t}}$$

Since both $P_K(\mathbf{t})$ and $P_C(\mathbf{t})$ are rational functions of the form $\frac{\mathbf{f}(\mathbf{t},\mathbf{t}^{-1})}{(1-\mathbf{t})^{d-1}}$, we have the second assertion of the theorem.

The proof that the Hilbert function $H_M(n)$ agrees with a polynomial for $n \gg 0$ uses simple calculus: Consider the Taylor expansion

$$\frac{1}{(1-t)^d} = \sum_n \binom{d+n-1}{d-1} \mathbf{t}^n$$

and from the representation $P_M(\mathbf{t}) = \frac{\mathbf{h}(\mathbf{t},\mathbf{t}^{-1})}{(1-\mathbf{t})^d}$, write

$$\mathbf{h}(\mathbf{t},\mathbf{t}^{-1}) = \sum_{j=-r}^{j=s} a_j \mathbf{t}^j$$

Taking into account that $H_M(n)$ is the coefficient of $\mathbf{t}^n$ in the expansion of $P_M(\mathbf{t})$ we have for $n \geq s$

$$H_M(n) = \sum_{j=-r}^{j=s} a_j \binom{d+n-j-1}{d-1}$$

This is a polynomial of degree $\leq d-1$ in the index n. Its coefficients are important invariants of M.

Example

Let $R = k[x_1, x_2, x_3]$, and let I be the ideal generated by the monomials x_1x_2, x_1x_3, x_2x_3. Set $M = R/I$.

$$0 \to (x_3, I)/I \to R/I \to R/(x_3, I) \to 0, \ (x_3, I)/I \simeq R/(x_1, x_2)[-1] = k[x_3][-1]$$

A calculation gives $(R/(x_3, I) = k[x_1, x_2]/(x_1x_2))$

$$\begin{aligned}
P_{R/I}(\mathbf{t}) &= P_{k[x_1,x_2]/(x_1x_2)}(\mathbf{t}) + P_{k[x_3][-1]}(\mathbf{t}) \\
&= \frac{1-\mathbf{t}^2}{(1-\mathbf{t})^2} + \frac{\mathbf{t}}{1-\mathbf{t}} \\
&= \frac{1+2\mathbf{t}}{1-t} \\
H_{R/I}(n) &= 3, \quad n \geq 1.
\end{aligned}$$

Outline

Assignment #22

- Let $\mathbf{K}_n$ be the complete graph on n vertices labeled by the indeterminates $x_1, \dots, x_n$. Let I_n be the ideal of the ring $R = k[x_1, \dots, x_n]$ (k a field) corresponding to it. ($\mathbf{K}_n$ is just a reminder that to each graph there is an attached ideal.) I_n is generated by all the monomials $x_i x_j$, $i \neq j$. Find the Hilbert functions of the graded modules I_n and R/I_n.

Outline

TakeHome #2

Do 5 Problems.

- Let G be the dihedral group D_4. Find the decomposition of the group ring $\mathbb{C}[G]$ into simple rings.
- 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.