Math 559: Commutative Algebra

Wolmer V. Vasconcelos

Set 4: CM Rings/Combinatorial Tools

Fall 2009

Outline

Modules of Finite Projective Dimension

Let **R** be a Noetherian ring and M a finitely generated **R**-module with a finite free resolution

$$0 \to F_m \to \cdots \to F_1 \to F_0 \to M \to 0.$$

We are going to relate

1. The length of the resolution;
2. The properties of the ideals generated by the minors of the matrices
$$\varphi_i : F_i \to F_{i-1};$$
3. Other invariants of M and of **R**.

Modules of Finite Projective Dimension

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 $t \leq m$, $0 : I_{t-1}(\varphi) = 0$ and $0 : I_t(\varphi) \neq 0$. 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 $0 \neq r \in 0 : I_t(\varphi)$; 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 $r \cdot I_t(\varphi) = 0$. $\square$

Auslander–Buchsbaum Equality

The following is an explanation of the difference between the (finitistic) global dimension of a ring and the projective dimension of one of its modules.

Theorem

Let $(\mathbf{R}, \mathfrak{m})$ *be a Noetherian local ring and let* M *be a nonzero finitely generated* $\mathbf{R}$*–module. If* $\operatorname{proj\,dim}_{\mathbf{R}} M < \infty$ *then*

$$\operatorname{proj\,dim}_{\mathbf{R}} M + \operatorname{depth} M = \operatorname{depth} \mathbf{R}. \tag{1}$$

Recall that the depth of a module M is the length of the longest M-regular sequence contained in $\mathfrak{m}$.

Proof

We induct on $r = \operatorname{codim} R$ and $p = \operatorname{proj\,dim}_R M$. We may assume that $p > 0$. Let

$$0 \to F_p \xrightarrow{\psi} F_{p-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi} F_0 \longrightarrow M \to 0 \quad (2)$$

be a minimal free resolution of M.

We compare the value of the formula (1) for M and for its first module of syzygies $K = \varphi(F_1)$. If $r = 0$, the maximal ideal $\mathfrak{m}$ has a non trivial annihilator and therefore ψ, with its entries all in $\mathfrak{m}$, cannot be injective.

Suppose first that $\mathfrak{m}$ is not an associated prime of M. Since $r > 0$, there exists $x \in \mathfrak{m}$ which is regular on M and R, and therefore on all the modules in (2). Tensoring the resolution with $R/(x)$ gives a minimal resolution of the same length for M/xM as an $R/(x)$–module. We now use the formula for $R/(x)$.
For the second case, suppose $\mathfrak{m}$ is an associated prime of M, and let $x \in \mathfrak{m}$ be a regular element of R. Tensoring the exact sequence

$$0 \to K \longrightarrow F_0 \longrightarrow M \to 0,$$

by $R/(x)$, gives the exact sequence (using, say, the snake lemma, or the reader's favorite tool from homological algebra)

$$0 \to {}_xM \longrightarrow K/xK \longrightarrow F_0/xF_0 \longrightarrow M/xM \to 0,$$

where ${}_xM$ is the set of elements of M annihilated by x. Note that $\mathfrak{m}$ is an associated prime of this submodule. We thus have that $\mathfrak{m}$ is an associated prime of K/xK.

On the other hand, a minimal resolution of K/xK over $R/(x)$ is obtained by tensoring that part of (2) that resolves K. From the previous case, $\operatorname{proj\,dim}_{R/(x)} K/xK = \operatorname{depth} R/(x) = r - 1$, and therefore $\operatorname{proj\,dim}_R M = r$, as desired. □

Modules of Finite Injective Dimension

The f.g. **R**-modules of finite injective dimension have very different properties:

Theorem

Let $(\mathbf{R}, \mathfrak{m})$ *be a Noetherian local ring and* $N \neq 0$ *be a module of finite injective dimension. Then for any f.g.* **R***-module* M*,*

$$\operatorname{inj\,dim} M = \operatorname{depth} N + \sup\{j : \operatorname{Ext}^j_{\mathbf{R}}(M, N) \neq 0\}.$$

This implies:

Corollary

All nonzero finitely generated **R***-modules of finite injective dimension have the same injective dimension.*

Acyclicity of Free Complexes

We next give the most widely used tool to check the acyclicity of free complexes. A fuller discussion may be found in many textbooks and we content ourselves with the skeleton of a proof.

Let $\varphi : R^m \to R^n$ be a homomorphism between free modules. Picking bases it can be represented by an $n \times m$ matrix $[a_{ij}]$, and $\operatorname{rank} \varphi$ is the largest integer r such that $[a_{ij}]$ has a nonzero minor of order r. It is easily seen to be the least integer r such that r^{th} exterior power $\wedge^r\varphi : \wedge^r(R^m) \to \wedge^r(R^n)$ is nonzero. This identification ensures that r is well defined. We denote by $I_r(\varphi)$ the ideal generated by all the minors of order r.

Buchsbaum-Eisenbud

Theorem (Buchsbaum–Eisenbud)

Let R be a Noetherian ring and let

$$\mathbb{F}_\bullet : \qquad 0 \to F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \to 0$$

be a complex of finitely generated free R–modules. For each $i = 1, \ldots, n$, denote by $r_i = r_i(\mathbb{F}) = \sum_{j=i}^{n} (-1)^{j-i} \operatorname{rank} F_j$. The following conditions are equivalent:

(a) *$\mathbb{F}$ is acyclic.*

(b) $\operatorname{grade} I_{r_i}(\varphi_i) \geq i$, *for* $i = 1, \ldots, n$.

Proof. $(\mathrm{a}) \Rightarrow (\mathrm{b})$: Let $\mathfrak{p}$ be any associated prime ideal of (0) in the ring R. Localizing $\mathbb{F}$ at $\mathfrak{p}$ gives a complex $\mathbb{F} \otimes R_{\mathfrak{p}}$ of free modules which is a free resolution of $L = \operatorname{coker} \varphi_1$. By the Auslander-Buchsbaum equality, L must be a free $R_{\mathfrak{p}}$–module. Thus the complex $\mathbb{F}_{\mathfrak{p}}$ splits completely which means that $r_i = \operatorname{rank}\ \varphi_i$ and all ideals $I_{r_i}(\varphi_i)$ localize to $R_{\mathfrak{p}}$ and consequently must contain regular elements. If x is a regular element of R in $\bigcap_i I_{r_i}(\varphi_i)$, tensoring $\mathbb{F}$ by $R/(x)$ gives the exact sequence

$$0 \to F_n \otimes R/(x) \longrightarrow F_{n-1} \otimes R/(x) \longrightarrow \cdots \longrightarrow F_1 \otimes R/(x),$$

on which we use the induction hypothesis since $r_i(\mathbb{F}) = r_i(\mathbb{F} \otimes R/(x))$.

(b) $\Rightarrow$ (a): By induction on all such shorter complexes, we assume that the subcomplex

$$0 \to F_n \xrightarrow{\varphi_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_r \xrightarrow{\varphi_r} F_{r-1},$$

is acyclic except possibly at F_r. By McCoy's Theorem and the hypothesis on $I_{r_n}(\varphi_n)$, φ_n is an injective homomorphism, so that $1 \leq r < n$. Set $B = \operatorname{image} \varphi_{r+1}$, $Z = \ker \varphi_r$ and consider the natural exact sequence

$$0 \to B \longrightarrow Z \longrightarrow H = H_r(\mathbb{F}) \to 0.$$

To show that $H = 0$, suppose otherwise and let $\mathfrak{p}$ be a minimal associated prime ideal of H. Localizing at $\mathfrak{p}$ we may assume that $\mathfrak{p}$ is the unique maximal ideal of R, and that $\operatorname{depth} R \geq n - r$. Since $n \geq 2$, and using the depth lemma repeatedly we obtain that $\operatorname{depth} B \geq 2$, $\operatorname{depth} Z \geq 2$ and therefore $\operatorname{depth} H > 0$, which contradicts the choice of $\mathfrak{p}$. $\square$

Syzygy Theorems

The bounds for projective dimensions arise from the fact that the depths of the ideals of maximal minors of the matrices in the complex increase:

$$0 \to F_m \to \cdots \to F_1 \to F_0 \to M \to 0$$

Outline

Regular Local Rings

Let **R** be a Noetherian local ring of maximal ideal $\mathfrak{m}$. By Krull's PIT, the minimal number of generators of $\mathfrak{m}$ is at least the Krull dimension of **R**.

Definition

R is a regular local ring if

$$\nu(\mathfrak{m}) = \dim \mathbf{R}.$$

- If $\dim \mathbf{R} = 0$, **R** is a field.
- If $\dim \mathbf{R} = 1$, $\mathfrak{m} = (x)$ contains properly some minimal prime ideal $\mathfrak{p}$. Thus for $u \in \mathfrak{p}$, $u = rx$, so $r \in \mathfrak{p}$. Therefore

$$\mathfrak{p} = x\mathfrak{p},$$

so $\mathfrak{p} = 0$ by Nakayama Lemma, that is **R** is a domain, more precisely a PID.

Regular Local Rings

- If $\dim \mathbf{R} = n$, $\mathfrak{m} = (x_1, \ldots, x_n)$, the local ring $\overline{\mathbf{R}} = \mathbf{R}/(x_1)$ has dimension most $n-1$ by Krull's PIT, but it cannot have dimension $< n-1$ as this would imply that $\mathfrak{m}/(x_1)$ would be a minimal prime of an deal generated by fewer that $n-1$ elements, $(\overline{y_1}, \ldots, \overline{y_r})$, $r < n-1$, and $\mathfrak{m}$ would be minimal over $(x_1, y_1, \ldots, y_r)$, contradicting Krull's.
- We have that $\mathbf{R} = \mathbf{R}/(x_1)$ is a regular local ring, and by induction it is a domain. If we choose the x_i not belonging to a minimal prime, (x_1) is a non minimal prime ideal.
- Use the argument of the case $\dim \mathbf{R} = 1$ to show that $\mathbf{R}$ is an integral domain.

Regular Local Rings

Theorem

If $\mathbf{R}$ *is a regular local ring of dimension* n *and* $\mathfrak{m} = (x_1, \ldots, x_n)$*, then* $\mathbf{x} = \{x_1, \ldots, x_n\}$ *is a regular sequence. In particular, the Koszul complex of* $\mathbf{x}$ *is a free resolution of the residue field* $\mathbf{R}/\mathfrak{m}$*,*

$$\mathbb{K}(\mathbf{x}) \to \mathbf{R}/\mathfrak{m}.$$

Example

$\mathbf{R} = k[[x_1, \ldots, x_n]]$, ring of formal power series in n variables.

Prime Avoidance

Proposition

Let R be a commutative ring. Let I be an ideal of a ring R and suppose that it is contained in the set theoretic union of a finite collection of ideals I_i

$$I \subset \bigcup_{i=1}^{s} I_i.$$

Then I is contained in one of these ideals in the following two cases:

1. *The I_i are prime ideals for all but at most 2 i's;*
2. *R contains an infinite field k.*

Proof

(1): We may assume that I is not contained in the union of fewer than s of the I_i. We argue by contradiction.

If $s = 2$, picking $a \in I \setminus I_1 \subset I_2$ and $b \in I \setminus I_2 \subset I_1$ then $a + b$ cannot be contained in either I_1 or I_2. Assume $s > 2$ and I_s is prime. Let $a \in I \setminus I_1 \cup \cdots \cup I_{s-1} \subset I_s$ and pick $b \in I \cdot I_1 \cdots I_{s-1} \setminus I_s$. Then $a + b$ cannot lie in any I_i.

(2) The case $s = 2$ being trivial, suppose $s > 2$ and assume I is not contained in the union of fewer I_i. This means that for every $t = 1, \ldots, s$, we can find

$$a_t \in I_t \setminus \bigcup_{i \neq t} I_i.$$

Consider, for each $c \in k$, a linear combination

$$b = a_1 + ca_2 + \cdots + c^{s-1} a_s = \sum_{t=1}^{s} c^{t-1} a_t.$$

Since k is infinite, we can find s different elements $c_1, \ldots, c_s \in k$ such that the corresponding $b_1, \ldots, b_s$ belong to the same subset, say, I_1. But I_1 is a k–vector space so that any linear combination of the b_t will belong to it; moreover the matrix

$$\begin{bmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^{s-1} \\ 1 & c_2 & c_2^2 & \cdots & c_2^{s-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_s & c_s^2 & \cdots & c_s^{s-1} \end{bmatrix}$$

has determinant different from zero (it is a Vandermonde determinant). Thus I_1 contains $a_1, \ldots, a_s$, contradicting the choice of the a_t's. □

Regular Local Rings: Homological Characterization

Theorem

Let $(\mathbf{R}, \mathfrak{m})$ *be a Noetherian local ring. The following conditions are equivalent:*

1. $\mathbf{R}$ *is a regular local ring;*
2. $\text{proj. dim.}_{\mathbf{R}}(\mathbf{R}/\mathfrak{m}) < \infty$*;*
3. *Every* $\mathbf{R}$*-module has finite projective dimension.*

Proof. (1) $\Rightarrow$ (2): If $\dim \mathbf{R} = n$, $\mathfrak{m} = (x_1, \ldots, x_n)$ we argued above that the x_i form a regular sequence. Thus the Koszul complex of the x_i gives a projective resolution of $\mathbf{R}/\mathfrak{m}$.

Regular Local Rings: Homological Characterization

(2) $\Rightarrow$ (3): Let $\text{proj. dim. }_{\mathbf{R}}(\mathbf{R}/\mathfrak{m}) = n$. Then

$$\text{Tor}_{n+1}^{\mathbf{R}}(\mathbf{R}/\mathfrak{m}, M) = 0$$

for any $\mathbf{R}$-module. This implies that if

$$0 \to K \to F_n \to \cdots \to F_0 \to M \to 0$$

is a minimal free presentation of M,

$$\text{Tor}_{n+1}(M, \mathbf{R}/\mathfrak{m}) = K/\mathfrak{m}K = 0$$

so $\text{proj dim }_{\mathbf{R}} M < n + 1$.

(3) $\Rightarrow$ (1): Suppose all f.g. **R**-modules has projective dimension at most n (and n is reached).

- Since we may assume $n > 0$, by McCoy's Theorem it follows that $\mathfrak{m}$ does not consists of zero divisors, that is $0 : \mathfrak{m} = 0$.
- Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be the associated prime ideals of **R**. Since $\mathfrak{p}_i \neq \mathfrak{m}$ for each i,

$$\mathfrak{m} \not\subset \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_m.$$

- By prime avoidance, there exists $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ that is not a zero divisor.

Regular Local Rings: Homological Characterization

- Choose a minimal set of generators of $\mathfrak{m}$, $\mathfrak{m} = (x_1, \ldots, x_n)$, $x_1 = x$.
- Set $I = (x_1\mathfrak{m}, x_2, \ldots, x_n)$ note

$$\mathfrak{m} = I + (x_1), \quad I \cap (x_1) = x_1\mathfrak{m}.$$

- This gives

$$\mathfrak{m}/x_1\mathfrak{m} = I/x_1\mathfrak{m} \oplus (x_1)/x_1\mathfrak{m} \simeq I/x_1\mathfrak{m} \oplus \mathbf{R}/\mathfrak{m}.$$

Regular Local Rings: Homological Characterization

- Let
$$0 \to F_m \to \cdots \to F_1 \to F_0 \to \mathfrak{m} \to 0$$
be a $\mathbf{R}$-projective resolution of $\mathfrak{m}$. Since x_1 is a regular element, tensoring with $\overline{\mathbf{R}} = \mathbf{R}/(x_1)$ gives a $\overline{\mathbf{R}}$-projective resolution of $\mathfrak{m}/x_1\mathfrak{m}$.
- Since $\mathbf{R}/\mathfrak{m}$ is a direct summand of $\mathfrak{m}/x_1\mathfrak{m}$, $\mathbf{R}/\mathfrak{m}$ has finite projective dimension over $\mathbf{R}/(x_1)$.
- By induction on the dimension, $\mathbf{R}/(x_1)$ is a regular local ring. It follows that $\mathbf{R}$ is also a regular local ring.

Localization of Regular Local Rings

Corollary

Let $\mathbf{R}$ *be a regular local ring and* $\mathfrak{p}$ *a prime ideal. Then* $\mathbf{R}_{\mathfrak{p}}$ *is a regular local ring.*

Proof.

Let

$$0 \to F_m \to \cdots \to F_1 \to F_0 \to \mathbf{R}/\mathfrak{p} \to 0$$

be a finite $\mathbf{R}$-resolution of $\mathbf{R}/\mathfrak{p}$. Localizing the complex at $\mathfrak{p}$ gives a free $\mathbf{R}_{\mathfrak{p}}$-resolution of $(\mathbf{R}/\mathfrak{p})_{\mathfrak{p}}$. But the latter is the residue field of $\mathbf{R}_{\mathfrak{p}}$. Now use the homological characterization of RLR . □

Corollary

Let k be a field and $\mathbf{A} = k[x_1, \ldots, x_n]$ be a ring of polynomials. For any prime ideal $\mathfrak{m}$ of $\mathbf{A}$, the localization $\mathbf{R} = \mathbf{A}_{\mathfrak{m}}$ is a RLR.

Proof. By the Hilbert Syzygy Theorem, every **A**-module has a finite free resolution. Let M be an **R**-module. M is also an **A**-module, so has a finite **A**-projective resolution

$$0 \to P_n \to \cdots \to P_0 \to M \to 0$$

Localizing at $\mathfrak{m}$ we get an **R**-projective resolution

$$0 \to P_n \otimes \mathbf{R} \to P_0 \otimes \mathbf{R} \to \cdots \to M \otimes \mathbf{R} = M \to 0$$

Jacobian Criterion

Example

Let $\mathbf{A} = \mathbb{C}[x_1, \ldots, x_n]/(\mathbf{f}(\mathbf{x}))$ be a hypersurface ring. If P is a prime ideal of $\mathbf{A}$, then $\mathbf{R} = \mathbf{A}_P$ is a regular local ring iff

$$(\mathbf{f}(\mathbf{x}), \frac{\partial \mathbf{f}}{\partial x_1}, \ldots, \frac{\partial \mathbf{f}}{\partial x_n}) \not\subset P.$$

Factoriality of Regular Local Rings

Theorem

Regular local rings are factorial.

We are going to make use the following observation:

Lemma

A Noetherian integral domain **R** *is factorial iff every nonzero prime ideal contains a nonzero prime element. More explicitly, every prime ideal* $\mathfrak{p}$ *of height one is principal.*

Proof. Noetherianess implies that every non-unit a has a decomposition

$$a = a_1 \cdot \cdots \cdot a_n$$

where the a_i are irreducible. For each i, by Krull's PIT, every minimal prime of (a_i) is of height 1, so pincipal by assumption, $(a_i) \subset \mathfrak{p}_i = (d_i)$. Thus $a_i = r_i d_i$, and r_i must be a unit.

Proof of Factoriality of RLR

Let $\mathbf{R}$ be a regular local ring of dimension n. If $n = 1$, the maximal ideal $\mathfrak{m}$ of $\mathbf{R}$ is principal, so $\mathbf{R}$ is a PID.

- Suppose $n > 1$. Let $\mathfrak{m} = (x_1, \ldots, x_n)$. Set $s = x_1$, we have seen that $\overline{\mathbf{R}} = \mathbf{R}/(s)$ is a RLR, in particular s is a prime element.
- $\mathfrak{p}$ be a prime ideal of height 1. To prove $\mathbf{R}$ is factorial we must show that all such ideals are principal.
- Let

$$0 \to F_m \to \cdots \to F_1 \to F_0 \to \mathfrak{p} \to 0$$

be a free resolution of $\mathfrak{p}$. Consider the ideal $\mathfrak{p}_s$ of the localization $\mathbf{R}_s$.

- Observe that every localization $\mathbf{R}_Q$ of $\mathbf{R}_s$ at one of its primes gives rise to a RLR of dimension $< n$, and therefore the prime ideal $\mathfrak{p}\mathbf{R}_S$ is principal. This means that the ideal $\mathfrak{p}_s$ is a projective $\mathbf{R}_s$-module.
- Localizing the free $\mathbf{R}$-resolution of $\mathfrak{p}$, gives an exact complex of pojective modules, so it splits completely

$$\mathfrak{p}_s \oplus F_1' \oplus F_3' \oplus \cdots \simeq F_0' \oplus F_2' \oplus \cdots$$

where $F_i' = (F_i)_s$. Thus we have

$$\mathfrak{p}_s \oplus M \simeq N$$

where M and N are free $\mathbf{R}_s$-modules of ranks $r-1$ and r, for some integer r.

Lemma

Let I be an ideal of the integral domain $\mathbf{A}$ with $I \oplus \mathbf{A}^{r-1} \simeq \mathbf{A}^r$. Then $I \simeq \mathbf{A}$, that is I is pincipal.

Proof. Taking the r-th exterior power of the isomorphim of modules, we have

$$\mathbf{A} = \wedge^r \mathbf{A}^r \simeq \bigoplus_{i+j=r} \wedge^i I \otimes \wedge^j \mathbf{A}^j.$$

Since I is projective thus local principal. This implies that $\wedge^i I$ is locally trivial for $i > 1$. Therefore $\mathbf{A} \simeq I$. □

End of Proof

- We claim that $\mathfrak{p}$ is a principal ideal. We have that $\mathfrak{p} \neq (s)$ and that $\mathfrak{p}_s = (a)\mathbf{R}_s$.
- In picking the generator a of $\mathfrak{p}_s$ we may assume $a \in \mathbf{R}$. a could be of the form $a = bs$ so that $\mathfrak{p} = b\mathbf{R}_s$ also. However this cannot go on indefinitly since by Krull's Intersection Theorem, $\bigcap(s^r) = 0$.
- Thus assume $\mathfrak{p}_s = a\mathbf{R}_s$, $a \notin (s)$. We claim $\mathfrak{p} = (a)$. Let $c \in \mathfrak{p}$. Then for some intger r, $s^r c \in (a)$,

$$s^r c = da,$$

which implies $s|d$, so we can remove a factor of s from the equation. And so on.,

Outline

Cohen-Macaulay Rings and Modules

Cohen–Macaulay rings are arguably the most important class of Noetherian rings. The terminology honors I. S. Cohen (1917-1955) and F. S. Macaulay (1862-1937). It includes the class of all regular rings, such as rings of polynomials over a field or the integers, rings of formal powers series over fields and convergent power series. They are a meeting ground for algebraic, analytic and geometric techniques.

Most Cohen–Macaulay rings however are “singular”, which rules out many geometric-analytic approaches but not wild enough to forbid them all. It may be said that their singularities are regular. Their significance arose also from the fact that they turn out in the solution of many important problems, such as the classical rings of invariants of reductive groups.

But what is a Cohen–Macaulay ring? The spirit of the answer to this question, paraphrasing Mel Hochster, is that they provide a setting for proving interesting and difficult results.
Before we give the technical definition, let us give an indication, in the setting of affine domains, of what those rings are like. Let A be an affine domain over a field k, and let $R = k[z_1, \ldots, z_d]$ be one of its Noether normalizations. Then A is Cohen–Macaulay if and only if A is a free module over the polynomial ring R. Note how this permits, in analogy with the study of rings of integers of number fields, the introduction of many constructions–ramification locus, differents—that reflect how (or how many) of the primes of A (in other words, the points of the associated variety) lie over the primes of R (that is, of the points of affine space).

Outline

the Main Rings

- Regular local rings
- Complete intersections
- Cohen–Macaulay rings
- Gorenstein rings
- Canonical modules
- Duality

Regular Local Rings

Let **R** be a Noetherian local ring of maximal ideal $\mathfrak{m}$. By Krull's PIT, the minimal number of generators of $\mathfrak{m}$ is at least the Krull dimension of **R**.

Definition

R is a regular local ring if

$$\nu(\mathfrak{m}) = \dim \mathbf{R}.$$

Main Results

Theorem

Let $(\mathbf{R}, \mathfrak{m})$ *be a Noetherian local ring. The following conditions are equivalent:*

1. $\mathbf{R}$ *is a regular local ring;*
2. $\text{proj. dim.}_{\mathbf{R}}(\mathbf{R}/\mathfrak{m}) < \infty$*;*
3. *Every* $\mathbf{R}$*-module has finite projective dimension.*

Theorem

Localizations of regular local rings are regular local rings.

Theorem

Regular local rings are factorial.

Complete Intersection

Definition

A local complete intersection is a ring isomorphic to $\mathbf{R}/(\mathbf{x}_1, \ldots, \mathbf{x}_r)$, with $\mathbf{R}$ a regular local ring and the $\mathbf{x}_i$ forming a regular sequence. If $r = 1$, $\mathbf{R}/(\mathbf{x}_1)$ is called a hypersurface ring.

Cohen–Macaulay Rings

Recall two concepts:

- height of an ideal I: the length of the shortest sequence of elements $x_1, \ldots, x_n$ of I such that I is contained in a minimal prime of $(x_1, \ldots, x_n)$.
- grade of an ideal I: the length of the longest sequence of elements $x_1, \ldots, x_n$ of I forming a regular sequence.

Definition

A Noetherian ring R is *Cohen–Macaulay* if $\operatorname{height} I = \operatorname{grade} I$ for each ideal.

Example

Let $\mathbf{R} = k[x_1, \ldots, x_d]$ be a ring of polynomials and let $\mathbf{G}$ be a finite group of k-automorphisms of $\mathbf{R}$.

- Let
$$\mathbf{S} = \mathbf{R}^{\mathbf{G}} = \{f \in \mathbf{R} : \sigma(f) = f, \quad \sigma \in \mathbf{G}\}$$
- $\mathbf{S}$ is the ring of $\mathbf{G}$-invariants of $\mathbf{R}$. It has many interesting properties.

Proposition

S *is a Noetherian subring of* $k[x_1, \ldots, x_d]$.

Proof.

- For each $f \in \mathbf{R}$, the coefficients of the polynomial

$$\prod_{\sigma \in \mathbf{G}} (t - \sigma(f))$$

  belong to **S**. These are the elementary symmetric functions of f.
- Consider the subring of **S** generated by the elementary symmetric functions of all x_i.
- $\mathbf{S}_0$ is Noetherian and **R** is integral over it. It follows that **R** is a f.g. $\mathbf{S}_0$-module. Since **S** is an $\mathbf{S}_0$-submodule of **R**, it is Noetherian.

Proposition

If the characteristic of k does not divide $|\mathbf{G}|$, $\mathbf{S}$ *is a Cohen-Macaulay ring.*

Proof.

- The mapping $\mathbf{R} \to \mathbf{S}$ given

$$f \to 1/|\mathbf{G}| \sum_{\sigma \in \mathbf{G}} \sigma(f)$$

  is a surjective homomorphism of $\mathbf{S}$-modules
- This gives an splitting of f.g. $\mathbf{S}$-modules, $\mathbf{R} = \mathbf{S} \oplus L$.
- Any ideal of $\mathbf{S}$ generated by a system of parameters $f_1, \ldots, f_d$, the f_i are also a system of parameters of $\mathbf{R}$ since $\mathbf{R}$ is integral over $\mathbf{S}$. Thus the f_i form a regular sequence in $\mathbf{R}$, and therefore they are a regular sequence on any summand of $\mathbf{R}$.

A calculation of Koszul complexes

Let $I = (\mathbf{x}) = (x_1, \ldots, x_n)$ be an ideal and M a nonzero $\mathbf{R}$-module. For simplicity suppose $\mathbf{R}$ is a local ring so that we don't have to worry about $M/IM \neq 0$ in calculation of I-depth of M.

Proposition

(I, y)–depth $M \leq 1 + I$–depth M.

Proof. We use the expression of depth in terms of the vanishing of Koszul complexes. Recall that if $\mathbb{K} = \mathbb{K}(\mathbf{x}; M)$ then I-depth M is q if $H_{n-q}(\mathbb{K})$ is the last nonvanishing homology module.

Let $\mathbb{K}' = \mathbb{K}(\mathbf{x}; M) \otimes \mathbb{K}(y)$. This is the Koszul complex of $\mathbf{x}, y$.

Proposition

Let $\mathbb{K}$ 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 $s \geq 0$ there is an exact sequence

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

Applying this Proposition to $\mathbb{K}' = \mathbb{K}(\mathbf{x}, y; M)$, it will follow that the last nonvanihing homology module has either the same index as that of $\mathbb{K}$, or one less. Thus the (I, y)–depth of M is at most 1 plus I-depth M.

Proposition

Let R be a Noetherian ring. If $\operatorname{height} \mathfrak{m} = \operatorname{grade} \mathfrak{m}$ *for each maximal ideal, then R is Cohen–Macaulay. In particular, if R is a local ring, it suffices to test this equation for the maximal ideal.*

Proof. If $\mathfrak{p}$ is maximal among the prime ideals with $\operatorname{height} \mathfrak{p} > \operatorname{grade} \mathfrak{p}$, let $\mathfrak{p} \subset \mathfrak{m} = \text{maximal ideal}$; we may assume that R is local (why?). Let $x \in \mathfrak{m} \setminus \mathfrak{p}$; then $\operatorname{grade}(\mathfrak{p}, x) \leq 1 + \operatorname{grade} \mathfrak{p}$ by the Proposition above, while $\operatorname{height}(\mathfrak{p}, x) \geq 1 + \operatorname{height} \mathfrak{p}$, thus contradicting $\operatorname{height}(\mathfrak{p}, x) = \operatorname{grade}(\mathfrak{p}, x)$. □

Corollary

Let $\mathfrak{p} \subset \mathfrak{q}$ be immediate primes (i.e. no other prime in–between) in a Cohen–Macaulay ring R. Then $\operatorname{height} \mathfrak{q} = 1 + \operatorname{height} \mathfrak{p}$. In particular, all saturated chains of prime ideals between two fixed primes have the same length.

Remark

Let R be a Cohen–Macaulay ring. If S is a multiplicative set (resp. x is a regular element) of R, then $S^{-1}R$ (resp. $R/(x)$) is also Cohen–Macaulay. The power series ring $R[[t]]$ is Cohen–Macaulay as t lies in the Jacobson radical.

As for the ring of polynomials $R[t]$, the situation is more interesting.

- Let $\mathfrak{m}$ be a maximal ideal of $R[t]$ and localize at $\mathfrak{p} = \mathfrak{m} \cap R$, in other words, we may assume that R is local and $\mathfrak{m}$ contracts to the maximal ideal of R.
- Then $\mathfrak{m} = (\mathfrak{p}, f)$, where f may be taken to be a nonzero monic polynomial and $\operatorname{height} \mathfrak{m} = 1 + \operatorname{height} \mathfrak{p}$.
- Finally, note that $\mathfrak{p}\text{–depth } R = \mathfrak{p}\text{–depth } R[t]/(f)$, since $R[t]/(f)$ is a free R–module.

Macaulay Theorem

Corollary (Macaulay Theorem)

Let k be a field and let $I = (f_1, \ldots, f_m) \subset k[x_1, \ldots, x_n]$ be an ideal of codimension m. Then every primary component of I has codimension m.

It follows from the properties of the Koszul complex that the grade of a maximal ideal $\mathfrak{m}$ (but not for an arbitrary prime ideal) is the depth of the local ring $R_{\mathfrak{m}}$. Thus the notion of a Cohen–Macaulay ring is a local property. We use this fact to justify the definition of a Cohen–Macaulay module M: For each maximal ideal (resp. for each prime ideal) $\mathfrak{m}$,
$\mathfrak{m}\text{–depth } M_{\mathfrak{m}} = \dim M_{\mathfrak{m}}$.

This permits giving a description of an affine Cohen–Macaulay ring A in module-theoretic terms.

Theorem

Let A be an affine algebra and let $k[\mathbf{z}] = k[z_1, \ldots, z_d] \hookrightarrow A$ be a Noether normalization. If A is equidimensional then A is a Cohen–Macaulay ring if and only if A is a free $k[\mathbf{z}]$–module.

Proof.

- For any maximal ideal $\mathfrak{p}$ of $k[\mathbf{z}]$, $\dim A_{\mathfrak{p}} = d$. For A to be Cohen–Macaulay as a ring amounts to say that it is Cohen–Macaulay as a $k[\mathbf{z}]$–module.
- But $k[\mathbf{z}]$ is a ring of global dimension d, and we can apply the Auslander-Buchsbaum equality to have that $A_{\mathfrak{p}}$ is a free $k[\mathbf{z}]_{\mathfrak{p}}$–module and thus A is a projective $k[\mathbf{z}]$–module (necessarily free by the theorem of Quillen–Suslin). □

In general, a Cohen–Macaulay affine ring A will break up into a direct product of affine rings, $A = A_1 \times \cdots \times A_r$, each of which is equi–dimensional.

Example

The finiteness of the projective dimension of a ring over another may come in very restrictive form. Here is one instance (whose converse will not always hold). Let A be an affine algebra over a field k and consider the sequence

$$0 \to \mathbb{D} \longrightarrow A^e = A \otimes_k A \longrightarrow A \to 0,\ x \otimes y \mapsto xy.$$

Then if the projective dimension of A over A^e is finite then A is Cohen–Macaulay. We can work with a localization of A; assume $\dim A = d$ and $\operatorname{depth} A = c$. Then $\operatorname{depth} A^e = 2c$. If $\operatorname{proj\,dim}_{A^e}(A)$ is finite it is at least d since $\mathbb{D}$ has height d. From the Auslander–Buchsbaum equality we have $d + c \leq 2c$, and therefore $d = c$.

Hilbert–Burch Theorem.

Let M be a finitely generated module over a Noetherian ring R. Suppose M has a projective resolution

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

If $m = n$ or M is a torsionfree R–module, the maximal minors of φ play decisive roles in the structure of M. We consider the elementary but important general description of ideals of projective dimension one.

Theorem (Hilbert–Burch)

Let $I = (a_1, \ldots, a_n)$ be an ideal of a Noetherian ring R with a free resolution of length one,

$$0 \to R^{n-1} \xrightarrow{\varphi} R^n \longrightarrow I \to 0.$$

There exists a regular element d of R such that $I = d \cdot \Delta$,

Proof. A sketch of the proof goes as follows. First, that I contains regular elements and Δ has grade two follow easily from formula of Auslander-Buchsbaum. Assume the ith basis element of R^n maps to a_i. Let

$$\varphi = \begin{bmatrix} a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n-1} \end{bmatrix}$$

be a matrix representation of φ, and denote by $\Delta_i = (-1)^i \det \varphi_i$ the signed determinant of the submatrix φ_i obtained by deleting the ith row of φ. Since

$$(a_1, \cdots, a_n) \cdot \varphi = 0, \quad \text{for } 1 \leq i < j \leq n,$$

it follows that

$$a_i \cdot \Delta_j = a_j \cdot \Delta_i.$$

These equations give an isomorphism between $(a_1, \ldots, a_n)$ and $(\Delta_1, \ldots, \Delta_n)$. □

Cohen–Macaulay Modules

There is also a notion of Cohen–Macaulay module which in fairness must be independent of the base ring.

Definition

A finitely generated R–module M is *Cohen–Macaulay* if

$$I\text{–depth } M = \text{height } (I/J)$$

for every ideal $I \supset J = \text{annihilator } M$.

For the purpose of this definition, we may as well assume that M is a faithful R–module. This definition is easier to manage when R is a local ring, or R is a graded ring and M is a graded module. (We only state the local version.)

Definition

Let M be a finitely generated module over a local ring $(R, \mathfrak{m})$. A system of parameters is a set $\mathbf{x} = \{x_1, \ldots, x_d\}$ of elements in $\mathfrak{m}$, $d = \dim M$, such that $\ell(M/(\mathbf{x})M) < \infty$.

These sets are often obtained by taking general linear combinations of the generators of $\mathfrak{m}$. It is useful in the following well-used test of the Cohen–Macaulay property.

Theorem

Let $(R, \mathfrak{m})$ be a Noetherian local ring, M a finitely generated R–module of positive rank, and $(\mathbf{x})$ an ideal generated by a system of parameters of R. Then M is Cohen–Macaulay if and only if $\ell(M/(\mathbf{x})M) = e(\mathbf{x}, R) \cdot \operatorname{rank} M$.

Here $e(\mathbf{x}, R)$ is the multiplicity of the ideal $(\mathbf{x})$. If R is a Cohen–Macaulay ring this is simply $\ell(R/(\mathbf{x}))$. The other notion, of the rank of a module, is defined in terms of the module $M \otimes_R K$, where K is the total ring of fractions of R. Thus, M has rank n if $M \otimes_R K \simeq K^n$; in particular, if R is a domain then every module has a rank.

Depth and Hyperplane Sections

We describe a useful aspect of the relation between the depth of a module E and the depth of the modules E/xE for families of elements x.

Proposition

Let $(R, \mathfrak{m})$ be a Noetherian local ring with infinite residue field, of Krull dimension d, let E be a finitely generated R–module and let s be an integer $s < d$. Suppose that for each subset $x_1, \ldots, x_s$ of a system of parameters of R contained in $\mathfrak{m} \setminus \mathfrak{m}^2$,

$$\operatorname{depth} E/(x_1, \ldots, x_s)E \geq 1.$$

Then $\operatorname{depth} E \geq s + 1$. In particular if $s = d - 1$ then E is Cohen–Macaulay.

Proof. We look at the case $s = 1$. If $\operatorname{depth} E > 0$, we choose $x_1 \in \mathfrak{m} \setminus \mathfrak{m}^2$ which is regular on E. The assertion is then clear. (The assumption that $R/\mathfrak{m}$ is infinite allows for the choice of x_1.)

Suppose then that $\mathfrak{m}$ is an associated prime of E. Denote by E_0 the submodule of E with support in $\mathfrak{m}$, that is, E_0 is the subset of elements of E annihilated by some power of $\mathfrak{m}$. This implies that in the exact sequence

$$0 \to E_0 \longrightarrow E \longrightarrow F \to 0,$$

the module F has positive depth. Let x_1 be a minimal parameter that is regular on F. Tensoring the exact sequence by $R/(x_1)$ (or using the kernel-cokernel sequence induced by multiplication by x_1) we obtain the exact sequence

$$0 \to E_0/x_1E_0 \longrightarrow E/x_1E \longrightarrow F/x_1F \to 0.$$

However, by assumption the module E/x_1E has positive depth so cannot contain a nonzero module, to wit E_0/x_1E_0, supported on $\mathfrak{m}$, so that by Nakayama lemma $E_0 = 0$. The general case follows by using descending induction on the module $E/(x_1, \ldots, x_{s-1})E$. $\square$

Perfect Ideals

The following isolates an important class of Cohen–Macaulay rings which are quotients of a given Cohen–Macaulay ring.

Definition

Let R be a Cohen–Macaulay local ring and let I be an ideal with finite projective dimension. By the Auslander-Buchsbaum Formula,

$$\dim R/I \geq \operatorname{depth} R/I \quad = \quad \dim R - \operatorname{proj\,dim}_R R/I.$$

In the case of equality, R/I is a Cohen–Macaulay ring. The ideal I is then said to be *perfect*.

This means that there is a free resolution

$$0 \to F_r \longrightarrow F_{r-1} \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 = R \longrightarrow R/I \to 0, \quad (3)$$

where $r = \operatorname{codim} I$.

An example ($r = 2$) is given by the Hilbert-Burch Theorem in the case of an $n \times (n-1)$ matrix whose maximal minors generate an ideal of height two.

It is a property of a perfect ideal I that if the resolution is dualized with respect to $\mathrm{Hom}_R(\cdot, R)$, the new complex is a resolution of the r–dimensional cohomology

$$0 \to F_0^* \longrightarrow F_1^* \longrightarrow \cdots \longrightarrow F_{r-1}^* \longrightarrow F_r^* \longrightarrow \mathrm{Ext}_R^r(R/I, R) \to 0. \quad (4)$$

Conversely, the ring R/I can be recovered from $\mathrm{Ext}_R^r(R/I, R)$:

$$R/I = \mathrm{Ext}_R^r(\mathrm{Ext}_R^r(R/I, R), R).$$

Gorenstein Rings

If $(A, \mathfrak{m})$ is an Artinian local ring which is a finite algebra over a field k, the dual vector space $A^* = \mathrm{Hom}_k(A, k)$ has a natural structure of an A–module: If $f \in A^*, r \in A$, then $(r \cdot f)(x) = f(rx)$. A^* is an injective A–module since

$$\mathrm{Hom}_A(E, A^*) = \mathrm{Hom}_k(E, k).$$

It is easy to see that A^* is the injective envelope of $A/\mathfrak{m}$. The condition that A be Gorenstein is then: $A^* \simeq A$, that is, A^* is generated by a single element. It is easy to describe the generator of A^*, being enough to pick $f \in A^*$ which does not vanish on the one-dimensional subspace $0 :_A \mathfrak{m}$ (the socle of A).

Example

Let k be a field and G an abelian group. Set $\mathbf{R} = k[G]$ the group ring over k. $\mathbf{R}$ is an injective module over itself. Check

$$\mathbf{R} \simeq \mathrm{Hom}_k(\mathbf{R}, k).$$

This isomorphism says that

$$\begin{aligned} \mathrm{Hom}_{\mathbf{R}}(M, \mathbf{R}) &\simeq \mathrm{Hom}_{\mathbf{R}}(M, \mathrm{Hom}_k(\mathbf{R}, k)) \simeq \mathrm{Hom}_k(M \otimes_{\mathbf{R}} \mathbf{R}, k) \\ &\simeq \mathrm{Hom}_k(M, k) \end{aligned}$$

Thus the functor $\mathrm{Hom}_{\mathbf{R}}(\cdot, \mathbf{R})$ is exact since $\mathrm{Hom}_k(\cdot, k)$ is so.

Definition

Let R be a regular local ring or a polynomial ring over a field k. A perfect ideal I of codimension r is called a *Gorenstein ideal* if

$$R/I \simeq \operatorname{Ext}^r_R(R/I, R).$$

The significance of this definition in terms of the resolution is the following. If R is a local ring or R is a graded ring and I is a homogeneous ideal, the modules F_i in a minimal resolution of R/I are essentially unique. Thus for a Gorenstein ideal I the modules F_i must satisfy

$$F_i \simeq F_{r-i}, \ \forall i.$$

(In the graded case this is only true after a uniform shift in the grading of the F_i's.)

Example

The premier example of a Gorenstein ring is a complete intersection: If R is a regular local ring and $\mathbf{f} = f_1, \ldots, f_m$ is a regular sequence, then $A = R/(\mathbf{f})$ is a Gorenstein ring.

On the other hand, $I = (x^3, y^3, z^4, xy^2 - xz^2, x^2z^2 - y^2z^2)$ is a Gorenstein ideal but not a complete intersection.

There are many other ways in which Gorenstein rings arise without being complete intersections. For example, let A be a finite dimensional k–algebra and denote $A^* = \mathrm{Hom}_k(A, k)$. Then the idealization of A^*,

$$B = A \oplus A^*,$$

is a Gorenstein ring. We leave to the reader to prove this assertion and to establish when these algebras are complete intersections.

There is a general and intrinsic definition of Gorenstein ring or ideal.

Definition

A Noetherian local ring R is a *Gorenstein ring* if it has finite injective dimension as a module over itself.

Properties of Gorenstein Rings

Theorem

Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension d. Then

(a) *R is a Gorenstein ring if and only if R is Cohen–Macaulay and for one (any) system of parameters $\mathbf{x} = x_1, \ldots, x_d$,*

$$((\mathbf{x}) : \mathfrak{m})/(\mathbf{x}) \simeq R/\mathfrak{m}.$$

(b) *If R is a Gorenstein local ring and I is a Cohen-Macaulay ideal of codimension r, not necessarily perfect, then R/I is a Gorenstein ring if and only if*

$$\operatorname{Ext}^r_R(R/I, R) \simeq R/I.$$

Theorem (cont'd)

If R is a Gorenstein local ring,

(c) *the mapping*

$$M \mapsto \operatorname{Ext}^r_R(M, R)$$

is a self-dual functor on the category of finitely generated Cohen-Macaulay R-modules of codimension r. In particular, if $(R, \mathfrak{m})$ is a Cohen–Macaulay local ring of dimension 1, then it is Gorenstein if and only if the functor $\operatorname{Hom}_R(\cdot, R)$ is self–dual on the category of torsionfree R–modules.

The condition (c) is interesting because it tells how the ring R interacts with the category of modules, in words, it permits us to construct interesting functors. These properties are characteristic of Gorenstein rings. It was Grothendieck who realized that suitably modified, (c) will still hold for many Cohen-Macaulay local rings.

Gorenstein Ideals of Codimension 3

In addition to perfect, Cohen–Macaulay ideals of codimension two, which are completely described by the Hilbert-Burch Theorem, another family of perfect ideals has a beautiful determinantal description.

Let R be a Gorenstein local ring and let I be a perfect, Gorenstein ideal of codimension 3. This implies that the ideal $I = (a_1, \ldots, a_n)$ has a minimal free resolution,

$$0 \to R \xrightarrow{\psi} R^n \xrightarrow{\varphi} R^n \longrightarrow I \to 0, \tag{5}$$

in which the matrix representation of ψ is $[a_1, \ldots, a_n]$. In fact, the following holds:

Theorem (Buchsbaum–Eisenbud)

If I is as above, there exists a minimal resolution such that:

(a) *The mapping φ is skew–symmetric (i.e. has a matrix representation with this property), and*

(b) *I is the ideal $P_{n-1}(\varphi)$ generated by the Pfaffians of the submatrices obtained by deleting the ith row and column of φ, for $i = 1 \ldots n$.*

Conversely, if φ is skew–symmetric and $P_{n-1}(\varphi)$ has codimension 3 (its maximum value), then $P_{n-1}(\varphi)$ is a Gorenstein ideal. (In particular, n must be odd.)

The Canonical Module of a Local Ring or Graded Ring

Definition

Let R be a Gorenstein local ring and let I be an ideal of codimension r, defining the ring $A = R/I$. The module

$$\omega_A = \mathrm{Ext}^r_R(A, R). \tag{6}$$

is the *canonical module* of A.

In the case of a finite k–algebra A the canonical module is $\omega_A = A^* = \mathrm{Hom}_k(A, k)$. As the notation indicates, ω_A depends only on A, not especially on R and I. Its basic property is the following extension of Theorem 43(c).

Theorem

If A is a Cohen-Macaulay local ring with a canonical module ω_A, then the mapping

$$M \mapsto \mathrm{Ext}^r_A(M, \omega_A)$$

is a self-dual functor on the category of finitely generated Cohen-Macaulay A-modules of codimension r.

Remark

If $r = \operatorname{codim} I$, and $\mathbf{x} = x_1, \ldots, x_r$ is a regular sequence contained in I, then

$$\omega_A \simeq ((\mathbf{x}) : I)/(\mathbf{x}),$$

from the way these Ext's are calculated.

If A is Cohen-Macaulay, ω_A is a Cohen–Macaulay module of the same dimension as A. In general the canonical module of a ring A retains many of the most interesting properties of A, and quite often improves on them.

The case of graded rings is rich in numerical information. If $R = k[z_1, \ldots, z_d]$ is a ring of polynomials over a field k, graded in the usual manner, the canonical module is $R[-d]$, not R itself, to ensure naturality in the category of graded modules. (Sometimes the shift is ignored harmlessly.)
If A is a finitely generated algebra over a field k and $R = k[z_1, \ldots, z_d]$ is a Noether normalization, then

$$\omega_A = \mathrm{Hom}_R(A, R[-d]) \tag{7}$$

which extends the formula in the case of fields.

Suppose further that A is a graded ring, $A = A_0 + A_1 + \cdots$, and R is such that $z_i \in A_1$. If A is Cohen–Macaulay, A is a free R–module,

$$A \simeq \bigoplus_i R[-d_i],$$

so that

$$\omega_A = \mathrm{Hom}_R(A, R[-d]) \simeq \bigoplus_i R[d_i - d].$$

If

$$H_A(\mathbf{t}) = \frac{h_0 + h_1\mathbf{t} + \cdots + h_r\mathbf{t}^r}{(1-\mathbf{t})^d},\ h_r \neq 0,$$

is the Hilbert–Poincaré function of A, this representation of ω_A gives also

$$H_{\omega_A}(\mathbf{t}) = \frac{\sum_i \mathbf{t}^{d-d_i}}{(1-\mathbf{t})^d} = (1/\mathbf{t})^s \frac{h_r + h_{r-1}\mathbf{t} + \cdots + h_0\mathbf{t}^r}{(1-\mathbf{t})^d},\ s = \sup\{d_i\} - d.$$

Reading Depth

If A is a Cohen–Macaulay local ring with a canonical module ω_A, depths of modules can be expressed as follows.

Proposition

For any finitely generated A–module M,

$$\operatorname{depth} M \quad = \quad \dim A - \sup\{\, r \mid \operatorname{Ext}^r_A(M, \omega_A) \neq 0 \,\}.$$

Proof. The proof is immediate (but a pleasant calculation).

Exercises

Exercise (Peskine)

Let R be a local Cohen–Macaulay ring of Krull dimension $d > 0$, with a canonical module ω_R. Suppose that ω_R is isomorphic to an ideal of R (equivalently, suppose the total ring of fractions of R is a Gorenstein ring). Prove that $S = R/\omega_R$ is a Gorenstein ring of Krull dimension $d - 1$.

Exercise

Let R be a local Cohen–Macaulay ring and let $x_1, \ldots, x_n$ be a regular sequence. Prove that the ideal I generated by all products $x_{i_1} \cdots x_{i_k}$ of k distinct x_i is perfect.

Exercise

*Let R be a ring of polynomials and let I be a monomial ideal. Prove that if I is a Cohen–Macaulay ideal then its radical $\sqrt{I}$ is also Cohen–Macaulay (*Hint*: use polarization).*

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,

$$\mathbf{R}_n = (x_1, \ldots, x_d)^n$$

- 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.

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 $\dim_k M_n < \infty$.

Associated primes of graded modules

Proposition

If M is a finitely generated graded module then every associated prime ideal $\mathfrak{p}$ is homogeneous.

Proof. Let $\mathfrak{p} = 0 : x$ for some $x \in M$.

- If $x \in M_r$ for some r, and $\mathbf{a} = a_1 + \cdots + a_r$, $\deg(a_i)$ distinct, then $\mathbf{a}x = 0$ implies $a_i x = 0$ fo each a_i, that is $a_i \in \mathfrak{p}$. That is, $\mathfrak{p}$ is homogeeous.
- Suppose $x = x_1 + \cdots + x_s$, $\deg(x_i)$ distinct. Let us argue that $\mathfrak{p}$ is homogeneous by induction on the number of components of x. Let $\mathbf{a} = a_1 + \ldots + a_r \in \mathfrak{p}$. Assume $a_1 \notin \mathfrak{p}$. Since

$$\mathbf{a}x = a_1 x_1 + \text{higher degree terms} = 0,$$

$a_1 x_1 = 0$.

- Note that $x' = a_1 x \neq 0$, since $a_1 \notin 0 : x = \mathfrak{p}$.
- x' is shorter than x.
- If $rx'0 = 0$, $ra_1 \in \mathfrak{p}$, so $r \in \mathfrak{p}$. Thus

$$\mathfrak{p} = 0 : x'$$

so by induction $\mathfrak{p}$ is homogeneous.

Dimension of graded modules

Proposition

Let M be a finitely generated graded $\mathbf{R}$-module.

1. *There is a filtration of graded submodules*

$$M = M_n \supset M_{n-1} \supset \cdots \supset M_1 \supset M_0 = 0$$

   such $M_i/M_{i-1} \simeq \mathbf{R}/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is homogeneous.
2. *Every associated prime of M occurs as one of the $\mathfrak{p}_i$.*
3. *The minimal primes in the set $\{\mathfrak{p}_i\}$ are associated primes of M.*

Proof

Use induction on the set of graded submodules of M. Let L be maximal, Consider the exact sequence $0 \to L \to M \to N \to 0$.

If $L \neq M$, let $\mathfrak{p}$ be an associated prime of the graded module N, $\mathfrak{p} = 0 : x$, for some homogeneous element $x \in N$. Lift x to the homogeneous element $y \in M$ and consider $L' = (L, y)$. ETC

Hyperplane section

Let $\mathbf{R} = \bigoplus_{n \geq 0} \mathbf{R}_n$. The elements of $\mathbf{R}_n$ are called n-forms, while those of $\mathbf{R}_1$ are said to be hyperplanes.

Let M be a finitely generated graded $\mathbf{R}$-module. Let

$$\operatorname{Ass}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}.$$

We have seen that the $\mathfrak{p}_i$ are graded ideals.

Proposition

There is a form h not contained in any $\mathfrak{p}_i \neq \mathfrak{m}$. Moreover, if $\mathbf{R}_0$ is an infinite field, h can be chosen in $\mathbf{R}_1$.

Proof

Let us move a few frames forward.

Generic hyperplane section

Proposition

Let $h \in \mathbf{R}_+$ be a form that is not contained in any associated prime of M except possibly in the ideal $\mathfrak{m} = \mathbf{R}_+$. Then

$$L = \{x \in M : hx = 0\}$$

is an Artinian submodule of M, more precisely L is annihilated by some power of $\mathfrak{m}$.

Proof.

- Let $\mathfrak{p}$ be an associated prime of L. We claim that $\mathfrak{p} = \mathfrak{m}$.
- Since $h \in \mathfrak{p}$ and $\mathfrak{p}$ is also an associated prime of M, by the choice of h, $\mathfrak{p} = \mathfrak{m}$.

The remainder follows from the next observation:

Lemma

Let $\mathbf{R}$ *be a Noetherian ring and* M *a f.g.* $\mathbf{R}$*-module. If* $\operatorname{Ass}(M) = \{\mathfrak{p}\}$*, then the annihilator of* M *is* $\mathfrak{p}$*-primary, in particular* $\mathfrak{p}^n M = 0$ *for some integer.*

Proof. Let $M = \langle x_1, \ldots, x_n \rangle$ and $I = \operatorname{ann}(M)$. There is an embedding

$$0 \to \mathbf{R}/I \hookrightarrow M \oplus \cdots \oplus M,$$

$$\overline{1} \to (x_1, \ldots, x_n)$$

and thus $\operatorname{Ass}(\mathbf{R}/I) = \{\mathfrak{p}\}$.

In the proposition above, M is a f.g. over the Artinian ring $\mathbf{R}/\operatorname{ann}(M)$.

Prime Avoidance

Proposition

Let $A = A_0[A_1]$ be a Noetherian graded algebra over the local ring $(A_0, \mathfrak{m})$ with infinite residue field, generated by elements of degree 1. Let $P_1, \ldots, P_r$ be a family of homogeneous prime ideals that do not contain A_1. Then there exists $h \in A$ satisfying

$$h \in A_1 \setminus \mathfrak{m}A_1 \cup \bigcup_{i=1}^{r} P_i.$$

Furthermore, if the P_i's include all the associated primes of A that do not contain A_1 then $0 : (0 : hA)$ contains some power of A_+.

Another version: replace $\mathfrak{m}A_1$ by $A_2 + A_3 + \cdots$.

Proof

Denote by $C_1, \ldots, C_r$ the components of degree 1 of these homogeneous ideals. Consider the vector space $V = A_1/\mathfrak{m}A_1$ over the residue field $A_0/\mathfrak{m}$ and its subspaces $V_i = (C_i + \mathfrak{m}A_1)/\mathfrak{m}A_1$. By Nakayama lemma and the choices of the P_i's, $V_i \neq V$, $\forall i$. Since $A_0/\mathfrak{m}$ is infinite, it follows that

$$V \neq \bigcup_{i=1}^{r} V_i,$$

by any of the usual tricks.

(For example, let $e_1, \ldots, e_n$ be a basis V. Since each V_i is a proper subspace, it is contained in the locus of the linear polynomial $f_i(\mathbf{x}) = a_{i1}x_1 + \cdots + a_{in}x_n$. Then any point where

$$f(\mathbf{x}) = \prod_{i=1}^{r} f_i(\mathbf{x})$$

For the second assertion, choose then $h \in A_1$ whose image in V does not lie in any V_i. Let $\mathfrak{P}$ be a minimal prime of $0 : (0 : hA)$; it suffices to show that $A_+ \subset \mathfrak{P}$. (If h is a regular element, $0 : (0 : hA) = A$.)

Note that $\mathfrak{P}$ consists of zero divisors and contains h. This means that $\mathfrak{P}$ is an associated prime of A but distinct from any of the P_i, and therefore must contain A_+. $\square$

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 $\operatorname{coker} \mathbf{f} = N/\mathbf{f}(M) = C$ 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 $k_{n-1} - m_{n-1} + m_n - c_n = 0$.
- Info we assemble as

$$\begin{aligned} 0 &= \sum_n (k_{n-1} - m_{n-1} + m_n - c_n)\mathbf{t}^n \\ &= \mathbf{t}\sum_n k_{n-1}\mathbf{t}^{n-1} + \sum_n m_n\mathbf{t}^n - \mathbf{t}\sum_{n-1} m_{n-1}\mathbf{t}^{n-1} - \sum_n c_n\mathbf{t}^n \end{aligned}$$

- Which we solve for $\sum_n m_n\mathbf{t}^n$.

Rationality of the Hilbert Series

Theorem

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

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

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

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

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

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

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:

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

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

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

- 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.

Hilbert Polynomial

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

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

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 $n \geq s$

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

Recurrence

Observe that for $n > s = \deg \mathbf{h}_M(\mathbf{t})$, the coefficients a_n are related by the recurrence relation

$$c_0 a_n + c_1 a_{n-1} + \cdots + c_d a_{n-d} = 0$$

where the c_j are the coefficients of the expansion of $(1 - \mathbf{t})^d$.

Hilbert Polynomial

The Poincaré-Hilbert series of graded $\mathbf{R}$-module M,

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

can be written

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

where $\mathbf{h}_M(0) \neq 0$. We will also remove any $1-\mathbf{t}$ factor out of $\mathbf{h}_M(\mathbf{t})$, that is $\mathbf{h}_M(1) \neq 0$.

For our purpose here we assume $a = 0$. Now expand $\mathbf{h}_M(\mathbf{t})$–known as the **h**-polynomial of M–as

$$\mathbf{h}_M(\mathbf{t}) = \sum_{j=0}^{m} \frac{\mathbf{h}^j(1)}{j!}(\mathbf{t}-1)^j.$$

Hilbert Polynomial

Proposition

The Hilbert polynomial of M,

$$H_M(n) = \sum_{j=0}^{d-1} (-1)^j e_j(M) \binom{n+d-j-1}{d-j-1},$$

where $e_j(M)$ are integers given by

$$e_j(M) = \frac{\mathbf{h}_M^{(j)}(1)}{j!}.$$

If $H_M(n) \neq 0$, the coefficient $e_0(M) = \mathbf{h}_M(1) > 0$ and is called the multiplicity of M.

Proof

The assertion that $e_0(M) > 0$ follows since $H_M(n) = \dim M_n$ for all $n \gg 0$ and therefore its leading coefficient must be non-negative. The assertion that the $e_j(M)$ are integers is a consequence of the following elementary observation:

Lemma

Let $\mathbf{f}(x) \in \mathbf{Q}[x]$ *be polynomial such that* $\mathbf{f}(n) \in \mathbb{Z}$ *for* $n \in \mathbb{Z}$. *Writing* $\mathbf{f}(x)$ *in the basis*

$$\{p_j(x) = \binom{x}{j}, \quad j \geq 0\},$$

$$\mathbf{f}(x) = \sum_{j \geq 0} a_j p_j(x),$$

$a_i \in \mathbb{Z}$.

Proof

Apply induction to the function

$$\Delta(\mathbf{f})(\mathbf{x}) = \mathbf{f}(\mathbf{x}) - \mathbf{f}(\mathbf{x}-1) = \sum_{j\geq 0} a_j(p_j(x) - p_j(x-1))$$

But for $j \geq 1$,

$$p_j(x) - p_j(x-1) = \binom{x}{j} - \binom{x-1}{j} = \binom{x}{j-1} = p_{j-1}(x)$$

So by induction $a_j \in \mathbb{Z}$ for $j \geq 1$. This means that

$$\mathbf{f}(x) = \sum_{j\geq 1} a_j p_j(x) + a_0,$$

from which it follows that a_0 is the difference between two $\mathbb{Z}$-value functions.

Hilbert Function and Krull Dimension

Now we clarify the relationship between the Krull dimension of graded module and the degree of its Hilbert polynomial.

Proposition

Let M be a f.g. graded $\mathbf{R}$-module such its Hilbert polynomial $H_M(n)$ has degree $d-1>0$ and multiplicity $e_0(M)$. Let $h \in \mathbf{R}_m$ be a form that is not contained in any associated prime of M with the possible exception of $\mathfrak{m}$. Then the degree of $H_{M/hM}(n)$ is $d-2$ and $e_0(M/hM) = me_0(M)$.

Proof. Let $K = 0 :_M h$ and set $C = M/hM$. Consider the exact sequence

$$0 \to K[-m] \to M[-m] \xrightarrow{\varphi} M \to C \to 0,$$

where φ is the homogeneous homomorphism defined by multiplication by h.

K is an Artinian module, so its Hilbert polynomial trivial. It follows that

$$\begin{aligned} H_C(n) &= H_M(n) - H_{M[-m]}(n) = H_M(n) - H_M(n-m) \\ &= \sum_{j=0}^{d-1} (-1)^j e_j(M) \binom{n+d-j-1}{d-j-1} \\ &- \sum_{j=0}^{d-1} (-1)^j e_j(M) \binom{n-m+d-j-1}{d-j-1} \\ &= m \cdot e_0(M) \binom{n+d-2}{d-2} + \text{lower degree terms} \end{aligned}$$

We leave to the reader the examination of the case $d = 1$ and the proof of the following corollary:

Corollary

Let M be a f.g. graded $\mathbf{R}$-module. The Krull dimension of M is equal to the degree of the Hilbert polynomial of M plus 1.

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

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

11/2 Calculations

- Let $A = \bigoplus_n A_n$ be a f. g. graded $k[x_1, \ldots, x_r]$-module
- Let $B = \bigoplus_n B_n$ be a f. g. graded $k[y_1, \ldots, y_s]$-module
- Set

$$C = \bigoplus_n C_n, \quad C_n = \bigoplus (A_i \otimes B_{n-i})$$

- C is a f.g. graded $k[x_1, \ldots, x_r; y_1, \ldots, y_s]$-module
- Its Hilbert function, $c_n = \dim C_n$, satisfies

$$c_n = \sum a_i b_{n-i}$$

$A \otimes B$

The Hilbert series of $A \otimes B$ is:

$$P_{A\otimes B}(\mathbf{t}) = P_A(\mathbf{t}) \cdot P_B(\mathbf{t}) = \frac{\mathbf{h}_A(\mathbf{t}) \cdot \mathbf{h}_B(\mathbf{t})}{(1-\mathbf{t})^r (1-\mathbf{t})^s}$$

Veronese Product

A different construction is: Suppose $A = \bigoplus_n A_n$ is a graded algebra. Set

$$\mathbf{V} = \bigoplus V_n, \quad V_n = A_n \otimes A_n$$

The Hilbert function of $\mathbf{V}$ is $v_n = \dim V_n = a_n^2$. Can we express $P_{\mathbf{V}}(\mathbf{t})$ in terms of $P_A(\mathbf{t})$?

Exercises

- Let $\mathbf{K}_n$ be the complete graph on n vertices labeled by the indeterminates $x_1, \ldots, x_n$. Let I_n be the ideal of the ring $R = k[x_1, \ldots, x_n]$ (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.

Hilbert Functions and Free Resolutions

Let $\mathbf{R} = k[x_1, \ldots, x_d]$ and M a finitely generated graded $\mathbf{R}$-module. The syzygy theorem guarantees the existence of finite free resolution of M, of length at most d. (Recall...) One can embed additional information in the resolution using graded free modules and homogeneous homomorphisms.

- If $M = \sum M_n$ is a graded module, for $a \in \mathbb{Z}$, $L = M[-a]$ is the graded module whose component of degree n is $L_n = M_{n-a}$.
- In case $M = \mathbf{R}$, $L = \mathbf{R}[-a]$ has $L_n = 0$ for $n < a$. The Hilbert-Poincaré series of $\mathbf{R}[-a]$ is

$$\frac{\mathbf{t}^a}{(1-\mathbf{t})^d}$$

- Thus a free **R**-module F with generators of degrees $a_1 \ldots, a_r$ has for Hilbert series

$$\frac{\sum \mathbf{t}^{a_i}}{(1-\mathbf{t})^d}$$

To create graded, free resolution for the graded **R**-module M, we proceed as follows:

- Let $\mathbf{V} = M/(x_1, \ldots, x_d)M$. **V** is a graded k-vector space:

$$\mathbf{V} = ke_1 \oplus ke_2 \oplus \cdots \oplus ke_n,$$

  where e_i has degree a_i.
- Map the free **R**-module $F = \mathbf{R}[-a_{01}] \oplus \cdots \oplus \mathbf{R}[-a_{0n}]$ to M so that $\mathbf{R}[-a_i]$ is mapped into a homogeneous representative of e_i.

- By Nakayama Lemma, $\varphi_0 : F_0 \to M$ is a surjection, and φ_0 is homogeneous.
- Let $K_1 = \ker \varphi_0$. K_1 is graded and we repeat on it the process above: There is a homogeneous map $\varphi_1 : F_1 \to F_0$ where $F_1 = \bigoplus \mathbf{R}[-a_{1j}]$ so that reduction mod $\mathfrak{m} = (x_1, \ldots, x_d)$ gives a homogeneous isomorphism of of graded vector spaces $F_1/\mathfrak{m}F_1 \simeq K_1/\mathfrak{m}K_1$.

Putting it together gives a homogeneous free resolution

$$0 \to F_d \to F_{d-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

where

$$\varphi_i : \bigoplus_j \mathbf{R}[-a_{i,j}] \to \bigoplus_j \mathbf{R}[-a_{i-1,j}]$$

where φ_i homgeneous.
In each degree n, we have exact sequences of vector spaces

$$0 \to V_d \longrightarrow V_{d-1} \longrightarrow \cdots \longrightarrow V_1 \longrightarrow V_0 \to M_n \to 0$$

and therefore

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

Thus the Hilbert series of M can be written as

$$P_M(\mathbf{t}) = \frac{\sum_{i,j} (-1)^i \mathbf{t}^{a_{ij}}}{(1-\mathbf{t})^d}$$

The numerator of $P_M(\mathbf{t})$ is a polynomial $\mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})$. If $\mathbf{h}(1,1) = 0$, $\mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})$ is divisible by $1 - \mathbf{t}$. Proceeding we arrive at a representation

$$P_M(\mathbf{t}) = \frac{\mathbf{h}(\mathbf{t}, \mathbf{t}^{-1})}{(1-\mathbf{t})^m}, \quad \mathbf{h}(1,1) \neq 0$$

Proposition

m is the Krull dimension of the module M, and $\mathbf{h}(1,1)$ is a positive integer called its multiplicity, $\deg(M)$.

Outline

Topologies

Definition

A topological abelian group **G** is an abelian endowed with a topology so that the operations $\mathbf{G} \times \mathbf{G} \to \mathbf{G}$, $(x, y) \to x + y$ and $\mathbf{G} \to \mathbf{G}$, $x \to -x$ are continuous.

- If (O) is closed, the diagonal of $\mathbf{G} \times \mathbf{G}$ is closed, when **G** is Hausdorff.
- If U is a neighborhood of O, then $a + U$ is a neighborhood of a since $x \to a + x$ is a homeomorphism.

Proposition

Let $\mathbf{H}$ *be the intersection of all neighborhoods of* O *in* $\mathbf{G}$*. Then*

1. $\mathbf{H}$ *is a subgroup.*
2. $\mathbf{H}$ *is the closure of* O*.*
3. $\mathbf{G}/\mathbf{H}$ *is Hausdorff.*
4. $\mathbf{G}$ *is Hausdorff iff* $\mathbf{H} = 0$*.*

Proof.

1. Follows from the continuity of the group operations.
2. $x \in \mathbf{H} \Leftrightarrow 0 \in x - U$ for all neighorhoods U of O.
3. (2) implies that the cosets of $\mathbf{H}$ are all closed; thus points are closed in $\mathbf{G}/\mathbf{H}$ and so $\mathbf{G}/\mathbf{H}$ is Hausdorff.
4. Thus $\mathbf{H} = 0 \Rightarrow \mathbf{G}$ is Hausdorff, and converse is trivial.

Cauchy Sequences

Definition

Let **G** be a topological abelian group.

1. A Cauchy Sequence in **G** is a sequence (a_n) of elements of **G**, such that for any neighborhood U of O, there is an integer $s(U)$ with the property

$$x_m - x_n \in U \quad \forall m, n \geq s(U).$$

2. Two Cauchy sequences are equivalent if $x_n - y_n \to 0$.
3. The set of all equivalence classes of Cauchy sequences is denoted $\widehat{\mathbf{G}}$.

Cauchy Sequences=CS

- If (x_n) and (y_n) are CS, $(x_n + y_n)$ is a CS and its class $\widehat{\mathbf{G}}$ depends only on the classes of (x_n) and (y_n).
- For $x \in \mathbf{G}$, the constant sequence (x) is a CS, and its class $\phi(x)$ is an element of $\widehat{\mathbf{G}}$, and $\phi : \mathbf{G} \to \widehat{\mathbf{G}}$ is a group homomorphism.
- $\ker(\phi) = \bigcap U$, for all neighborhoods of O
- If $\mathbf{f} : \mathbf{G} \to \mathbf{H}$ is a homomorphism of topological groups, there is a homomorphism $\widehat{\mathbf{f}} : \widehat{\mathbf{G}} \to \widehat{\mathbf{H}}$ which is continuous. Moreover, $\widehat{\mathbf{f} \circ \mathbf{g}} = \widehat{\mathbf{f}} \circ \widehat{\mathbf{g}}$.

Special Neighborhoods

- Will use neigborhoods which are subgroups

$$\mathbf{G} = G_0 \supset G_1 \supset \cdots \supset G_n \supset$$

- U is a neighborhood of 0 iff $G_n \subset U$ for some n.
- $\mathbb{Z}$: $G_n = p^n\mathbb{Z}$
- G_n are open and closed: If $x \in G_n$, $x + G_n \subset G_n$, so G_n is open, while the complement of G_n is $\bigcup h + G_n$, $h \notin G_n$.

- If $\bigcap G_n = (0)$, the topology is metric:

$$d(x, y) = 2^{-n} \leftrightarrow x - y \in G_n \setminus G_{n+1}$$

- If G is a ring and the G_n are proper ideals, $d(u, 0) = 1$ for all units $u \in G$.

-

Inverse Systems

- This setting leads to an algebraic formulation of completion.If (x_n) is a CS the image of (x_n) in $\mathbf{G}/G_n$ is ultimately constant, say equal to c_n: When we pass from $n+1$ to n, $c_{n+1} \to c_n$ under the projection

$$\mathbf{G}/G_{n+1} \xrightarrow{\theta_{n+1}} \mathbf{G}/G_n$$

- Thus (x_n) defines a coherent sequence (c_n)

$$\theta_{n+1}(c_{n+1}) = c_n \quad \forall n$$

- $\widehat{\mathbf{G}}$ is the set of all coherent sequences with obvious structure.

Inverse Systems

Definition

A sequence of groups $\{A_n\}$ and homomorphisms

$$\theta_{n+1} : A_{n+1} \to A_n$$

is an inverse system. The group of all coherent sequences is called the inverse limit of the sequence. Notation: $\varprojlim A_n$. The system is surjective if all θ_n are surjective.

Exactness

Proposition

If $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ *is an exact sequence of inverse systems then*

$$0 \to \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n$$

is always exact. If, moreover, $\{A_n\}$ *is a surjective system, then*

$$0 \to \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n \to 0$$

is exact.

Proof

- Let $A = \prod_{n=1}^{\infty} A_n$, and define $d^A : A \to A$ by $d^A(a_n) = a_n - \theta_{n+1}(a_{n+1})$.
- Then $\ker d^A = \varprojlim A_n$. Define d^B and d^C.
- The exact sequence of inverse systems define the diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

By the snake lemma, it gives an exact sequence

$$0 \to \ker d^A \to \ker d^B \to \ker d^C \to \operatorname{coker} d^A \to \operatorname{coker} d^B \to \operatorname{coker} d^C \to 0$$

To complete the proof, to show that d^A is surjective one observes that it suffices to solve inductively the equations

$$x_n - \theta_{n+1}(x_{n+1}) = a_n$$

for $x_n \in A_n$, given $a_n \in A_n$

Corollary

Let $0 \to G' \longrightarrow G \xrightarrow{p} G'' \to 0$ *be an exact sequence of groups. Let* G *have the topology defined by a sequence* $\{G_n\}$ *of subgroups, and give* G', G'' *the induced topologies, i.e. by the sequences* $\{G' \cap G_n\}$, $\{pG_n\}$. *The following is exact*

$$0 \to \widehat{G'} \longrightarrow \widehat{G} \longrightarrow \widehat{G''} \to 0$$

Proof. Apply the previous proposition to

$$0 \to G'/G' \cap G_n \to G/G_n \to G''/pG_n \to 0.$$

Applying this to $G' = G_n$, then G/G_n has the discrete topology, so $\widehat{G''} = G''$.

Corollary

$\widehat{G'}$ is a subgroup of $\widehat{G}$ and $\widehat{G}/\widehat{G_n} = G/G_n$.

Proposition

$\widehat{\widehat{G}} = \widehat{G}$.

Definition

If $G \simeq \widehat{G}$, we say G is complete.

I-adic Topology

- If $I \subset \mathbf{R}$, the ideals $\{I^n\}$ define the I-adic topology of $\mathbf{R}$: the ring operations are continuous. $\mathbf{R}$ is a topological ring.
- If $\bigcap I^n = 0$, the topology is Hausdorff.
- The completion $\widehat{\mathbf{R}}$ of $\mathbf{R}$ is a topological ring, $\phi : \mathbf{R} \to \widehat{\mathbf{R}}$ is a continuous homomorphism of kernel $\bigcap I^n$.
- If M is an $\mathbf{R}$-module, the I-adic topology of M is defined by the submodules $\{I^n M\}$.

Example

Let $I \subset \mathbf{R}$. For any $u \in I$ and units $a_n \in \mathbf{R}$,

$$c_n = a_0 + a_1 u + \cdots + a_n u^n$$

are Cauchy sequences.

$\mathbf{R} = \mathbb{Z}$, $I = (p)$, p prime. Then $\widehat{\mathbb{Z}}$ is the ring of *p*-adic integers:

$$\sum_{n=0}^{\infty} a_n p^n, \quad 0 \leq a_n \leq p-1.$$

We have $p^n \to 0$ as $n \to \infty$.

Artin–Rees Lemma

This is a backbone of commutative algebra of nearly the same pedigree as Hilbert results in the 1870's papers.

Theorem (Artin-Rees Lemma)

Let R be a Noetherian ring and let I and J be two ideals. There exists an integer c such that for all $n \geq c$ the following equality holds

$$J \cap I^n = I^{n-c}(J \cap I^c). \tag{8}$$

Proof. Let $a_1, \ldots, a_n$ be a generating set of the ideal I and consider the R-subalgebra of the ring of polynomials $A = R[t]$,

$$B = R[a_1 t, \ldots, a_n t].$$

Since R is Noetherian and B is finitely generated, B is also Noetherian.
Grading A in the usual fashion, B is a graded subalgebra, the Rees algebra of I:

$$B = R + It + I^2 t^2 + \cdots + I^n t^n + \cdots .$$

Define $L_n = J \cap I^n$ and set

$$\mathcal{L} = L_0 + L_1 t + L_2 t^2 + \cdots + L_n t^n + \cdots .$$

$\mathcal{L}$ is clearly a homogeneous ideal of B, so there is a finite set of forms that generates it,

$$\mathcal{L} = (b_1 t^{d_1}, \ldots, b_s t^{d_s}).$$

In

$$\mathcal{L} = (b_1 t^{d_1}, \ldots, b_s t^{d_s}),$$

let $c = \sup\{d_1, \ldots, d_s\}$; for $n \geq c$, we must have

$$L_n = \sum_{i=1}^{s} I^{n-d_i} b_i,$$

from which the assertion

$$J \cap I^n = I^{n-c}(J \cap I^c)$$

follows.

Krull Intersection Theorem

Theorem

Let R be a Noetherian ring and let I be an ideal of R. If

$$L = \bigcap_{n \geq 1} I^n,$$

then $L = I \cdot L$. In particular, if I is contained in the Jacobson radical of R, then

$$\bigcap_{n \geq 1} I^n = 0.$$

Proof. It suffices to put $J = L$ in the Artin-Rees Lemma. The second assertion follows from Nakayama lemma:

Theorem (Nakayama Lemma)

Let M be a finitely generated R module and J its Jacobson radical. If $M = JM$, then $M = 0$.

Remark

Actually, using the Nakayama lemma one can give another description of L. Consider the multiplicative set $S = \{1 + a,\ a \in I\}$. In the ring $S^{-1}R$ the ideal $S^{-1}I$ is contained in the Jacobson radical. Thus the equality $S^{-1}L = S^{-1}I \cdot S^{-1}L$ implies (by Nakayama lemma) that $S^{-1}L = 0$. This means that there is $x \in I$ such that $(1 + x)L = 0$.

Remark

The theorem above applies equally to modules; more precisely, if M is a finitely generated R–module, then

$$L = \bigcap_{n \geq 1} I^n M,$$

satisfies $L = I \cdot L$.
This can be readily seen by making use of the idealization trick*, consisting in giving the direct sum $S = R \oplus M$ a ring structure by decreeing*

$$(a, x) \cdot (b, y) = (a \cdot b, a \cdot y + b \cdot x).$$

Now one applies the theorem to the ring S and its ideal $I \oplus M$.

Another important use of the Artin–Rees lemma is to the identification of two topologies defined by the powers of an ideal I. If M is a finitely generated module over a Noetherian ring R, then the family of submodules $\{I^n M \mid \forall n \geq 0\}$ defines a system of neighborhoods of $0 \in M$. If $N \subset M$ is a submodule, there are two topologies defined on N, the induced one, $\{I^n M \cap N\}$, and its own I-adic topology. The Artin-Rees lemma identifies them.

Completion

Proposition

Let $\mathbf{R}$ *be a Noetherian ring,* I *an* $\mathbf{R}$*-ideal and* $0 \to A \longrightarrow B \longrightarrow C \to 0$ *be an exact sequence of f.g.* $\mathbf{R}$*-modules. Then there is an exact sequence*

$$0 \to \widehat{A} \longrightarrow \widehat{B} \longrightarrow \widehat{C} \to 0$$

for their I*-adic completion. In other words, completion is an exact functor on the category of f.g.* $\mathbf{R}$*-modules.*

Corollary

For any f.g. $\mathbf{R}$*-module* M*,*

$$\widehat{M} \simeq M \otimes \widehat{\mathbf{R}}.$$

In particular, $\widehat{\mathbf{R}}$ *is a flat* $\mathbf{R}$*-module.*

Proof. Clearly $\widehat{\mathbf{R}} = \mathbf{R} \otimes \widehat{\mathbf{R}}$. If M is a f.g. $\mathbf{R}$-module, there is a free presentation

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

There is a commutative diagram of exact rows

$$\begin{array}{ccccccc}
\widehat{\mathbf{R}} \otimes \mathbf{R}^m & \longrightarrow & \widehat{\mathbf{R}} \otimes \mathbf{R}^n & \longrightarrow & \widehat{\mathbf{R}} \otimes M & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\widehat{\mathbf{R}}^m & \longrightarrow & \widehat{\mathbf{R}}^n & \longrightarrow & \widehat{M} & \longrightarrow & 0
\end{array}$$

Since the two vertical maps on the left are isomorphisms, $\widehat{\mathbf{R}} \otimes M \simeq \widehat{M}$ also.

Associated Graded Rings/Modules

Let **R** be a Noetherian ring and M a finitely generated **R**-module. A descending filtration of M is a sequence of submodules $\mathcal{M} = \{M_i, i \geq 0\}$

$$M = M_0 \supset M_1 \supset \cdots \supset M_n \supset M_{n+1} \supset \cdots$$

Definition

The associated graded module of $\mathcal{M}$ is the module

$$\bigoplus_{n \geq 0} M_n / M_{n+1}.$$

Associated Graded Rings/Modules

Definition

Let I be an $\mathbf{R}$-ideal and M an $\mathbf{R}$-module. The I-adic filltration of M is $\{M_n, M_n = I^n M\}$. The module

$$\mathrm{gr}_I(M) = \bigoplus_{n \geq 0} M_n / M_{n+1}$$

is its associated graded module.

- If $M = \mathbf{R}$, $G = \mathrm{gr}_I(\mathbf{R})$ is a ring and $\mathrm{gr}_I(M)$ is a $\mathrm{gr}_I(\mathbf{R})$-module.
- If $\mathbf{R}$ is a Noetherian ring, then G is a Noetherian ring and $\mathrm{gr}_I(M)$ is a finitely generated G-module.

Example

Example

If $\mathbf{R} = k[[x_1, \ldots, x_d]]$, $I = (x_1, \ldots, x_d)$,

$$\mathrm{gr}_I(\mathbf{R}) = k[x_1, \ldots, x_d].$$

Functorial Properties

- If $\varphi : M \to N$ is a module homomorphism, $\varphi_n : \mathfrak{m}^n M \to \mathfrak{m}^n N$, and induces a homogeneous homomorphism

$$\mathrm{gr}\,(\varphi) : \mathrm{gr}_I(M) \to \mathrm{gr}_I(N), \quad \mathrm{gr}\,(\varphi)_n : \mathfrak{m}^n M/\mathfrak{m}^{n+1} M \to \mathfrak{m}^n N/\mathfrak{m}^{n+1} N$$

- If $0 \to P \xrightarrow{\phi} M \xrightarrow{\varphi} N \to 0$ is a SES, the following is a complex exact on the right

$$0 \to \mathrm{gr}_I(P) \xrightarrow{\mathrm{gr}\,(\phi)} \mathrm{gr}_I(M) \xrightarrow{\mathrm{gr}\,(\varphi)} \mathrm{gr}_I(N) \to 0$$

- $\ker(\mathrm{gr}\,(\phi)) = \bigoplus_n \phi^{-1}(\mathfrak{m}^n M) \cap \mathfrak{m}^n P/\mathfrak{m}^{n+1} P$
  $\ker(\mathrm{gr}\,(\varphi)) = \bigoplus_n \varphi^{-1}(\mathfrak{m}^n N) \cap \mathfrak{m}^n M/\mathfrak{m}^{n+1} M$

Noetherianess

Definition

Let M be an A–module. A chain

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n \supseteq \cdots ,$$

where the M_n are submodules of M, is called a *filtration* of M, and denoted by (M_n).

It is an *I–filtration* if $IM_n \subseteq M_{n+1}$ for all n, and a *stable I–filtration* if $IM_n = M_{n+1}$ for all sufficiently large n. Thus, $(I^n M)$ is a stable I–filtration.

Lemma

If (M_n) and (M'_n) are stable I–filtration of M, then they have bounded difference: that is, there exists an integer n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$. Hence all stable I–filtrations determine the same topology on M, namely the I–topology.

Proof. Enough to take $M'_n = I^n M$. Since $IM_n \subseteq M_{n+1}$ for all n, we have $I^n M \subseteq M_n$; also $IM_n = M_{n+1}$ for all $n \geq n_0$ say, hence $M_{n+n_0} = I^n M_{n_0} \subseteq I^n M$. □

Let A be a Noetherian ring and I an ideal and let (M_n) be an I-filtration. Set

$$\begin{aligned} A^* &= A \oplus I \oplus I^2 \oplus \cdots \\ M^* &= M_0 \oplus M_1 \oplus M_2 \oplus \cdots \end{aligned}$$

M^* is an A^*-module.

Lemma

Let A be a Noetherian ring, M a finitely generated A–module, (M_n) an I–filtration of M. Then the following are equivalent :

(i) *M^* is a finitely generated A^*–module.*

(ii) *The filtration (M_n) is stable.*

Proof. Each M_n is finitely generated, hence so is each $Q_n = \bigoplus_{r=0}^{n} M_r$: this is a subgroup of M^* but not (in general) an A^*–submodule. However, it generated one, namely

$$M^* = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots \oplus I^r M_n \oplus \cdots .$$

Since Q_n is finitely generated as an A–module, M_n^* is finitely generated as an A^*–module. The M_n^* form an ascending chain, whose union is M^*. Since A^* is Noetherian, M^* is finitely generated as an A^*–module if and only if the chain stops, i.e., $M^* = M_{n_0}^*$ for some n_0 if and only if $M_{n_0+r} = I^r M_{n_0}$ for all $r > 0$ if and only if the filtration is stable. □

Proposition (10.15)

If A is Noetherian, $\widehat{A}$ its I–adic completion, then

(i) $\widehat{I} = \widehat{A}I \simeq \widehat{A} \otimes_A I$;

(ii) $\widehat{I^n} = (\widehat{I})^n$;

(iii) $I^n/I^{n+1} \simeq \widehat{I}^n/\widehat{I}^{n+1}$;

(iv) $\widehat{I}$ *is contained in the Jacobson radical of* $\widehat{A}$.

Proof. Since A is Noetherian, I is finitely generated. implies that the map

$$\widehat{A} \otimes_A I \to \widehat{I},$$

whose image is $\widehat{A}I$, is an isomorphism. This proves (i). Now apply (i) to I^n and we deduce that

$$\widehat{I^n} = \widehat{A}I^n = (\widehat{A}I)^n = (\widehat{I})^n.$$

From the above, we now deduce

$$A/I^n \simeq \widehat{A}/\widehat{I}^n$$

from which (iii) follows by taking quotients. By (ii) we see that $\widehat{A}$ is complete for its $\widehat{I}$–topology. Hence for any $x \in \widehat{I}$

$$(1-x)^{-1} = 1 + x + x^2 + \cdots$$

converges in $\widehat{A}$, so that $1 - x$ is a unit. This implies that $\widehat{I}$ is contained in the Jacobson radical of $\widehat{A}$. □

Proposition

Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal. Then the $\mathfrak{m}$–adic completion $\widehat{A}$ of A is a local ring with maximal ideal $\widehat{\mathfrak{m}}$.

Proof. By the previous proposition (iii), we have $\widehat{A}/\widehat{\mathfrak{m}} \simeq A/\mathfrak{m}$, hence $\widehat{A}/\widehat{\mathfrak{m}}$ is a field and so $\widehat{\mathfrak{m}}$ is a maximal ideal. By (iv) of the same proposition, it follows that $\widehat{\mathfrak{m}}$ is the Jacobson radical of $\widehat{A}$ and so is the unique maximal ideal. Thus $\widehat{A}$ is a local ring. $\square$

Proposition

Let A be a Noetherian ring, I an ideal of A. Then

(i) *$G_I(A)$ is Noetherian;*

(ii) *$G_I(A)$ and $G_{\widehat{I}}(\widehat{A})$ are isomorphic as graded rings ;*

(iii) *if M is a finitely generated A–module and (M_n) is a stable I–filtration of M, then $G(M)$ is a finitely generated graded $G_I(A)$–module.*

Proof. (i) Since A is Noetherian, I is finitely generated, say by $x_1, \ldots, x_s$. Let $\overline{x}_i$ be the image of x_i in I/I^2, then $G(A) = (A/I)[\overline{x}_1, \ldots, \overline{x}_s]$. Since A/I is Noetherian, $G(A)$ is Noetherian by the Hilbert basis theorem.

(ii) $I^n/I^{n+1} \simeq \widehat{I}^n/\widehat{I}^{n+1}$ by (10.15)(iii).

(iii) There exists n_0 such that $M_{n_0+r} = I^r M_{n_0}$ for all $r \geq 0$, hence $G(M)$ is generated by $\bigoplus_{n \leq n_0} G_n(M)$. Each $G_n(M) = M_n/M_{n+1}$ is Noetherian and annihilated by I, hence is a finitely generated A/I–module, hence $\bigoplus_{n \leq n_0} G_n(M)$ is generated by a finite number of elements (as an A/I–module), hence $G(M)$ is finitely generated as a $G(A)$–module. □

Lemma (10.23)

Let $\phi : A \to B$ be a homomorphism of filtered group, i.e., $\phi(A_n) \subseteq B_n$, and let $G(\phi) : G(A) \to G(B)$, $\widehat{\phi} : \widehat{A} \to \widehat{B}$ be the induced homomoprhisms of the associated graded and completed groups. Then

(i) *$G(\phi)$ injective $\Rightarrow$ $\widehat{\phi}$ is injective.*

(ii) *$G(\phi)$ surjective $\Rightarrow$ $\widehat{\phi}$ is surjective.*

Proof. Consider the commutative diagram of eact sequnces

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n/A_{n+1} & \longrightarrow & A/A_{n+1} & \longrightarrow & A/A_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle G_n(\phi)} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \\ 0 & \longrightarrow & B_n/B_{n+1} & \longrightarrow & B/B_{n+1} & \longrightarrow & B/B_n & \longrightarrow & 0 \end{array}$$

This gives the exact sequnce

$$0 \to \ker\left(G_n(\phi)\right) \to \ker\left(\alpha_{n+1}\right) \to \ker\left(\alpha_n\right) \to \operatorname{coker}\left(G_n(\phi)\right)$$

$$\to \operatorname{coker}\left(\alpha_{n+1}\right) \to \operatorname{coker}\left(\alpha_n\right) \to 0.$$

From this we see, by induction on n, that $\ker\left(\alpha_n\right) = 0$ (case (i)) or $\operatorname{coker}\left(\alpha_n\right) = 0$ (case (ii)). Moreover in case (ii) we also have $\ker\left(\alpha_{n+1}\right) \to \ker\left(\alpha_n\right)$ surjective. Taking the inverse limit of the homomorphisms α_n and applying a previous proposition, the lemma follows. □

Proposition (10.24)

Let A be a ring, I an ideal of A, M an A–module, (M_n) an I–filtration of M. Suppose that A is complete in the I–topology and that M is Hausdorff in its filtration topology (i.e., that $\bigcap_n M_n = 0$. Suppose also that $G(M)$ is a finitely generated $G(A)$–module. Then M is a finitely generated A–mdoule.

Proof. Pick a finite set of generators of $G(M)$, and split them up into their homogeneous components, say ξ_i $(1 \leq i \leq \nu)$ where ξ_i has degree say $n(i)$, and is therefore the image of say $x_i \in M_{n(i)}$. Let F^i be the module A with the stable I-filtration given by $F^i_k = I^{k+n(i)}$ and put $F = \bigoplus_{i=1}^{r} F_i$. Then mapping the generator 1 of each F^i to x_i defines a homomorphism

$$\phi : F \to M$$

of filtered groups, and $G(\phi) : G(F) \to G(M)$ is a homomorphism of $G(A)$–modules. By construction it is surjective. Hence by (10.23) (ii) $\widehat{\phi}$ is surjective.

Consider now the diagram

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ \widehat{F} & \xrightarrow[\widehat{\phi}]{} & \widehat{M} \end{array}$$

Since F is free and $A = \widehat{A}$ it follows that α is an isomorphism. Since M is Hausdorff β is injective. The surjectivity of $\widehat{\phi}$ thus implies the surjectivity of ϕ, and this means that $x_1, \ldots, x_r$ generated M as an A–module. $\square$

Corollary (10.25)

With the hypotheses of (10.24), if $G(M)$ is a Noetherian $G(A)$–module, then M is a Noetherian A–module.

Proof. We have to show that every submodule M' of M is finitely generated. Let $M'_n = M' \cap M_n$; then (M'_n) is an I–filtration of M' and the embedding $M'_n \to M_n$ gives rise to an injective homomorphism $M'_n/M'_{n+1} \to M_n/M_{n+1}$, hence to an embedding of $G(M')$ in $G(M)$. Since $G(M)$ is Noetherian, $G(M')$ is finitely generated; also M' is Hausdorff, since $\bigcap M'_n \subseteq \bigcap M_n = 0$; hence by (10.24), M' is finitely generated. □

Theorem

If A is a Noetherian ring, I an ideal of A, then the I–completion $\widehat{A}$ of A is Noetherian.

Proof. By (10.22), we know that

$$G_I(A) = G_{\widehat{I}}(\widehat{A})$$

is Noetherian. Now apply (10.25) to the complete ring $\widehat{A}$, taking $M = \widehat{A}$ (filtered by $\widehat{I}^n$, and so Hausdorff). □

Corollary

If A is a Noetherian ring, the power series ring $B = A[[X_1, \ldots, X_n]]$ in n variables is Noetherian. In particular, $k[[X_1, \ldots, X_n]]$ (k a field) is Noetherian.

Proof. $A[X_1, \ldots, X_n]$ is Noetherian by the Hilbert basis theorem, and B is its completion for the $(X_1, \ldots, X_n)$–adic topology. □

Outline

Monomial Ideals

The settings for computations that we will consider are rings of polynomials

$$R = R_n(k) = k[x_1, \ldots, x_n],$$

where k is a finite field or a finite extension of $\mathbb{Q}$, or in a few cases, rings where coding can be done as efficiently as with those basic fields.

The problems themselves are concerned with affine rings over k – and are therefore adequately modeled by an ideal of some $R_n(k)$ – or by a subring of $R_n(k)$:

- $R/I,\ \ I \subset R$
- $k[f_1, \ldots, f_m],\ \ f_i \in R$.

Topics

- Polynomial rings and their orderings
- Division algorithms
- Buchberger algorithm
- Computation of syzygies
- Computation of Hilbert functions

The treatment here is only intended to sketch out basic concepts and algorithms and point out its capabilities, focusing instead on the interface between the algorithms and algebra itself. It will become clear that this interfacing takes place over an open set not just a thin layer of activities.

Gröbner Basics

Division algorithms are key tools for processing in rings of polynomials. The most straightforward of these is probably *pseudo–division*. It consists in a minor modification of ordinary long division of polynomials in one variable with coefficients in a field.
For more general coefficients, it works as follows: Let $f(x)$ and $g(x)$ be elements of $R[x]$,

$$f(x) = a_r x^r + \cdots + a_0, \quad a_r \neq 0.$$

If $\deg g(x) = s \geq r$, then there are polynomials $q(x), p(x)$ such that

$$a_r^{s-r+1} g(x) = p(x) f(x) + q(x), \quad \deg q(x) < \deg f(x).$$

Division Algorithms

Let $\mathbf{R} = k[x_1, \ldots, x_d]$ and $I = \{\mathbf{f}_1, \ldots, \mathbf{f}_n\}$ be a collection of polynomials.

Question: For $\mathbf{f} \in \mathbf{R}$, how to find canonical? representations

$$\mathbf{f} = \sum_n \mathbf{g}_i \mathbf{f}_i + r$$

- $d = 1$: Long division
- $\deg \mathbf{f}_i = \deg \mathbf{f} = 1$: Gaussian algorithm
- Classical approach: Convert to linear algebra (Grete Hermann)
- $\mathbf{f}_i$ monomial: Sweet method

Polynomial Rings, Monomials, Orderings and Weight Vectors

Let k be a field, and let R be the polynomial ring $k[x_1, \ldots, x_n]$. Suppose I is an ideal of R given by a set $\{f_1, \ldots, f_m\}$ of generators. The study of the ring R/I is helped by the knowledge of canonical bases for the k–vector space R/I. The purpose of division algorithms in R is to provide us with such bases.

Let us fix a ring of polynomials $R = k[x_1, \ldots, x_n]$ over a field k. Denote by $\mathbb{M}$ the set of all monomials

$$\mathbf{x}^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \tag{9}$$

(including 1). $\mathbb{M}$ is a multiplicative monoid isomorphic to the additive monoid $\mathbb{N}^n$.

Given an element $f \in R$, it is written

$$f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha \mathbf{x}^\alpha$$

in a manner that facilitates the processing under multiplication or division. This is usually achieved by picking orders on $\mathbb{M}$ that are compatible with multiplication.

Definition

An *admissible partial order* T is a partial order $>_T$ on $\mathbb{M}$ with the property

- $m >_T 1$ for any non constant monomial m;
- If $m_1 >_T m_2$ and $m_3 \in \mathbb{M}$ then $m_1 \cdot m_3 >_T m_2 \cdot m_3$.

If $>_T$ is a total order we say that it is a *term order* (or *term ordering* or even a *monomial ordering*).

A basic example of a term ordering is the *lexicographic* order (*lex* for short):

$$m_1 = x_1^{a_1} \cdots x_n^{a_n} >_{lex} x_1^{b_1} \cdots x_n^{b_n} = m_2$$

if

$$a_1 = b_1, \cdots, a_{r-1} = b_{r-1}, a_r > b_r, \text{ for } 1 \leq r \leq n.$$

Product of Orderings

More general term orderings arise by combining several admissible partial orders through their lexicographic product of orderings. If $T_1, \ldots, T_s$ are such partial orders, the product order

$$T = T_1 \times_{lex} T_2 \times_{lex} \cdots \times_{lex} T_s$$

is defined as above

$$m_1 >_T m_2 \Longleftrightarrow m_1 =_{T_1} m_2, \ldots, m_1 =_{T_{r-1}} m_2, m_1 >_{T_r} m_2, \text{ for } 1 \leq r \leq s$$

Degree Orderings

Among term orderings noteworthy are those that place emphasis on the degrees of the polynomials. They are obtained as the product of deg, the total degree partial order, and T_2 another partial order. For instance, if T_2 is *lex*, their product is the so–called graded lexicographic ordering:

$$(a_1, \ldots, a_n) < (b_1, \ldots, b_n) \Leftrightarrow$$
$$\text{first nonzero entry of } \left(\sum b_i - \sum a_i, b_1 - a_1, \ldots, b_n - a_n\right) \text{ is positive.}$$

Particularly striking properties are enjoyed by the *reverse lexicographic order*, defined by changing the last requirement above to: the last nonzero entry is negative. Macaulay introduced it in his fundamental studies on Hilbert functions. Bayer and Stillman have discovered many of its interesting properties and incorporated its efficiencies into their *Macaulay* program.

As these examples already indicate, it is necessary to consider more general partial orderings of $\mathbb{M}$ as constituent blocks for term orderings. A simple mechanism is to embed the monoid $\mathbb{N}^n$ into a real vector space V: each element $w \in V^*$ (the dual of V) induces a partial order on $\mathbb{M}$, compatible with its composition law, by

$$\mathbf{x}^{\mathbf{a}} < \mathbf{x}^{\mathbf{b}} \Leftrightarrow w(\mathbf{a}) < w(\mathbf{b}). \tag{10}$$

We refer to w as a *weight vector*.

Initial Ideals

Orderings are the means to pass back and forth between the monoid of all monomials and $\mathbb{N}^n$. We define the homomorphism

$$\log : \mathbb{M} \longrightarrow \mathbb{N}^n,$$

by

$$\log(x_1^{a_1} \cdots x_n^{a_n}) = (a_1, \ldots, a_n).$$

Let us fix, for our discussion, a term order which we denote simply by $>$.

If $f = \sum_\alpha c_\alpha \mathbf{x}^\alpha \in R$, the *support* of f is the subset of $\mathbb{N}^n$

$$\operatorname{supp}(f) = \{\, \alpha \mid c_\alpha \neq 0\},$$

while the *Newton polytope* of f is the convex hull of $\operatorname{supp}(f)$.

If $0 \neq f \in R$, $f = C(f) \cdot M(f) + \sum a_i M_i$, where $M(f)$ is the highest monomial that occurs in the representation of f; $0 \neq C(f)$ is its leading coefficient; the product $L(f) = C(f) \cdot M(f)$ is the *leading term* or *initial term* $\operatorname{in}(f)$ of f. We define $\log(f) = \log(M(f))$.

A more common notation is to denote the *leading coefficient* of f by

$$\mathrm{lc}(f) = c_\beta,\ \beta = \max\{\ \alpha \in \mathrm{supp}(f)\},$$

$in(f) = \mathbf{x}^\beta$ is the *initial monomial* and $\mathrm{lt}(f) = c_\beta \cdot \mathbf{x}^\beta$ is the *leading term* of f:

$$\log(f)$$

$$f = c_\beta \cdot x^\beta + \sum c_i \cdot x^{\alpha_i}, \qquad c_\beta \neq 0,\ \beta > \alpha_i$$

$$\mathrm{lt}(f) = \mathrm{lc}(f) \cdot in(f)$$

For a nonzero ideal I, define $\log(I)$ to be the union of $\log(f)$, $0 \neq f \in I$. This defines a sub–monoid of $\mathbb{N}^n$, stable under the addition of quadrants:

$$\log(I) = \log(I) + \mathbb{N}^n.$$

By the Hilbert basis theorem there are finitely many elements $g_1, \ldots, g_r$ in I so that

$$\log(I) = \bigcup(\log(g_i) + \mathbb{N}^n),\ 1 \leq i \leq r.$$

Definition

The *initial ideal* of I for the term order $>$ is the ideal

$$in_>(I) = (x^a,\ \text{for all } a \in \log(I)). \tag{11}$$

The ideal $in_>(I)$ is highly dependent on the chosen ordering; once $>$ is fixed, the ideal is denoted simply by $in(I)$.

Definition

The set $\{g_1, \ldots, g_r\}$ of elements of I is a Gröbner *basis* if

$$in(I) = (in(g_1), \ldots, in(g_r)). \tag{12}$$

Normal Form Representation

We begin to use the notion of orderings for the study of arbitrary ideals. The discussion assumes the choice of a term order.

A first simple observation–but still of great significance–is that the images of the monomials

$$x^a \text{ where } a \in \mathbb{N}^n \setminus \log(I) = \Delta_I,$$

form a basis for the k–vector space R/I. They are the *standard monomials* associated to the Gröbner basis. The Gröbner basis G is said to be *reduced* if

$$\operatorname{supp}(f - \operatorname{lt}(f)) \subset \Delta_I, \quad \forall f \in G.$$

Definition

For a given $f \in R$, the unique polynomial

$$\text{NormalForm}(f) = \sum c_a x^a, \tag{13}$$

where each x^a is a standard monomial, such that

$$f - \text{NormalForm}(f) \in I,$$

is the *normal form* of f with respect to the chosen ordering.

Macaulay Theorem

We have the following fundamental fact:

Theorem (Macaulay Theorem)

Given an ideal I there exists a monomial ideal $in(I)$ such that the set $B = \{\mathbf{x}^a \notin in(I)\}$ is a basis of R/I. More concretely, the mapping

$$\boxed{\text{NormalForm}\colon R/I \longrightarrow R/in(I)} \tag{14}$$

is an isomorphism of k-vector spaces.

Division Algorithms

The setting in this section is a ring of polynomials $R = k[x_1, \ldots, x_n]$ over a computable field. We sketch out Buchberger algorithm.

Definition

Let R be a ring and let I be an ideal generated by $F = \{f_1, \ldots, f_m\}$. The *syzygies* of the f_i's are the tuples $(r_1, \ldots, r_m) \in R^m$ such that

$$\sum_{i=1}^{m} r_i f_i = 0.$$

The simplest of all syzygies are *Koszul syzygies*,

$$f \cdot g - g \cdot f = 0,$$

where f, g are elements of the ring R. A refinement is

$$A \cdot g - B \cdot f = 0,$$

if $f = A \cdot h$, $g = B \cdot h$, where h is a common divisor. For larger sets of elements this step will be further refined using the division that Gröbner bases permit.

Taken together the syzygies of the set F form a submodule of R^m, the *module of syzygies* of the f_i's. When another set of generators for I is chosen, the corresponding module of syzygies is closely related to the first in a manner originally observed by Fitting.

When the f_i's are monomials, the module of syzygies of F is generated by Koszul relations. For more general sets F, we are going to use this as a tool to get the syzygies of appropriate sets of generators of the ideal (F).

There are other notions of syzygies associated to the set F, of which we recall two. First, consider a homomorphism

$$\varphi : k[T_1, \ldots, T_m] \mapsto R, \quad \varphi(T_i) = f_i.$$

$I = \ker(\varphi)$ is the ideal of *algebraic* syzygies of the f_i's. A more general notion, useful in the theory of blowup algebras, deals with mappings such as φ but with a different source:

$$\varphi : k[x_1, \ldots, x_r, T_1, \ldots, T_m] \mapsto R, \quad \varphi(T_i) = f_i,$$

where $k[x_1, \ldots, x_r] \subset R$. It is surprising that ultimately all these kinds of syzygies are going to be dealt with in the same manner.

Buchberger Algorithm

Here one seeks to divide a polynomial g by a finite collection $f_1, \ldots, f_m$ of polynomials,

$$g = \sum_{i=1}^{m} h_i f_i + \text{remainder}, \tag{15}$$

in which 'remainder' has some appropriate minimizing property.

The following deceptively simple statement embodies the efficacy of Gröbner bases as the generating set of choice for an ideal of a polynomial ring.

Proposition

Let I be an ideal of R and let $>$ be a term ordering of R. A set

$$\{g_1, \ldots, g_r\} \subset I,$$

is a Gröbner basis of I with respect to $>$ if and only if every nonzero element of I can be written as

$$f = \sum a_i g_i, \quad \textit{with } \log(f) \geq \log(a_i g_i).$$

In particular, a Gröbner basis of I is a generating set for I.

The proof is contained in the very definition of the Gröbner basis. Note the close parallel with the Euclidean algorithm in the ring $k[t]$ and the elements of Gaussian elimination.

The previous proposition is a basis for solving several general questions about the ideal I, particularly the membership problem. There remains to find such bases. This results from the following analysis due to Buchberger.

Let I be defined by a generating set $F = \{f_1, \ldots, f_m\}$. One must have a criterion to decide whether $\log(F) = \{\log(f_1), \ldots, \log(f_m)\}$ generates $\log(I)$, and if not, a device to add new elements to the f_i's. These steps come together in the same argument.

Reduction

We begin with the observation on how to add a possible new generator to F. Let f be a nonzero element of I. If $in(f)$ is not a multiple of any of the $in(f_i)$'s, one has a new generator. However, even if $in(f)$ is already a multiple of a $in(f_i)$, f may still contribute a new generator. To see this, suppose that the leading monomial $M(f)$ of f is divisible by the leading monomial $M(f_i)$ of f_i, and pick $q \in R$ such that $\log(f - qf_i) < \log(f)$. It is also usual to effect this operation on the next largest monomial of f which does not belong to the span of the $M(f_i)$'s. On iterating we end up with an element

$$g \quad = \quad f - \sum_i a_i f_i,$$

with the property that $g = 0$ or $\log(g)$ is not divisible by $\log(F)$. In either case we say that f *reduces* to g relative to F.

If $g = 0$, f is ignored; otherwise adding $\log(g)$ to the submonoid of $\mathbb{N}^n$ generated by the $\log(f_i)$'s gives rise to a larger submonoid. The Hilbert basis theorem guarantees that such additions cannot go on forever.

S–resultant

The issue is how to pick appropriate elements of I. The basic step goes to the core of both the Euclidean and Gaussian algorithms. It is embodied in the notion of the (resultant) S–polynomial attached to two polynomials $f, g \in R$: If $M(f)$ and $M(g)$ are their leading monomials, set

$$S(f,g) := a_g \cdot f - (C(f)/C(g)) \cdot b_f \cdot g, \tag{16}$$

where $a_g \cdot M(f) = b_f \cdot M(g)$ is the least common multiple of $M(f)$ and $M(g)$. The collections of such objects have a very natural place in the theory of Taylor resolutions.

The Buchberger algorithm is made up of the following result and the scheme that follows to produce the required elements.

Theorem

A set of generators $F = \{f_1, \ldots, f_m\}$ of the ideal I is a Gröbner basis of I if and only if the S–polynomial $S(f_i, f_j)$ of each pair (f_i, f_j) of elements of F reduces to 0 *with respect to F.*

Proof. The proof of the necessity is clear. For the converse, let f be an element of I. We may assume that f is its own normal form with respect to F. Let $f = \sum_j h_j f_j$, and consider the $\log(h_j f_j)$'s (for $h_j \neq 0$). $\log(f)$ cannot be equal to one of the $\log(h_j f_j)$, as it is already in normal form. This means that there must be some cancelling out at the top monomial occurring in the products $h_j f_j$.

More precisely, suppose

$$M(h_1) \cdot M(f_1) = M(h_2) \cdot M(f_2) = \cdots = M(h_k) \cdot M(f_k)$$

are the top monomials that occur in the right hand side of the representation of f. Their cancelling out means that the vector of leading terms

$$(L(h_1), \ldots, L(h_k))$$

is a syzygy of

$$(L(f_1), \ldots, L(f_k)).$$

But it is an elementary fact that such relations are combinations of the syzygies of pairs $\{C(f_r)M(f_r), C(f_s)M(f_s)\}$. This means that we have a representation

$$f = \sum_j h'_j f_j + \sum a_{rs} S(f_r, f_s),$$

where $\log(h'_j f_j) < \log(h_1 f_1)$. An easy induction completes the proof. □

Proposition (Buchberger Algorithm)

Let $F = \{f_1, \ldots, f_m\}$ be a set of generators of the ideal I, and let $>_T$ be a term order for $\mathbb{M}$.

$G := F$.

$B := \{(f_1, f_2) \mid f_1, f_2 \in F, \text{ and } f_1 \neq f_2\}$.

while $B \neq \emptyset$ *do*

$(f_1, f_2) :=$ a pair in B

$B := B \setminus \{f_1, f_2\}$

$g :=$ normal form of $S(f_1, f_2)$ with respect to G

if $g \neq 0$, *then*

$B := B \cup \{(g, h) \mid h \in G\}$

$G := G \cup \{g\}$

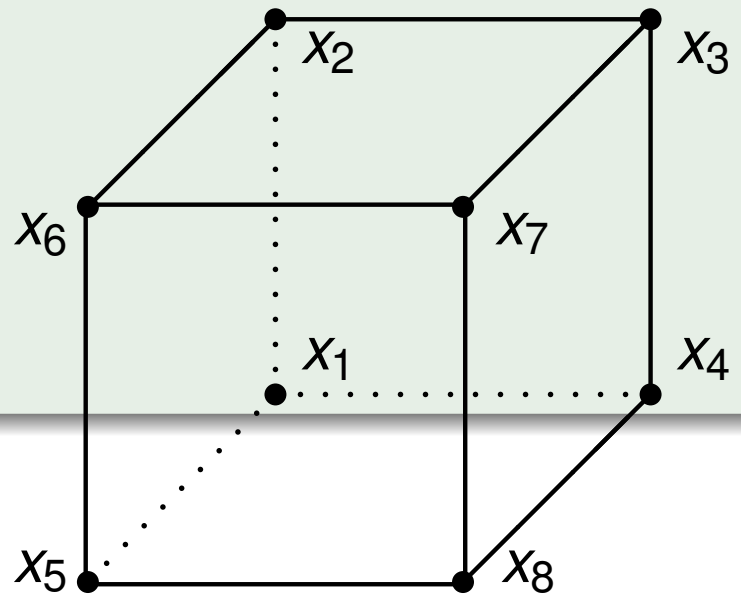
Example

Let $R = k[x, y, z]$ be a polynomial ring over a field k with the reverse lexicographic ordering and let $f_1 = y^4 - x^2z^2$, $f_2 = x^3 - y^2z$ and $f_3 = xy - z^2$. Applying the algorithm in this setting gives the reduced Gröbner basis for the ideal I generated by the f_i's:

$$f_1,\ f_2,\ f_3,\ xz^5 - z^6,\ yz^5 - z^6,\ y^2z^3 - xz^4,\ y^3z - x^2z^2,\ x^2z^3 - xz^4.$$

Example

Let $R = k[x_1 \ldots, x_8]$ be a polynomial ring over a field k and let G be the bipartite graph



Let $k[G]$ be the k-subring of R spanned by the set of monomials $f_{ij} = x_i x_j$ so that x_i is adjacent to x_j and let $P(G)$ be the toric ideal of $k[G]$, that is, $P(G)$ is the kernel of the graded homomorphism

$$\varphi\colon B = k[t_{ij}] \longrightarrow k[G], \quad \text{induced by} \quad \varphi(t_{ij}) = f_{ij}.$$

$P(G)$ is a Cohen-Macaulay prime ideal of codimension 5, whose generators are determined by the edge cycles contained in the graph: to the cycle

$\{\alpha_1, \beta_1, \ldots, \alpha_s, \beta_s\}$, associate the binomial $T_{\alpha_1} \cdots T_{\alpha_s} - T_{\beta_1} \cdots T_{\beta_s}$.

If the terms in B are ordered by the reverse lexicographical ordering

$$t_{14} > t_{23} > t_{12} > t_{56} > t_{37} > t_{26} > t_{34} > t_{78} > t_{15} > t_{48} > t_{67} > t_{58},$$

then a reduced Gröbner basis for $P(G)$ is

$$\begin{array}{lll}
h_1 = t_{15}t_{48} - t_{14}t_{58}, & h_5 = t_{14}t_{26}t_{78} - t_{12}t_{48}t_{67}, & h_9 = t_{26}t_{78}t_{15} - t_{12}t_{67} \\
h_2 = t_{37}t_{26} - t_{23}t_{67}, & h_6 = t_{14}t_{56}t_{37} - t_{34}t_{15}t_{67}, & h_{10} = t_{56}t_{37}t_{48} - t_{34}t_{6} \\
h_3 = t_{12}t_{56} - t_{26}t_{15}, & h_7 = t_{23}t_{78}t_{15} - t_{12}t_{37}t_{58}, & h_{11} = t_{56}t_{78} - t_{67}t_{58} \\
h_4 = t_{14}t_{23} - t_{12}t_{34}, & h_8 = t_{23}t_{56}t_{48} - t_{26}t_{34}t_{58}, & h_{12} = t_{34}t_{78} - t_{37}t_{48}.
\end{array}$$

A curious feature here is that this basis is actually shorter than a 'natural' basis provided by all the edge cycles.
Consider the ideal $I = (h_1, h_2, h_3, h_4, h_{12})$. Notice that I is a complete intersection because the leading terms of the h_i's are relatively prime and therefore $\{h_1, h_2, h_3, h_4, h_{12}\}$ is a Gröbner basis for I.

The theoretical cost of these computations can be staggering, doubly exponential in the number of variables. This feature was already present in the classical analysis of the cost of computation in polynomial ideal theory by Grete Hermann. On the other hand, the dynamic behavior of Buchberger algorithm benefits from the average cost of the computation (linear in the number of variables). Furthermore, unlike the classical methods that had to work out always from a worst case assumption, Gröbner bases algorithms are eminently programmable.

Except for a few cases, it is impossible to predict what the normal form of the S–polynomial of two elements will look like. One of the exceptions, exhibited in the examples above, is that of an ideal generated by binomials: all polynomials in the process will be binomials. But even here, the worst case complexity is not any better.

Computation of Syzygies

Let $R = k[x_1, \ldots, x_n]$ be the ring of polynomials over a field k and let I be an ideal given by a set $\{f_1, \ldots, f_m\}$ of generators. In concrete situations, these generators carry along many mutual relationships. Furthermore, they were likely obtained in a 'natural' setting.
There are several strategies adapted for computation of the properties of the ring R/I:

- Transformation of the object into another with similar numerical data (*Hilbert Functions*).
- Comparison of objects by looking at their *syzygies*. Broadly, it is simpler to study an algebraic object **M** when it is *free*: the methods typical of linear algebra may be imported. Lacking freeness, one uses a presentation

$$\mathbf{K} \longrightarrow \mathbf{F} \longrightarrow \mathbf{M} \rightarrow 0,$$

  where **F** is a free object; **M** is equally well coded by the relations **K**. Typical examples are the (linear) relations of a set of generators of a module of an R–module or the (algebraic) relations of the generators of an affine k–algebra.
- Classical and modern elimination theory.
- Factorization techniques.

Gröbner Bases and Syzygies

Here we just outline how the first–order syzygies of an ideal $I = (F) = (f_1, \ldots, f_n)$ may be determined in principle. The generators are going to be taken as ordered, and we write one of its syzygies as a column vector $v \in R^n$ such that $F \cdot v = 0$. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis of I. For each pair of polynomials $\{g_i, g_j\}$ in G the S–polynomial $S(g_i, g_j)$ has a reduction

$$S(g_i, g_j) = a_j g_i - a_i g_j = \sum_{k=1}^{m} h_k g_k, \tag{17}$$

Buchberger Theorem.

In particular the vector

$$\begin{bmatrix} h_1 \\ \vdots \\ h_i - a_j \\ \vdots \\ h_j + a_i \\ \vdots \\ h_m \end{bmatrix} \tag{18}$$

is a syzygy of G. The following elementary fact ([Schreyer]) is extremely useful.

Theorem

The syzygies of G are generated by the vectors (18).

Proof. We leave its proof to the reader. □

Assembling the Syzygies

It is necessary to convert the syzygies of a Gröbner basis G into the syzygies of the basis F from which it was derived. It involves the two matrices that convert one set of generators into the other. The following observations were kindly pointed out to us by H.-G. Gräbe.

Denote by

$$\begin{aligned} F &= (f_1, \ldots, f_n) \\ G &= (g_1, \ldots, g_s). \end{aligned}$$

the ordered given generators and the computed Gröbner basis of a module Q, respectively. This gives rise to two transition matrices A and B

$$\begin{aligned} G &= F \cdot A \\ F &= G \cdot B, \end{aligned}$$

the first of which is obtained in the execution of the Buchberger algorithm, while the other is the representation of the elements of F by the normal form algorithm.

The syzygies of F are the column vectors $v \in R^m$ such that $F \cdot v = 0$. The module of syzygies of G is that described above, and at issue is how to convert from one module to the other.

Proposition

If S_G is a basis for the syzygies of G then the columns of

$$\left[\ E - A \cdot B \ \middle|\ A \cdot S_G\ \right]$$

is a basis for the syzygies of F, with E the $n \times n$ identity matrix.

Proof. The columns of this matrix are clearly syzygies of F. Conversely, if $F \cdot v = 0$, then $B \cdot v \in S_G$. In this case

$$\begin{aligned} v &= (E - A \cdot B) \cdot v + A \cdot B \cdot v \\ &\subset \text{column space}(E - A \cdot B) + \text{column space}(A \cdot S_G), \end{aligned}$$

which proves the assertion. □

Gröbner Bases over Rings

If k is a ring and $R = k[x_1, \ldots, x_n]$, any term ordering $<$ on the monomials $\mathbf{x}^\alpha$ permits the development of several aspects of Gröbner bases techniques to this extended setting. We recall here some aspects.

Let us fix a term order. Let I be an ideal of R and denote by $in(I)$ the ideal of all leading terms of elements of I.

Definition

A Gröbner basis of I is a family of polynomials

$$h_\alpha = f_\alpha + \text{lower order terms} \in I,$$

whose leading terms f_α span $in(I)$.

If R is Noetherian, the ideal $in(I)$ will be finitely generated. However, if I is finitely generated but R is not Noetherian then $in(I)$ may well be not finitely generated.
Unlike the field case, we now must keep track of the full leading term instead of just the leading monomial. If $f_\alpha, \alpha \in \Sigma$ is a set of monomials that generates $in(I)$, the leading coefficients of the f_α's now play an important role. There are significant similarities and contrasts, of which we consider a few cases.

Proposition

Suppose that the leading coefficients of the f_α's are all 1*. Then R/I is a free k–module with a basis given by the standard monomials.*

Computation of Gröbner Bases

There are two instances when the computation over Gröbner bases over $R[\mathbf{T}]$ can be dealt with much in the same manner as the case of a field.

Suppose k is a field, $R = k[\mathbf{x}]$, $A = R[\mathbf{T}]$, and $<$ is a product term order for monomials of A so that $x_i < T_j$. If I is an ideal of $A = R[\mathbf{T}]$, and we consider associated Gröbner bases G_1 and G_2, the first when only the order on the monomials on the T_j's are taken into account and the other when all monomials are considered.

$$\begin{aligned} G_1 &= \{g_\alpha(x)\mathbf{T}^\alpha + \text{lower order terms},\ \alpha \in \Sigma\} \\ G_2 &= \{\mathbf{x}^\beta \mathbf{T}^\gamma + \text{lower order terms},\ (\beta, \gamma) \in \Sigma'\}. \end{aligned}$$

It is clear that we can obtain a Gröbner basis equivalent to G_1 by arranging each polynomial in G_2 in the distributed form with respect to the T_j's.

A different kind of difficulty is that of a ring such as $R = \mathbb{Z}$. Here it is clear that Buchberger algorithm will produce a Gröbner basis provided that in the course of taking the S–resultant of pairs of polynomials, say $f = a\mathbf{T}^{\alpha} + \cdots$ and $g = b\mathbf{T}^{\beta} + \cdots$, one sets $S(f, g) = c \cdot f - d \cdot g$, where

$$c = \frac{b}{\gcd(a, b)}\mathbf{T}^{\gamma} \quad d = \frac{a}{\gcd(a, b)}\mathbf{T}^{\delta},$$

so that $\alpha + \gamma = \beta + \delta$ and $\operatorname{supp}(\gamma) \cap \operatorname{supp}(\delta) = \emptyset$.

Hilbert Functions

Let $A = k[x_1, \ldots, x_n]/I$ be a graded ring over the field k and denote by $H_A(\mathbf{t})$ its Hilbert function. The key to the computation of $H_A(\mathbf{t})$ is Macaulay Theorem: If $<$ is a term ordering and $I' = in(I)$ is the corresponding initial ideal, then $H_A(\mathbf{t}) = H_{A'}(\mathbf{t})$, where $A' = k[x_1, \ldots, x_n]/I'$.

We indicate some of the known approaches to find the coding of Hilbert functions by Hilbert–Poincaré series of algebras defined by monomial ideals. The more delicate points of these strategies, the aspects that must be carefully assembled to obtain optimization of coding, will not be treated here.

Suppose $I = (m_1, \ldots, m_r)$, where the m_i are monomials in the indeterminates $x_1, \ldots, x_n$. A theoretical approach is via Taylor resolutions, and derives the Hilbert–Poincaré series directly from the projective resolution of R/I. But this resolution can have as many as 2^r terms, which militates against its use if r is large.

Example: Monomials of Degree Two

We illustrate the kind of assemblage that takes place by considering a very straightforward case.

The usual path has been to "filter" the graded module R/I by other graded modules. Let us indicate this by treating one example in great detail. Suppose the monomials m_i are of degree two and square-free. The monomials model a graph G whose vertex set is $\{x_1, \ldots, x_n\}$, and whose edges are $\{x_k, x_\ell\}$ if $x_k x_\ell$ is one of the m_i; the algebra R/I is denoted $k[G]$. Adding variables to the monomial ideal corresponds to considering graphs with isolated vertices.

Let us derive the Hilbert–Poincaré series of $k[G]$ in terms of series for graphs with fewer vertices.

Proposition

Let G be a graph, and $P_G(\mathbf{t})$ the Hilbert–Poincaré series of the associated ring $k[G]$. For any vertex $x \in V(G) = \{x_1, \ldots, x_n\}$ we have

$$P_G(\mathbf{t}) = P_{G-x}(\mathbf{t}) + \frac{\mathbf{t}}{1-\mathbf{t}} P_{G-N(x)-x}(\mathbf{t})$$

with

$$P_\emptyset(\mathbf{t}) = 1.$$

Here $G - x$ denotes the graph obtained from G by deleting the vertex x, and $G - N(x) - x$ the graph from which x and all its neighbors $N(x)$ have been deleted.

Proof. Let $I = \{m_1, \ldots, m_s,\ x_{i_1}x_n, \ldots, x_{i_k}x_n\}$ where the $x_{i_1}, \ldots, x_{i_k}$ are the neighbors of the vertex x_n and the $m_1, \ldots, m_s$ are the remaining edges. We write $I = (x_nL, J)$, where $L = \{x_{i_1}, \ldots, x_{i_k}\}$ and $J = \{m_1, \ldots, m_s\}$.

From the exact sequence

$$0 \to (x_n, J)/I \longrightarrow R/I \longrightarrow R/(x_n, J) \to 0,$$

since $I\colon x_n = (L, J)$, we obtain the exact sequence

$$0 \to R/(L, J)(-1) \longrightarrow k[G] \longrightarrow k[G - x_n] \to 0$$

from which we have the equality of series

$$P_G(\mathbf{t}) = \mathbf{t} \cdot P_{R/(L,J)}(\mathbf{t}) + P_{G-x_n}(\mathbf{t}).$$

Finally, note that x_n is not a vertex of the graph represented by (L, J), so that

$$R/(L, J) = k[G - N(x_n) - x_n][x_n],$$

and therefore

$$P_{R/(L,J)}(\mathbf{t}) = \frac{1}{1 - \mathbf{t}} \cdot P_{k[G-N(x_n)-x_n]}(\mathbf{t}),$$

to complete the proof. □

This device may also be used for more general ideals, like those generated by squarefree monomials of arbitrary degrees. For example, if Δ is a simplicial complex and x is one of its vertices, and

$$\Delta = x * \Delta_1 \cup \Delta_2$$

is a disjoint decomposition, then one has an exact sequence

$$0 \to k[\Delta_1 \cup \Delta_2][-1] \longrightarrow k[\Delta] \longrightarrow k[\Delta_2] \to 0,$$

of face rings, with a corresponding relation of their Hilbert functions.

General Monomials

Given a monomial ideal I and a monomial f there is the exact sequence

$$0 \to R/(I\colon f)(-d) \longrightarrow R/I \longrightarrow R/(I,f) \to 0,$$

where $d = \deg f$. It follows that

$$P_{R/I}(\mathbf{t}) = P_{R/(I,f)}(\mathbf{t}) + \mathbf{t}^d P_{R/(I\colon f)}(\mathbf{t}).$$

The researchers have an abbreviated notation for these series:

$$\langle I\rangle = \langle I,f\rangle + \mathbf{t}^d\langle I\colon f\rangle.$$

Here are two approaches that have been used. They further differ in the way that corner cases are handled.

(a) (Bayer-Stillman) The equality above can be used backwards: If J is an ideal and $J = (I, f)$, then

$$\langle J \rangle = \langle I \rangle - \mathbf{t}^d \langle I : f \rangle,$$

where both I and $I : f$ have fewer generators that J. This is the approach that was originally implemented in *Macaulay*.

(b) (Bigatti-Caboara-Robbiano) In this approach, used in *CoCoA*, f is chosen to be a variable that occurs in the monomials: $R/(I, f)$ is defined over fewer variables, while the ideal $I : f$ is given as follows. If $I = (fL, J)$, and f does not occur in the monomials of J, then $I : f = (L, J)$. Taking for f the highest power of a variable x_n that occur in the monomials strips that variable from all monomials of $I : f$, but may complicate the handling of (I, f), except when the degree is very low.

Outline

Toolkit

In this section we treat some fundamental devices to manipulate ideals of rings of polynomials to form new rings and to set up the conditions to help ascertain the presence of certain properties in rings, modules and their morphisms.

- Nuts and bolts
- Rings of endomorphisms
- Noether normalization
- Fitting ideals
- Integral extensions
- Flatness and Cohen–Macaulayness testing

Elimination techniques have been in the forefront of applications of Gröbner bases to ideal theory from very early. The required adjunction of new variables is often very natural and appealing despite the potential threat of combinatorial explosion.

There are related two operations with ideals which are pervasive in the constructions. They are:

- The formation of ideal quotients,

$$I : J = \{ x \in R \mid x \cdot J \subset I \}$$

  in a ring of polynomials R
- The construction of the ring of endomorphisms $\mathrm{Hom}_R(I, I)$ of an ideal I in an affine domain R.

Their key role occurs since (i) through $I : J$ one perturbs the primary decomposition of I in a reasonably controlled form, and (ii) $\mathrm{Hom}_R(I, I)$ leads to a new algebra which is an integral extension of R. They represent basic manipulations with the functor Ext of homological algebra.

Another major process, necessary to study morphisms of rings, is Noether normalization. It provides a baseline, adequate for Gröbner basis computation, from which to convert problems into others that may be amenable to linear algebra techniques.

Elimination Techniques

Elimination Theory is concerned with the determination of the image of a morphism between algebraic varieties

$$\varphi : Y \mapsto X.$$

Its computational aspect consists in the development of techniques to solve the following problem. Given a homomorphism of rings

$$\psi : A \mapsto B,$$

and an ideal $L \subset B$, determine the ideal

$$I = \psi^{-1}(L) \subset A.$$

Strictly speaking these two formulations are not equivalent except under conditions controlled by the fundamental:

Elimination Techniques

Theorem (Main Theorem of Elimination Theory)

Let R be a Noetherian ring and let $\mathbb{P}^n_R$ be a projective space over $\mathrm{Spec}(R)$. The projection

$$\mathrm{p} : \mathbb{P}^n_R \mapsto \mathrm{Spec}(R)$$

is a closed mapping.

In actual practice, A and B are affine rings and the issue is to find a description of the image of the corresponding morphism of affine varieties. The most important case is that of a ring B which is a polynomial ring over A, $B = A[\mathbf{T}] = A[T_1, \ldots, T_m]$.

Elimination Techniques

Let R be the polynomial ring $k[x_1, \ldots, x_n]$, let t be an indeterminate over R, and put $B = R[t]$. Let I be an ideal of B. The technique of elimination of variables is based on the following:

Proposition

Let T be an ordering of the variables such that $t >_T \mathbf{x}^{\mathbf{a}}$ for any monomial in the x_i's. Let F be a Gröbner basis of I. Then $F \cap R$ is a Gröbner basis of $I \cap R$.

Proof. Follows immediately from the division algorithm. □

Elimination Techniques

Replacing $t \mapsto \mathbf{T}$ in the Gröbner basis calculation, the full set $\mathbf{T}$ can be eliminated. Alternatively the T_i can be successively eliminated.

Corollary

If I and J are two ideals of R, then $I \cap J$ can be computed.

Proof. To apply the Proposition, we must show how $I \cap J$ can be obtained as the contraction of some ideal $L \subset R[t]$.
We claim that if t is a new variable, then
$I \cap J = (I \cdot t, J \cdot (1-t)) \cap R$. Indeed, if $a \in I \cap J$, then

$$a = at + (1-t)a.$$

On the other hand, any element of $(I \cdot t, J \cdot (1-t)) \cap R$,

$$b = \sum a_i h_i(t) t + \sum b_j g_j(t)(1-t),\ a_i \in I,\ b_j \in J,\ h_i(t), g_j(t) \in R[t],$$

evaluates to itself if $t \mapsto 0$ or $t \mapsto 1$, but it is mapped into J in

The ability to compute syzygies gives a distinct advantage in carrying out the ideal theoretic operations mentioned earlier. For instance, the computation of the intersection of two ideals $I = (a_1, \ldots, a_m)$ and $J = (b_1, \ldots, b_n)$ is now handled as that of finding the syzygies of the matrix

$$\begin{bmatrix} 1 & a_1 & \cdots & a_m & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 & b_1 & \cdots & b_n \end{bmatrix}.$$

The desired intersection is the ideal generated by the entries at $(1, \cdots)$

Corollary (Radical Membership)

If $f \in R$ and I is an ideal, then $f \in \sqrt{I}$ can be decided.

Proof. If t is a variable, and R is any commutative ring, then $f \in \sqrt{I}$ if and only if $(I, 1 - tf) = R[t]$. (Details left as an exercise.) □

Homomorphisms of Affine Rings

A k–homomorphism

$$\psi : A = k[x_1, \ldots, x_s]/(f_1, \ldots, f_m) \mapsto B = k[y_1, \ldots, y_r]/J,$$

of two affine k–algebras is the assignment

$$x_i \mapsto g_i(y_1, \ldots, y_r) \in k[y_1, \ldots, y_r], \ i = 1, \ldots, s$$

such that $f_j(g_1, \ldots, g_s) \in J$, for all i.

Image of a Morphism

Another application of elimination is to determine the image of a mapping between affine spaces. Let $\phi\colon \mathbb{A}^r \mapsto \mathbb{A}^s$ be a polynomial mapping between two affine spaces defined over a field k. Denote by I the ideal of all polynomials $h(Y_1, \ldots, Y_s) \in k[Y_1, \ldots, Y_s]$ that vanish on the image of ϕ:

$$\{x \in k^r \mid h(\phi_1(x), \ldots, \phi_s(x)) = 0\}.$$

Proposition

Let k be an infinite field and let ϕ be as above. Then

$$I = (Y_i - \phi_i(X),\ i = 1, \ldots, s) \cap k[Y].$$

Proof. For $h(Y) \in I$ we have

$$\begin{aligned} h(Y_1, \ldots, Y_s) &= h(\phi_1(X) + (Y_1 - \phi_1(X)), \ldots, \phi_s(X) + (Y_s - \phi_s(X)) \\ &= h(\phi_1(X), \ldots, \phi_s(X)) + \sum_i h_i(X, Y)(Y_i - \phi_i(X)). \end{aligned}$$

In one direction the assertion follows since $h(\phi_1(X), \ldots, \phi_s(X))$ vanishes identically. The converse is clear. □

More generally, suppose $\phi\colon V \mapsto W$ is a morphism of affine subvarieties of $\mathbb{A}^r$ and $\mathbb{A}^s$ respectively.

Proposition

Let I_V and I_W denote the ideals defining V and W. Then

(a) *The image of V lies in W if and only if $h(\phi(x)) = 0$ for any $h \in I_W$.*

(b) *The closure of the image of V is defined by the ideal*

$$I = (I_V + (Y_i - \phi_i(X),\ i = 1, \ldots, s)) \cap k[Y].$$

Proof. We leave the verifications to the reader.

Example

A motivation for deciding the membership question in rings of polynomials is provided by the following formulation by D. Bayer of the 4-color question. Let $\mathcal{M}$ be a map made up of the regions $R_i,\ i \in A$, that we want to color with, say, 4 colors. The 'colors' we use will be the four roots of 1. In the ring of polynomials

$$R = k[x_i,\ i \in A],$$

let I be the ideal generated by all $f_i = x_i^4 - 1$ and the polynomials

$$h_{ij} = x_i^3 + x_i^2 x_j + x_i x_j^2 + x_j^3,$$

associated to each neighboring pair of regions R_i, R_j. Noting that h_{ij} only vanishes along with f_i, f_j when the roots of these polynomials are chosen to be distinct, it follows from the Nullstellensatz that $I \neq R$ if and only if $\mathcal{M}$ is 4-colorable.

Regular Elements and Ideal Quotients

Two of the most common manipulations with ideals concern the underlying primary decompositions.

Definition

Given two ideals I and J of a ring R, the *ideal quotient* of I by J is the ideal

$$I\colon J = \{r \in R \mid r \cdot J \subset I\}.$$

It will figure prominently in our constructions, so that we must have several ways to find it.

Proposition

An element $f \in R$ is regular modulo the ideal I if and only if one of the following conditions hold in $R[t]$:

(a) $((I \cdot t, (1-t) \cdot f) \cap R) \cdot f^{-1} = I.$

(b) $(I, 1 - f \cdot t) \cap R = I.$

The first formula computes $I :_R f$, whereas the second determines

$$I : \langle f \rangle = \bigcup_{n \geq 1} (I :_R f^n).$$

Perhaps the most direct approach is: If $J = (a_1, \ldots, a_n)$, it can be computed as

$$I \colon J = \bigcap_{i=1}^{n} (I \colon a_i).$$

An alternative is the following construction.

Proposition

Let t be a variable over the ring R and let

$$f = a_1 + a_2 t + \cdots + a_n t^{n-1}.$$

Then

$$I \colon J = (I \cdot R[t] \colon f) \cap R.$$

Saturation

Definition

Let I and J be two ideal of the ring R. The saturation of I with respect to J is the limit ideal quotient

$$I : \langle J \rangle = I : J^{\infty} = \bigcup_{k} (I : J^{k}).$$

Proposition

Let f be the polynomial defined above and let y be a fresh variable. Then

$$I\colon J^{\infty} = ((I, y - f)\colon y^{\infty}) \cap R.$$

Comparison of Ideals

One of the most common tasks faced is that of comparing two ideals I and J for containment. It is usually set up by assuming $I \subset J$, after replacing $J \mapsto I + J$. Since several systems have implemented the quotient of ideals operation,

$$I = J \iff I : J = (1). \tag{19}$$

When I and J are homogeneous ideals, one can also just compare their Hilbert functions:

$$I = J \Leftrightarrow H_{R/I}(\mathbf{t}) = H_{R/J}(\mathbf{t}) \Leftrightarrow H_I(\mathbf{t}) = H_J(\mathbf{t}).$$