April 22: Integral closure of ideals, multiplicity, and the Rees multiplicity theorem, part 2

Integral closure of ideals revisited

Our next Theorem is a special case of one of the main theorems in the theory of reductions of ideals due to Northcott and Rees. Their famous 1953 paper titled Reductions of ideals in local rings is one of the most frequently cited papers in commutative algebra.

For the theorem below, we will use the Noether Normalization Theorem, one version of which is the following:

Let k be an infinite field and B a finitely generated, graded k algebra, which is generated over k by homogenous elements of degree one.

If $\dim(B) = r$, then there exist $b_1, \ldots, b_r \in B_1$, such that $b_1, \ldots, b_r$ are algebraically independent over k and B is a finite module over $A := k[b_1, \ldots, b_r]$.

Integral closure of ideals revisited

Theorem F5. Let $(R, \mathfrak{m})$ be a local ring with infinite residue field k. Then, for any $\mathfrak{m}$-primary ideal $I \subseteq R$, there exists an ideal J, generated by a system of parameters, such that $\overline{J} = \overline{I}$.

Proof. Let $\mathcal{R}$ denote the Rees ring of R with respect to I, so that $R := R[It] = R \oplus It \oplus I^2t^2 \oplus \cdots$. The k-algebra $B := \mathcal{R}/\mathfrak{m}\mathcal{R}$ is a finitely generated, graded k-algebra generated by homogeneous elements of degree one over k. Note, that as a graded k-algebra, $B = k \oplus I/\mathfrak{m}I \oplus I^2/\mathfrak{m}I^2 \oplus \cdots$.

By Noether's Normalization Lemma, there exist $b_1, \ldots, b_r \in B_1$, such that $b_1, \ldots, b_r$ are algebraically independent over k and B is a finite module over $A := k[b_1, \ldots, b_r]$. Note that each $b_i = \overline{a_i}$, for some $a_i \in I \backslash \mathfrak{m}I$.

We are now in an Artin-Rees like situation. B is a finite, graded module over the graded ring A, and as such we can take finitely many homogenous elements $c_1, \ldots, c_s \in B$ that generate B as an A-module.

If n is the maximum degree of any c_j, then it follows that for all $t \geq 0$, $B_{n+t} = A_t \cdot B_n$.

In particular, $B_{n+1} = A_1 B_n$.

Integral closure of ideals revisited

Interpreting this in terms of R, we have $I^{n+1} \subseteq JI^n + \mathfrak{m}I^{n+1}$, where $J = (a_1, \ldots, a_r)R$.

We note two things: (i) $I^{n+1} \subseteq JI^n$, by Nakayama's lemma and

(ii) $\dim(B) = \dim(R)$. This follows since (Atiyah-MacDonald, Chapter 11),

$$\mathcal{R}/I\mathcal{R} = \bigoplus_{\mathfrak{n} \geq 0} I^n/I^{n+1},$$

the associated graded ring of R with respect to I, has dimension equal to $\dim(R)$.

Since $\mathfrak{m}^n\mathcal{R} \subseteq I\mathcal{R} \subseteq \mathfrak{m}\mathcal{R}$, it follows that $\mathcal{R}/I\mathcal{R}$ and B have the same dimension.

Thus, $r = d$ and J is generated by a system of parameters.

Since $J \subseteq I$ and $JI^n \subseteq I^{n+1}$, we have $JI^n = I^{n+1}$.

Integral closure of ideals revisited

We now show $\overline{J} = \bar{I}$. Let $q \subseteq R$ be a minimal prime ideal. By Lemmma B3, it is enough to show that the image of I in R/q and the image of J in R/q have the same integral closure.

Since the identity $I^{n+1} = JI^n$ also holds modulo q, we may replace R/q by R and assume that R is an integral domain.

Let V be a DVR between R and its quotient field. Then, $I^{n+1}V = JI^nV$.

Since the ideals IV and JV are principal ideals, we may cancel I^n from both sides of this equation to get $IV = JV$.

Since this holds for all DVRs V, we have $\overline{I} = \overline{J}$, by Theorem A5. □

We now begin our discussion of multiplicities. As expected, we will prove a standard result about the existence of Hilbert polynomials associated to graded modules over a graded ring.

The following is a key technical lemma needed for the induction part of the proof of the existence of Hilbert polynomials. For this lemma, we need the following remark concerning primary decomposition in modules. Note, in this case, for example, the zero submodule of M is an intersection of primary submodules, each of which is a graded submodule of M.

Remark. Let A be a Noetherian ring and M a finitely generated A-module. A submodule $N \subseteq M$ is said to be *P-primary*, for the prime ideal $P \subseteq A$ if $\mathrm{Ass}_A(M/N) = P$.

Note that if $I \subseteq A$ is an ideal, then this is saying the same thing as I is P-primary, since then $\mathrm{Ass}_A(R/I)$ is P-primary.

If A is a graded ring and M, N are graded modules, then the associated primes are homogeneous.

Superficial elements

Lemma G5. Let $A = \bigoplus_{n\geq 0} A_n$ be a finitely generated R-algebra, where $A_0 = (R, \mathfrak{m}, k)$ is a local ring with infinite residue field. Write $\mathcal{M}$ for the homogeneous maximal ideal $(\mathfrak{m}, A_+)A$. We assume that A is a standard, graded R-algebra, i.e., $A = R[A_1]$. Let $M = \bigoplus_{n\geq 0} M_n$ be a finitely generated, graded A-module.

If $\mathrm{Ass}(M) \neq \mathcal{M}$, then there exists $f \in A_1$ and $c > 0$ such that $(0 :_M f)_n = 0$, for all $n \geq c$. In other words, elements in M annihilated by f are concentrated in degrees less than c.

Proof. Let $(0) = N_1 \cap \cdots \cap N_r \cap N_{r+1} \cap \cdots \cap N_2$ be a primary decomposition, where for $1 \leq i \leq r$, $\mathrm{Ass}_A(M/N_i) = Q_i$ does not contain A_+ and for $r+1 \leq i \leq s$, $A_+ \subseteq Q_i = \mathrm{Ass}(M/N_i)$.

We claim there exists $f \in A_1$ such that $f \notin Q_1 \cup \cdots \cup Q_r$. Suppose the claim holds. Take $c > 0$ such that for $r+1 \leq i \leq s$, $(M/N_i)_n = 0$, for $n \geq c$. This is possible since each M/N_i is annihilated by a power of A_+.

Then for $n \geq c$, if $b \in M_n$ and $fb = 0$, on the one hand, $fb \in N_i$ for all $1 \leq i \leq r$, which, by the choice of f, implies $b \in N_i$, all i.

Superficial elements

On the other hand, by the choice of c, $b \in N_{r+1} \cap \cdots \cap N_s$.

Thus b belongs to all of the primary components of (0), so $b = 0$.

For the claim, consider the k-vector space $V := A_1/\mathfrak{m}A_1$ and the subspaces $L_i := ((Q_i)_1 + \mathfrak{m}A_1)/\mathfrak{m}A_1$, $1 \leq i \leq r$. These are proper subspaces of V, for if say, $L_i = V$, then $A_1 = (Q_i)_1 + \mathfrak{m}A_1$.

Since A is a standard graded algebra, this implies $A_+ \subseteq Q_i + \mathcal{M}A_+$, which by Nakayama's lemma (the graded version) implies $A_+ \subseteq Q_i$, a contradiction.

Thus, the subspaces L_i are proper subspaces of V, and since k is infinite, there exists $\overline{f} \in V \backslash (L_1 \cup \cdots \cup L_r)$.

Thus, $f \in A_1$, but f is not in any Q_i, as required. □

Comments

Definition and comments. One can draw a similar conclusion to Lemma 5G if k is not infinite. One uses the homogeneous form of prime avoidance. This, together with the definition of the Q_j, imply that $A_+ \not\subseteq Q_1 \cup \cdots \cup Q_r$, and thus, there exists a homogeneous ring element f not in $Q_1 \cup \cdots \cup Q_r$, and the conclusion of the lemma still holds for this f.

However, f may not be homogeneous of degree one. Such elements are called superficial elements, and if $f \in A_d$, then f is a superficial element of degree d. Thus, superficial elements of some positive degree exist, but superficial elements of degree one need not always exist.

Facts about numerical polynomials. A numerical polynomial is a polynomial $P(x) \in \mathbb{Q}$ such that $P(n) \in \mathbb{Z}$, for all $n \in \mathbb{Z}$ (or equivalently, all $n \in \mathbb{N}$).

Note that the polynomial associated to the binomial coefficient, $\binom{x+d}{d} := \frac{1}{d!} \cdot (x+d)(x+d-1)\cdots(x+1)$ is a numerical polynomial of degree d.

A function $f : \mathbb{Z} \to \mathbb{Z}$ is said to *agree with a numerical polynomial for* $n >> 0$ if there exists $n_0 \in \mathbb{N}$ and a numerical polynomial $F(x)$ such that $f(n) = F(n)$, for all $n \geq n_0$.

We will use the following two facts.

Comments

(i) Any numerical polynomial $P(x)$ of degree d can be written uniquely as

$$P(x) = e_0 \binom{x+d}{d} + e_1 \binom{x+d-1}{d-1} + \cdots + e_d \binom{x+0}{0},$$

with the $e_j \in \mathbb{Z}$.

To see this, first note that since each $\binom{x+d}{d}$ has degree d, these polynomials form a basis for $\mathbb{Q}[x]$ as a vector space over $\mathbb{Q}$.

Thus any polynomial in $\mathbb{Q}[x]$ can be written uniquely as a $\mathbb{Q}$-linear combination of the $\binom{x+j}{j}$.

However, if $P(x)$ is a numerical polynomial, then one can show by induction on the degree of $P(x)$ that the coefficients e_j above must be integers.

Note also, that if $P(n) \in \mathbb{N}$, for $n \in \mathbb{N}$, then $e_0 \in \mathbb{N}$.

Comments

(ii) Suppose $f : \mathbb{N} \to \mathbb{N}$ has the property that $f(n+1) - f(n)$ agrees with a numerical polynomial of degree d for $n >> 0$. Then $f(n)$ agrees with a numerical polynomial of degree $d+1$ for $n >> 0$.

To see this, suppose suppose $f(n+1) - f(n) = P(n)$, for $n >> 0$, where

$$P(x) = \sum_{j=0}^{d} e_j \binom{x+d-j}{d-j}.$$

Set

$$F(x) := \sum_{j=0}^{d} e_j \binom{x+d-j}{d-j+1}.$$

Then, for $n >> 0$,

$$\begin{aligned} F(n+1) - F(n) &= \sum_{j=0}^{d} e_j \{ \binom{n+1+d-j}{d-j+1} - \binom{n+d-j}{d-j+1} \} \\ &= \sum_{j=0}^{d} e_j \binom{n+d-j}{d-j} \\ &= f(n+1) - f(n). \end{aligned}$$

Comments

It follows that $(F-f)(n+1)-(F-f)(n)=0$, for $n>>0$. Thus, $(F-f)(n)=c$, a constant for $n>>0$.

Therefore, $f(n)=F(n)-c$, for $n>>0$, which shows that $f(n)$ agrees with a numerical polynomial of degree $d+1$ for $n>>0$.

Comments on extending the residue field. (i) Let $(R,\mathfrak{m},k)$ be local ring with finite residue field k. Take an indeterminate y and consider the ring the ring $R[y]_{\mathfrak{m}R[y]}$. This ring is denoted $R(y)$.

Then $R(y)$ is a faithfully flat local extension of R whose maximal ideal is $\mathfrak{m}R(y)$ and whose residue field $k(y)$ is infinite. Let $U\subseteq V$ be two R-modules such that $\lambda(V/U)=1$. Then there is an exact sequence

$$0\to U\to V\to k\to 0.$$

If we tensor this exact sequence with $R(y)$, we have

$$0\to U\otimes R(y)\to V\otimes R(y)\to k(y)\to 0,$$

where $k(y)$ is the residue field of $R(y)$.

Comments

Thus, $\lambda_{R(y)}(V \otimes R(y)/U \otimes R(y)) = 1$. It follows that if C is a finite length R-module having length c, then $C \otimes R(y)$ is a finite length $R(y)$-module with length c.

In particular, if $J \subseteq R$ is an $\mathfrak{m}$-primary ideal, then, since $JR(y) = J \otimes R(y)$, $\lambda(R/J) = \lambda(R(y)/JR(y))$.

(ii) Now suppose A is a standard graded ring, finitely generated as an algebra over $A_0 = (R, \mathfrak{m}, k)$. Then $\tilde{A} := A \otimes_R R(y)$ is a standard graded ring, finitely generated as an algebra over $R(y)$ and if M is a finite, graded A-module, then $\tilde{M} := M \otimes_R R(y)$ is a finite, graded $\tilde{A}$-module.

It is straightforward to show that since $R(y)$ is faithfully flat over R, then $\tilde{A}$ is faithfully flat over A. In fact, if $U = R[y] \backslash \mathfrak{m}R[y]$, then $\tilde{A}$ can be identified with $A[y]_U$.

Now suppose $\dim(M) = d$. Then $\dim(A/J) = d$, where J is the annihilator of M. If we take a set of generators $x_1, \ldots, x_r$ of M,
then we have an exact sequence

$$0 \to J \to A \xrightarrow{\phi} M \oplus \cdots \oplus M,$$

where $\phi(a) = (ax_1, \ldots, ax_d)$, for all $a \in A$.

Comments

If we tensor this exact sequence with $\tilde{A}$, we have an exact sequence

$$0 \to J \otimes_A \tilde{A} \to \tilde{A} \stackrel{\phi\otimes 1}{\to} \tilde{M} \oplus \cdots \oplus \tilde{M},$$

where $\phi \otimes 1$ takes $\tilde{a} \in \tilde{A}$ to $\tilde{a}(x_i \otimes 1)$ in each component. Since the $x_0 \otimes 1$ generate $\tilde{M}$, we have $J \otimes_A \tilde{A} = J\tilde{A}$ is the annihilator of $\tilde{M}$.

Now, the fibers over the faithfully flat extension $A/J \subseteq \tilde{A}/J\tilde{A}$ are just the fibers over $P \subseteq A$ for the inclusion $A \subseteq \tilde{A}$, for those primes P with $J \subseteq P$. Since the fibers of the inclusion $A \subseteq \tilde{A}$ are zero dimensional[1], it follows that $\dim(A/J) = \dim(\tilde{A}/J\tilde{A})$. Hence $\dim(M) = \dim(\tilde{M})$.

Finally, the discussion in (i) above shows that

$$\lambda_{R(y)}(\tilde{M}_n) = \lambda_{R(y)}(R(y) \otimes_R M_n) = \lambda_R(M_n),$$

for all $n \geq 0$.

This shows that in finding the Hilbert polynomial of a graded module, we may assume that the degree zero component of the underlying ring has an infinite residue field.

[1] If $p \subseteq A$ is a prime ideal, then the fiber over P in $\tilde{A}$ is just $k(p)(y)$.

Therem H5. Let $A = \bigoplus_{n\geq 0} A_n$ be a finitely generated R-algebra, where $A_0 = (R, \mathfrak{m}, k)$ is a local Artinian ring. We assume that A is a standard, graded R-algebra, i.e., $A = R[A_1]$. Let $M = \bigoplus_{n\geq 0} M_n$ be a finitely generated, graded A-module. Then $H_M(n) := \lambda_R(M_n) < \infty$, for all n and $H_M(n)$ agrees with a numerical polynomial $P_M(x)$ of degree $\dim(M) - 1$, for $n >> 0$.

Proof. To see that $\lambda(M_n) < \infty$ for all n, note that

$$M_0 \oplus M_1 \oplus \cdots \oplus M_n = M/M_{\geq n+1}$$

is a finite A-module annihilated by A_+^{n+1}. Thus, it is a finite A/A_+^{n+1}-module. This latter ring is finite over R, which implies that $M_0 \oplus M_1 \oplus \cdots \oplus M_n$ is a finite R-module.

Thus, each M_j is a finite R-module, and therefore has finite length.

To show the existence of $P_M(n)$, by the comments above, if need be, we may replace A by $R(y) \otimes_R A$ and M by $R(y) \otimes_R M$. This preserves the lengths and dimensions in question, so we may pass to $R(y)$ and upon changing notation assume that residue field of R is infinite.

Hilbert Polynomials

We induct on $\dim(M)$. If $\dim(M) = 0$, then any prime ideal Q minimal over the annihilator of M is a maximal ideal.

On the other hand, since M is a graded A-module, its associated primes are graded. Since $A_0 = R$ is local, $\mathcal{M}$ is the only graded maximal ideal.

Thus some power of A_+ is contained in the annihilator of M, which implies $M_n = 0$, for $n >> 0$.

Thus, we may take $P_M(x)$ to be the zero polynomial, which by standard convention has degree -1.

Now suppose $\dim(M) > 0$. Then $\mathrm{Ass}(M) \neq \mathcal{M}$, so by Lemma G5, there exists $f \in A_1$ a superficial element on M.

We will assume f has been chosen as in the proof of Lemma G5. Suppose $c > 0$ satisfies $(0 :_M f)_n = 0$, for all $n \geq c$.

We have an exact sequence of graded A-modules

$$M \xrightarrow{\cdot f} M \to M/fM \to 0,$$

which induces an exact sequence of R-modules

$$M_{n-1} \xrightarrow{\cdot f} M_n \to (M/fM)_n \to 0,$$

for all n.

Our choice of n implies that the sequence

$$0 \to M_{n-1} \xrightarrow{\cdot f} M_n \to (M/fM)_n \to 0,$$

is exact for all $n \geq c+1$. It follows that $H_M(n) - H_M(n-1) = H_{M/fM}(n)$, for all $n \geq c+1$.

Hilbert Polynomials

Our choice of f, and $\dim(M) > 0$, imply that f is not in any prime minimal over the annihilator of M, so that $\dim(M/fM) = \dim(M) - 1$.

By induction, $H_{M/fM}(n)$ agrees with a numerical polynomial $P_{M/fM}(x)$ of degree $\dim(M/fM) - 1$ for $n >> 0$.

On the other hand, since $H_M(n) - H_M(n-1) = H_{M/fM}(n)$, for all $n \geq c+1$, by the second remark above concerning numerical polynomials, $H_M(n)$ agrees with a numerical polynomial, say $P_M(x)$, for $n >> 0$ whose degree equals $1 + \mathrm{degree}(P_{M/fM}(x))$.

But $1 + \mathrm{degree}(P_{M/fM}(x)) = \dim(M) - 1$, which is what we want. □

Definition. The function $H_M(n)$ above is called the Hilbert function of M, while the polynomial $P_M(x)$ is called the Hilbert polynomial of M.