Math 711: Lecture of October 20, 2006

We next prove illustrate the method of reduction to characteristic p by proving the Briançon-Skoda theorem for polynomial rings over a field of characteristic 0 by that method.

We need Noether normalization over a domain, and we first give a lemma:

Lemma. *Let A be a domain and let $f \in A[x_1, \ldots, x_n]$. Let $N \geq 1$ be an integer that bounds all the exponents of the variables occurring in the terms of f. Let ϕ be the A-automorphism of $A[x_1, \ldots, x_n]$ such that $x_i \mapsto x_i + x_n^{N^i}$ for $i < n$ and such that x_n maps to itself. Then the image of f under ϕ, when viewed as a polynomial in x_n, has leading term ax_n^m for some integer $m \geq 1$, with $a \in A - \{0\}$. Thus, over A_a, $\phi(f)$ is a scalar in A_a times a polynomial in x_n that is monic.*

Proof. Consider any nonzero term of f, which will have the form $c_\alpha x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, where $\alpha = (a_1, \ldots, a_n)$ and c_α is a nonzero element in A. The image of this term under ϕ is

$$c_\alpha (x_1 + x_n^N)^{a_1} (x_2 + x_n^{N^2})^{a_2} \cdots (x_{n-1} + x_n^{N^{n-1}})^{a_{n-1}} x_n^{a_n},$$

and this contains a unique highest degree term: it is the product of the highest degree terms coming from all the factors, and it is

$$c_\alpha (x_n^N)^{a_1} (x_n^{N^2})^{a_2} \cdots (x_n^{N^{n-1}})^{a_{n-1}} x_n^{a_n} = c_\alpha x_n^{a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1}}.$$

The exponents that one gets on x_n in these largest degree terms coming from distinct terms of f are all distinct, because of uniqueness of representation of integers in base N. Thus, no two exponents are the same, and no two of these terms can cancel. Therefore, the degree m of the image of f is the same as the largest of the numbers

$$a_n + a_1 N + a_2 N^2 + \cdots + a_{n-1} N^{n-1}$$

as $\alpha = (a_1, \ldots, a_n)$ runs through n-tuples of exponents occurring in nonzero terms of f, and for the choice α_0 of α that yields m, $c_{\alpha_0} x_n^m$ occurs in $\phi(f)$, is the only term of degree m, and and cannot be canceled. It follows that $\phi(f)$ has the required form. $\square$

Theorem (Noether normalization over a domain). *Let R be a finitely generated extension algebra of a Noetherian domain A. Then there is an element $a \in A - \{0\}$ such that R_a is a module-finite extension of a polynomial ring $A_a[z_1, \ldots, z_d]$ over A_a.*

Proof. We use induction on the number n of generators of R over A. If $n = 0$ then $R = A$. We may take $d = 0$. Now suppose that $n \geq 1$ and that we know the result for algebras generated by $n - 1$ or fewer elements. Suppose that $R = A[\theta_1, \ldots, \theta_n]$ has n generators. If the θ_i are algebraically independent over K then we are done: we may take $d = n$

and $z_i = \theta_i$, $1 \le i \le n$. Therefore we may assume that we have a nonzero polynomial $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ such that $f(\theta_1, \dots, \theta_n) = 0$. Instead of using the original θ_j as generators of our K-algebra, note that we may use instead the elements

$$\theta_1' = \theta_1 - \theta_n^N, \theta_2' = \theta_2 - \theta_n^{N^2}, \dots, \theta_{n-1}' = \theta_{n-1} - \theta_n^{N^{n-1}}, \theta_n' = \theta_n$$

where N is chosen for f as in the preceding Lemma. With ϕ as in that Lemma, we have that these new algebra generators satisfy $\phi(f) = f(x_1 + x_n^N, \dots, x_{n-1} + x_n^{N^{n-1}}, x_n)$ which we shall write as g. We replace A by A_a, where a is the coefficient of x_n^m in g. After multiplying by $1/a$, we have that g is monic in x_n with coefficients in $A_a[x_1, \dots, x_{n-1}]$. This means that θ_n' is integral over $A_a[\theta_1', \dots, \theta_{n-1}'] = R_0$, and so R_a is module-finite over R_0. Since R_0 has $n-1$ generators over A_a, we have by the induction hypothesis that $(R_0)_b$ is module-finite over a polynomial ring $A_{ab}[z_1, \dots, z_{d-1}] \subseteq (R_0)_b$ for some nonzero $b \in A$, and then R_{ab} is module-finite over $A_{ab}[z_1, \dots, z_d]$ as well. $\square$

We can now prove:

Theorem (generic freeness). *Let A be a Noetherian domain. Let M be a finitely generated module over a finitely generated A-algebra R. Then there exists $a \in A - \{0\}$ such that M_a is A_a-free. In particular, there exists $a \in A - 0$ such that R_a is A_a-free.*

Proof. Note that we may localize at an element repeatedly (but finitely many times), since one can achieve the same effect by localizing at one element, the product of the elements used. We use Noetherian induction on M and also induction on $\dim(\mathcal{K} \otimes_A M)$, where $\mathcal{K} = \mathrm{frac}\,(A)$. If a module has a finite filtration in which the factors are free, the module is free. (By induction, this comes down to the case where there are two factors, N, and M/N. When M/N is free, the short exact sequence $0 \to N \to M \to M/N \to 0$ is split, so that $M \cong M/N \oplus N$.) We may take a finite prime cyclic flitration of M, and so reduce to the case where $M = R/P$. We may replace R by R/P and so assume that $R = M$ is a domain. By the Noether Normalization Theorem for domains, we may replace A by A_a for $a \in A - \{0\}$ and so assume that R is module-finite over a polynomial ring $R_0 = A[x_1, \dots, x_n]$ over A. We may then replace R by R_0, viewing R as a module over R_0. This module has a prime cyclic filtration in which each factor is either $A[x_1, \dots, x_n]$, which is already free, or a quotient B_i of it by a nonzero prime ideal, and $\dim(\mathcal{K} \otimes_A B) < n$. Thus, for each B_i we can choose $a_i \in A - \{0\}$ such that $(B_i)_{a_i}$ is A_{a_i}-free, and localizing at the product a produces a module with a finite filtration by free modules, which will be itself free. $\square$

We have the following consequence:

Corollary. *Let κ be a field that is finitely generated as a $\mathbb{Z}$-algebra. Then κ is a finite field. Hence, the quotient of a finitely generated $\mathbb{Z}$-algebra by a maximal ideal is a finite field.*

Proof. The second statement is immediate from the first statement. To prove the first statement, first suppose that κ has characteristic $p > 0$. The result that κ is a finite algebraic extension of $\mathbb{Z}/p\mathbb{Z}$ is then immediate from Hilbert's Nullstellensatz (or Zariski's Lemma). If not, then $\mathbb{Z} \subseteq \kappa$. We can localize at one element $a \in \mathbb{Z} - 0$ such that $\kappa_a = \kappa$ is $\mathbb{Z}_a$-free. But if G is a nonzero free $\mathbb{Z}_a$-module and p is a prime that does not divide a, then $pG \neq G$. Thus, $p\kappa \neq \kappa$, contradicting that κ is a field. $\square$

Discussion: reduction of the Briançon-Skoda theorem for polynomial rings over fields of characteristic 0 to the case of positive prime characteristic p. Let K be a field of characteristic 0, let $f_1, \ldots, f_n \in K[x_1, \ldots, x_d]$, a polynomial ring over K, let k be a positive integer, and let $g \in \overline{I^{n+k-1}}$. We want to prove that $g \in (f_1, \ldots, f_n)^k$, and we assume otherwise.

The condition that $g \in \overline{I^{n+k-1}}$ implies that there is an equation

$$g^m + i_1 g^{m_1} + \cdots + i_m = 0$$

where each $i_j \in (I^{n+k-1})^j = I^{(n+k-1)j}$. Thus, for each j we can write i_j as a sum of multiples of monomials of degree $(n+k-1)j$ in $f_1, \ldots, f_n$: call the polynomials that occur as coefficients in all these expressions $h_1, \ldots, h_N$. Let A be the subring of K generated over the integers $\mathbb{Z}$ by all the coefficients of g, $f_1, \ldots, f_n$ and $h_1, \ldots, h_N$. Thus, the elements $g, f_1, \ldots, f_n, h_1, \ldots, h_N \in A[x_1, \ldots, x_d]$, and if we let $I_A = (f_1, \ldots, f_n)A[x_1, \ldots, x_n]$, the equation $(*)$ holds in $A[x_1, \ldots, x_d]$, so that $g \in \overline{I_A^{n+k-1}}$ in $A[x_1, \ldots, x_n]$.

The idea of the proof is very simple: we want to choose a maximal ideal μ of A and take images in the polynomial ring $\kappa[x_1, \ldots, x_d]$, where $\kappa = A/\mu$. We will then be able to contradict the characteristic p Briançon-Skoda theorem, which will complete the proof for polynomial rings in equal characteristic 0. The only obstruction to carrying this idea through is to maintain the condition $g \notin I_A^k$ after we kill μ. We can achieve this as follows. Consider the sort exact sequence:

$$0 \to gA[x_1, \ldots, x_d]/I_A^k \to A[x_1, \ldots, x_d]/I_A^k \to A[x_1, \ldots, x_d]/(I_A^k, g) \to 0.$$

We can localize at a single element $a \in A - \{0\}$ so that all terms becomes A_a-free. The first term remains nonzero when we do this, since that is true even if we tensor further with K over A_a. We may replace A by A_a, and so there is no loss of generality in assuming that all three modules are A-free. This means that the sequence is split exact over A, and remains exact when we apply $A/\mu \otimes_A \_$. Moreover, the first term remains nonzero. Since A/μ has characteristic p, we have achieved the contradiction we sought. $\square$

Our next objective is to study multiplicities of modules on ideals primary to the maximal ideal of a local ring, and connections with integral dependence of ideals.

Let $M \neq 0$ be a finitely generated module over a local ring (R, m, K) and let I be an m-primary ideal. Recall that the function $\mathrm{Hilb}_{M,I}(n) = \ell(M/I^{n+1}M)$, where $\ell(N)$ denotes the *length* of N, agrees with a polynomial in n for $n \gg 0$ whose degree is the Krull dimension d of M (which is the same as the Krull dimension of $R/\mathrm{Ann}_R M$). The leading term of this function has the form $\dfrac{e}{d!}\, n^d$, where e is a positive integer called the *multiplicity* of M on I, and which we denote $e_I(M)$. If $I = m$, we refer simply to the *multiplicity* of M. In particular, we may consider the *multiplicity* $e(R) = e_m(R)$ of R. See the Lecture Notes from March 17 from Math 615, Winter 2004. Clearly, we may alternatively define

$$e_I(M) = d! \lim_{n\to\infty} \frac{\ell(M/I^{n+1}M)}{n^d}.$$

If $M = 0$, we make the convention that $e_I(M) = 0$.

Proposition. *Let (R, m, K) be local, M a finitely generated R-module of Krull dimension d, N a finitely generated R-module and I, J m-primary ideals of R.*

(a) *If $\mathfrak{A} \subseteq \mathrm{Ann}_R M$, then $e_I(M)$ is the same as the multiplicity of M regarded as an $(R/\mathfrak{A})$-module with respect to the ideal $I(R/\mathfrak{A})$.*

(b) *If $\dim(N) < d$, then $d! \lim\limits_{n\to\infty} \dfrac{\ell(N/m^{n+1}N)}{n^d} = 0$.*

(c) *If $I \subseteq J$ are m-primary, $e_J(M) \le e_I(M)$.*

(d) *If $\dim(M) = 0$, $e_I(M) = \ell(M)$*

(e) *If $\dim(M) > 0$, then for any m-primary ideal J of R, $e_I(JM) = e_I(M)$.*

(f) *If $M \subseteq N$ where N is a finitely generated R-module, and $M_n = I^n N \cap M$, then*

$$e_I(M) = d! \lim_{n\to\infty} \frac{\ell(M/M_{n+1})}{d^n}.$$

In case $\dim(M) < d$, the limit is 0.

(g) *If M has a finite filtration with factors N_i, then $e_I(M)$ is the sum of the $e_I(N_i)$ for those values of i such that N_i has Krull dimension d.*

Proof. The statement in (a) is immediate from the definition, since $I^{n+1}M = (IR/\mathfrak{A})^{n+1}M$.

To prove part (b), simply note that $\ell(N/m^{n+1}N)$ is eventually a polynomial in n of degree $\dim(N) < d$.

For (c), note that if $I \subseteq J$, then $I^{n+1} \subseteq J^{n+1}$ so that there is a surjection $M/I^{n+1}M \twoheadrightarrow M/J^{n+1}M$, and $\ell(M/I^{n+1}M) \ge \ell(M/J^{n+1}M)$ for all n.

In the case of (d), $I^{n+1}M = 0$ for $n \gg 0$, while $0! = n^0 = 1$.

To prove (e), choose a positive integer c such that $I^c \subseteq J$. Then $\ell(JM/I^{n+1}JM) = \ell(M/I^{n+1}JM) - \ell(M/JM) \le \ell(M/I^{n+1+c}M$. The last length is given for $n \gg 0$ by a polynomial with leading term $\dfrac{e_I(M)}{d!}n^d$, since substituting $n + c$ for n in a polynomial does not change its leading term. This shows $e_I(JM) \le e_I(M)$. On the other hand, $\ell(M/I^{n+1}JM) - \ell(M/JM) \ge \ell(M/I^{n+1}M) - \ell(M/JM)$. When we multiply by $\dfrac{d!}{n^d}$ and take the limit, the constant term $\ell(M/JM)$ yields 0 (note that this argument fails when $d = 0$). This shows that $e_I(JM) \geq e_I(M)$.

For part (f), note that by the Artin-Rees lemma, there is a constant c such that $I^{n+c}N \cap M \subseteq I^n M$, so that $I^{n+c}M \subseteq I^{n+c}N \cap M \subseteq I^n M$. Thus, the limit is trapped between

$$d! \lim_{n\to\infty} \frac{\ell(M/I^{n+1}M)}{n^d}$$

and

$$d! \lim_{n\to\infty} \frac{\ell(M/I^{n+c+1}M)}{n^d}.$$

Again, the leading term of the Hilbert polynomial does not change when we substitute $n + c$ for n, and so these two limits are both $e_I(M)$ when $d = \dim(M)$, and 0 when $\dim(M) < d$.

Finally, for part g, we may reduce by induction to the case of filtrations with two factors, so that we have a short exact sequence $0 \to N_1 \to M \to N_2 \to 0$. Then for each n we have a short exact sequence $0 \to N)1/(I^{n+1}M \cap N_1) \to M/I^{n+1}M \to N_2/I^{n+1}N_2 \to 0$, so that

$$\ell(M/I^{n+1}M) = \ell\big(N_1/(I^{n+1}M \cap N_1)\big) + \ell\big(N_2/I^{n+1}N_2\big).$$

We may multiply by $d!/n^d$ and take the limit of both sides as $n \to \infty$, using part (b) and (f) of the Proposition. □

Corollary. *Let (R, m, K) be local, $M \neq 0$ finitely generated of Krull dimension d, and I an m-primary ideal. Then*

$$e_I(M) = \sum_{P\in \mathrm{Ass}(M) \text{ with } \dim(R/P)=d} \ell_{R_P}(M_P) e_I(R/P).$$

Proof. If we take a finite filtration of M by prime cyclic modules and apply part (g) of the Proposition above, the only primes P for which the corresponding cyclic modules R/P make a nonzero contributions are those primes, necessarily in $\mathrm{Supp}(M)$, such that $\dim(R/P) = d$, and these are the same as the primes in $\mathrm{Ass}(M)$ such that $\dim(R/P) = d$. It therefore suffices to see, for each such P, how many times $R//P$ occurs in such a filtration. *A priori*, it is not even clear that the number cannot vary. However, if we localize at P, all terms different from R/P become 0, and the remaining copies of $(R/P)_P \cong R_P/PR_P$ give a filtratiion of M_P by copies of the residue class field of R_P. Hence, the number of times R/P occurs in any prime cyclic flitration of M is $\ell_{R_P}(M_P)$. □

Remark. In the statement of the Corollary, we may write $e(M_P)$ instead of $\ell_{R_P}(M_P)$, where $e(M_P)$ is the multiplicity of M_P over R_P with respect to the maximal ideal, by part (d) of the Proposition.

Theorem. *Let (R, m, K) be local and $I \subseteq J$ m-primary ideals such that J is integral over I. Then for every finitely generated R-module M of positive Krull dimension, $e_I(M) = e_J(M)$.*

Proof. The condition that J is integral over I implies that for some integer k, $J^k = IJ^{k-1}$, and then for all $n \geq 0$, $J^{n+k} = I^{n+1}J^{k-1}$. See the Theorem on p. 2 of the Lecture Notes of September 13. Then $e_J(M) = e_J(J^k M)$ by part (e) of the Proposition above, and so

$$e_J(M) = d! \lim_{n\to\infty} \frac{\ell(J^k M/I^n J^k M)}{n^d} = d! \lim_{n\to\infty} \frac{\ell(M/J^k M) + \ell(J^k M/I^n J^k M)}{n^d}$$

since we have added a constant in the numerator and the denominator is n^d with $d \geq 1$. This becomes

$$d! \lim_{n\to\infty} \frac{\ell(M/I^n J^k M)}{n^d} = d! \lim_{n\to\infty} \frac{\ell(M/J^{n+k} M)}{n^d}$$

which gives $e_J(M)$ because the leading term of the Hilbert polynomial does not change when we substitute $n + k$, where k is a constant, for n. $\square$

Lemma. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a faithfully flat map of local rings such that mS is primary to $\mathfrak{n}$. Then for every R-module M, $\dim(S \otimes_R M) = \dim(M)$.*

Proof. We use induction on $\dim(M)$. We may work with the factors in a prime cyclic filtration of M, and so reduce to the case $M = R/P$. Then S/PS is flat over R/P, and we may replace R by R/P. Thus, we may assume that R is a domain. If $\dim(R) = 0$ $m = 0$ and $\mathfrak{n}$ is nilpotent, so that $\dim(S) = 0$. If $\dim(R) > 0$ choose $x \in m$. Then x is not a zerodivisor in m, and, since S is flat, not a zerodivisor in S. We may make a base change from R to R/xR. By the induction hypothesis, $\dim(S/xS) = \dim(R/xR)$, and so $\dim(S) = \dim(S/xS) + 1 = \dim(R/xR) + 1 = \dim(R)$. $\square$

Proposition. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a faithfully flat map of local rings such that $\mathfrak{n} = mS$. In particular, this holds when $S = \widehat{R}$ or $S = R(t)$ for an indeterminate t. Let M be a finitely generated R-module, and I an m-primary ideal. Then $e_I(M) = e_{IS}(S \otimes_R M)$.*

Proof. Quite generally, when S is flat over R and N has a finite filtration with factors N_i, then $S \otimes M$ has a finite filtration with factors $S \otimes_R N_i$. Since $M/In + 1M$ has a filtration with $\ell(M/I^{n+1}M$ factors all equal to $K = R/m$, it follows that $(S \otimes_R M)/(IS)^{n+1}M \cong S \otimes_R (M/I^{n+1}M)$ has a filtration with $\ell(M/I^{n+1}M)$ factors equal to $S \otimes K \cong S/mS = S/\mathfrak{n} = L$, and so $\ell_S\big((S \otimes_R M)/(IS)^{n+1}M\big) = \ell(M/I^{n+1}M)$. $S \otimes_R M$ and M have the same dimension, by the Lemma, the result is immediate. $\square$

This means that questions about multiplicities typically reduce to the case where the ring has an infinite residue field, and likewise to the case where the ring is complete. Since ideals primary to the maximal ideal in a local ring (R, m, K) have analytic spread $d = \dim(R)$, when K is infinite each m-primary ideal will be integral over a d-generator ideal which must, of course, be generated by a system of parameters. Hence, multiplicities can, in general, be computed using ideals that are generated by a system of parameters, and we shall be particularly interested in this case.