MATH 615: WINTER 2019

TOPICS IN COMMUTATIVE ALGEBRA: LECTURES ON INTEGRAL CLOSURE, THE BRIANÇON-SKODA THEOREM, TIGHT CLOSURE, AND VARIOUS NOTIONS OF MULTIPLICITY

by Mel Hochster

Lecture of January 9, 2019

These lectures will deal with several advanced topics in commutative algebra, including the Lipman-Sathaye Jacobian theorem and its applications, including, especially, the Briançon-Skoda theorem, and the existence of test elements in tight closure theory: basic tight closure theory will be developed as needed. In turn, tight closure theory will be used to prove theorems related to the Briançon-Skoda theorem. Moreover, intersection multiplicities, Hilbert-Samuel multiplicities of local rings, Hilbert-Kunz multiplicities, and other notions will be studied, and interactions with the theory of integral closure of ideals will be developed.

A special (but very important) case of the Lipman-Sathaye theorem is as follows:

Theorem (Lipman-Sathaye). *Let $R \subseteq S$ be a homomorphism of Noetherian domains such that R is regular and S is a localization of a finitely generated R-algebra. Assume that the integral closure S' of S is module-finite over S and that the extension of fraction fields* $\mathrm{frac}\,(S)/\mathrm{frac}\,(R)$ *is a finite separable algebraic extension. Then the Jacobian ideal $\mathcal{J}_{S/R}$ multiplies S' into S.*

Both the Jacobian ideal and the notion of integral closure will be treated at length below. We shall also prove a considerably sharper version of the theorem, in which several of the hypotheses are weakened. An algebra S that is a localization of a finitely generated R-algebra is called *essentially of finite type* over R. The hypothesis that the integral closure of S is module-finite over S is a weak assumption: it holds whenever S is essentially of finite type over a field or over a complete local ring, and it tends to hold for the vast majority of rings that arise naturally: most of the rings that come up are *excellent*, a technical notion that implies that the integral closure is module-finite.

While the Briançon-Skoda theorem can be proved in equal characteristic by the method of reduction to characteristic $p > 0$, where tight closure methods may be used, the only known proof in mixed characteristic uses the Lipman-Sathaye theorem. Another application is to the calculation of the integral closure of a ring, while a third is to the construction of test elements for tight closure theory. Our emphasis is definitely on the Briançon-Skoda theorem which, in one of its simplest forms, may be formulated as just below. We shall denote by $\overline{J}$ the integral closure of the ideal J: integral closure of ideals will be discussed in detail in the sequel.

Theorem (Briançon-Skoda). *If I is an ideal of a regular ring and is generated by n elements, then $\overline{I^n} \subseteq I$.*

Before beginning our discussion of integral closure, we mention two corollaries of the Briançon-Skoda theorem that are of some interest. First:

Corollary. *Suppose that $f \in \mathbb{C}\{z_1, \ldots, z_n\}$ is a convergent power series in n variables with complex coefficients that defines a hypersurface with an isolated singularity at the origin, i.e., f and its partial derivatives $\partial f/\partial z_i$, $1 \leq i \leq n$, have an isolated common zero at the origin. Then f^n is in the ideal generated by the partial derivatives of f in the ring $\mathbb{C}\{z_1, \ldots, z_n\}$.*

This answers affirmatively a question raised by John Mather. Second:

Corollary. *Let $f_1, \ldots, f_{n+1}$ be polynomials in n variables over a field. Then $f_1^n \cdots f_n^n \in (f_1^{n+1}, \ldots, f_{n+1}^{n+1})$.*

For example, when $n = 2$ this implies that if $f, g, h \in K[x, y]$ are polynomials in two variables over a field K then $f^2g^2h^2 \in (f^3, g^3, h^3)$. This statement is rather elementary: the reader is challenged to prove it by elementary means.

We shall need to develop the subject a bit before we can see why these are corollaries: we postpone the explanation for the moment.

In these notes all given rings are assumed to be commutative, associative, and to have a multiplicative identity 1, unless otherwise stated. Most often given rings will be assumed to be Noetherian as well, but we postpone making this a blanket assumption.

Our next objective is to review some facts about integral elements and integral ring extensions.

Recall that if $R \subseteq S$ are rings then $s \in S$ is *integral* over R if, equivalently, either

(1) s satsifies a monic polynomial with coefficients in R or

(2) $R[s]$ is finitely generated as an R-module.

The elements of S integral over R form a subring of S containing R, which is called the *integral closure* of R in S. If S is an R-algebra, S is called *integral* over R if every element is integral over the image of R in S. S is called *module-finite* over R if it is finitely generated as an R-module. If S is module-finite over R it is integral over R. S is module-finite over R if and only if it is finitely generated as an R-algebra and integral over R. S is integral over R if and only if every finitely generated R-subalgebra is module-finite over R.

Given a commutative diagram of algebras

$$\begin{tikzcd}
S \arrow[r, "f"] & U \\
R \arrow[u] \arrow[r] & T \arrow[u]
\end{tikzcd}$$

and an element $s \in S$ integral over the image of R, the image of S in U is integral over the image of T. One can see this simply by applying the homomorphism f to the monic equation s satisfies. When the vertical maps are inclusions, we see that the integral closure of R in S maps into the integral closure of T in U.

Note also that if $R \to S$ and $S \to T$ are both module-finite (respectively, integral) then $R \to T$ is also module-finite (respectively, integral).

The total quotient ring of the ring R is $W^{-1}R$, where W is the multiplicative system of all nonzerodivisors. We have an injection $R \hookrightarrow W^{-1}R$. If R is a domain, its total quotient ring is its field of fractions. If R is reduced, R is called *normal* or *integrally closed* if it is integrally closed in its total quotient ring. Thus, a domain R is integrally closed if and only if every fraction that is integral over R is in R.

Let $(H, +)$ be an additive commutative semigroup with additive identity 0. A commutative ring R is said to be *H-graded* if it has a direct sum decomposition

$$R \cong \bigoplus_{h \in H} R_h$$

as abelian groups such that $1 \in R_0$ and for all $h, k \in H$, $R_h R_k \subseteq R_{h+k}$. Elements of R_h are then called *homogeneous elements* or *forms* of *degree* h. If s is the sum of nonzero forms $s_1 + \cdots + s_n$ of mutually distinct degrees h_i, then $s_i \in R_{h_i}$ is called the *homogenous component* of s of degree h_i. The homogeneous components in other degrees are defined to be 0. The most frequent choices for H are the nonnegative integers $\mathbb{N}$ and the integers $\mathbb{Z}$.

Theorem. *Let $R \subseteq S$ be an inclusion of $\mathbb{N}$-graded (or $\mathbb{Z}$-graded) rings compatible with the gradings, i.e., such that $R_h \subseteq S_h$ for all h. Then the integral closure of R in S is also compatibly graded, i.e., every homogeneous component of an element of S integral over R is integral over R.*

Proof. First suppose that R has infinitely many units of degree 0 such that the difference of any two is a unit. Each unit u induces an endomorphism θ_u of R whose action on forms of degree d is multiplication by u^d. Then $\theta_u \theta_v = \theta_{uv}$, and θ_u is an automorphism whose inverse is $\theta_{u^{-1}}$. These automorphisms are defined compatibly on both R and S: one has a commutative diagrams

$$\begin{tikzcd}
S \arrow[r, "\theta_u"] & S \\
R \arrow[u] \arrow[r, "\theta_u"'] & S \arrow[u]
\end{tikzcd}$$

for every choice of unit u. If $s \in S$ is integral over R, one may apply θ_u to the equation of integral dependence to obtain an equation of integral dependence for $\theta_u(s)$ over R. Thus, θ_u stabilizes the integral closure T of R in S. (This is likewise true for $\theta_{u^{-1}}$, from which one deduces that θ_u is an automorphism of T, but we do not really need this.)

Suppose we write

$$s = s_{h+1} + \cdots + s_{h+n}$$

for the decomposition into homogeneous components of an element $s \in S$ that is integral over R, where each s_j has degree j. What we need to show is that each s_j is integral over R. Choose units $u_1, \ldots, u_n$ such that for all $h \neq k$, $u_h - u_k$ is a unit — we are assuming that these exist. Letting the θ_{u_i} act, we obtain n equations

$$u_i^{h+1} s_{h+1} + \cdots + u_i^{h+n} s_{h+n} = t_i, \quad 1 \leq j \leq n,$$

where $t_i \in T$. Let M be the $n \times n$ matrix $\bigl(u_i^{h+j}\bigr)$. Let V be the $n \times 1$ column vector $\begin{pmatrix} s_{h+1} \\ \vdots \\ s_{h+n} \end{pmatrix}$ and let W be the $n \times 1$ column vector $\begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$. In matrix form, the displayed equations are equivalent to $MV = W$. To complete this part of the argument, it will suffice to show that the matrix M is invertible over R, for then $V = M^{-1}W$ will have entries in T, as required. We can factor u_i^{h+1} from the ith row for every i: since all the u_i are units, this does not affect invertibility and produces the Van der Monde matrix $\bigl(u_i^{j-1}\bigr)$. The determinant of this matrix is the product

$$\prod_{j>i} (u_j - u_i)$$

(see the Discussion below), which is invertible because every $u_j - u_i$ is a unit.

In the general case, suppose that

$$s = s_{h+1} + \cdots + s_{h+n}$$

as above is integral over R. Let t be an indeterminate over R and S. We can give this indeterminate degree 0, so that $R[t] = R_0[t] \otimes_{R_0} R$ is again a graded ring, now with 0th graded piece $R_0[t]$, and similarly $S[t]$ is compatibly graded with 0th graded piece $S_0[t]$. Let $U \subseteq R_0[t]$ be the multiplicative system consisting of products of powers of t and differences $t^j - t^i$, where $j > i \geq 0$. Note that U consists entirely of monic polynomials. Since all elements of U have degree 0, we have an inclusion of graded rings $U^{-1}R[t] \subseteq U^{-1}S[t]$. In $U^{-1}R[t]$, the powers of t constitute infinitely many units of degree 0, and the difference of any two distinct powers is a unit. We may therefore conclude that every s_j is integral over $U^{-1}R[t]$, by the case already done. We need to show s_j is integral over R itself.

Consider an equation of integral dependence

$$s_j^d + f_1 s_j^{d-1} + \cdots + f_d = 0,$$

where every $f_i \in U^{-1}R[t]$. Then we can pick an element $G \in U$ that clears denominators, so that every $Gf_i = F_i \in R[t]$, and we get an equation

$$Gs_j^d + F_1 s_j^{d-1} + \cdots + F_d = 0.$$

Let G have degree m, and recall that G is monic in t. The coefficient of t^m on the left hand side, which is an element of S, must be 0, and so its degree jd homogeneous component must be 0. The contribution to the degree jd component of this coefficient from Gs_j^d is, evidently, s_j^d, while the contribution from $F_i s_j^{d-i}$ clearly has the form $r_i s_j^{d-i}$, where $r_i \in R$ has degree ji. This yields the equation

$$s_j^d + r_1 s_j^{d-1} + \cdots + r_d = 0,$$

and so s_j is integral over R, as required. □

Discussion: Van der Monde matrices. Let $u_1, \ldots, u_n$ be elements of a commutative ring. Let M be the $n \times n$ matrix $\bigl(u_i^{j-1}\bigr)$.

(a) We want to show that the determinant of M is $\prod_{j>i}(u_j - u_i)$. Hence, M is invertible if $u_j - u_i$ is a unit for $j > i$. It suffices to prove the first statement when the u_i are indeterminates over $\mathbb{Z}$. Call the determinant D. If we set $u_j = u_i$, then D vanishes because two rows become equal. Thus, $u_j - u_i$ divides D in $\mathbb{Z}[u_1, \ldots, u_n]$. Since the polynomial ring is a UFD and these are relatively prime in pairs, the product P of the $u_j - u_i$ divides D. But they both have degree $1 + 2 + \cdots + n - 1$. Hence, $D = aP$ for some integer a. The monomial $x_2 x_3^2 \cdots x_n^{n-1}$ obtained from the main diagonal of matrix in taking the determinant occurs with coefficient 1 in both P and D, so that $a = 1$. □

(b) We can also show the invertibility of M as follows: if the determinant is not a unit, it is contained in a maximal ideal. We can kill the maximal ideal. We may therefore assume that the ring is a field K, and the u_i are mutually distinct elements of this field. If the matrix is not invertible, there a nontrivial relation on the columns with coefficients $c_0, \ldots, c_{n-1}$ in the field. This implies that the nonzero polynomial

$$c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$$

has n distinct roots, $u_1, \ldots, u_n$, in the field K, a contradiction. □

Lecture of January 11, 2019

Corollary. *If a R is integrally closed in S, then $R[t]$ is integrally closed in $S[t]$. If R is a normal domain, then $R[t]$ is normal.*

Proof. The integral closure of $R[t]$ in $S[t]$ will be graded and so spanned by integral elements of $S[t]$ of the form st^k, where s is homogenous. Take an equation of integral dependence for st^k of degree, say, n on $R[t]$. The coefficient of t^{kn} is 0, and this gives an equation of integral dependence for s on R. For the second part, $R[t]$ is integrallly closed in $K[t]$, where $K = \mathrm{frac}\,(R)$, and $K[t]$ is integrally closed in $K(t) = \mathrm{frac}\,(R[t])$ since $K[t]$ is a UFD. □

We next want to discuss integral closure of ideals.

Let R be any ring and let I be an ideal of R. We define an element u of R to be *integral over* I or to be in the integral closure $\overline{I}$ of I if it satisfies a monic polynomial $f(z)$ of degree n with the property that the coefficient of z^{n-t} is in I^t, $1 \leq t \leq n$. We shall use the temporary terminology that such a monic polynomial is I-*special*. Note that the product of two I-special polynomials is I-special, and hence any power of an I-special polynomial is I-special.

Let t be an indeterminate over R and let $R[It]$ denote the subring of the polynomial ring $R[t]$ generated by the elements it for $i \in I$. This ring is called the *Rees ring* of I. It is $\mathbb{N}$-graded, with the grading inherited from $R[t]$, so that the k th graded piece is It^k.

It follows easily that the integral closure of $R[It]$ in $R[t]$ has the form

$$R + J_1t + J_2t^2 + \cdots + J_kt^k + \cdots$$

where, since this is an R-algebra, each J_k is an ideal of R. We note that with this notation, $J_1 = \overline{I}$. To see this, note that if rt, where $r \in R$ is integral over $R[It]$, satisfying an equation of degree n, then by taking homogeneous components of the various terms we may find an equation of integral dependence in which all terms are homogeneous of degree n. Dividing though by t^n then yields an equation of integral dependence for r on I. This argument is reversible. (Exercise: in this situation, show that J_k is the integral closure of I^k.) We note several basic facts about integral closures of ideals that follow easily either from the definition or this discussion.

Proposition. *Let I be an ideal of R and let $u \in R$.*

(a) *The integral closure of I in R is an ideal containing I, and the integral closure of $\overline{I}$ is $\overline{I}$.*

(b) *If $h : R \to S$ is a ring homomorphism and u is integral over I then $h(u)$ is integral over IS. If J is an integrally closed ideal of S then the contraction of J to R is integrally closed.*

(c) *u is integral over I if and only if its image modulo the ideal N of nilpotent elements is integral over $I(R/N)$. In particular, the integral closure of (0) is N.*

(d) *The element u is integral over I if and only if for every minimal prime P of R, the image of u modulo P is integral over $I(R/P)$.*

(e) *Every prime ideal of R and, more generally, every radical ideal of R is integrally closed.*

(f) *An intersection of integrally closed ideals is integrally closed.*

(g) *In a normal domain, a principal ideal is integrally closed.*

(h) *If S is an integral extension of R then $\overline{IS} \cap R = \overline{I}$.*

Proof. That $I \subseteq \overline{I}$ is obvious. If r is in the integral closure of $\overline{I}$ then rt is integral over $R[\overline{I}t]$. But this ring is generated over $R[It]$ by the elements r_1t such that $r_1 \in \overline{I}$, i.e., such that r_1t is integral over $R[It]$. It follows that $R[\overline{I}t]$ is integral over $R[It]$, and then rt is integral over $R[It]$ by the transitivity of integral dependence. This proves (a).

The first statement in (b) is immediate from the definition of integral dependence: apply the ring homomorphism to the equation of integral dependence. The second statement in (b) is essentially the contrapositive of the first statement.

The "only if" part of (c) follows from (b) applied with $S = R/N$. The "if" part follows from (d), and so it will suffice to prove (d).

The "only if" part of (d) likewise follows from (b). To prove the "if" part note that the values of I-special polynomials on u form a multiplicative system: hence, if none of them vanishes, we can choose a minimal prime P of R disjoint from this multiplicative system, and then no $I(R/P)$-special polynomial vanishes on the image of u in R/P.

(e) follows from the second statement in (c) coupled with the second statement in (b), while (f) is immediate from the definition. To prove (g), suppose that b is an element of R and $a \in \overline{bR}$. If $b = 0$ it follows that $a = 0$ and we are done. Otherwise, we may divide a degree n equation of integral dependence for a on bR by b^n to obtain an equation of integral dependence for a/b on R. Since R is normal, this equation shows that $a/b \in R$, and, hence, that $a \in bR$.

Finally, suppose that $r \in R$ is integral over IS. Then rt is integral over $S[ISt]$, and this ring is generated over $R[It]$ by the elements of S, each of which is integral over R. It follows that $S[ISt]$ is integral over $R[It]$, and so rt is integral over $R[It]$ by the transitivity of integral dependence. □

Recall that a domain V with a unique maximal ideal m is called a *valuation domain* if for any two elements one divides the other. This implies that for any finite set of elements, one of the elements divides the others, and so generates the same ideal that they all do together. We shall use the term *discrete valuation ring*, abbreviated DVR, for a Noetherian valuation domain: in such a ring, the maximal ideal is principal, and every nonzero element of the maximal ideal is a unit times a power of the generator of the maximal ideal. A DVR is the same thing as a local principal ideal domain (PID).

We recall the following terminology: (R,m,K) is *quasilocal* means that R has unique maximal ideal m and residue class field $K = R/m$. Sometimes K is omitted from the notation. We say that (R, m, K) is *local* if it is quasilocal and Noetherian.

The next result reviews some facts about integral closures of rings and integrally closed rings.

Theorem. *Let R be an integral domain.*

(a) *R is normal if and only if R is an intersection of valuation domains with the same fraction field as R. If R is Noetherian, these may be taken to be the discrete valuation rings obtained by localizing R at a height one prime.*

(b) *If R is one-dimensional and local, then R is integrally closed if and only if R is a DVR. Thus, a local ring of a normal Noetherian domain at a height one prime is a DVR.*

(c) *If R is Noetherian and normal, then principal ideals are unmixed, i.e., if $r \in R$ is not zero not a unit, then every associated prime of rR has height one.*

Proof. For (a) and (b) see [M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969], Corollary 5.22, Proposition 9.2 and Proposition 5.19, respectively, and [O. Zariski and P. Samuel, *Commutative Algebra*, D. Van Nostrand Company, Princeton, New Jersey, 1960], Corollary to Theorem 8, p. 17; for (c) see H. Matsumura, *Commutative Algebra*, W.A. Benjamin, New York, 1970], §17. □

For the convenience of the reader we shall give a proof of (a) below in the case where R is not necessarily Noetherian.

Lecture of January 14, 2019

Examples of integral closure of ideals. Note that whenever $r \in R$ and $I \subseteq R$ is an ideal such that $r^n = i_n \in I^n$, we have that $r \in \overline{I}$. The point is that r is a root of $z^n - i_n = 0$, and this polynomial is monic with the required form.

In particular, if x, y are any elements of R, then $xy \in \overline{(x^2,\, y^2)}$, since $(xy)^2 = (x^2)(y^2) \in I^2$. This holds even when x and y are indeterminates.

More generally, if $x_1, \,\ldots\,, x_n \in R$ are any elements and $I = (x_1^n, \,\ldots\,, x_k^n)R$, then every monomial $r = x_1^{i_1} \cdots x_k^{i_k}$ of degree n (here the i_j are nonnegative integers whose sum is n) is in $\overline{I}$, since

$$r^n = (x_1^n)^{i_1} \cdots (x_k^n)^{i_k} \in I^n,$$

since every $x_j^n \in I$ and $\sum_{j=1}^k i_j = n$.

Now let K be any field of characteristic $\neq 3$, and let $X,\, Y,\, Z$ be indeterminates over K. Let

$$R = K[X,\, Y,\, Z]/(X^3 + Y^3 + Z^3) = K[x,\, y,\, z],$$

which is a normal domain with an isolated singularity. Here, we are using lower case letters to denote the images of corresponding upper case letters after taking a quotient: we shall frequently do this without explanatory comment. Let $I = (x, y)R$. Then $z^3 \in I^3$, and so $z \in \overline{I}$. This shows that an ideal generated by a system of parameters in a local ring need not be integrally closed, even if the elements are part of a minimal set of generators of the maximal ideal. It also follows that $z^2 \in \overline{I^2}$, where I is a two generator ideal, while $z^2 \notin I$. Thus, the Briançon-Skoda theorem, as we stated it for regular rings, is not true for R. (There is a version of the theorem that *is* true: it asserts that for an n-generator ideal I, $\overline{I^n} \subseteq I^*$, where I^* is the *tight closure* of I. But we are not assuming familiarity with tight closure here.)

Here is another example. Let $x,\, y,\, u,\, v$ be indeterminates over a field K and $R = K[x, y, u, v]$. Let $J = (x, y) \cap (u, v) = (x, y)(u, v) = (xu, yu, xv, yv)$. Then J is integral over $I = (xu, yv, xv + yu)$, since the generators of J not in I, namely xv, yu, are the roots of the equation $z^2 - (xv + yu)z + (xv)(yu) = 0$, where the second coefficient is in I and the third coefficient $= (xu)(yv) \in I^2$.

We next want to give a proof that, even when a normal domain R is not Noetherian, it is an intersection of valuation domains. We first show:

Lemma. *Let L be a field, $R \subseteq L$ a domain, and $I \subset R$ a proper ideal of R. Let $x \in L - \{0\}$. Then either $IR[x]$ is a proper ideal of $R[x]$ or $IR[1/x]$ is a proper ideal of $R[1/x]$.*

Proof. We may replace R by its localization at a maximal ideal containing I, which only makes the problem harder. If $IR[1/x]$ is not proper we obtain an equation

$$(\#) \quad 1 = j_0 + j_1(1/x) + \cdots j_m(1/x^m),$$

where all of $j_i \in I \subseteq m$. This yields

$$(\#\#) \quad (1 - j_0)x^m = j_1 x^{m-1} + \cdots j_m.$$

Since $1 - j_0$ is a unit, this shows that x is integral over R. Hence m lies under a maximal ideal of $R[x]$, and $mR[x]$ is proper. $\square$

Corollary. *Let $R \subseteq L$, a field, and let $I \subset R$ be a proper ideal of R. Then there is a valuation domain V with $R \subseteq V \subseteq L$ such that $IV \neq V$.*

Proof. Consider the set $\mathcal{S}$ of all rings S such that $R \subseteq S \subseteq L$ and $IS \neq S$. This set contains R, and so is not empty. The union of a chain of rings in $\mathcal{S}$ is easily seen to be in $\mathcal{S}$. Hence, by Zorn's lemma, $\mathcal{S}$ has a maximal element V. We claim that V is a valuation domain with fraction field L. For let $x \in L - \{0\}$. By the preceding Lemma, either $IV[x]$ or $IV[1/x]$ is a proper ideal. Thus, either $V[x] \in \mathcal{S}$ or $V[1/x] \in \mathcal{S}$. By the maximality of V, either $x \in V$ or $1/x \in V$. $\square$

We now can prove the result we were aiming for.

Corollary. *Let R be a normal domain with fraction field L. Then R is the intersection of all valuation domains V with $R \subseteq V \subseteq L$.*

Proof. Let $x \in L - R$. It suffices to find V with $R \subseteq V \subseteq L$ such that $x \notin V$. Let $y = 1/x$. We claim that y is not a unit in $R[y]$, for its inverse is x, and if y were a unit we would have

$$x = r_0 + r_1(1/x) + \cdots + r_n(1/x)^n$$

for some positive integer n and $r_j \in R$. Multiplying through by x^n gives an equation of integral dependence for x on R, and since R is normal this yields $x \in R$, a contradiction. Since $yR[y]$ is a proper ideal, by the preceding Corollary we can choose a valuation domain V with $R[y] \subseteq V \subseteq K$ such that yV is a proper ideal of V. But this implies that $x \notin V$. $\square$

We note the following example of a non-Noetherian valuation domain. Let $R = K[x, y]$ be a polynomial ring in two variables over a field K, which has fraction field $L = K(x, y)$. Then we have a chain of polynomial rings $K[x, y] \subseteq K[x, y/x] \subseteq K[x, y/x^2] \subseteq \cdots \subseteq K[x, y/x^n] \subseteq L$. Let S be the union of the rings $R_n = K[x,\, y/x^n]$: since a directed union of normal domains is normal, S is normal. The ideal $m = (x)S + (y/x^n : n \geq 1)S$ is a maximal ideal, and there exists a valuation domain $(V, \mathcal{M})$ with $S \subseteq V \subseteq L$ such that mV is proper ideal, i.e., $m \subseteq \mathcal{M}$. Then V is not Noetherian, since x is in the maximal ideal and y is a nonzero element in the intersection of the ideals x^nV.

The following important result can be found in most introductory texts on commutative algebra, including [M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts, 1969], which we refer to briefly as Atiyah-Macdonald.

Theorem. *If R is a normal Noetherian domain, then the integral closure S of R in a finite separable extension $\mathcal{G}$ of its fraction field $\mathcal{F}$ is module-finite over R.*

Proof. See Proposition 5.19 of Atiyah-MacDonald for a detailed argument. We do mention the basic idea: choose elements $s_1, \ldots, s_d$ of S that are basis for $\mathcal{G}$ over $\mathcal{F}$, and then the discriminant $D = \det\bigl(\mathrm{Trace}_{\mathcal{G}/\mathcal{F}}\, s_i s_j\bigr)$, which is nonzero because of the separability hypothesis, multiplies S into the Noetherian R-module $\sum_{i=1}^{d} Rs_i$. □

Theorem (Nagata). *Let R be a complete local domain. Then the integral closure of R in a finite field extension of its fraction field is a finitely generated R-module.*

Proof. Because R is module-finite over a formal power series ring over a field, or, if R does not contain a field, over a DVR whose fraction field has characteristic zero, we may replace the original R by a formal power series ring, which is regular and, hence, normal. Unless R has characteristic p the extension is separable and we may apply the Theorem just above.

Thus, we may assume that R is a formal power series ring $K[[y_1, \ldots, y_n]]$ over a field K of characteristic p. If we prove the result for a larger finite field extension, we are done, because the original integral closure will be an R-submodule of a Noetherian R-module. This enables us to view the field extension as a purely inseparable extension followed by a separable extension. The separable part may be handled using the Theorem just above. It follows that we may assume that the field extension is contained in the fraction field of $K^{1/q}[[x_1, \ldots, x_n]]$ with $x_i = y_i^{1/q}$ for all i. We may adjoin the x_i to the given field extension, and it suffices to show that the integral closure is module-finite over $K[[x_1, \ldots, x_n]]$, since this ring is module-finite over $K[[y_1, \ldots, y_n]]$. Thus, we have reduced to the case where $R = K[[x_1, \ldots, x_n]]$ and the integral closure S will lie inside $K^{1/q}[[x_1, \ldots, x_n]]$, since this ring is regular and, hence, normal.

Now consider the set $\mathcal{L}$ of leading forms of the elements of S, viewed in the ring $K^{1/q}[[x_1, \ldots, x_n]]$. Let d be the degree of the field extension from the fraction field of R to that of S. We claim that any $d+1$ or more $F_1, \ldots, F_N$ of the leading forms in $\mathcal{L}$ are linearly dependent over (the fraction field of) R for, if not, choose elements s_j of S which have them as leading forms, and note that these will also be linearly independent over R, a contradiction (if a non-trivial R-linear combination of them were zero, say $\sum_j r_j s_j = 0$, where the r_j are in R, and if F_j has degree d_j while the leading form g_j of r_j has degree d'_j, then one also gets $\sum_j g_j F_j = 0$, where the sum is extended over those values of j for which $d_j + d'_j$ is minimum). Choose a maximal set of linearly independent elements f_j of $\mathcal{L}$. Let K' denote the extension of K generated by all of their coefficients. Since there are only finitely many, $T = K'[[x_1, \ldots, x_n]]$ is module-finite over R. But T contains every element L of $\mathcal{L}$, for each element of $\mathcal{L}$ is linearly dependent over R on the f_j, and so is in the fraction field of T, and has its q th power in $R \subseteq T$. Since T is regular, it is normal, and so must contain L.

Thus, the elements of $\mathcal{L}$ span a finitely generated R-submodule of T, and so we can choose a finite set $L_1, \ldots, L_k \subseteq \mathcal{L}$ that span an R-module containing all of $\mathcal{L}$,. We can then choose finitely many elements $s_1, \ldots, s_k$ of S whose leading forms are the $L_1, \ldots, L_k$.

Let S_0 be the module-finite extension of R generated by the elements $s_1, \ldots, s_k$. We complete the proof by showing that $S_0 = S$. We first note that for every element L of $\mathcal{L}$, S_0 contains an element s whose leading form is L. To see this, observe that if we write L as an R-linear combination $\sum_j r_j L_j$, the same formula holds when every r_j is replaced by its homogeneous component of degree $\deg L - \deg L_j$. Thus, the r_j may be assumed to be homogeneous of the specified degrees. But then $\sum_j r_j s_j$ has L as its leading form.

Let $s \in S$ be given. Recursively choose $u_0, u_1, \ldots, u_n, \ldots \in S_0$ such that u_0 has the same leading form as s and, for all n, u_{n+1} has the same leading form a $s - (u_0 + \cdots + u_n)$. For all $n \geq 0$, let $v_n = u_0 + \cdots + u_n$. Then $\{v_n\}_n$ is a Cauchy sequence in S_0 that converges to s in the topology given by the powers m_T^h of the maximal ideal of $T = K'[[x_1, \ldots, x_n]]$. Since S_0 is module-finite over $K[[x_1, \ldots, x_n]]$, S_0 is complete. By Chevalley's lemma, which is discussed below, when we intersect the m_T^h with S_0 we obtain a sequence of ideals cofinal with the powers of the maximal ideal of S_0. Thus, the sequence, which converges to s, is Cauchy with respect to the powers of the maximal ideal of S_0. Since, as observed above, S_0 is complete, we have that $s \in S_0$, as required. $\square$

Lecture of January 16, 2019

In the proof of the preceding Theorem, we used Chevalley's Lemma:

Theorem. *Let M be a finitely generated module over a complete local ring (R, m, K). Let $\{M_n\}_n$ be a decreasing sequence of submodules whose intersection is 0. Then for all $k \in \mathbb{N}$ there exists N such that $M_n \subseteq m^k M$.*

Proof. For all h, the modules $M_n + m^h M$ are eventually stable (we may consider instead their images in the Artinian module $M/m^h M$, which has DCC), and so we may choose n_h such that $M_n + m^h M = M_{n'} + m^h M$ for all $n, n' \geq n_h$. We may replace n_h by any larger integer, and so we may assume that the sequence n_h is increasing. We replace the original sequence by the $\{M_{n_h}\}_h$. Thus we may assume without loss of generality that $M_n + m^hM = M_{n'} + m^hM$ for all $n,\, n' \geq h$. We claim $M_k \subseteq m^kM$ for all k: if not, choose k and $v_k \in M_k - m^kM$. Now choose $v_{k+1} \in M_{k+1}$ such that $v_{k+1} \equiv v_k \bmod m^kM$, and, recursively, for all $s \geq 0$ choose $v_{k+s} \in M_{k+s}$ such that $v_{k+s+1} \equiv v_{k+s} \bmod m^{k+s}M$: this is possible because $M_{k+s} \subseteq M_{k+s+1} + m^{k+s}M$. This gives a Cauchy sequence with nonzero limit. Since all terms are eventually in any given M_n, so is the limit (each M_n is m-adically closed), which is therefore in the intersection of the M_n. $\square$

We have been assuming that valuation domains V are integrally closed. It is very easy to see this: if f is in the fraction field L of V but not in V, then $x = 1/f$ is in the maximal ideal m of V. Some maximal $\mathcal{M}$ of the integral closure V' lies over m, and so x is not a unit of V', i.e., $f \notin V'$. Thus, $V' = V$.

It is also easy to see that if $K \subseteq L$ are fields and V is a valuation domain with fraction field L, then $V \cap K$ is a valuation domain with fraction field K. Moreover, if V is a DVR, then $V \cap K$ is a DVR or is K. For the first statement, each $f \in K - \{0\}$ has the property that f or $1/f$ is in V, and, hence, in $V \cap K$, as required. Now suppose that V is a DVR and that x generates the maximal ideal. Let $W = V \cap K \neq K$. Each nonzero element of the maximal ideal m of W has the form ux^k in V, where k is a positive integer. Choose an element y of the maximal ideal of W such that k is minimum. Then every $z \in m$ is a multiple of y in V, and the multiplier is in W. Thus, m is principal. It follows that every nonzero element m has the form uy^t, where $t > 0$, since it is clear that the intersection of the powers of m is zero.

We next want to prove:

Theorem. *Let R be a Noetherian domain. Then the integral closure R' of R is the intersection of the discrete valuation rings between R and its fraction field L.*

Proof. Let $f = b/a$ be an element of L not in R', where $a,\, b \in R$ and $b \neq 0$. It suffices to find a DVR containing R and not b/a: we may then intersect it with L. Localize at a prime of R in the support of the R-module $(R' + Rf)/R'$. Since localization commutes with integral closure we may assume that (R, m, K) is local. Nonzero elements of R are nonzerodivisors in $\widehat{R}$ by flatness, and so the fraction field of R embeds in the total quotient ring of $\widehat{R}$, and we may view b/a as an element of the total quotient ring of $\widehat{R}$. If $b + \mathfrak{p}$ is in the integral closure of $a(R/\mathfrak{p})$ for every minimal prime $\mathfrak{p}$ of $\widehat{R}$, then b is integral over $a\widehat{R}$. If the equation that demonstrates the integral dependence has degree n, we find that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \ldots\,,\, ba^{n-1},\, a^n)\widehat{R}$, and since $\widehat{R}$ is faithfully flat over R, this implies that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \ldots\,,\, ba^{n-1},\, a^n)R$ as well. Dividing by a^n then shows that b/a is integral over R, a contradiction. Thus, we can choose a minimal prime $\mathfrak{p}$ of $\widehat{R}$ such that $b + \mathfrak{p}$ is not integral over $a\widehat{R}/\mathfrak{p}$. It follows that $\overline{b}/\overline{a}$ is not integral over $\widehat{R}/\mathfrak{p}$, where the bars over the letters indicate images in $\widehat{R}/\mathfrak{p}$. Note that R injects into $\widehat{R}/\mathfrak{p}$. Thus, the integral closure $(\widehat{R}/\mathfrak{p})'$ of $\widehat{R}/\mathfrak{p}$ does not contain $\overline{b}/\overline{a}$, and since it is module-finite over $\widehat{R}/\mathfrak{p}$ by the last Theorem of the Lecture of January 14, it is a normal Noetherian ring. Thus, it is an intersection of DVR's by part (a) of the last Theorem of the Lecture of January 11, and we can choose a DVR V containing $(\widehat{R}/\mathfrak{p})'$ and not $\overline{b}/\overline{a}$, which is the image of b/a, so that V contains the isomorphic image of R but not the image of b/a. Now we may intersect V with the fraction field of R. □

Theorem. *Let R be any ring and let $I \subseteq J$ be ideals of R.*

(a) *$r \in R$ is integral over I if and only if there exists an integer n such that $(I+rR)^{n+1} = I(I+rR)^n$. Thus, if J is generated over I by one element, then J is integral over I if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(b) *If $J^{n+1} = IJ^n$ with $n \in N$ then $J^{n+k} = I^k J^n$ for all $k \in \mathbb{N}$.*

(c) *If $J^{n+1} = IJ^n$ and $Q \supseteq J$ is an ideal and $r \in \mathbb{N}$ an integers such that $Q^{r+1} = JQ^r$, then $Q^{n+r+1} = IQ^{n+r}$.*

(d) *If J is integral over I and generated over I by finitely many elements, then there is an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$. If R is Noetherian then J is integral over I if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(e) *If R is a domain and M is a finitely generated faithful R-module such $JM = IM$ then J is integral over I. If R is a Noetherian domain, then J is integral over I if and only if there is a finitely generated faithful R-module M such that $JM = IM$.*

Proof. Note that

$$(I+rR)^n = I^n + rI^{n-1} + \cdots + r^t I^{n-t} + \cdots + r^n R.$$

Comparing the expansions for $(I+rR)^{n+1}$ and $I(I+rR)^n$, we see that the condition for equality is simply that r^{n+1} be in $I(I+rR)^n = r^n I + \cdots + I^{n+1}$, and this is precisely the condition for r to satisfy an equation of integral dependence on I of degree $n+1$. This proves (a).

We prove (b) by induction on k. The result is clear if $k=0$ and holds by hypothesis if $k=1$. Assuming that $J^{n+k} = I^k J^n$, for $k \geq 1$ we have that

$$J^{n+k+1} = J^{n+k}J = (I^k J^n)J = I^k J^{n+1} = I^k I J^n = I^{k+1} J^n,$$

as required. This proves (b).

For (c), note that $Q^{r+n+1} = J^{n+1}Q^r = (IJ^n)Q^r = I(J^n Q^r) = IQ^{n+r}$.

It follows by induction on the number of elements needed to generate J over I that if J is finitely generated over I and integral over I then there is an integer n such that$J^{n+1} = IJ^n$.

Next, we want to show that if R is Noetherian and $J^{n+1} = IJ^n$ then J is integral over I. The condition continues to hold if we consider the images of I, J modulo a minimal prime of R, and so it suffices to consider the case where R is a domain. Moreover, if $I = (0)$ the result is immediate, and so we may assume that $I \neq 0$. Thus, J^n is a faithful

R-module, and so the proof will be complete once we have established the first sentence of part (e).

Suppose that $JM = IM$ and let $u_1, \ldots, u_n$ be generators for M. Let r be an element of J. Then for every ν we can write $ru_\nu = \sum_{\mu=1}^{n} i_{\mu\nu}u_\mu$ where the $i_{\mu\nu} \in I$. Let $\mathbf{1}$ denote the size n identity matrix, and let B denote the size n matrix $(i_{\mu\nu})$. Let U be an $n \times 1$ column vector whose entries are the u_i. Then, in matrix notation, $rU = BU$, so that $(r\mathbf{1} - B)U = 0$. Let C be the transpose of the cofactor matrix of $r\mathbf{1} - B$. Then $C(r\mathbf{1} - B)$ is $D\mathbf{1}$, where $D = \det(r\mathbf{1} - B)$ is the characteristic polynomial of B evaluated at r. It is easy to see that the characteristic polynomial of a matrix with entries in I is I-special. Now, when we multiply the equation $(r\mathbf{1}-B)U = 0$ on the left by C we find that $D\mathbf{1}U = 0$, i.e., that $DU = 0$, and since D kills all the generators of M and M is faithful, it follows that $D = 0$, giving an equation of integral dependence for r on I. This proves the first sentence of part (e), and also completes the proof of (d).

Finally, if R is a Noetherian domain and J is integral over I, then if $I = (0)$ we have that $J = (0)$ and we may choose $M = R$, while if $I \neq (0)$ then $J \neq (0)$. In this case we can choose n such that $J^{n+1} = IJ^n$, and we may take $M = J^n$. □

Lecture of January 18, 2019

The next Theorem gives several enlightening characterizations of integral closure. We first note:

Lemma. *Let I be an ideal of the ring R, $r \in \overline{I}$, and $h : R \to S$ a homomorphism to a normal domain S such that IS is principal. Then $h(r) \in IS$.*

Proof. By persistence of integral closure, $h(r) \in \overline{IS}$. But IS is a principal ideal of a normal domain, and so integrally closed, which implies that $r \in IS$. □

Theorem. *Let R be a ring, let I be an ideal of R, and let $r \in R$.*

(a) *$r \in \overline{I}$ if and only if for every homomorphism from R to a valuation domain V, $r \in IV$.*

(b) *$r \in \overline{I}$ if and only if for every homomorphism f from R to a valuation domain V such that the kernel of f is a minimal prime P of R, $f(r) \in IV$. (Thus, if R is a domain, $r \in \overline{I}$ if and only if for every valuation domain V containing R, $r \in IV$.) Moreover, it suffices to consider valuation domains contained in the fraction field of R/P.*

(c) *If R is Noetherian, $r \in \overline{I}$ if and only if for every homomorphism from R to a DVR V, $r \in IV$.*

(d) *If R is Noetherian, $r \in \overline{I}$ if and only if for every homomorphism f from R to a DVR V such that the kernel of f is a minimal prime of R, $f(r) \in IV$. (Thus, if R is a domain, $r \in \overline{I}$ if and only if for every DVR V containing R, $r \in IV$.) Moreover, it suffices to consider valuation domains contained in the fraction field of R/P.*

(e) *If R is a domain and $I = (u_1, \dots, u_n)R$ is a finitely generated ideal, let*

$$S_i = R[\frac{u_1}{u_i}, \dots, \frac{u_n}{u_i}] \subseteq R_{u_i},$$

and let T_i be the integral closure of S_i. Then $r \in R$ is in $\overline{I}$ if and only if $r \in IT_i$ for all i.

(f) *Let R be a Noetherian domain. Then $r \in \overline{I}$ if and only if there is a nonzero element $c \in R$ such that $cr^n \in I^n$ for all $n \in \mathbb{N}$. (Note: I^0 is to be interpreted as R even if $I = (0)$.)*

(g) *Let R be a Noetherian domain. Then $r \in \overline{I}$ if and only if there is a nonzero element $c \in R$ such that $cr^n \in I^n$ for infinitely many values of $n \in \mathbb{N}$.*

Proof. We first observe that in any valuation domain, every ideal is integrally closed: every ideal is the directed union of the finitely generated ideals it contains, and a directed union of integrally closed ideals is integrally closed. In a valuation domain every finitely generated is principal, hence integrally closed, since a valuation domain is normal, and it follows that every ideal is integrally closed.

Now suppose that $r \in \overline{I}$. Then for any map of f of R to a valuation domain V, we have that $r \in \overline{IV} = IV$. This shows the "only if" part of (a). To complete the proof of both (a) and (b) it will suffice to show that if $f(r) \in IV$ whenever the kernel of f is a minimal prime, then $r \in \overline{I}$. But if $r \notin \overline{I}$ this remains true modulo some minimal prime by part (d) of the Proposition whose statement begins on the second page of the Lecture Notes for Janaury 11, and so we may assume that R is a domain, and that rt is not integral over $R[It]$. But then, by the last Corollary on the second page of the Lecture Notes of January 14, we can find a valuation domain V containing $R[It]$ and not rt (in the Noetherian case V may be taken to be a DVR by the second Theorem on the first page of the Lecture Notes from January 16). Then $r \in \sum_{j=1}^{n} i_j v_j$ with the $i_j \in I$ and the $v_j \in V$ implies $rt = \sum_{j=1}^{n} (i_j t) v_j \in V$ (since each $i_j t \in It \subseteq V$), a contradiction. The fact that it suffices to consider only those V within the fraction field of R/P follows from the observation that one may replace V by its intersection with that field.

The proofs of (c) and (d) in the Noetherian case are precisely the same, making use of the parnthetical comment about the Noetherian case given in the paragraph above.

To prove (e) first note that the expansion of I to S_i is generated by u_i, since $u_j = \frac{u_j}{u_i} u_i$, and so $IT_i = u_i T_i$ as well. If $r \in \overline{I}$ then $r \in IT_i$ by the preceding Lemma. Now suppose instead that we assume that $r \in IT_i$ for every i instead. Consider any inclusion $R \subseteq V$, where V is a valuation domain. Then in V, the image of one of the u_j, say u_i, divides all the others, and so we can choose i such that $S_i \subseteq V$. Since V is normal, we then have $T_i \subseteq V$ as well, and then $r \in IT_i$ implies that $r \in IV$. Since this holds for all valuation domains containing R, $r \in \overline{I}$.

Finally, it will suffice to prove the "only if" part of (f) and the "if" part of (g). If $I = (0)$ we may choose $c = 1$, and so we assume that $I \neq 0$. Suppose that $J = I + Rr$ and choose $h \in \mathbb{N}$ so that $J^{h+1} = IJ^h$, so that $J^{n+h} = I^n J^h$ for all $n \in \mathbb{N}$: see parts (a) and (c) on the second page of the Lecture Notes from January 16. Choose c to be a nonzero element of J^h. Then, for all n, $cr^n \in J^{n+h} = I^n J^h \subseteq I^n$, as required.

Now suppose that c is a nonzero element such that $cr^n \in I^n$ for arbitrarily large values of n. If $r \notin \overline{I}$ we can choose a discrete valuation v such that the value of v on r is smaller than the value of v on any element of I: then $v(r) + 1 \leq v(u)$ for all $u \in I$. Choose $n > v(c)$. Then $nv(r) + n \leq v(w)$ for all $w \in I^n$. But if we take $w = cr^n$ we have $v(w) = v(c) + nv(r) < nv(r) + n \leq v(w)$, a contradiction. □

For those familiar with the theory of schemes, we note that the condition in part (e) can be described in scheme-theoretic terms. There is a scheme, the *blow-up* Y of $X = \operatorname{Spec} R$ along the closed subscheme defined by I, which has a finite open cover by open affines corresponding to the affine schemes $\operatorname{Spec} S_i$. The normalization Y' of Y, i.e., the *normalized blow-up*, has a finite open cover by the open affines $\operatorname{Spec} T_i$. I corresponds to a sheaf of ideals on X, which pulls back (locally, via expansion) to a sheaf of ideals $\mathcal{J}$ on Y'. The integral closure of I is then the ideal of global sections of $\mathcal{J}$ intersected with R.

Discussion: the notion of analytic spread. Let (R, m, K) be a local ring and let $J \subseteq m$ be an ideal of R. It is of interest to study the least integer a such that J is integral over an ideal generated by a elements. If $I \subseteq J$ and J is integral over I, then I is called a *reduction* of J. Thus, we are interested in the minimum number of generators of a reduction.

We recall that the *associated graded ring*, denoted $\mathrm{gr}_I(R)$, of R with respect to the ideal I is the $\mathbb{N}$-graded ring

$$R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots \oplus I^n/I^{n+1} \oplus \cdots\,,$$

so that the k th graded piece is I^k/I^{k+1}. The multiplication is such that if $u \in I^j$ represents a j-form $\overline{u} \in I^j/I^{j+1}$ and $v \in I^k$ represents a k-form $\overline{v} \in I^k/I^{k+1}$, then uv represents the product $\overline{u}\,\overline{v} \in I^{j+k}/I^{j+k+1}$. This ring is generated by its forms of degree 1: moreover, given a set of generators of I as an ideal, the images of these elements in I/I^2 generate $\mathrm{gr}_I(R)$ as an (R/I)-algebra. Thus, if R is Noetherian, so is $\mathrm{gr}_I(R)$.

Now suppose that $(R,\, m,\, K)$ is a local ring, and view $K = R/m$ as an R-algebra. The ring $K \otimes_R \mathrm{gr}_I(R)$ is a finitely generated K-algebra. We may also write this as

$$K \oplus I/mI \oplus I^2/mI^2 \oplus \cdots \oplus I^n/mI^n \oplus \cdots\,.$$

The *analytic spread* of $I \subseteq R$ is defined to be the Krull dimension of the ring $K \otimes_R \mathrm{gr}_I(R)$. This ring is generated over K by its forms of degree 1, and the images in I/mI of any set of generators for I as an ideal generate $K \otimes \mathrm{gr}_I(R)$ as a K-algebra. We use $\mathfrak{an}(I)$ to denote the analytic spread of I. Our next main objective is to prove:

Theorem. *Let (R, m, K) be a local ring and J a proper ideal. Then the number of generators of any reduction of J is at least $\mathfrak{an}(J)$, and if K is infinite, J has a reduction with $\mathfrak{an}(J)$ generators.*

Lecture of Janaury 23, 2019

We have already noted that when (R, m, K) is a local ring and $I \subseteq m$ an ideal we may identify

$$K \otimes_R \mathrm{gr}_I(R) \cong R/m \oplus I/mI \oplus I^2/mI^2 \oplus \cdots \oplus I^n/mI^n \oplus \cdots .$$

S is called a *standard graded* A-algebra if S is finitely generated as an A-algebra, $\mathbb{N}$-graded with $S_0 = A$, and the 1-forms S_1 of S generate S as an A-algebra. In this case, S_n is finitely generated as an A-module for all n, by the monomials of degree n in the finite set of algebra generators in S_1. If S is a standard graded K-algebra, where K is a field, then R has a unique homogeneous maximal ideal $\mathfrak{m} = \bigoplus_{n=1}^{\infty} S_n$, the K-span (and even the span as an abelian group) of all elements of positive degree.

We note as well that if $R[It] \subseteq R[t]$ is the Rees ring, then

$$(R/I) \otimes_R R[It] \cong R[It]/IR[It] = \frac{R + It + I^2t^2 + \cdots + I^nt^n + \cdots}{I + I^2t + I^3t^2 + \cdots + I^{n+1}t^n + \cdots},$$

and it is quite straightforward to identify this with $\mathrm{gr}_I R$.

Since $(R/m) \otimes_R (R/I) \cong R/m$, it follows that

$$K \otimes_R \mathrm{gr}_I(R) \cong (R/m) \otimes_R \big((R/I) \otimes_R R[It]\big) \cong \big((R/m) \otimes_R (R/I)\big) \otimes_R R[It] \cong K \otimes_R R[It],$$

so that we may also view $K \otimes_R \mathrm{gr}(R)$ as $K \otimes_R R[It]$.

We give two preliminary results. Recall that in Nakayama's Lemma one has a *finitely generated module* M over a ring (R, m) with a unique maximal ideal, i.e., a quasilocal ring. The lemma states that if $M = mM$ then $M = 0$. By applying the result to M/N, one can conclude that if M is finitely generated (or finitely generated over N), and $M = N + mM$, then $M = N$. In particular, elements of M whose images generate M/mM generate M: if N is the module they generate, we have $M = N + mM$. Less familiar is the homogeneous form of the Lemma: it does not need M to be finitely generated, although there can be only finitely many negative graded components (the detailed statement is given below).

First recall that if H is an additive semigroup with 0 and R is an H-graded ring, we also have the notion of an H-graded R-module M: M has a direct sum decomposition

$$M = \bigoplus_{h \in H} M_h$$

as an abelian group such that for all $h, k \in H$, $R_h M_k \subseteq M_{h+k}$. Thus, every M_h is an R_0-module. A submodule N of M is called graded (or homogeneous) if

$$N = \bigoplus_{h \in H} (N \cap M_h).$$

An equivalent statement is that the homogeneous components in M of every element of N are in N, and another is that N is generated by forms of M.

Note that if we have a subsemigroup $H \subseteq H'$, then any H-graded ring or module can be viewed as an H'-graded ring or module by letting the components corresponding to elements of $H' - H$ be zero.

In particular, an $\mathbb{N}$-graded ring is also $\mathbb{Z}$-graded, and it makes sense to consider a $\mathbb{Z}$-graded module over an $\mathbb{N}$-graded ring.

Nakayama's Lemma, homogeneous form. *Let R be an $\mathbb{N}$-graded ring and let M be any $\mathbb{Z}$-graded module such that $M_{-n} = 0$ for all sufficiently large n (i.e., M has only finitely many nonzero negative components). Let I be the ideal of R generated by elements of positive degree. If $M = IM$, then $M = 0$. Hence, if N is a graded submodule such that $M = N + IM$, then $N = M$, and a homogeneous set of generators for M/IM generates M.*

Proof. If $M = IM$ and $u \in M$ is nonzero homogeneous of smallest degree d, then u is a sum of products $i_t v_t$ where each $i_t \in I$ has positive degree, and every v_t is homogeneous, necessarily of degree $\geq d$. Since every term $i_t v_t$ has degree strictly larger than d, this is a contradiction. The final two statements follow exactly as in the case of the usual form of Nakayama's Lemma. □

Lemma. *Let $S \to T$ be a degree preserving K-algebra homomorphism of standard graded K-algebras. Let $\mathfrak{m} \subseteq S$ and $\mathfrak{n} \subseteq T$ be the homogeneous maximal ideals. Then T is a finitely generated S-module if and only if the image of S_1 in T_1 generates an $\mathfrak{n}$-primary ideal.*

Proof. By the homogeneous form of Nakayama's lemma, T is finitely generated over S if and only if $T/\mathfrak{m}T$ is a finite-dimensional K-vector space, and this will be true if and only if all homogeneous components $[T/\mathfrak{m}T]_s$ are 0 for $s \gg 0$, which holds if and only if $\mathfrak{n}^s \subseteq \mathfrak{m}T$ for all $s \gg 0$. □

Proposition. *Let (R, m, K) be a local ring. If $I \subseteq J \subseteq m$ are ideals, then J is integral over I if and only if the image of I in $J/mJ = [K \otimes_R \operatorname{gr}(R)]_1$ generates an $\mathfrak{n}$-primary ideal in $T = K \otimes_R \operatorname{gr}_J(R)$, where $\mathfrak{n}$ is the homogeneous maximal ideal in T.*

Proof. First note that J is integral over I if and only if $R[Jt]$ is integral over $R[It]$, and this is equivalent to the assertion that $R[Jt]$ is module-finite over $R[It]$, since $R[Jt]$ is finitely generated as an R-algebra, and, hence, as an $R[It]$-algebra.

If this holds, we have that $K \otimes_R R[Jt]$ is a finitely generated module over $K \otimes_R R[It]$, and, since the image of I generates the maximal ideal $\mathfrak{m}$ in $S = K \otimes_R \mathrm{gr}_I(R) \cong K \otimes_R R[It]$, the preceding Lemma implies that the latter statement will be true if and only if the image of I in $J/mJ = [K \otimes_R \mathrm{gr}_J(R)]_1$ generates an $\mathfrak{n}$-primary ideal in $T = K \otimes_R \mathrm{gr}_J(R)$.

The proof will be complete if we can show that when T is module-finite over S, then $R[Jt]$ is module-finite over $R[It]$. Let $j_1 \in J^{d_1}, \ldots, j_h \in J^{d_h}$ be elements whose images in $J^{d_1}/mJ^{d_1}, \ldots, J^{d_h}/mJ^{d_h}$, respectively, generate T as an S-module. We claim that $j_{d_1}t^{d_1}, \ldots, j_{d_h}t^{d_h}$ generate $R[Jt]$ over $R[It]$. To see this, note that the fact that these elements generate T over S implies that for every N,

$$J^N = \sum_{1 \leq i \leq h \text{ such that } d_i \leq n} I^{N-d_i} j_{d_i} + mJ^N.$$

For each fixed N, we may apply the usual form of Nakayama's Lemma to conclude that

$$J^N = \sum_{1 \leq i \leq h \text{ such that } d_i \leq n} I^{N-d_i} j_{d_i}.$$

and so, for all N, we have

$$J^N t^N = \sum_{1 \leq i \leq h \text{ such that } d_i \leq n} I^{N-d_i} t^{N-d_i} j_{d_i} t^{d_i},$$

which is just what we need to conclude that $j_{d_1}t^{d_1}, \ldots, j_{d_h}t^{d_h}$ generate $R[Jt]$ over $R[It]$. □

The following fact is often useful.

Proposition. *Let K be an infinite field, $V \subseteq W$ vector spaces, and let $V_1, \ldots, V_h$ be vector subspaces of W such that $V \subseteq \bigcup_{i=1}^h V_i$. Then $V \subseteq V_i$ for some i.*

Proof. If not, for each i choose $v_i \in V - V_i$. We may replace V by the span of the v_i and so assume it is finite-dimensional of dimension d. We may replace V_i by $V_i \cap V$, so that we may assume every $V_i \subseteq V$. The result is clear when $d = 1$. When $d = 2$, we may assume that $V = K^2$, and the vectors $(1, c)$, $c \in K - \{0\}$ lie on infinitely many distinct lines. For $d > 2$ we use induction. Since each subspace of $V \cong K^d$ of dimension $d - 1$ is covered by the V_i, each is contained in some V_i, and, hence, equal to some V_i. Therefore it suffices to see that there are infinitely many subspaces of dimension $d-1$. Write $V = K^2 \oplus W$ where $W \cong K^{d-2}$. The line L in K^2 yields a subspace $L \oplus W$ of dimension $d - 1$, and if $L \neq L'$ then $L \oplus W$ and $L' \oplus W$ are distinct subspaces. □

Also note:

Proposition. *Let M be an $\mathbb{N}$-graded or $\mathbb{Z}$-graded module over an $\mathbb{N}$-graded or $\mathbb{Z}$-graded Noetherian ring S. Then every associated prime of M is homogeneous. Hence, every* *minimal prime of the support of M is homogeneous and, in particular the associated (hence, the minimal) primes of S are homogeneous.*

Proof. Any associated prime P of M is the annihilator of some element u of M, and then every nonzero multiple of $u \neq 0$ can be thought of as a nonzero element of $S/P \cong Su \subseteq M$, and so has annihilator P as well. Replace u by a nonzero multiple with as few nonzero homogeneous components as possible. If u_i is a nonzero homogeneous component of u of degree i, its annihilator J_i is easily seen to be a homogeneous ideal of S. If $J_h \neq J_i$ we can choose a form F in one and not the other, and then Fu is nonzero with fewer homgeneous components then u. Thus, the homogeneous ideals J_i are all equal to, say, J, and clearly $J \subseteq P$. Suppose that $s \in P - J$ and subtract off all components of s that are in J, so that no nonzero component is in J. Let $s_a \notin J$ be the lowest degree component of s and u_b be the lowest degree component in u. Then $s_a\, u_b$ is the only term of degree $a+b$ occurring in $su = 0$, and so must be 0. But then $s_a \in \mathrm{Ann}_S\, u_b = J_b = J$, a contradiction. □

Corollary. *Let S be a standard graded K-algebra of dimension d with homogeneous maximal ideal $\mathfrak{m}$, where K is an infinite field. Then there are forms $L_1, \ldots, L_d$ of degree 1 in R_1 such that $\mathfrak{m}$ is the radical of $(L_1, \ldots, L_d)S$.*

Proof. The minimal primes of a graded algebra are homogenous, and $\dim(S)$ is the same as $\dim(S/P)$ for some minimal prime P of R. Then $P \subseteq \mathfrak{m}$, and

$$\dim(S) = \dim(S/P) = \dim(S/P)_{\mathfrak{m}} \leq \dim S_{\mathfrak{m}} \leq \dim(S),$$

so that $\dim(S) = \dim(S_{\mathfrak{m}}) = \mathrm{height}\,\mathfrak{m}$. If $\dim(S) = 0$, $\mathfrak{m}$ must be the unique minimal prime of S, and therefore is itself nilpotent. Otherwise, S_1 cannot be contained in the union of the minimal primes of S, or the Proposition just above would imply that it is contained in one of them, and S_1 generates $\mathfrak{m}$. Choose $L_1 \in S_1$ not in any minimal prime, and then $\dim(S/L_1) = d-1$. Use induction. If $L_1, \ldots, L_k$ have been chosen in S_1 such that $\dim\bigl(S/(L_1, \ldots, L_k)S\bigr) = d-k < d$, choose $L_{k+1} \in S_1$ not in any minimal prime of $(L_1, \ldots, L_k)S$ (if S_1 were contained in one of these, $\mathfrak{m}$ would be, and it would follow that height $\mathfrak{m} \leq k$, a contradiction). Thus, we eventually have $L_1, \ldots, L_d$ such $\dim(S/\bigl(L_1, \ldots, L_d)S\bigr) = 0$, and then by the case where $d = 0$ we have that $\mathfrak{m}$ is nilpotent modulo $(L_1, \ldots, L_d)S$. □

We are now ready to prove the result that we have been aiming for:

Theorem. *Let (R, m, K) be local and $J \subseteq R$ an ideal. Then any reduction I of J has at least $\mathfrak{an}(J)$ generators. Moreover, if K is infinite, there is a reduction with $\mathfrak{an}(J)$ generators.*

Proof. The problem of giving $i_1, \ldots, i_a \in J$ such that J is integral over $(i_1, \ldots, i_a)R$ is equivalent to giving a elements of J/mJ that generate an $\mathfrak{m}$-primary ideal of $S = K \otimes_R \mathrm{gr}_J(R)$, where $\mathfrak{m}$ is the homogeneous maximal ideal of S. Clearly, we must have $a \geq \dim(S) = \mathfrak{an}(J)$. If K is infinite, the existence of suitable elements follows from the Corollary just above. □

Discussion. If $(R,\, m,\, K)$ is local and t is an indeterminate over R, let $R(t)$ denote the localization of the polynomial ring $R[t]$ at $mR[t]$. Then $R \to R(t)$ is a faithfully flat map of local rings of the same dimension, and the maximal ideal of $R(t)$ is $mR(t)$ while the residue class field of $R(t)$ is $K(t)$. If $J \subseteq m$, $\mathfrak{an}(J)$ is the least number of generators of an ideal over which $JR(t)$ is integral. In fact, $K(t) \otimes \mathrm{gr}_{JR(t)}R(t) \cong K(t) \otimes_K \big(K \otimes_R \mathrm{gr}_J(R)\big)$, so that $\mathfrak{an}(J) = \mathfrak{an}\big(JR(t)\big)$.

Remark. If I and J are any two ideals of any ring R, $\overline{I}\,\overline{J} \subseteq \overline{IJ}$. There are many ways to see this. E.g., if $r \in \overline{I}$, $s \in \overline{J}$ and $R \to V$ is any homomorphism to a valuation domain, then $r \in IV$ and $s \in JV$, whence $rs \in (IV)(JV) = (IJ)V$. Thus, $rs \in \overline{IJ}$ for every such r and s, and the elements rs generate $\overline{I}\,\overline{J}$. □

We shall prove below that if R is local and J is any proper ideal, then $\dim(R) = \dim(\mathrm{gr}_J R)$. Assume this for the moment. It then follows that $\dim\big(K \otimes_R \mathrm{gr}_J(R)\big) \le \dim(R)$. We define the *big height* of a proper ideal J of a Noetherian ring to be the largest height of any minimal prime of J. (The height is the smallest height of any minimal prime of J.) We then have:

Proposition. *For any proper ideal J of a local ring $(R,\, m,\, K)$, the analytic spread of J lies between the big height of J and* $\dim(R)$.

Proof. That $\mathfrak{an}(I) \le \dim(R)$ follows from the discussion above, once we have shown that $\dim(R) = \dim(\mathrm{gr}_J R)$. Let P be a minimal prime of J. We want to show that $\mathrm{height}\, P \le \mathfrak{an}(J)$. After replacing R by $R(t)$, if necessary, we have that J is integral over an ideal I with $a = \mathfrak{an}(J)$ generators. Then J is contained in the radical of I. In R_P we have that P is the radical of JR_P, since P is a minimal prime of J, and so is contained in the radical of IR_P. Thus, $\mathrm{height}\, P \le a = \mathfrak{an}(J)$, as required. □

Corollary. *If K is infinite, every proper ideal J of a local ring $(R,\, m,\, K)$ of Krull dimension d is integral over an ideal generated by at most d elements.* □

Proposition. *Let $(R,\, m,\, K)$ be local, and J a proper ideal. Then for every positive integer n, the ideals J and J^n have the same analytic spread.*

Proof. The Rees ring of J^n may be identified with $R[J^n t^n]$ since t^n is an indeteminate over R, and this is a subring of $R[Jt]$ over which the larger ring is module-finite, since the nth power of any element of Jt is in $R[J^n t^n]$. The injectivity is retained when we apply $K \otimes_R \_\_$, since tensor commutes with direct sum, and the module-finite property continues to hold as well. It follows that $K \otimes \mathrm{gr}_J(R)$ is a module-finite extension of $K \otimes_R \mathrm{gr}_{J^n} R$, and so these two rings have the same dimension. □

In general, if X is a matrix and B is a ring, $B[X]$ denotes the ring generated over B by the entries of X. We frequently use this notation when these entries are indeterminates, in which case $B[[X]]$ denotes the formal power series ring over B in which the variables are the entries of X. If $M = \big(r_{ij}\big)$ is a matrix over a ring R and t is a nonnegative integer,

$I_t(M)$ denotes the ideal of R generated by the size t minors of M. By convention, this ideal is R if $t = 0$ and is (0) if t is strictly larger than either of the dimensions of the matrix M.

Example. Let $I \subseteq (R,\, m,\, K)$ and let r be a nonzerodivisor. Then $R[It] \cong R[rIt]$: in fact rt is algebraically independent of R, so that there is an R-isomorphism $R[t] \to R[rt]$ mapping $t \mapsto rt$, and this induces an R-isomorphism $RI[t] \cong R[rIt]$. It follows that $K \otimes_R R[It] \cong K \otimes_R R[rIt]$, and so $\mathfrak{an}(I) = \mathfrak{an}(Ir)$. $Ir \subseteq rR$ which has analytic spread one. If $I = m$, or if I is m-primary, the analytic spread of I and of Ir is $\dim{(R)}$. Thus, the smaller of two ideals may have a much larger analytic spread than the larger ideal.

Example. Let K be a field and let $X = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{pmatrix}$ be a $2 \times n$ matrix of formal indeterminates over K. Let $K[X]$ be the polynomial ring in the entries of X, and let $A = K[X]/I_2(X)$. This ring is known to be a normal ring with an isolated singularity of dimension $n{+}1$. One can see what the dimension is as follows: we may tensor with algebraic closure of K without changing the dimension (this produces an integral extension), and so we may assume that K is algebraically closed. The algebraic set Z in $\mathbb{A}^{2n}$ defined by $I_2(X)$ corresponds to $2 \times n$ matrices of rank at most one. We can map $\mathbb{A}^n \times \mathbb{A}^1$ to Z by sending (v, c) to the matrix whose first row is v and whose second row is cv. This map is not onto, but its image contains the open set consisting of matrices whose first row is not 0. It follows that the dimension of Z is $n + 1$. (This ring is also known to be Cohen-Macaulay. Cf. [M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. of Math. **93** (1972), 1020–1058].) The same properties hold if we localize A at the ideal generated by the entries of X (and if we complete). Call the local ring obtained S. Let P be the prime ideal $(x_1,\, \dots\,, x_n)R$. Then $A = S/P$ is either the localization of $K[y_1,\, \dots\,, y_n]$ at $(y_1,\, \dots\,, y_n)$ or its completion. In any case, R/P has dimension n, so that P is a height one prime of S. But its analytic spread is n. In fact, $\mathrm{gr}_P(S)$ has the form $A[u_1,\, \dots\,, u_n]$ where the u_i satisfy the relations $y_i u_j - y_j u_i = 0$. If we kill only these relations we get a domain of dimension $n + 1$ that maps onto $\mathrm{gr}_P(S)$. Since $\mathrm{gr}_P(S)$ has the same dimension as S (we have not proved this yet, but will shortly), the map onto $\mathrm{gr}_P(S)$ cannot have a nonzero kernel, i.e., it is an isomorphism. But then $K \otimes \mathrm{gr}_P(S) \cong K[u_1,\, \dots\,, u_n]$ has dimension n.

We next want to prove the assertion that the local ring $(R,\, m,\, K)$ and the ring $\mathrm{gr}_J R$ have the same dimension. In order to do so, we review the dimension formula. Recall that a Noetherian ring R is *catenary* if for any two prime ideals $P \subseteq Q$, any two saturated chains of prime ideals joining P to Q have the same length. Localizations and homomorphic images of catenary rings are clearly catenary. R is *universally catenary* if every polynomial ring in finitely many variables over R is catenary. It is equivalent to assert that every algebra essentially of finite type over R is catenary. A ring is called *Cohen-Macaulay* if in each of its local rings some (equivalently, every) system of parameters is a regular sequence. Cohen-Macaulay rings are catenary and, therefore, universally catenary, since a polynomial ring over a Cohen-Macaulay ring is Cohen-Macaulay. Regular rings are Cohen-Macaulay, and, hence, universally catenary. A complete local ring is a homomorphic image of a regular ring and so is also universally catenary. If $\mathcal{F} \subseteq \mathcal{G}$ are fields, $\mathrm{tr.\,deg.}(\mathcal{G}/\mathcal{F})$ denotes the transcendence degree over $\mathcal{G}$ over $\mathcal{F}$.

Theorem (dimension formula). *Let $R \subseteq S$ be Noetherian domains such that S is finitely generated over R, and call the fraction fields $\mathcal{F}$ and $\mathcal{G}$, respectively. Let Q be a prime ideal of S lying over P in R. Let K and L be the residue class fields of R_P and S_Q, respectively. Then*

$$\mathrm{height}\,Q - \mathrm{height}\,P \leq \mathrm{tr.\,deg.}(\mathcal{G}/\mathcal{F}) - \mathrm{tr.\,deg.}(L/K),$$

with equality if R is universally catenary.

Lecture of January 25, 2019

We shall soon return to our treatment of the dimension formula, which was stated in the Lecture of January 23, but we first want to make some additional remarks about the behavior of analytic spread.

Theorem. *Let K be a field, and T a finitely generated $\mathbb{N}$-graded K-algebra with $T_0 = K$. Let $\mathcal{M}$ be the homogenous maximal ideal of T. Let $F_1, \ldots, F_s$ be homogeneous polynomials of the same positive degree d in T, and let $I = (F_1, \ldots, F_s)T$. Then $\mathfrak{an}(IT_{\mathcal{M}})$ is the Krull dimension of the ring $K[F_1, \ldots, F_s] \subseteq T$, and hence is the same as the maximum number of algebraically independent elements in $K[F_1, \ldots, F_s]$. over K.*

Proof. We shall show that $K[F_1, \ldots, F_s] \cong K \otimes_{T_{\mathcal{M}}} \mathrm{gr}_I(T_{\mathcal{M}})$. We view the latter is

$$K \otimes_{T_{\mathcal{M}}} T_{\mathcal{M}}[IT_{\mathcal{M}}t] \cong (K \otimes_T T[It])_{\mathcal{M}}$$

and the ring on the right is the same as $K \otimes_T T[It]$, because elements of $T - \mathcal{M}$ map to units in K and so already are invertible in this ring. Note that K here is $T/\mathcal{M}$, and so this ring is also the same as $T[It]/\mathcal{M}T[It]$.

Now there is a map $K[F_1, \ldots, F_s] \to T[It]$ that sends $F_j \mapsto F_jt$, $1 \leq j \leq s$. To see that this is well-defined, note that the ideal of relations on the F_j over K is homogeneous. Thus, it suffices to see that if $H \in K[Y_1, \ldots, Y_s]$ is a *homogeneous* polynomial of degree μ such that $H(F_1, \ldots, F_s) = 0$, then $H(F_1t, \ldots, F_st) = 0$. But the left hand side is $t^\mu H(F_1, \ldots, F_d) = t^\mu \cdot 0 = 0$. We then get a composite map

$$K[F_1, \ldots, F_s] \to T[It] \twoheadrightarrow T[It]/\mathcal{M}T[It].$$

This map is clearly surjective, since the image of T in the quotient is K and It is generated by the F_jt. We need only prove that the kernel is 0. It is homogeneous: let G be an element of the kernel that is homogeneous of degree h in $F_1, \ldots, F_s$. Then G has degree hd in

$x_1, \ldots, x_n$. If G is in the kernel then Gt^h is in $\mathcal{M}I^h t^h$, and $G \in \mathcal{M}I^h$. However, all nonzero elements of this ideal have components of degree at least $hd + 1$ in $x_1, \ldots, x_n$, a contradiction unless $G = 0$.

The final statement is a general characterization of Krull dimension in finitely generated K-algebras. □

Remark. This result gives another way to compute the analytic spread of the height one prime in a determinantal ring analyzed in the last Example (beginning at the bottom of p. 5) in the Lecture Notes of January 23. It is immediate that the analytic spread is n.

Example. The Example discussed in the Remark just above shows that height one primes that have arbitrarily large analytic spread. In a regular local ring a height one prime is principal, and so its analytic spread is 1. But there are height two primes of arbitarily large analytic spread. Let X be an $n \times (n+1)$ matrix of indeterminates over a field K and let P be the ideal generated by the size n minors of X in the polynomial ring $K[X]$. Then the analytic spread of P in $K[X]_{\mathcal{M}}$, where $\mathcal{M}$ is generated by the entries of X, is $n+1$ by the Theorem above, for the minors of algebraically independent over K. (This is true even if we specialize the leftmost $n \times n$ submatrix to be yI_n. The minors are y^n and, up to sign, the products $y^{n-1}x_{i,n+1}$, $1 \leq i \leq n$.) These primes have height two: the algebraic set of $n \times (n+1)$ matrices of rank at most $n-1$ has dimension $n^2 + n - 2$. (On the open set where the first $n-1$ rows are algebraically independent, the space consisting of choices for the first $n-1$ rows has dimension $(n-1)(n+1)$; the choices for the final row are linear combinations of the first $n-1$ rows, and are parametrized by $\mathbb{A}^{n-1}$, giving dimension $n^2 - 1 + (n-1)$.)

Recall that a map of quasilocal rings $h : (R, m) \to (S, n)$ is called *local* if $h(m) \subseteq n$. (The map of a local ring onto its residue class field is local, while the inclusion of a local domain that is not a field in its fraction field is *not* local.)

Proposition. *Let (R, m, K) be local.*

(a) *If $h : (R, m, K) \to (S, n, L)$ is a local homomorphism, and $I \subseteq m$ is an ideal of R, then $\mathfrak{an}(I) \geq \mathfrak{an}(IS)$.*

(b) *If I and J are proper ideals of R, then $\mathfrak{an}(I + J) \leq \mathfrak{an}(I) + \mathfrak{an}(J)$.*

(c) *Let I and J are proper ideals of R. If either $\mathfrak{an}(I)$ or $\mathfrak{an}(J)$ is 0, then $\mathfrak{an}(IJ) = 0$. If the analytic spreads are positive, $\mathfrak{an}(I\,J) \leq \mathfrak{an}(I) + \mathfrak{an}(J) - 1$.*

Proof. We replace $R \to S$ by $R(t) \to S(t)$ if necessary, and the ideals considered by their expansions. We may therefore assume the residue class fields are infinite.

For part (a), if I is integral over an ideal I_0 with $a = \mathfrak{an}(I)$ generators, then IS is integral over I_0S.

For part (b) simply note that if I_0 is as above and J is integral over J_0 with $b = \mathfrak{an}(J)$ generators, then $I + J$ is integral over $I_0 + J_0$, which has at most $a + b$ generators.

To prove part (c), first note that the analytic spread of I is 0 if and only if I consists of nilpotents. Thus, if either a or b is 0, then IJ consists of nilpotents and $\mathfrak{an}(I\,J) = 0$ as well. Now suppose that both analytic spreads are positive and that I_0 and J_0 are as above. Map the polynomial ring $T = \mathbb{Z}[X_1, \,\ldots\,, X_a, Y_1, \,\ldots\,, Y_b] \to R$ so that $(X_1, \,\ldots\,, X_a)T$ maps onto I_0 and $(Y_1, \,\ldots\,, Y_b)T$ maps onto J_0. Since IJ is integral over I_0J_0, it suffices to show that $\mathfrak{an}(I_0J_0) \leq a + b - 1$. Let $\mathcal{M}$ be the inverse image of m in T. Then $\mathcal{M}$ is a prime ideal of T that is either $(X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b)T$ or $pT + (X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b)T$. Let $A = T_{\mathcal{M}}$. Let $\mathcal{I} = (X_1, \,\ldots\,, X_a)A$ and $\mathcal{J} = (Y_1, \,\ldots\,, Y_b)A$. Then we have an induced local map $T_{\mathcal{M}} \to R$ such that $\mathcal{I}R = I_0$ and $\mathcal{J}R = J_0$. By part (a), it will suffice to show that $\mathfrak{an}(\mathcal{I}\,\mathcal{J}) \leq a + b - 1$.

Let $\mathfrak{A}$ denote the ideal $(X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b) \subseteq T$, and let $\mathfrak{B}$ denote the ideal $(X_1, \,\ldots\,, X_a)(Y_1, \,\ldots\,, Y_b)T$. There are two cases. First suppose that $\mathcal{M} = \mathfrak{A}$. Then $T_{\mathcal{M}}$ contains the rational numbers, and may be viewed instead as the localization of the polynomial ring $\mathbb{Q}[X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b]$ at $(X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b)$. Then, since the elements X_iY_j are forms of the same degree, the Theorem above applies, and the analytic spread is the transcendence degree of $\mathbb{Q}[X_iY_j : 1 \leq i \leq a, 1 \leq j \leq b]$ over $\mathbb{Q}$. But the fraction field of this domain is generated by the elements $X_1Y_1, \,\ldots\,, \, X_1Y_b$ and the elements X_j/X_1, $2 \leq i \leq a$, since $(X_i/X_1)(X_1Y_j) = X_iY_j$ (which also shows that each X_j/X_1 is in the fraction field). These $b+(a-1)$ elements are easily seen to be algebraically independent. Exactly the same calculation of transcendence degree if $\mathbb{Q}$ is replaced by any other field κ.

In the remaining case, $\mathcal{M} = \mathfrak{A} + pT$. In this case, note that since $\mathfrak{B}^n$ and $\mathfrak{B}^{n+1}$ are both free $\mathbb{Z}$-modules spanned by the monomials in $X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b$ that they contain, each $\mathfrak{B}^n/\mathfrak{B}^{n+1}$ is free over $\mathbb{Z}$. It follows that p is not a zerodivisor on $\mathrm{gr}_{\mathfrak{B}}T$. Let $\kappa = T/\mathcal{M} \cong \mathbb{Z}/p\mathbb{Z}$. Then

$$\kappa \otimes_T \mathrm{gr}_{\mathfrak{B}}T \cong \kappa \otimes_{T/pT} \big((\mathbb{Z}/p\mathbb{Z}) \otimes_{\mathbb{Z}} \mathrm{gr}_{\mathfrak{B}}T\big).$$

Let

$$\overline{T} = T/pT \cong \kappa[X_1, \,\ldots\,, X_a, \; Y_1, \,\ldots\,, Y_b],$$

and $\overline{\mathfrak{B}} = \mathfrak{B}\overline{T}$, Because p is not a zerodivisor on $\mathrm{gr}_{\mathfrak{B}}(T)$, we have that

$$(\mathbb{Z}/p\mathbb{Z}) \otimes_{\mathbb{Z}} \mathrm{gr}_{\mathfrak{B}}T \cong \mathrm{gr}_{\overline{\mathfrak{B}}}\overline{T},$$

and this is the ring whose dimension we need to calculate: as in the proof of the Theorem above, localization at $\mathcal{M}$ has no effect on this ring, since the image of $T - \mathcal{M}$ consists of units in κ. We are now in the same situation as in the first case, except that we are working with $\kappa[X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b]$ instead of $\mathbb{Q}[X_1, \,\ldots\,, X_a, \, Y_1, \,\ldots\,, Y_b]$. □

We are now ready to continue with our treatment of the dimension formula, stated in the Lecture of January 23. Recall that we are assuming that $R \subseteq S$ are Noetherian domains with fraction fields $\mathcal{F}$ and $\mathcal{G}$ respectively, that Q is a prime ideal of S lying over P in R, that $K = R_P/PR_P$, and that $L = S_Q/QS_Q$. We must show that

$$\mathrm{height}\, Q - \mathrm{height}\, P \leq \mathrm{tr.\,deg.}\mathcal{G}/\mathcal{F} - \mathrm{tr.\,deg.}L/K,$$

with equality of R is universally catenary. Equality also holds if S is a polynomial ring over R.

Before beginning the proof, we make the following observation. Let P_0 be a prime ideal of a local domain D. In general, $\dim(D/P_0) \leq \dim(D) - \operatorname{height} P_0$, while equality holds if D is catenary. The inequality, which is equivalent to the statement that $\dim(D) \geq \operatorname{height} P_0 + \dim(D/P_0)$, follows from the following observation. We can "splice" a saturated chain of primes of length $k = \dim(D/P_0)$ ascending from P_0 to the maximal ideal m of D (corresponding to a chain of primes of length k in D/P_0) with a chain of primes of length h descending from P_0 to (0). This yields a chain of saturated primes from m to (0) in D that has length $h+k$. If, moreover, D is catenary then all saturated chains from m to (0) have the same length, and this is $\dim(D)$, so that $h+k = \dim(D)$.

Proof of the dimension formula. By adjoining generators of S to R one at a time, we can construct a chain of rings

$$R = S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n$$

such that for each i, $0 \leq i \leq n$, we have that S_{i+1} is generated over S_i by one element. Let $Q_i = Q \cap S_i$ for each i. Note that when R is universally catenary, every S_i is universally catenary. It will suffice to prove the dimension formula (whether the inequality or the equality) for each inclusion $S_i \subseteq S_{i+1}$. When we add the results, each term associated with S_i for i different from 0 and n occurs twice with opposite signs. The intermediate terms all cancel, and we get the required result.

We henceforth assume that $S = R[x]$, where x need not be an indeterminate over R. By replacing R and S by R_P and $R_P \otimes_R S$, we may assume that (R, P, K) is local. We consider two cases, according as whether x is transcendental or algebraic over R.

Case 1. x is transcendental over R. Then the primes of $S = R[x]$ lying over P correspond to the primes of $R[x]/PR[x] \cong K[x]$, a polynomial ring in one variable. There are two subcases.

Subcase 1a. Q corresponds to the prime ideal (0) in $K[x]$, i.e., $Q = PR[x]$. In this case $S_Q \cong R(x)$ has the same dimension as R, so that $\operatorname{height} Q = \operatorname{height} P$. We have that $\operatorname{tr.deg.}(\mathcal{G}/\mathcal{F}) = 1$, and $L \cong K(x)$, so that $\operatorname{tr.deg.}(L/K) = 1$ as well. Since $0 = 1 - 1$, we have the required equality whether R is universally catenary or not.

Subcase 1b. Q is generated by $PR[x]$ and a monic polynomial g of positive degree whose image $\overline{g}$ mod P is irreducible in $K[x]$. The height of Q is evidently has height $\operatorname{height} P + 1$: a system of parameters for P together with g will give a system of parameters for $R[x]_Q$. The left hand side of the inequality is therefore 1, while the right hand side is $1 - 0$, because $L \cong K[x]/(\overline{g})$. Again, we have the required equality whether R is universally catenary or not.

Case 2. x is algebraic over R. Let X be an indeterminate and map $R[X] \twoheadrightarrow R[x] = S$ as

R-algebras by sending $X \mapsto x$. We have a commutative diagram:

$$\begin{tikzcd}
\mathcal{F}[X] \arrow[r] & \mathcal{G} \\
R[X] \arrow[r] \arrow[u] & S \arrow[u]
\end{tikzcd}$$

where the horizontal arrows are surjective and the vertical arrows are inclusions. By hypothesis, the top horizontal arrow has a kernel, which will be the principal ideal generated by a monic polynomial h of positive degree: the minimal polynomial of x over $\mathcal{F}$. The kernel P_0 of $R[X] \twoheadrightarrow S$ may therefore be described as $h\mathcal{F}[X] \cap R[X]$. We claim that P_0 is a height one prime of $R[X]$. To see this, we calculate $R[X]_{P_0}$. Since $R \subseteq S$, P_0 does not meet R, and $R - \{0\}$ becomes invertible in R_{P_0}. Thus, R_{P_0} is the localization of $\mathcal{F}[X]$ at the expansion of P_0, which is $h\mathcal{F}[x]$, and is a one-dimensionsial ring. Let $\mathcal{Q}$ denote the inverse image of Q in $R[X]$. Then $\mathcal{Q}$ contains P and, in fact, lies over P. It also contains P_0. There are again two subcases, depending on what $\mathcal{Q}$ is.

Subcase 2a. $\mathcal{Q} = PR[X]$. In this subcase the right hand side of the dimension formula is $0 - 1$. The height of $\mathcal{Q}$ is the same as height P, and killing P_0 decreases it at least by 1 as required. If R is universally catenary it decreases by exactly 1.

Subcase 2b. $\mathcal{Q}$ has the form $PR[X] + fR[X]$, where $f \in R[X]$ is monic of positive degree and irreducible mod P. The right hand side of the dimension formula is $0 - 0$. The height of $\mathcal{Q}$ is height $P + 1$. Killing P_0 decreases it by least 1, and by exactly 1 in the universally catenary case. □

Remark. If S is a polynomial ring over R, we can choose the chain so that S_{i+1} is always a polynomial ring in one variable over S_i. We are always in Case 1 of the proof, and so equality holds in the dimension formula without assuming that R is universally catenary.

Lecture of January 28, 2019

Let R be any ring and $I \subseteq R$ any ideal. By the *extended Rees ring* or *second Rees ring* of I over R we mean the ring $R[It, 1/t] \subseteq R[t]$. In this context we shall standardly write v for $1/t$. Note that if I is proper, v is *not* a unit of $R[It,\, v]$. This ring is $\mathbb{Z}$-graded. Written out as a sum of graded pieces

$$R[It,\, v] = \cdots + Rv^k + \cdots + Rv^2 + Rv + R + It + I^2t^2 + \cdots + I^nt^n + \cdots .$$

The element v generates a homogeneous principal ideal, and

$$vR[It,\, v] = \cdots + Rv^k + \cdots + Rv^2 + Rv + I + I^2t + I^3t^2 + \cdots + I^{n+1}t^n + \cdots .$$

From this it follows easily that $R[It,\, v]/(v) \cong \mathrm{gr}_I R$. There is a composite surjection

$$R[It,\, v] \twoheadrightarrow \mathrm{gr}_I R \twoheadrightarrow R/I.$$

When I is the unit ideal of R we have that $R[It, v] = R[t, t^{-1}]$.

When (R, m, K) is local and I is proper we further have a composite surjection

$$R[It, v] \twoheadrightarrow R/I \to R/m = K,$$

and the kernel is a maximal ideal $\mathcal{M}$ of $R[It, v]$. Explicitly,

$$\mathcal{M} = \cdots + Rv^k + \cdots + Rv^2 + Rv + m + It + I^2t^2 + \cdots + I^nt^n + \cdots .$$

Theorem. *Let (R, m, K) be local, let $I \subseteq R$ be proper, and let $R[It, v]$ and $\mathcal{M}$ be as in the paragraphs just above,*

(a) *The Krull dimension of $R[It, 1/t]$ is $\dim(R) + 1$, and this is the height of $\mathcal{M}$.*

(b) $\dim\bigl(\mathrm{gr}_I(R)\bigr) = \dim(R)$.

Proof. Let

$$\mathcal{P} = \cdots + mv^k + \cdots + mv^2 + mv + m + It + I^2t^2 + \cdots + I^nt^n + \cdots ,$$

which is the contraction of $mR[t, 1/t]$ to $R[It, v]$. Then $\mathcal{P} \subseteq \mathcal{M}$ and $R[It, v]/\mathcal{P} \cong K[v]$, a polynomial ring in one variable over a field. The height of $\mathcal{P}$ is the same as the height of m: when we localize at $\mathcal{P}$ in $R[It, v]$, v becomes invertible, so that $t = 1/v$ becomes an element of the localized ring. But $R[It, v][t] = R[t, v]$, and the expansion of $\mathcal{P}$ is $mR[t, 1/t]$. The localization at the expansion is just $R(t)$ (note that when we localize $R[t]$ at $mR[t]$, v becomes an element of the ring), which we already know has the same dimension as R. Thus, $\operatorname{height}\mathcal{P} = \dim(R)$. Since $\mathcal{M} = \mathcal{P} + vR[It, v]$ is strictly larger than $\mathcal{P}$, we have that $\operatorname{height}\mathcal{M} \geq \dim(R) + 1$. To complete the proof of (a), it will suffice to show that $\dim(R[It, v]) \leq \dim(R) + 1$, for then $\operatorname{height}\mathcal{M} \leq \dim(R) + 1$ as well.

We first reduce to the case where R is a domain. To do so, we want to understand the minimal primes of $S = R[It, v]$. If $\mathfrak{q}$ is any prime of S, it lies over some prime of R, and this prime contains a minimal prime $\mathfrak{p}$ of R. We shall show that there is a unique minimal prime $\widetilde{\mathfrak{p}}$ of S containing $\mathfrak{p}$, and it will follow that every minimal prime has the form $\widetilde{\mathfrak{p}}$. To see this, note that $\mathfrak{q}$ cannot contain v, for v is not a zerodivisor in S. Hence, $\mathfrak{q}$ corresponds via expansion to a minimal prime of S_v containing $\mathfrak{p}$. But $S_v \cong R[t, v]$, and $\mathfrak{p}R[t, 1/t]$ is already a minimal prime of $R[t, 1/t]$. It follows that $\mathfrak{q} = \mathfrak{p}R[t, 1/t] \cap S$, and this is the minimal prime $\widetilde{\mathfrak{p}}$. Note that $R[It, 1/t]/\widetilde{\mathfrak{p}}$ embeds in $(R/\mathfrak{p})[t, 1/t]$, and that the image is the extended Rees ring of $I(R/\mathfrak{p})$. Therefore, it suffices to show that the dimension of each of these Rees rings over a domain D obtained by killing a minimal prime of R has dimension at most $\dim(D) + 1 \leq \dim(R) + 1$, and we may therefore assume without loss of generality that R is a local domain.

But S is then a domain finitely generated over R. If the fraction field of R is $\mathcal{F}$, then the fraction field of S is $\mathcal{F}(t)$. If Q is any prime ideal of S, Q lies over, say, P in R, and the residue class fields of R_P and S_Q are κ_P and κ_Q respectively, then the dimension formula yields

$$\mathrm{height}\, Q \leq \mathrm{height}\, P + \mathrm{tr.\,deg.}(\mathcal{F}(t)/\mathcal{F}) - \mathrm{tr.\,deg.}(\kappa_Q/\kappa_P) \leq \mathrm{height}\, P + 1 \leq \dim(R) + 1,$$

as required.

But killing a nonzerodivisor in a local domain drops the dimension by one. If μ denotes the maximal ideal of the $\mathrm{gr}_I R$ that is the sum of R/I and the graded components of positive degree, we leave it as an exercise to see that the Krull dimension of $\mathrm{gr}_I R$ is the same as the Krull dimension of $(\mathrm{gr}_I R)_\mu$. Since $(\mathrm{gr}_I R)_\mu$ is obtained by killing the nonzerodivisor v in $S_{\mathcal{M}}$, we have that $\dim\big(\mathrm{gr}_I(R)\big) = \dim(S_{\mathcal{M}}) - 1 = \dim(R)$. □

Corollary. *Let $x_1, \ldots, x_n$ be a system of parameters in a local ring (R, m, K). Let F be a homogenous polynomial of degree d in $R[X_1, \ldots, X_n]$ such that $F(x_1, \ldots, x_n) = 0$. That is, F gives a relation over R on the monomials of degree d in $x_1, \ldots, x_n$. Then all coefficients of F are in m.*

Proof. Consider the associated graded ring $\mathrm{gr}_I(R)$, where $I = (x_1, \ldots, x_n)R$. This ring is generated by the images $\overline{x}_1, \ldots, \overline{x}_n$ of $x_1, \ldots, x_n$ in $I/I^2 = [\mathrm{gr}_I(R)]_1$. Let $A = R/I$, an Artin local ring. By the preceding Theorem, $\dim\big(\mathrm{gr}_I(R)\big) = n$. But $\mathrm{gr}_I(R) = A[\overline{x}_1, \ldots, \overline{x}_n]$. Killing the maximal ideal m/I of A does not affect the dimension of this ring. It follows that the quotient has dimension n, so that $K[\overline{x}_1, \ldots, \overline{x}_n]$ is a polynomial ring in $\overline{x}_1, \ldots, \overline{x}_n$. If $F(x_1, \ldots, x_n) = 0$ and has a coefficient outside m, we find the $\overline{F}(\overline{z}_1, \ldots, \overline{z}_n) = 0$ in $K[\overline{x}_1, \ldots, \overline{x}_n]$, where $\overline{F}$ is the image of F mod m and so is a nonzero polynomial in the $K[\overline{x}_1, \ldots, \overline{x}_n]$. This forces the dimension of $K \otimes_R \mathrm{gr}_I(R)$ to be smaller than n, a contradiction. □

We next want to prove two consequences of the Briançon-Skoda Theorem that were stated without proof in as Corollaries at the bottom of p. 1 and the top of p. 2 of the Lecture Notes of January . 9 The next result generalizes the first Corollary.

Theorem (corollary of the Briançon-Skoda Theorem). *Let R be a regular Noetherian ring of Krull dimension n and let $f_1, \ldots, f_{n+1}$ be elements of R. Then*

$$f_1^n \cdots f_{n+1}^n \in (f_1^{n+1}, \ldots, f_{n+1}^{n+1})R.$$

Proof. Call the product on the left g and the ideal on the right I. If $g \notin I$, then $(I + Rg)/I$ is not zero, and we can localize at a prime in its support. Therefore, we may without loss of generality that assume that (R, m, K) is a regular local ring of dimension at most n. Second, if $g \notin I$ this remains true when we replace R by $R(t)$, since $R(t)$ is faithfully flat over R. We also have that $R(t)$ and R have the same dimension. Thus, we may assume that R has an infinite residue class field. Let $h = f_1 \cdots f_{n+1}$, so that $g = h^n$. Since $h^{n+1} \in I^{n+1}$, $h \in \overline{I}$. Since $\mathfrak{an}(I) \leq \dim(R) \leq n$ and the residue class field is infinite, I is integral over an ideal I_0 with at most n generators. Then $h \in \overline{I_0}$, and it follows from the Briançon-Skoda theorem that $h^n \in I_0 \subseteq I$, as required. $\square$

Discussion: consequences of the condition that $\mathrm{gr}_I R$ be a domain. Let I be a proper ideal of R. We assume that $\bigcap_n I^n = (0)$. This is automatic if R is a Noetherian domain. Suppose that $\mathrm{gr}_I R$ is a domain. Then it follows that R must be a domain, for if $fg = 0$ with $f, g \neq 0$ we have $f \in I^r - I^{r+1}$ for some r (we call r the I-adic order of f) and $g \in I^s - I^{s+1}$ for some s. Then the product of the nonzero elements $[f] \in [\mathrm{gr}_I R]_r = I^r/I^{r+1}$ and $[g] \in [\mathrm{gr}_I R]_s$ in I^s/I^{s+1} is nonzero in the domain $\mathrm{gr}_I R$, and this shows that $fg \in I^{r+s} - I^{r+s+1}$ has I-adic order $r+s$ and is not 0. This proves that R is a domain, and also shows that I-adic order is a valuation on R taking values in $\mathbb{Z}$. R is contained in the corresponding Noetherian discrete valuation ring (V, tV) of its fraction field, where the generator t of the maximal ideal of V can be taken to be the image of any element in $I - I^2$. Moreover, since I^n is the inverse image of the integrally closed ideal $t^n V$ (this is a principal ideal in a normal domain), all of the ideals I^n are integrally closed.

Note that when (R, m, K) of Krull dimension d is regular, if $f_1, \ldots, f_d$ is any minimal set of generators of the maximal ideal (called a *regular system of parameters*), then $\mathrm{gr}_m R$ is a homomorphic image of $K[x_1, \ldots, x_d]$, where the x_i are the images of the f_i in m/m^2. Since $gr_m R$ has the same Krull dimension d as R, $R[x_1, \ldots, x_d] \twoheadrightarrow \mathrm{gr}_m R$ cannot have a nonzero kernel, which shows that R is regular if and only $\mathrm{gr}_m R$ is isomorphic with a polynomial ring in d variables over the residue class field. Since this ring is a domain, R is a domain, and we have an m-adic valuation on R, which gives a map $(R, m) \hookrightarrow (V, tV)$ that carries m into tV, the maximal ideal of V. Hence:

Corollary. *If (R, m) is a local Noetherian domain, there exists a valuation ring (V, tV) of* $\mathrm{frac}\,(R)$ *such that R is a subring of V and $m \subseteq tV$.*

Proof. It suffices to find an injection $R \subseteq (V, tV)$ such that $m \subseteq tV$ for any Noetherian valuation domain V, since we may intersect V with $\mathrm{frac}\,(R)$.

Because $R \hookrightarrow \widehat{R}$ is flat, nonzero elements of R are nonzerodivisors in $\widehat{R}$, and $R - \{0\}$ is disjoint from any minimal prime P of $\widehat{R}$. Hence, $R \hookrightarrow \widehat{R}/P$, and so we may assume without loss of generality that R is a complete local domain. By the structure theory of complete local rings, R is then module-finite over a complete regular local ring (A, m_A). The m_A-adic valuation on A gives an injection $A \hookrightarrow W$ were W is a Noetherian discrete valuation domain, and we may replace W by its completion and so assume it is complete. We may think of W as a subring of the algebraic closure of its fraction field $\mathcal{F}$, and we may think of the generators of R as elements of $\mathcal{F}$. Then the ring $W_1 = W[R] \subseteq \mathcal{F}$ is generated over W by finitely many integral elements, and so is a domain module-finite over W. By the lemma below, W_1 is local, and its integral closure W_2, which is a module-finite extension domain of W_1 by Nagata's theorem, is local. But a normal local domain of dimension one is a Noetherian discrete valuation domain. $\square$

Lemma. *Let (R, m, K) be a complete local ring and let S be a module-finite extension of R. Then S is a finite product of local rings. Hence, if S is a domain, then S is local.*

Proof. S/mR is a module finite extension of K and so it is an Artin ring. The maximal ideals of S correspond bijectively to the maximal ideals of S/mS (they must lies over m) and so there are finitely many, $Q_1, \dots, Q_s$. Then $Q_1 \cap \cdots \cap Q_s$ is the radical of mS, and has a power contained in mS. Since S is module-finite over R, it is complete with respect to mS. Thus, S is the inverse limit of the rings S/m^tS, and so it is also the inverse limit of the rings $S/(Q_1 \cap \cdots \cap Q_s)^t$. But the ideals $Q_1, \dots, Q_s$ are pairwise comaximal, since they are maximal, and so are their t th powers. It follows that

$$(Q_1 \cap \cdot \cap Q_s)^t = (Q_1 \cdots Q_s)^t = Q_1^t \cdots Q_s^t = Q_1^t \cap \cdots \cap Q_s^t.$$

By the Chinese remainder theorem,

$$S/(Q_1 \cap \cdots \cap Q_s)^t \cong S/(Q_1^t \cap \cdots \cap Q_s^t) \cong (S/Q_1^t) \times \cdots \times (S/Q_s^t),$$

by the Chinese remainder theorem. But S/Q_j^t is already local and so is it is naturally isomorphic with $S_{Q_j}/Q_j^tS_{Q_j}$. Since inverse limit commutes with finite products, S is isomorphic with the product of the completions of the local rings S_{Q_j}. □

A homomorphism $h : (B, P) \to (C, Q)$ of quasilocal rings is called *local* if $h(P) \subseteq Q$.

Theorem. *Let (R, m, K) be a local ring and $I \subseteq m$ an ideal. Then $x \in \overline{I}$ if and only if for every local map of R to a Noetherian valuation domain V, $x \in IV$. Moreover, we need only consider local maps $R \to V$ such that the kernel is a minimal prime P of R and V is a valuation of* $\mathrm{frac}\,(R/P)$.

In consequence, $\overline{I}$ is the intersection of the m-primary integrally closed ideals that contain I.

Proof. Since integral closure may be tested modulo every minimal prime, we reduce at once to the case where R is a domain, and since we may intersect a Noetherian valuation domain with te fraction field of R, it suffices to show that if $x \notin \overline{I}$ there exists a local inclusion map $R \subseteq V$,where V is a Noetherian valuation domain, such that $x \not inIV$. Consider the ring $T = R[I/x] = R[f/x : f \in I] \subseteq \mathrm{frac}\,(R)$, which is a finitely generated R-algebra, and so Noetherian, since if $I = (f_1, \dots, f_s)R$ this is the same as $R[f_i/x : 1 \leq i \leq s]$. Then $(m,\, I/x)R[I/x] = m + I/x + I^2/x^2 + \cdots + I^k/x^k + \cdots$, where any single element is a finite sum. I We shall show that this is a proper ideal of $R[I/x]$. Otherwise, we have $1 = u + i_1/x + i_2/x^2 + \cdots + i_k/x^k$ with $i_j \in I^j$, $1 \leq j \leq k$. If we have this equation, multiply by x^k to get $(1-u)x^k - i_1x^{k-1} - \cdots - i_k = 0$. Since $u \in m$, $1-u$ is a unit and we may multiply by its inverse to get an equation of integral dependence for x on I, a contradiction. Since $(m, I/x)R[I/x]$ is a proper ideal of T, we can localize T at prime Q that contains it, and then choose a Noetherian valuation domain V such that $T_Q \subseteq V$ is a local map. If $x \in IV$, then since $IV = fV$ for some generator f of I, we $x \in fV$, i.e., $x/f \in V$. This is a contradiction, since $f/x \in Q$ is in the maximal ideal of V.

For the second statement, note that if $x \notin IV$, then x is not in the contraction of IV to R, which contains I, is integrally closed, since IV is, and is m-primary (contractions of ideals primary to a given prime are primary to the contraction of the prime). □

We next observe:

Theorem. *Let R denote $\mathbb{C}\{\{z_1, \dots, z_n\}\}$ or $\mathbb{C}[[z_1, \dots, z_n]]$, the convergent or formal powers series ring in n variables. Let f be in the maximal ideal of R, and let I be the ideal generated by the partial derviatives $\partial f/\partial z_i$ of f. Then f is integrally dependent on I.*

Proof. If not, we can chnoose a local inclusion of R to a discrete valuation ring V in such a way that the image f is not in IV. Note that V cannot be just a field here, for then f maps to 0. Replace V by its completion: we may assume that V is complete. Since we are in the equal characteristic 0 case, the image of $\mathbb{C}$ in V can be extended to a coefficient field. Thus, we may assume that $V = L[[x]]$, where $\mathbb{C} \subseteq L$ and m maps into (x).

Let $h : R \to L[[x]]$ be the map, and $h(z_i) = g_i(x)$, $1 \leq i \leq n$. Then f maps to $f\bigl(g_1(x), \dots, g_n(x)\bigr)$. The key point is that the chain rule holds here, by a formal calculation. Thus,

$$\frac{d}{dx}\bigl(h(f)\bigr) = \sum_{i=1}^{n} h(\partial f/\partial z_i)\frac{dg_i(x)}{dx}.$$

It follows that the derivative of $h(f)$ is in IV. But over a field of characteristic 0, the derivative of a nonzero non-unit v has order exactly one less than that of v. Hence, $f \in IV$ as well. □

Theorem (corollary of the Briançon-Skoda theorem). *With hypotheses as in the preceding Theorem, f^n is in the ideal generated by its partial derivatives.*

Proof. This is immediate from the preceding Theorem and the Briançon-Skoda Theorem. □

Lecture of January 30, 2019

Following Lipman and Sathaye [J. Lipman and A. Sathaye, *Jacobian ideals and a theorem of Briançon-Skoda*, Michigan Math. J. **28** (1981), 199–222] we present the Briançon-Skoda Theorem in a generalized form:

Briançon-Skoda Theorem (Lipman-Sathaye version). *Let R be a Noetherian normal domain, and let I_0 be an ideal of R such that $\mathrm{gr}_{I_0}(R)$ is regular. Let $n \geq 1$ and let I be an ideal of R generated over I_0 by n elements, say $f_1, \dots, f_n$. Let $k \geq 1$ be any positive integer. Then $\overline{I^{n+k-1}} \subseteq I^k$.*

The version stated in the Lecture of January 9 is the case where $I_0 = 0$ and $k = 1$. Notice that the result is non-trivial even when $n = 1$, where it states that all the powers of I are integrally closed.

We shall first explain how this result follows from the Lipman-Sathaye Jacobian Theorem (although this will take a while), and then focus on the proof of the latter. We need an intermediate result:

Theorem (Lipman-Sathaye). *Let B be a Noetherian normal integral domain, and let $v \in B - \{0\}$ be such that B/vB is regular. Let t denote the inverse of v in the fraction field of B. Let $f_1, \dots, f_n \in B$ and let $S = B[f_1t, \dots, f_nt]$. Let S' be the integral closure of S in its field of fractions. Then $v^{n-1}S' \subseteq S$.*

We want to see that the second theorem implies the first. We need some preliminary facts.

Lemma. *Let be any ring, and I an ideal of R.*

(a) *The integral closure of the extended Rees ring $R[It, v]$ in $R[t, v]$ in degree k is $\overline{I^k}t^k$ (if $k \leq 0$, let $I^k = R$). That is, the integral closure in $R[t, v]$ is*

$$\cdots + Rv^k + \cdots + Rv^2 + Rv + R + \overline{I}t + \overline{I^2}t^2 + \cdots + \overline{I^m}t^m + \cdots.$$

If R is a normal domain, this is also the integral closure of R in its fraction field.

(b) *Suppose that R is a Noetherian domain and that $\mathrm{gr}_I R$ is an integral domain (or that its localization at every prime ideal of R is an integral domain). Then every power of I is integrally closed.*

Proof. (a) The integral closure in $R[IT, v]$ is $\mathbb{Z}$-graded. The result for nonnegative degrees is clear. In positive degree k, if rt^k is integral over $R[It, v]$ it satisfies a monic polynomial of degree d for some d, and the sum of the coefficients of t^{dk} must be 0. Just as in the case of $R[It]$, this yields an equation establishing the integral dependence of r on I^k. The final statement follows because when R is normal, so is $R[t, v]$, and so $R[t, v]$ must contain the normalization of $R[It, v]$.

(b) If $\overline{I^n}/I^n \neq 0$, we may preserve this while localizing. Since integral closure commutes with localization, we may assume that R is local. If I expands to the unit ideal, there is nothing to prove. Otherwise, $\mathrm{gr}_I(R)$ is $\mathbb{N}$-graded over the local ring R/I. When $\mathrm{gr}_I(R)$ is a domain, we can define a valuation on R whose value on a nonzero element r is the unique nonnegative integer h such that $r \in I^h - I^{h+1}$. I^n is then the contraction of the nth power of the maximal ideal of a discrete valuation ring. □

Proof that the second theorem implies the Briançon-Skoda theorem. Let $B = R[I_0t, v]$. Then $B/vB \cong \mathrm{gr}_{I_0}(R)$ is regular, and B is normal by the Lemma above. Then $S = B[f_1t, \dots, f_nt] = R[It, v]$ is the extended Rees ring of I over R. It follows that in degree $n+k-1$, S' is $\overline{I^{n+k-1}t^{n+k+1}}$. The fact that $v^{n-1}S' \subseteq S$ implies that $v^{n-1}[S']_{n+k-1} \subseteq [S]_k = I^kt^k$, and so $\overline{I^{n+k-1}} \subseteq I^k$. □

Until further notice, R denotes a Noetherian domain with fraction field $\mathcal{K}$, and S denotes an algebra essentially of finite type over R (i.e., a localization at some multiplicative system of a finitely generated R-algebra) such that S is torsion-free and *generically étale* over R, by which we mean that $\mathcal{L} = \mathcal{K} \otimes_R S$ is a finite product of finite separable algebraic field extensions of $\mathcal{K}$. Note that $\mathcal{L}$ may also be described as the total quotient ring of S.

We shall denote by S' the integral closure of S in $\mathcal{L}$. We shall prove that S' is module-finite over S if R is regular (and more generally).

If A and B are subsets of $\mathcal{L}$ we denote by $A :_{\mathcal{L}} B$ the set $\{u \in \mathcal{L} : uB \subseteq A\}$. If C is a subring of $\mathcal{L}$ and A is a C-module, then $A :_{\mathcal{L}} B$ is also a C-module.

We shall write $\mathcal{J}_{S/R}$ for the Jacobian ideal of S over R. If S is a finitely generated R-algebra, so that we may think of S as $R[X_1, \ldots, X_s]/(f_1, \ldots, f_h)$, then $\mathcal{J}_{S/R}$ is the ideal of S generated by the images of the size s minors of the Jacobian matrix $(\partial f_j/\partial x_i)$ under the surjection $R[X] \to S$. This turns out to be independent of the presentation, as we shall show below. Moreover, if $u \in S$, then $\mathcal{J}_{S_u/R} = \mathcal{J}_{S/R}S_u$. From this one sees that when S is essentially of finite type over R and one defines $\mathcal{J}_{S/R}$ by choosing a finitely generated subalgebra S_0 of S such that $S = W^{-1}S_0$ for some multiplicative system W of S_0, if one takes $\mathcal{J}_{S/R}$ to be $\mathcal{J}_{S_0/R}S$, then $\mathcal{J}_{S/R}$ is independent of the choices made. We shall consider the definition in greater detail later. The result we aim to prove is:

Theorem (Lipman-Sathaye Jacobian theorem). *Let R be regular domain*[1] *with fraction field $\mathcal{K}$ and let S be an extension algebra essentially of finite type over R such that S is torsion-free and generically étale over R. Let $\mathcal{L} = \mathcal{K} \otimes_R S$ and let S' be the integral closure of S in $\mathcal{L}$. Then $S' :_{\mathcal{L}} \mathcal{J}_{S'/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$.*

Note that, since $\mathcal{J}_{S'/R}$ is an ideal of S', we have that $S' \subseteq S' :_{\mathcal{L}} \mathcal{J}_{S'/r}$. The statement that $S' \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$ implies that $\mathcal{J}_{S/R}S' \subseteq S$, i.e., that $\mathcal{J}_{S/R}$ "captures" the integral closure S' of S (all we mean by this is that it multiplies S' into S).

We next want to explain why the Jacobian ideal is well-defined. We assume first that S is finitely presented over R. To establish independence of presentation we first show that this ideal is independent of the choice of generators for the ideal I. Obviously, it can only increase as we use more generators. If we have two different sets of generators, we can compare the Jacobian ideal obtained from each with the one obtained from their union. It suffices to show that the Jacobian ideal does not change when we enlarge the set of generators. By enlarging the set of generators still further we may assume that the new generators are obtained from the original ones by operations of two kinds: enlarging the set of generators with one which is a multiple of one of the original generators by an element of the ring, or by one which is the sum of two of the original generators. Let us denote by ∇f the column vector consisting of the partial derivatives of f with respect to the variables. Since $\nabla(gf) = g\nabla f + f\nabla g$ and the image of a generator f in S is 0, it follows that the image of $\nabla(gf)$ in S is the same as the image of $g\nabla f$ when $f \in I$. Therefore, the minors formed using $\nabla(gf)$ as a column are multiples of corresponding minors using ∇f instead, once we take images in S. Since $\nabla(f_1 + f_2) = \nabla f_1 + \nabla f_2$, minors formed using $\nabla(f_1 + f_2)$ as a column are sums of minors from the original matrix. Thus, independence from the choice of generators of I follows.

[1] We can weaken the regularity hypotheses on R quite a bit: instead, we may assume that R is a Cohen-Macaulay Noetherian normal domain, that the completion of every local ring of R is reduced, and that for every height one prime Q of S', if $P = Q \cap R$, then R_P is regular.

Now consider two different sets of generators for S over R. We may compare the Jacobian ideals obtained from each with that obtained from their union. This, it suffices to check that the Jacobian ideal does not change when we enlarge the set of generators $f_1, \ldots, f_s$ of the algebra. By induction, it suffices to consider what happens when we increase the number of generators by one. If the new generator is $f = f_{s+1}$ then we may choose a polynomial $h \in R[X_1, \ldots, X_s]$ such that $f = h(f_1, \ldots, f_s)$, and if $g_1, \ldots, g_h$ are generators of the original ideal then $g_1, \ldots, g_h$, $X_{s+1} - h(X_1, \ldots, X_s)$ give generators of the new ideal. Both dimensions of the Jacobian matrix increase by one: the original matrix is in the upper left corner, and the new bottom row is $(0\ 0\ \ldots\ 0\ 1)$. The result is then immediate from

Lemma. *Consider an $h+1$ by $s+1$ matrix M over a ring S such that the last row is $(0\ 0\ \ldots\ 0\ u)$, where u is a unit of S. Let M_0 be the h by s matrix in the upper left corner of M, obtained by omitting the last row and the last column. Then $I_s(M_0) = I_{s+1}(M)$.*

Proof. If we expand a size $s+1$ minor with respect to its last column, we get an S-linear combination of size s minors of M_0. Therefore, $I_{s+1}(M) \subseteq I_s(M_0)$. To prove the other inclusion, consider any s by s submatrix Δ_0 of M_0. We get an $s+1$ by $s+1$ submatrix Δ of M by using as well the last row of M and the appropriate entries from the last column of M. If we calculate $\det(\Delta)$ by expanding with respect to the last row, we get, up to sign, $u\det(\Delta_0)$. This shows that $I_s(M_0) \subseteq I_{s+1}(M)$. □

This completes the argument that the Jacobian ideal $\mathcal{J}_{S/R}$ is independent of the presentation of S over R.

We next want to observe what happens to the Jacobian ideal when we localize S at one (or, equivalently, at finitely many) elements. Consider what happens when we localize at $u \in S$, where u is the image of $h(X_1, \ldots, X_s) \in R[X_1, \ldots, X_s]$, where we have chosen an R-algebra surjection $R[X_1, \ldots, X_s] \twoheadrightarrow S$. We may use $1/u$ as an additional generator, and introduce a new variable X_{s+1} that maps to $1/u$. We only need one additional equation, $X_{s+1}h(X_1, \ldots, X_s) - 1$, as a generator. The original Jacobian matrix is in the upper left corner of the new Jacobian matrix, and the new bottom row consists of all zeroes except for the last entry, which is $h(X_1, \ldots, X_s)$. Since the image of this entry is u and so invertible in $S[u^{-1}]$, the Lemma above shows that the new Jacobian ideal is generated by the original Jacobian ideal. We have proved:

Proposition. *If S is a finitely presented R-algebra and T is a localization of S at one (or finitely many) elements, $\mathcal{J}_{T/R} = \mathcal{J}_{S/R}T$.* □

Lecture of February 1, 2019

We next want to extend the definition of the Jacobian ideal to the case where S is a localization of a finitely generated R-algebra, even though S itself may not be finitely generated over R.

Suppose that $S = W^{-1}S_1$ where S_1 is finitely generated over the Noetherian ring R. As mentioned earlier, we want to define $\mathcal{J}_{S/R}$ to be $\mathcal{J}_{S_1/R}S = W^{-1}\mathcal{J}_{S_1/R}$. We only need to check that the result is independent of the choice of S_1 and W. First note that we may replace S_1 by its image in S (and W by its image as well). To see this, let $\mathfrak{A}$ be the kernel of the map $S_1 \to S$. Then $\mathfrak{A}$ is killed by some element of $w \in W$, and, by the Proposition at the end of the Lecture Notes for January 29, we may replace S_1 by its localization at w. But $(S_1)_w$ injects into S. Let $T \cong S_1/\mathfrak{A}$ be the image of S_1 in S. Then $T_w \cong (S_1)_w$, and so $\mathcal{J}_{S_1/R}$ and $\mathcal{J}_{T/R}$ both expand to $\mathcal{J}_{T_w/R}$. It follows that $\mathcal{J}_{S_1/R}$ and $\mathcal{J}_{T/R}$ will have the same expansion to S. Now suppose that S is the localization of finitely generated R-subalgebras $S_i \subseteq S$ at the multiplicative systems W_i, $i = 1, 2$. We want to show that $J_{S_i/R}S$ is independent of i.

First note that each element in a finite set of generators for S_2 over R is multiplied into S_1 by an element of W_1. By multiplying these elements of W_1 together, we can find $w_1 \in W_1$ such that $S_2 \subseteq (S_1)_{w_1}$. Since S_1 and $(S_1)_{w_1}$ produce the same result when their Jacobian ideals are expanded to S, we may replace S_1 by $(S_1)_{w_1}$, and so assume that $S_2 \subseteq S_1$. But we can similarly find $w_2 \in W_2$ such that $S_1 \subseteq (S_2)_{w_2}$. Then $(S_1)_{w_2} = (S_2)_{w_2} = S_0$, say. It is then clear that $\mathcal{J}_{S_i/R}S = \mathcal{J}_{S_0}S$ for $i = 1, 2$. This shows that $\mathcal{J}_{S/R}$ is well-defined independent of choices.

There is another approach to defining $\mathcal{J}_{S/R}$ for localizations of finitely generated R-algebras. First note that given a derivation D of a ring T, i.e., a map $D : T \to T$ that is a homomorphism of additive groups and satisfying $D(f_1f_2) = f_1D(f_2) + D(f_1)f_2$ for all f_1, $f_2 \in T$, it induces a unique derivation $\widetilde{D} : W^{-1}T \to W^{-1}T$ such that diagram

$$\begin{tikzcd} W_T \arrow[r, "\widetilde{D}"] & W_T \\ T \arrow[u] \arrow[r, "D"] & T \arrow[u] \end{tikzcd}$$

commutes. One gets $\widetilde{D}$ by letting

$$\widetilde{D}(f/w) = \frac{wDf - fDw}{w^2}.$$

(One needs to check that this is well-defined.) In consequence the partial differentiation operators $\dfrac{\partial}{\partial X_j}$ extend uniquely from the polynomial ring $R[X_1, \ldots, X_s]$ to any localization $W^{-1}R[X_1, \ldots, X_s]$. Given a finitely generated R-algebra S_0 and a multiplicative system $W_0 \subseteq S_0$, we can choose a surjection $T = R[X_1, \ldots, X_s] \twoheadrightarrow S_0$, and let W be the inverse image of W_0 in T, which is a multiplicative system in T. Then we have a surjection $W^{-1}T \twoheadrightarrow W_0^{-1}S_0 = S$, and so we can write $S \cong W^{-1}R[X_1, \ldots, X_s]/(f_1, \ldots, f_h)$. We can then define $\mathcal{J}_{S/R}$ as the expansion of $I_s\big((\partial f_j/\partial X_i)\big)$ to S. We leave it to the reader to show that this produces the same ideal as our earlier definition of $\mathcal{J}_{S/R}$

Remark. Suppose that we are calculating the Jacobian ideal of $S = R[X_1, \ldots, X_s]/I$ over R. If we modify the elements $f_1, \ldots, f_s \in I$ by adding elements $g_1, \ldots, g_s \in I^2$, the image of the Jacobian minor det $(\partial f_j/\partial x_i)$ does not change. The point is that each of the partial derivatives of an element of I^2 is in I, by the product rule, and so the image of every partial derivative of any g_j in S is 0. We shall make use of this trick later.

Definition: the conductor. Let S be a reduced Noetherian ring and S' its integral closure. The *conductor*, denoted $\mathfrak{C}_{S'/S}$, for $S \subseteq S'$ is $\{s \in S : S's \subseteq S\}$.

It is easily checked that $\mathfrak{C}_{S'/S}$, which by definition is contained in S, is actually an ideal of S'. Thus, it is an ideal of both S and S'. It may also be characterized as the largest ideal of S which is an ideal of S'.

Examples. Let x be an indeterminate over the field K, and let $S = K[x^2,\, x^3] \subseteq K[x]$. Then $S' = K[x]$, and the conductor is the maximal ideal $(x^2,\, x^3)S$, which contains all powers of x. However if we let $T = K[x^3, x^5] \subseteq K[x]$, then T may also be described as $K[x^3, x^5, x^6, x^8, x^9, x^{10}, \ldots]$. It is still the case that $T' = K[x]$, but now the conductor is $(x^8, x^9, x^{10})T$.

We next state an easy Corollary of the Jacobian theorem (but keep in mind that we have not yet proved the Jacobian theorem).

Corollary. . *Let R be a regular local ring and let $f_1, \ldots, f_n, v_1, \ldots, v_n \in R$, with the $v_i \neq 0$. Let $S = R[f_1/v_1, \ldots, f_n/v_n]$. Then $v_1 \cdots v_n \in \mathcal{J}_{S/R}$ and, hence, $v_1 \cdots v_n S' \subseteq S$. In other words, $v_1 \cdots v_n \in \mathfrak{C}_{S/R}$.*

Proof. $S = R[X_1, \ldots, X_n]/I$ for an a suitable ideal I, where X_j maps to f_j/v_j. Hence, we can include the elements $v_jX_j - f_j$ as the first n generators of I, and it follows that the first n rows of the Jacobian matrix form a diagonal matrix with $v_1, \ldots, v_n$ on the diagonal. Hence, $v_1 \cdots v_n$ is one of the minors. □

We want to restate the Jacobian theorem with a slight refinement that makes use of the basic facts about the conductor. The statement that $S' :_{\mathcal{L}} \mathcal{J}_{S'/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$ is equivalent to the statement $\mathcal{J}_{S/R}(S' :_{\mathcal{L}} \mathcal{J}_{S'/R}) \subseteq S$. Since $S' :_{\mathcal{L}} \mathcal{J}_{S'/R}$ is an S'-module, so is the left hand side. Therefore, the left hand side is an ideal of S' that is contained in S, and so it is contained in $\mathfrak{C}_{S'/S}$. Therefore, we can reformulate the Jacobian theorem as follows:

Theorem (Lipman-Sathaye Jacobian theorem). *Let R be regular domain*[2] *with fraction field $\mathcal{K}$ and let S be an extension algebra essentially of finite type over R such that S is torsion-free and generically étale over R. Let $\mathcal{L} = \mathcal{K} \otimes_R S$ and let S' be the integral closure of S in $\mathcal{L}$. Then $\mathcal{J}_{S/R}(S' :_{\mathcal{L}} \mathcal{J}_{S'/R}) \subseteq \mathfrak{C}_{S'/S}$.*

We have already proved that the second Theorem of Lipman and Sathaye (stated on the first page of the Lecture Notes of January 30) implies the Lipman-Sathaye version of

[2] Or: let R be a Cohen-Macaulay Noetherian normal domain such that the completion of every local ring of R is reduced, and such that for every height one prime Q of S', if $P = Q \cap R$, then R_P is regular.

the Briançon-Skoda Theorem. The conclusion of this second Theorem can be phrased as follows: $v^{n-1} \in \mathfrak{C}_{S'/S}$. The easy Corollary of the Jacobian theorem stated above gives a *weakened* version of the result we want right away: we can take $v_1 = \cdots = v_n = v$, and we find that $v^n \in \mathfrak{C}_{S'/S}$ under the hypotheses of the second Theorem. This gives a likewise weakened version of the Briançon-Skoda theorem, in which the conclusion is that $\overline{I^{n+k}} \subseteq I^k$ for $k \geq 1$. We will need to do quite a bit of work to decrease the exponent on the left by one.

The Lemma we need to do this, whose proof will occupy us for a while, is the following:

Key Lemma. *Let S be essentially of finite type, torsion-free and genercially étale over R, a regular domain. Let $v \in R$ be such that R/vR is regular. Suppose $f \in R - vR$, and $f/v \in S$. Then $\mathcal{J}_{S'/R} \subseteq vS'$.*

The conclusion implies that $1/v \in S' :_{\mathcal{L}} \mathcal{J}_{S'/R}$. Coupled with the Jacobian Theorem, which tell us that $\mathcal{J}_{S/R}(S' :_{\mathcal{L}} \mathcal{J}_{S'/R}) \subseteq \mathfrak{I}$, we have that $\mathcal{J}_{S/R} \cdot (1/v) \subseteq \mathfrak{I}$, and since we already know that $v^n \in \mathcal{J}_{S/R}$, we can conclude that $v^n/v \in \mathfrak{I}$. Thus, $v^{n-1}S' \subseteq S$, as required.

Remark. For the moment we have been assuming that S' is module-finite over S: we shall prove this later.

There are two proofs that are still hanging besides the fact that S' is module-finite over S: one is for the Key Lemma stated just above, and the other is for the Jacobian theorem itself. We shall address the Key Lemma first. We need several preliminaries.

Recall that the *embedding dimension* of a local ring $(T,\, \mathfrak{m},\, L)$ is the least number of generators of $\mathfrak{m}$, and, by Nakayama's Lemma, is the same the L-vector space dimension of $\mathfrak{m}/\mathfrak{m}^2$. Also recall that a local ring is *regular* if its embedding dimension and Krull dimension are equal. By a theorem, a regular local ring is an integral domain. A minimal set of generators of $\mathfrak{m}$ is always a system of parameters and is called a *regular system of parameters.* If we kill one element in a regular system of parameters, the Krull dimension and embedding dimension both drop by one, and the ring is still regular. It follows that a regular system of parameters for a regular local ring T is a regular sequence, and that the quotient of T by the ideal generated by part of a regular system of parameters is again a regular local ring. The converse is true:

Lemma. *Let $(T, \mathfrak{m})$ be a regular local ring and $\mathfrak{A} \subseteq \mathfrak{m}$ an ideal. Then $S = T/\mathfrak{A}$ is regular if and only if $\mathfrak{A}$ is generated by part of a regular system of parameters (equivalently, part of a minimal set of generators for $\mathfrak{m}$). In particular, if T and S are both regular than $\mathfrak{A}$ must be generated by* $\dim(T) - \dim(S)$ *elements.*

Proof. It remains only to show that if $T/\mathfrak{A}$ is regular, then $\mathfrak{A}$ is generated by part of a regular system of parameters. If $\mathfrak{A} = 0$ we may use the empty subset of a regular system of parameters as the set of generators. Assume $\mathfrak{A} \neq 0$. We use induction on $d = \dim(T)$. If $\mathfrak{A} \subseteq m^2$, then killing $\mathfrak{A}$ decreases the Krull dimension, but the embedding dimension stays the same. But then the quotient cannot be regular. Therefore, we may choose an element of x_1 of $\mathfrak{A}$ that is not in m^2. The element x_1 is part of a regular system of parameters. If $d = 1$ then x_1 generates $\mathfrak{m}$, which must be $\mathfrak{A}$, and we are done. If not, we have that T/x_1T is regular and we may apply the induction hypothesis to conclude $\mathfrak{A}/x_1T$ is generated by part of regular system of parameters $\overline{x}_2, \dots, \overline{x}_k$ for T/x_1T. Let x_j in T map to $\overline{x}_j$, $2 \leq j \leq d-1$. Then $(x_1, \dots, x_k) = T$ and $x_1, \dots, x_k$ is part of a regular system of parameters for T. $\square$

Notation. Given m polynomials $F_1, \dots, F_m \in R[X_1, \dots, X_m]$, we write $\dfrac{\partial(F_1, \dots, F_m)}{\partial(X_1, \dots, X_m)}$ for $\det\bigl(\partial F_j/\partial X_i\bigr)$.

Also note that if T is a ring and W is a multiplicative system such that $W^{-1}T$ is quasilocal, then $W^{-1}T \cong T_{\mathcal{Q}}$, where $\mathcal{Q}$ is the contraction of the maximal ideal of $W^{-1}T$ to T. On the one hand, we have a map $T \to W^{-1}T$ such that the image of $T - \mathcal{Q}$ is invertible, and this induces a map $\mathcal{T}_{\mathcal{Q}} \to W^{-1}T$ that lifts the identity map $T \to T$. On the other hand, the map $T \to T_{\mathcal{Q}}$ must carry W outside $\mathcal{Q}T_{\mathcal{Q}}$, and so we get an induced map $W^{-1}T \to T_{\mathcal{Q}}$ that lifts the identity on T. It is then easy to check that these are mutual inverses.

Lemma. *Let $(R, m, K) \subseteq (S, \mathfrak{m}, L)$ be a local map of regular local rings such that S is essentially of finite type over R and the extension of fraction fields is algebraic. Then for some integer m, S is a localization of $R[X_1, \dots, X_m]/(F_1, \dots, F_m)$ for suitable polynomials $F_1, \dots, F_m$, and, hence, $\mathcal{J}_{S/R}$ is the principal ideal $\dfrac{\partial(F_1, \dots, F_m)}{\partial(X_1, \dots, X_m)}S$.*

Proof. Choose a surjection $R[X_1, \dots, X_m] \twoheadrightarrow S$, and let $\mathcal{Q}$ be the inverse image of the maximal ideal of S in $R[X_1, \dots, X_m]$. Thus, $S \cong R[X]_{\mathcal{Q}}/\mathfrak{A}$. We need to see that the number of generators of $\mathfrak{A}$ is m: we can assume that they are in $R[X]$ by clearing denominators if necessary, since elements of $R[X] - \mathcal{Q}$ are units. By the preceding Lemma, since both $R[X]_{\mathcal{Q}}$ and its quotient by $\mathfrak{A}$ are regular, $\mathfrak{A}$ is generated by height $\mathcal{Q} - \dim(S)$ elements, and we therefore want to show that height $\mathcal{Q} - \dim(S) = m$. To see this, first note that by the dimension formula,

$$(*) \quad \dim(S) = \dim(R) - \mathrm{tr.\,deg.}(L/K).$$

Since $\mathcal{Q} \supseteq m$, $\mathcal{Q}$ corresponds to a prime P of $K[X_1, \dots, X_m]$, and

$$(**) \quad \text{height}\,\mathcal{Q} = \dim(R) + \text{height}\,P,$$

while L is the fraction field of $K[X_1, \dots, X_m]/P$, and so

$$(***) \quad \mathrm{tr.\,deg.}(L/K) = \dim\bigl(K[X_1, \dots, X_m]/P\bigr) = m - \text{height}\,P.$$

Thus, using $(*)$ and $(**)$, we have:

$$\text{height}\,\mathcal{Q} - \dim(S) = \dim(R) + \text{height}\,P - \bigl(\dim(R) - \mathrm{tr.\,deg.}(L/K)\bigr)$$

and using $(***)$ this is

$$\text{height}\, P + \text{tr. deg.}(L/K) = \text{height}\, P + (m - \text{height}\, P) = m,$$

as required. □

Corollary. *Let $R_0 \subseteq R_1 \subseteq R_2$ be regular domains such that R_i is essentially of finite type over R_0 for $i = 1, 2$ and* frac (R_2) *is algeraic over* frac (R_0)*. Then*

$$\mathcal{J}_{R_2/R_0} = \mathcal{J}_{R_2/R_1}\mathcal{J}_{R_1/R_0}.$$

Lecture of February 4, 2019

We prove the Corollary stated at the end of the Lecture of February 1.

Proof. If the ideals are different, we may localize at a prime of R_2 in the support of the module which is their sum modulo their intersection. Thus, we may assume without loss of generality that R_2 is local. We may replace R_1 by its localization at the contraction of the maximal ideal of R_2, and R_0 by its localization at the contraction of the maximal ideal of R_2 (or of R_1: the contractions are the same). Thus, we may assume that we are in the case where $R_0 \hookrightarrow R_1 \hookrightarrow R_2$ are local and the homomorphisms are local. By the Lemma near the bottom of the page 4 of the Lecture Notes of February 1, we have that

$$R_1 \cong R_0[X_1, \ldots, X_m]_{\mathcal{P}}/(F_1, \ldots, F_m)$$

for some m and prime $\mathcal{P}$ of $R_0[X_1, \ldots, X_m]$. Then $\mathcal{J}_{R_1/R_0}$ is generated by the image of $\dfrac{\partial(F_1, \ldots, F_m)}{\partial(X_1, \ldots, X_m)}$. Likewise,

$$R_2 \cong (R_1[Y_1, \ldots, Y_s])_{\mathcal{Q}}/(G_1, \ldots, G_s).$$

Again, $\mathcal{J}_{R_2/R_1}$ is generated by the image of $\dfrac{\partial(G_1, \ldots, G_s)}{\partial(Y_1, \ldots, Y_s)}$. It follows that we can write R_2 as a localization of

$$R_0[X_1, \ldots, X_m, Y_1, \ldots, Y_s]/(F_1, \ldots, F_m, G_1, \ldots, G_s),$$

where the F_j do not involve the Y_i. This means that the Jacobian matrix has the block form

$$\begin{pmatrix} M_F & N \\ 0 & M_G \end{pmatrix}$$

where M_F is $\bigl(\partial F_j/\partial X_i\bigr)$ and M_G is $\bigl(\partial G_j/\partial Y_i\bigr)$. We have that $\mathcal{J}_{R_2/R_0}$ is generated by the image of the determinant of this matrix. No matter what N is, this determinant is

$$\det(M_F)\det(M_G) = \frac{\partial(F_1, \, \ldots\, , F_m)}{\partial(X_1, \, \ldots\, , X_m)}\,\frac{\partial(G_1, \, \ldots\, , G_s)}{\partial(Y_1, \, \ldots\, , Y_s)}$$

as required. □

There are now three results whose proof are hanging: one is the proof that S' is module-finite over S, the second is the proof of the Key Lemma, which is stated on p. 3 of the Lecture Notes of February 1, and the third is the proof of the Jacobian Theorem itself. We begin with the proof of the Key Lemma. This will involve studying quadratic transforms of a regular local ring along a valuation. We first indicate our approach to the proof of the Key Lemma.

Proof of the Key Lemma: step 1. We are trying to show that $\mathcal{J}_{S'/R} \subseteq vS'$. Assume the contrary. Consider the primary decomposition of vS'. Since we are assuming that S' is module-finite over S (we still need to prove this), S' is a normal Noetherian ring, and the associated primes of vS' have height one. We may choose such a prime Q such that $\mathcal{J}_{S'/R}$ is not contained in the corresponding primary ideal in the primary decomposition of vS'. Since the elements of $S' - Q$ are not zerodivisors on this primary ideal, we also have that $\mathcal{J}_{S'_Q/R}$ is not contained in $S'_Q = V$. Thus, for the purpose of proving the Key Lemma, we may replace S' by V, which is a discrete valuation ring, and we may replace R by its localization at the contraction of Q to R. Note that because $f/v \in S$ with $f \notin vR$, we have that $f = (f/v)v \in vS \subseteq vS' \subseteq Q$ and the contraction of Q to R contains both v and f, and has height at least 2, since vR is prime.

In the remainder of the argument we may therefore assume[3] that $(R,\, m,\, K)$ is regular local, and we may replace S' by a discrete value ring $V = S'_Q$ essentially of finite type over R, where the map $R \subseteq V$ is local.

We now digress to discuss quadratic transforms. We first want to prove:

Lemma. *Let $(R,\, m,\, K)$ be regular local with regular system of parameters $x_1, \, \ldots\, , x_d$. Then $T = R[x_2/x_1, \, \ldots\, , x_d/x_1] = R[m/x_1]$ is regular, and the images of $x_2, \, \ldots\, , x_d$ are algebraically independent over K in $T/x_1T \cong K[\overline{x}_2, \, \ldots\, , \overline{x}_d]$.*

Proof. If we localize T at a prime that does not contain x_1, the resulting ring is a localization of R_{x_1}, and is therefore regular. For primes that contain x_1, it suffices to show that the localization is regular after killing x_1, and this follows from the fact that T/x_1T is regular even without localizing. It therefore suffices to prove that T/x_1T is a polynomial ring.

[3] Note that in the refined version of the Jacobian theorem, it was assumed that R_P is regular if P lies under a height one prime of S', so that we may make this reduction even in that case.

First note that
$$T = \bigcup_k m^k/x_1^k,$$
where $m^k/x_1^k = \{u/x_1^k : u \in m^k\}$, and this is an increasing union since $m^k/x_1^k = x_1 m^k/x_1^{k+1}$. (It is clear that $m^k/x_1^k \subseteq T$, and the product of the jth and kth terms in the union is the $(j+k)$th term.) Hence, if there is a relation among the $\overline{x}_j$, $2 \le j \le n$, we may lift it obtain a nonzero polynomial g whose nonzero coefficients are units of R (we get them by lifting elements of K to R) such that $g(x_2/x_1, \ldots, x_d/x_1) = x_1 t$ where $t \in m^k/x_1^k$. We multiply both sides by x_1^N where $N \ge k$ is also larger than the absolute value of any negative exponent on x_1 occurring on the left. The left hand side becomes a nonzero homogeneous polynomial G of degree N in $x_1, \ldots, x_d$ whose nonzero coefficients are units. The right hand side is in $x_1 \cdot x_1^{N-k} m^k \subseteq x_1^{1+N-k} m^k \subseteq m^{N+1}$. This gives a nonzero relation of degree N on the images of $x_1, \ldots, x_d$ in $\mathrm{gr}_m(R)$, a contradiction, since when R is regular this is a polynomial ring in the images of the x_j. $\square$

Definition. Let (R, m, K) be a regular local ring of Krull dimension $d \ge 2$ and let suppose that $R \subseteq V$ is a local map to discrete valuation ring V. Let $\mathrm{ord}_V = \mathrm{ord}$ denote the corresponding valuation. By the *immediate* or *first quadratic transform* of R *along* V we mean the following: let $x_1, \ldots, x_d$ be a regular system of parameters for R numbered so that $\mathrm{ord}(x_1) \le \mathrm{ord}(x_j)$ for $j \ge 2$, let $T = R[x_2/x_1, \ldots, x_d/x_1]$, and then the first quadratic transform is T_P, where P is the contraction to T of the maximal ideal of V. Then T_P is again regular, and we have a local map $T_P \subseteq V$. We may therefore iterate to obtain a sequence of quadratic transforms of R, called the *quadratic sequence* of R *along* V. The sequence is finite if it eventually contains a ring of dimension 1, i.e., a DVR. (Note that if R is a discrete valuation ring with regular parameter x, the quadratic transform process does not change R.) We are aiming to prove that the sequence is finite whenever the transcdence degree of the residue class field of V essentially of finite type over R and the extension $\mathrm{frac}(V)$ is algebraic over $\mathrm{frac}(R)$, which, by the dimension formula corresponds to the case where the transcendence degree of the residue class field extension is $d-1$. We shall also show that the last ring in the quadratic sequence along V is $V \cap \mathrm{frac}(R)$ in this case.

Lecture of February 6, 2019

Remark. The quadratic transform of (R, m, K) along V is independent of the choice of regular system of parameters. If $x \in m$ has minimum order in V, the quadratic transform is the localization of $R[m/x]$ at the contraction P of the maximal ideal of V. If y also has minimum order, then $y/x \notin P$, and so $x/y \in R[m/x]_P$. Since $(u/x)(x/y) = u/y$ for all $u \in m$, it follows that
$$R[m/y] \subseteq R[m/x]_P.$$
If Q is the contraction of the maximal ideal of V to $R[m/y]$, we have that elements of $R[m/y] - Q$ are not in $PR[m/x]_P$, and therefore have inverses in $R[m/x]_P$. Thus,
$$R[m/y]_Q \subseteq R[m/x]_P.$$

The other inclusion follows exactly similarly. □

Remark. The first quadratic transform (T_1, m_1, K_1) of the regular local ring (R, m, K) has dimension at most $\dim(R)$, and $\dim(T) = \dim(R) - \operatorname{tr.deg.}(K_1/K)$. In fact, since R is regular, it is universally catenary and the dimension formula holds. Since the two fraction fields are equal, the transcendence degree of the the extension of fraction fields is 0. □

Remark. A local inclusion of valuation domains with the same fraction field must be the identity map. For say that $(W, m_W) \subseteq (V, m_V)$ with $m_W \subseteq m_V$. If $f \in V - W$, then $1/f \in W$. Since $f \notin W$, $1/f \in m_W$. But then $1/f \in m_V$, which contradicts $f \in V$. □

Lemma. *Let $x_1, \ldots, x_d$ be a regular sequence in the ring R with $d \geq 2$.*

(a) *Consider $T = R[x_2/x_1] \subseteq R_{x_1}$. Then $T \cong R[X]/(x_1X - x_2)$. Moreover, $x_1, x_3, \ldots .x_d$ is a regular sequence in $R[x_2/x_1]$.*

(b) *Consider $T = R[x_2/x_1, \ldots, x_d/x_1] \subseteq R_{x_1}$. Then*

$$T \cong R[X_2, \ldots, X_d]/(x_1X_i - x_i : 2 \leq i \leq d).$$

Moreover, $\mathcal{J}_{T/R} = x_1^{d-1}T$.

Proof. (a) Since x_1, x_2 is a regular sequence in R, x_1, $x_1X - x_2$ is a regular sequence in $R[X]$: killing x_1 produces $(R/x_1R)[X]$, and the image of the second element is $-x_2$.

We claim that x_1 is not a zerodivisor modulo $(x_1X - x_2)$, for if $x_1f = (x_1X - x_2)g$ in $R[X]$, then $g = hx_1$ by the paragraph above. Since x_1 is not a zerodivisor in $R[X]$, we find that $f = (x_1X - x_2)h$.

This means that $R[X]/(x_1X - x_2)$ injects into its localization at x_1, which we may view as $R_{x_1}/(x_1X - x_2)$. Since x_1 is a unit, we may take $X - x_2/x_1$ as a generator of the ideal in the denominator, and so the quotient is simply R_{x_1}. The image of $R[X]/(x_1X - x_2)$ is then $R[x_2/x_1] \subseteq R_{x_1}$.

The last statement in part (a) follows because if we kill x_1 in $R[X]/(x_1X - x_2)$, we simply get $\big(R/(x_1, x_2)\big)[X]$. The images of $x_3, \ldots, x_d$ form a regular sequence in this polynomial ring, because that was true in $R/(x_1, x_2)$.

Part (b) now follows by induction on d: as we successively adjoin x_2/x_1, x_3/x_1 and so forth, the hypothesis we need for the next fraction continues to hold. The final statement is then immediate, because the Jacobian matrix calculated from the given presentation is x_1 times the size $d - 1$ identity matrix. □

We also note:

Proposition. *Let $(R, m, K) \subseteq V$ be an inclusion of a regular local ring in a DVR, let $v \in m$ be such that R/vR is regular, and let $x \in m$ have minimal order in V. Let T be the first quadratic transform of R along V. Then either $v_1 = v/x$ is a unit of T, or else T/v_1T is regular. If the first quadratic transform is a DVR, it is always the case that v_1 is a unit.*

Proof. Extend v to a regular system of parameters $\mathcal{S}$ for R. If v itself has minimum order in V, then v/x is a unit of T. If not, then x is a unit of T times some element $x_1 \in \mathcal{S}$, and $v_1T = v_1'T$ if $v_1' = v/x_1$. Hence, we may assume without loss of generality that $x = x_1$ and $v = x_2$ in the regular system of parameters $\mathcal{S}$. Then x_1 and x_2/x_1 are in the maximal ideal of T, and to show that they form a regular sequence in T, it suffices to show that they form a regular sequence in the ring

$$R[x_1,\, x_2/x_1,\, \dots\,,\, x_d/x_1].$$

However, mod (x_1), this ring becomes the polynomial ring $K[\overline{x}_2,\, \dots\,,\, \overline{x}_d]$, and the image of x_2/x_1 is $\overline{x}_2$.The quotient of T by this regular sequence is a localization of the polynomial ring $K[\overline{x}_3,\, \dots\,,\, \overline{x}_d]$, and so is regular. Hence, $x_1, x_2/x_1$ is part of a regular system of parameters for T, and so $x_2/x_1 = v/x = v_1$ is a regular parameter. Note that in this case $\dim(T) \geq 2$, so that if T is a DVR we must have that v_1 is a unit. □

We are now ready to prove the result mentioned at the end of the Lecture Notes for February 4 concerning finiteness of the sequence of quadratic transforms under certain conditions: we follow the treatment in [S. Abhyankar, *Ramification theoretic methods in algebraic geometry*, Annals of Mathematics Studies Number **43**, Princeton University Press, Princeton, New Jersey, 1959], Propositon 4.4, p. 77.

Theorem (finiteness of the quadratic sequence). *Let $(R, m, K) \subseteq (V, \mathfrak{n}, L')$ be a local inclusion of a regular local ring R of dimension d with fraction field $\mathcal{K}$ in a discrete valuation ring. Let $T_0 = R$, and let (T_i, m_i, K_i) denote the i th quadratic transform of R along V, so that for each $i \geq 0$, T_{i+1} is the first quadratic transform of T_i along V. Then the union of the T_i is a discrete valuation ring W with $W \subseteq V$.*

If V is essentially of finite type over R and $\mathrm{frac}\,(V)$ *is an algebraic extension of* $\mathrm{frac}\,(R)$ *(by the dimension formula, it is equivalent to assume that* $\mathrm{tr.\,deg.}(L'/K) = d-1$*), then this sequence is finite, i.e., some T_h is a DVR. For this h, $T_h = W = V \cap \mathcal{K}$. so that $V \cap \mathcal{K}$ is essentially of finite type over R, and the transcendence degree of the residue field of $V \cap \mathcal{K}$ over K is $d - 1$.*

Proof. By the dimension formula, for every i,

$$\dim(T_i) = \dim(R) - \mathrm{tr.\,deg.}(K_i/K),$$

so that

$$\mathrm{tr.\,deg.}(L'/K_i) = \mathrm{tr.\,deg.}(L'/K) - \mathrm{tr.\,deg.}(K_i/K) =$$

$$d-1-\mathrm{tr.\,deg.}(K_i/K) = \big(\dim(R) - \mathrm{tr.\,deg.}(K_i/K)\big) - 1 = \dim(T_i) - 1.$$

Therefore, at every stage, we have that $T_i \subseteq V$ satsifies the same condition that $R \to V$ did. Let (W, N, L) denote the union of the T_i. W is the union of ascending sequence of local rings and local inclusions, and so is at least quasi local, and $W \subseteq V$ is local.

We claim that W must be a valuation domain of $\mathcal{K}$. If not, choose $x \in \mathcal{K}$ such that neither x nor $1/x$ is in W, i.e., neither is in any T_i. Write $x = y_0/z_0$ where y_0, $z_0 \in T_0 = R$. These are both in the maximal ideal of T_0 (if z_0 were a unit, we would have $x \in T_0$, while if y_0 were a unit, we would have $1/x \in T_0$). If u_0 is a minimal generator of m_0 of minimum order in V, then $x = y_1/z_1$ where $y_1 = y_0/u_0$ and $z_1 = z_0/u_0$ are in T_1. We once again see that y_1 and z_1 must both belong to m_1. These have positive order in V, but $\mathrm{ord}_V(y_0) > \mathrm{ord}_V(y_1)$ and $\mathrm{ord}_V(z_0) > \mathrm{ord}_V(z_1)$. We recursively construct y_i and z_i in m_i such that $x = y_i/z_i$, and $\mathrm{ord}_V(y_0) > \cdots > \mathrm{ord}_V(y_i)$ while $\mathrm{ord}_V(z_0) > \cdots > \mathrm{ord}_V(z_i)$. At the recursive step let u_i be a minimal generator of m_i such that $\mathrm{ord}_V(u_i)$ is minimum. Then $x = y_{i+1}/z_{i+1}$ where $y_{i+1} = y_i/u_i \in T_{i+1}$ and $z_{i+1} = z_i/u_i \in T_{i+1}$. As before, the fact that $x \notin T_{i+1}$ and $1/x \notin T_{i+1}$ yields that y_{i+1} and z_{i+1} are both in m_{i+1}, as required, and we also have that $\mathrm{ord}_V(y_i) > \mathrm{ord}_V(y_{i+1})$ and $\mathrm{ord}_V(z_i) > \mathrm{ord}_V(z_{i+1})$. This yields that $\{\mathrm{ord}_V(y_i)\}_i$ is a strictly decreasing sequence of nonnegative integers, a contradiction. It follows that W is a valuation domain, and since $W \subseteq V$ is local, it must be a DVR, with maximal ideal generated by the element of W of smallest order in V.

Now assume that V is essentially of finite type over R and that $\mathrm{frac}(V)$ is algebraic over $\mathrm{frac}(R)$, so that $\mathrm{tr.\,deg.}(L'/K) = d-1$. Assume that the sequence T_i is infinite. We obtain a contradiction.

Since the dimension is non-increasing it is eventually stable, and, by replacing R by T_j for $j \gg 0$, we might as well assume that the dimension of T_i is stable throughout. We call the stable value d, and we may assume that $d \geq 2$. It follows that every K_i is algebraic over K. We know that (W, N, L) is the ascending union of the (T_i, m_i, K_i): N is the union of the m_i and L is the union of the K_i, and so is algebraic over K.

Since $W \subseteq V \cap \mathcal{K}$ is a local inclusion of valuation domains with the same fraction field, we can conclude from the third Remark on the first page of the Notes for this Lecture that $W = V \cap \mathcal{K}$. Then $W \subseteq V$ is essentially of finite type, and $\mathrm{frac}(V)$ is algebraic over $\mathrm{frac}(W) = \mathrm{frac}(R)$. It follows that the extension of residue class fields from L to L' is also algebraic, by the dimension formula. However, since we have passed to the tail subsequence in which the dimension of T_i is constant, we have that each residue class field of any of the T_i is algebraic over the residue class field of its predecessor. Thus, the residue class field of W, which is a directed union of these, is algebraic over the the residue class field of each T_i. Hence, the residue class field of V is algebraic over the residue class field of each T_i. Since the T_i supposedly have dimension ≥ 2, this contradicts the dimension formula for $T_i \subseteq V$.

Therefore, the quadratic sequence along V is finite, and the last term T_h is a DVR, and is W, Since $W \subseteq V \cap \mathcal{K}$ is local, $W = V \cap \mathcal{K}$. Since $W = T_h$, it is essentially of finite type over R. The final statement of the theorem follows from the dimension formula. □

Proof of the Key Lemma, second step. We recall the situation: R is a regular domain with fraction field $\mathcal{K}$, v is an element such that R/vR is regular, S is a reduced torsion-free algebra essentially of finite type over R that is generically étale, $y \in R - vR$ is such that $y/v \in S$, and we want to prove that $\mathcal{J}_{S'/R} \subseteq vS'$. In the first step, we replaced S' by its localization $(V, \mathfrak{n}, L')$ at a minimal prime of vS' and R by its localization at the contraction of that minimal prime. Thus, we have that $(R,\, m,\, K) \subseteq V$ is local, where $\dim(R) = d$. Since V is essentially of finite type over R, the dimension formula yields that the $\operatorname{tr.deg.}(L'/K) = d - 1$. It will suffice to show that $\mathcal{J}_{V/R} \subseteq vV$. As noted, we may assume that $d \geq 2$. Consider the sequence of quadratic transforms

$$R = (T_0,\, m_0,\, K_0) \subseteq \cdots \subseteq (T_i,\, m_i,\, K_i) \subseteq \cdots \subseteq (T_h,\, m_h,\, K_h) \subseteq \cdots$$

By the Theorem on the finiteness of the quadratic sequence, we have that for some h, $T_h = V \cap \mathcal{K} = W$, which is therefore essentially of finite type over R. The condition $y/v \in S - R$ shows that $h \geq 1$. By the multiplicative property of Jacobian ideals stated in the Corollary at the end of the Lecture of February 1, we have that $\mathcal{J}_{V/R} = \mathcal{J}_{V/W}\mathcal{J}_{W/R}$. It therefore suffices to prove that $\mathcal{J}_{W/R} \subseteq vW$, and so we may henceforth assume that $V = W$ has fraction field $\mathcal{K}$ and is obtained from R by a finite sequence of quadratic transforms along V.

Lecture of February 8, 2019

Proof of the Key Lemma: final step. We are now in the case where $(R,\, m,\, K)$ is regular local of dimension $d \geq 2$, $(R,\, m,\, K) \subseteq (V, \mathfrak{n}, L)$ is local, where $V \subseteq \mathcal{K}$, the fraction field of R, and V is a DVR essentially of finite type over R. In particular, $\mathrm{tr.\,deg.}(L/K) = d-1$ and we have a finite sequence of quadratic transforms along V

$$(R,\, m,\, K) = (T_0,\, m_0, K_0) \subseteq (T_1,\, m_1, K_1) \subseteq \cdots \subseteq (T_h,\, m_h,\, K_h) = (V,\, \mathfrak{n},\, L)$$

where $h \geq 1$, and $\dim{(T_i)} = d_i \geq 2$ for $i < h$. We must show that $\mathcal{J}_{V/R} \subseteq vV$, where $v \in R$ is such that R/vR is regular. Let $u_i \in m_i$ have minimum order in V for $0 \leq i \leq h-1$. Let $v_1 = v/u_0 \in T_1$. Recursively, so long as $v_i \in T_i$ is not a unit, we know by induction and the Proposition on p. 2 of the Lecture Notes of February 6 that v_i is a regular parameter in T_i and we may define $v_{i+1} = v_i/u_i \in T_{i+1}$. The Proposition just cited shows that either v_{i+1} is a unit of T_{i+1} or a regular parameter.

For some smallest $k \leq h$, v_k is a unit of T_k, for the same Proposition shows that if v_{h-1} is not a unit of T_{h-1}, then v_h is a unit of T_h: see the final statement of that same Proposition. Then

$$v = u_0v_1 = u_0u_1v_2 = \cdots = u_0u_1\cdots u_{k-1}v_k,$$

where v_k is a unit of T_k and, hence, of V. Thus,

$$(*) \quad vV = u_0u_1\cdots u_{k-1}V$$

for some $k \leq h$. On the other hand, the Corollary at the end of the Lecture of February 1 shows that $\mathcal{J}_{V/R} = \mathcal{J}_{T_1/T_0}\mathcal{J}_{T_2/T_1}\cdots\mathcal{J}_{T_h/T_{h-1}}$. The last statement in part (b) of the Lemma on the first page of the Lecture Notes of February 6 shows that $\mathcal{J}_{T_{i+1}/T_i}$ is generated by $u_i^{d_i-1}$. Thus,

$$(**) \quad \mathcal{J}_{V/R} = u_0^{d_0-1}\cdots u_{h-1}^{d_{h-1}-1}V,$$

and each exponent $d_j - 1$ is at least one. The inclusion $\mathcal{J}_{V/R} \subseteq vV$ is now obvious from inspection of $(*)$ and $(**)$. □

The module-finite property for normalizations.

We shall now address the problem of proving that S' is module-finite over S. Several of the details of the argument are left to the reader in Problem Set #2. The result we aim to prove is this:

Theorem (finiteness of the normalization). *Let S be torsion-free, generically étale, and essentially of finite type over a normal Noetherian domain R. Suppose that the completion of every local ring of R is reduced (which holds if R is either regular or excellent). Then the normalization S' of S over R is module-finite over S.*

We first give some preliminary results.

Lemma. *Let S be a Noetherian domain and b a nonzero element such that R_b is normal.*

(a) S is normal if and only if R_P is normal for every associated prime of b.

(b) $\{Q \in \text{Spec}\,(S) : R_Q \text{ is not normal}\}$ is the union of the sets $V(P)$, where P is an associated prime of P such that S_P is not normal, and so is Zariski closed.

(c) If S_m has module-finite integral closure for every maximal ideal m of S, then S has module-finite integral closure.

Proof. (a) The condition is obviously necessary. To see sufficiency, let f be an element of the fraction field integral over S. Since S_b is normal, we can write $f = s/b^n$ from some integer $n \geq 1$. After replacing s by a multiple, we may assume that the annihilator of the image of s in S/b^nS is a prime, P, which will be an element of $\text{Ass}\,(S/b^nS)$. This is the same as $Ass(S/bS)$, since $S/bS \cong b^{n-1}S/b^nS \subseteq S/b^nS$, and S/b^n has a finite filtration with factos $b^tS/b^{t+1}S$ all of which are isomorphic with S/bS. Hence, $f \notin S_P$, with $P \in \text{Ass}\,(S/bS)$, as required.

(b) Since each S_P is not normal and S_P is localization of S_Q if $Q \supseteq P$, we have that $Z = \bigcup\{V(P) : P \in \text{Ass}\,(S/bS) \text{ and } S_P \text{ is not normal}\}$ is contained in the non-normal locus. Now suppose that Q is not in Z. We must show that S_Q is normal. But this follows from (a), since $S_Q[1/b]$ is a localization of S_b, and is normal, and the associated primes of b in S_Q are the expansions of the associated primes of b in S. By assumption, the associated primes P of b such that S_P is not normal are not contained in Q.

(c) Consider any module-finite extension T of S within its fraction field $\mathcal{K}$. Since S_b is normal, it must contain T, and so is equal to T_b. It follows that the non-normal locus Y_T in $\text{Spec}\,(T)$ is closed. The image X_T of Y_T in $\text{Spec}\,(S)$ is closed (Y_T is a finite union of sets of the form $V(Q)$. The image of $V(Q)$ is $V(P)$, where $P = Q \cap S$, by the going-up theorem.) If we take module finite extensions $S \subseteq T_1 \subseteq T_2$, then Y_{T_2} maps into Y_{T_1} (if Q_2 in T_2 lies over Q_1 in T_1 such that $(T_1)_{Q_1}$ is normal, then $(T_2)_{Q_1} = (T_1)_{Q_1}$, and so $(T_2)_{Q_2}$ must be normal.) Since closed sets have DCC (ideals have ACC), we can choose T so that X_T is minimal. We prove $X_T = \emptyset$. This means that T is normal, and so it *is* the normalization of S in $\mathcal{K}$. If $X_T \neq \emptyset$, choose $P \in X_T$. The integral closure D of S_P is module-finte over S_P, since this is true for S_m for any maximal ideal $m \supseteq P$. Choose finitely many integral fractions that span D over S_P. After we multiply by a suitable element of $S - P$, these will be integral fractions of S, and we may enlarge T by adjoining them: call the new ring W. Then W_P is normal, and so the localization of W at any prime lying over P is normal. This shows that $X_W \subseteq X_T - \{P\}$, a contradiction. □

Let $S = R[a_1/b_1, \ldots, a_h/b_h]$ where $b_1, \ldots, b_h$ are nonzerodivisors in R. This is a subring of R_b, where $b = b_1 \cdots b_h$, and each fraction can be written in the form a'_i/b. We may include b/b among these fractions, and so assume that some $a'_i = b$. Since every R-linear combination of the fractions is in S, if I is the ideal of R generated by the a'_i we have that $S = R[I/b]$, where $I/b = \{i/b : i \in I\} \subseteq R_b$. Here, I is an ideal containing b. We next observe:

Theorem (Rees). *Let (R, m, K) be a local ring such that $\widehat{R}$ is reduced. Let S be the ring obtained by adjoining finitely many fractions (elements of the total quotient ring) to R. Then the normalization S' of S is module-finite over S.*

Proof. We first consider the case where R is itself complete. The normalization R' of R will be the product of the normalizations of the quotients of R by its various minimal primes: we already know that each of these is module finite. Thus, we might as well replace R by R', and then we have a product and we can work with the factors separately. We therefore reduce to the case where R is a complete local domain, and we must show that the normalization of $R[I/b]$ is module-finite over $R[I/b]$ for some ideal I with $b \in I$.

We next show that when R is a complete normal local domain and I is an ideal of R, the integral closure of $R[It]$ is module-finite over R. We may assume $I \neq 0$. $R[It]$ has the same fraction field as $R[t]$, and the latter is integrally closed. The integral closure T is graded, and if it is not module-finite over $R[It]$ there is a strictly ascending chain of module-finite extensions $R[It] = T_0 \subset T_1 \subset \cdots \subset T_n \subset \cdots \subset T$, where T_{n+1} is obtained from T_n by adjoining one homogeneous element of T , not in T_n. Thus, all of the T_n are graded, and every T_{n+1}/T_n is a nonzero graded module. Its associated primes are homogeneous and so contained in $\mathcal{M} = m + ItR[It]$. Hence the elements of $R[It] - \mathcal{M}$ are nonzerodivisors on all the factors T_{n+1}/T_n, and the factors remain nonzero when we localize at $\mathcal{M}$. Since the map from $R_{\mathcal{M}}$ to its completion $R[[It]]$, which is a subring of $R[[t]]$ is faithfully flat, we obtain a strictly ascending chain of module-finite extensions of $R[[It]]$ by integral fractions. This is a contradiction, since $R[[It]]$ is a complete local domain. It follows that the integral closure T of $R[It]$ is module-finite over over $R[It]$. Note that in each degree j, T_j is isomorphic to an ideal of R (in fact, $\overline{I^j}$) and is a finitely generated R-modules. Suppose that T is generated over $R[It]$ by elements $r_1t^{d_1}, \dots, r_kt^{d^k}$ fro $d_1, \dots, d_k \in \mathbb{N}$, where $r_j \in \overline{I^{d_j}}$.

These elements generate $T_{bt} = \mathcal{B}$ over its subring $\mathcal{A} = R[It]_{bt}$. Since $B = \mathcal{B}_0 = [T_{bt}]_0$ (with respect to degree in t) is a direct summand as a module over itself of T_{bt} (the complement is $\bigoplus_{i\neq 0}[T_{bt}]_j$), it is normal, and so contains the normalization of $A = \mathcal{A}_0 = [R[It]_{bt}]_0 = R[I/f]$. It therefore suffices to show that B is module-finite over A. But $B \subseteq \sum_{j=1}^k r_jt^{d_j}[R[It]_{bt}]_{-d_j}]$. Note that $[R[It]_{bt}]_{-d} = \bigcap_{k\in\mathbb{N}}(It)^k(bt)^{-d+k} = \bigcup_{k\in\mathbb{N}}(I^k/b^k)b^{-d}t^{-d} = Ab^{-j}t^{-j}$. Thus $B \subseteq \sum_{j=1}^k A(r_j/b^{d_j})$ is module-finite over A, as required.

Now consider the case where R itself is not necessarily complete. If the result fails, then there is an infinite strictly ascending chain $S = S_0 \subseteq S_1 \subseteq S_2 \subseteq \dots$ of algebras generated by fractions over R, where S_{j+1} is module-finite over S_j for $j \geq 0$. But the chain $\widehat{R}[S_j]$ must be eventually stable, since the complete reduced ring $\widehat{R}$ will have finite normalization, so that $\widehat{R}[S_{j+1}] = \widehat{R}[S_j]$ for large j. But this implies $S_{j+1} = S_j$: otherwise some fraction over R is an $\widehat{R}$-linear combination of finitely many other such fractions but not an R-linear combination of them, and we can get a contradiction from this as follows. We may use a common denominator $r \in R$, not a zerodivisor, and write $a/r = \sum_{i=0}^s (a_i/r)\beta_i$ where the $a_i \in R$ and the $\beta_i \in \widehat{R}$. But then $a \in (a_1, \dots, a_s)\widehat{R} \cap R$, which implies $a \in (a_1, \dots, a_s)R$, say $a = \sum_{i=0}^{s} a_i b_i$ with $b_i \in R$, and that means we can replace the β_i by elements b_i of R. □

We also need the fact that finite separable algebraic field extensions do not disturb the property of being reduced:

Lemma. *Let B denoted a reduced ring containing a field $\mathcal{K}$, and let $\mathcal{L}$ be a finite seprable algebraic extension of $\mathcal{K}$. Then $\mathcal{L} \otimes_{\mathcal{K}} B$ is reduced.*

Proof. B is the directed union of finitely generated $\mathcal{K}$-algebas B_0: since $\mathcal{L}$ is $\mathcal{K}$- flat, $\mathcal{L} \otimes_{\mathcal{K}} B$ is the directed union of the rings $\mathcal{L} \otimes_{\mathcal{K}} B_0$. Therefore, we may assume that B is finitely generated over $\mathcal{K}$, and has finitely many minimal primes. B embeds in its total quotient ring, which is a finite product of fields. Thus, we may replace B by its total quotient ring, it suffices to prove the result when B is a product fields. It is easy to see that it suffices to consider the case where B is a field, and we may even enlarge B further to an algebraically closed field Ω. But $\mathcal{L} \cong \mathcal{K}[x]/f(x)$ where f is monic with distinct roots in Ω, and so $\mathcal{L} \otimes_{\mathcal{K}} \Omega \cong \Omega[x]/\bigl(f(x)\bigr)$. This ring is isomorphic with a finite product of copies of Ω by the Chinese Remainder Theorem, since the roots of f are distinct. □

We are now ready to prove the main theorem stated earlier on the module-finite property for S' over S.

Proof of the finiteness of the normalization. We first replace S by a subring finitely generated over R, of which it is a localization. Since localization commutes with normalization, it suffices to consider this subring. Thus, we may assume that S is finitely generated as an R-algebra. Second, the integral closure of S is the product of the integral closures of the domains obtained by killing a minimal prime of S. Thus, without loss of generality, it suffices to consider the case where S is a domain.

Each of the generators in a finite set of generators for S over R satisfies an algebraic equation over R with leading coefficient b_ν, say, and it follows that we may choose a nonzero element $r \in R$, the product of these leading coefficients, such that $S[1/b]$ is integral over $R[1/b]$. The integral closure of the normal domain $R[1/b]$ in the fraction field $\mathcal{L}$ of $S[1/b]$ is the same as the normalization of $S[1/b]$, and is module-finite over $S[1/b]$ by the first Theorem on p. 3 of the Lecture Notes of January 14. It follows that we may enlarge S by adjoining finitely many elements of its normalization and so obtain a domain with the property that $S[1/b]$ is normal for some nonzero b. It then follows from the first Lemma above that in order to prove that S has finite normalization, it suffices to prove this for S_Q for every maximal ideal Q of S. Choose $s \in S$ such that it generates $\mathcal{L}$ over $\mathcal{K}$. Let P be the contraction of Q to $R_1 = R[s]$. Then S_Q is a localization of $(R_1)_P[S]$, and S is generated over $(R_1)_P$ by elements of its fraction field.

Thus, to finish the argument, it suffices to show that the completion of $(R_1)_P$ is reduced. We may replace R by its localization at the contraction of P, and so we may assume that R is local with reduced completion. The completion of $(R_1)_P$ is one of the local rings of the completion of R_1 with respect to the maximal ideal of R. Thus, it suffices to show that this completion of R_1 is reduced. But this is $R_1 \otimes_R \widehat{R} \subseteq \mathcal{L} \otimes_R \widehat{R} \cong \mathcal{L} \otimes_{\mathcal{K}} (\mathcal{K} \otimes_R \widehat{R})$, and the result follows from the preceding Lemma because $\mathcal{K} \otimes_R \widehat{R}$ is reduced and $\mathcal{L}$ is finite separable algebraic over $\mathcal{K}$. □

Sketch of the proof of the Jacobian theorem.

We are ready to tackle the proof of the Jacobian theorem, but we first sketch the main ideas of the argument and then fill in the details.

Step 1: The local case suffices. Note that it is enough to prove the result when S is replaced by its various localizations at maximal ideals. Thus, we may assume that S is local, although we shall only make this assumption at certain points in the proof. When S is local we may also replace R its localization at the contraction of the maximal ideal of S, and so there is likewise no loss of generality in assuming that R is local and that $R \to S$ is local homomorphism (i.e., the maximal ideal of R maps into that of S).

Step 2: presenting S over R. Let T denote a localization of $R[X_1, \ldots, X_n]$ that maps onto S, and let I denote the kernel. Let U denote the complement in T of the set of minimal primes $P_1, \ldots, P_r$ of of I in T. Since S is reduced, $I = \bigcap_{i=1}^r P_i$. Since S is a torsion-free R-module, the minimal primes of I do not meet R, and correspond to the minimal primes of $I(\mathcal{K} \otimes T)$. Since killing any of these minimal primes produces an algebraic extension of $\mathcal{K}$, they must correspond to maximal ideals of $\mathcal{K}[X_1, \ldots, X_n]$, and it follows that the P_i all have the same height, which must be the same as the number of variables, n. Thus, $U^{-1}T$ is a semilocal regular ring in which each of the maximal ideals $\mathcal{M}_i = P_i U^{-1}T$ is generated by n elements.

Step 3: special sequences and the modules $W_{S/R}$. Call a sequence $g_1, \ldots, g_n$ of n elements of I *special* if it generates each of the $\mathcal{M}_i$ and is a regular sequence in T. We shall show that special sequences exist, and that there are sufficiently many of them that the images of the elements $\det(\partial g_j/\partial X_i)$ in S such that $g_1, \ldots, g_n$ is special generate the Jacobian ideal. Moreover, when $g_1, \ldots, g_n$ is special the image of $\det(\partial g_j/\partial X_i)$ in S is not a zerodivisor in S, and so has an inverse in $\mathcal{L}$. Given $\theta : T \to S$ and a special sequence $g_1, \ldots, g_n$ we define a map

$$\Phi\colon \frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \to \mathcal{L}$$

by sending the class of u to $\overline{u}/\gamma$, where $\overline{u}$ is the image of u in S and γ is the image of $\det(\partial g_j/\partial X_i)$ in S. It is clear that I kills $(g_1, \ldots, g_n)T :_T I/(g_1, \ldots, g_n)T$, so that this is an S-module. We shall show that Φ is injective. *A priori*, its image depends on the choice of $T \to S$ and on the choice of the special sequence $g_1, \ldots, g_n$, but the image turns out to be independent of these choices. Therefore, once we have shown all this we will have constructed a finitely generated canonically determined S-module $W_{S/R} \subseteq \mathcal{L}$.

Step 4: the behavior of the $W_{S/R}$ and the main idea of the argument. It will turn out that, quite generally, $W_{S/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$. Here, one should think of S as varying. The Jacobian Theorem then follows from two further observations. The first is that when S is normal, this is an equality The second is that when one enlarges S to $S_1 = S[s_1]$ by adjoining one integral fraction $s_1 \in \mathcal{L}$ (so that $S \subseteq S_1 \subseteq S'$), then $W_{S_1/R} \subseteq W_{S/R}$. Repeated application of this fact yields that $W_{S'/R} \subseteq W_{S/R}$ and then we have

$$S' :_{\mathcal{L}} \mathcal{J}_{S'/R} = W_{S'/R} \subseteq W_{S/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R},$$

and we are done. In the sequel we shall systematically fill in the details of the argument just outlined.

Lecture of Februarty 11, 2019

Detailed proof of the Jacobian theorem: existence of sufficiently many special sequences.

Note first that if R itself is a field then $S = \mathcal{L}$ and $S' = S$, so that $\mathcal{J}_{S/R} = \mathcal{J}_{S'/R}$ and there is nothing to prove. If R is finite then R must be a field, since R is a domain, and therefore we may assume without loss of generality that R is infinite in the remainder of the proof.

We shall need prime avoidance in the following form (cf. [I. Kaplansky, *Commutative Rings*, Revised Edition, Univ. of Chicago Press, Chicago, 1974], Theorem 124, p. 90.):

Lemma (prime avoidance for cosets). *Let R be any commutative ring, $x \in R$, $I \subseteq R$ an ideal and $P_1, \ldots, P_k$ prime ideals of R. Suppose that the coset $x + I$ is contained in $\bigcup_{i=1}^k P_i$. Then there exists j such that $Rx + I \subseteq P_j$.*

Proof. If $k = 1$ the result is clear. Choose $k \geq 2$ minimum giving a counterexample. Then no two P_i are comparable, and $x + I$ is not contained in the union of any $k - 1$ of the P_i. Now $x = x + 0 \in x + I$, and so x is in at least one of the P_j: say $x \in P_k$. If $I \subseteq P_k$, then $Rx + I \subseteq P_k$ and we are done. If not, choose $i_0 \in I - P_k$. We can also choose $i \in I$ such that $x + i \notin \bigcup_{j=1}^{k-1} P_i$. Choose $u_j \in P_j - P_k$ for $j < k$, and let u be the product of the u_j. Then $ui_0 \in I - P_k$, but is in P_j for $j < k$. It follows that $x + (i + ui_0) \in x + I$, but is not in any P_j, $1 \leq j \leq k$, a contradiction. □

The following somewhat technical "general position" lemma is needed to prove that Jacobian determinants arising from special sequences generate the Jacobian ideal.

Lemma (general position for generators). *Let $R \subseteq T$ be a commutative rings such that R is an infinite integral domain and let $P_1, \ldots, P_r$ be mutually incomparable prime ideals of T contracting to (0) in R. Let $N \geq n \geq 1$ be integers and let $M = (g_1 \ \ldots \ g_N)$ be a $1 \times N$ matrix over T with entries in $I = \bigcap_{j=1}^r P_r$. Let κ_j denote the field $T_{P_j}/P_jT_{P_j}$ for $1 \leq j \leq r$ and let V_j denote the κ_j-vector space $P_jT_{P_j}/P_j^2T_{P_j}$. Suppose that for all j, $1 \leq j \leq r$, the κ_j-span of the images of the g_t under the obvious map $I \subseteq P_j \to P_jT_{P_j} \twoheadrightarrow V_j$ has κ_j-vector space dimension at least n.*

Then one may perform elementary column operations on the matrix M over T so as to produce a matrix with the property that, for all j, $1 \leq j \leq r$, the images of any n of its distinct entries are κ_j-linearly independent elements of V_j.

Of course, the entries of the new matrix generate the ideal $(g_1, \dots, g_N)T$.

Proof. First note that the infinite domain R is contained in each of the κ_j.

We proceed by induction on the number of primes. If there are no primes there is nothing to prove. Now suppose that $1 \leq h \leq r$ and that column operations have already been performed so that any n entries have κ_j-independent images in V_j if $j < h$. (If $h = 1$ we may use M as is, since no condition is imposed.) We need to show that we can perform elementary column operations so that the condition also holds for $j = h$. Some n of the entries have κ_h-independent images in V_h: by renumbering we may assume that these are $g_1, \dots, g_n$. We now show that by induction on a, $n+1 \leq a \leq N$ that we may perform elementary column operations on the matrix so that

(1) The images of the entries of the matrix in each V_j for $j < h$ do not change and

(2) Any n of the images of $g_1, \dots, g_a$ in V_h are independent.

Choose $t \in T$ so that it is in the primes P_j for $j < h$ but not in P_h. Thus, t has nonzero image τ in κ_h. Let v_j denote the image of g_j in V_h. We may assume that the images of any n of the elements $g_1, \dots, g_{a-1}$ are independent in V_h. Thus, it will suffice to show that there exist $r_1, \dots, r_n \in R$ such that the image of $g_a + tr_1g_1 + \cdots tr_ng_n$ is independent of any $n-1$ of the vectors $v_1, \dots, v_{a-1}$ in V_h, i.e., such that $v_a + \tau r_1 v_1 + \cdots \tau r_n v_n$ is independent of any $n-1$ of the vectors $v_1, \dots, v_{a-1}$. (Note that condition (1) is satisfied automatically because the image of t is 0 in each κ_j for $j < h$.)

For each set D of $n-1$ vectors in $v_1, \dots, v_{a-1}$, there is a nonzero polynomial f_D in n variables over κ_h, and whose nonvanishing at the point $(r_1, \dots, r_n)$ guarantees the independence of $v_a + \tau r_1 v_1 + \cdots \tau r_n v_n$ from the vectors in D. To see this, choose a κ_h-basis for the space spanned by all the v_j and write the vectors in D and $v_a + \tau X_1 v_1 + \cdots \tau X_n v_n$ in terms of this basis. Form a matrix C from the coefficients. We can choose values of the X_i in R that achieve the required independence, and this means that some $n \times n$ minor of C does not vanish identically. (If v_a is independent of the vectors in D take all the X_i to be zero. Otherwise, v_a is in the κ_h-span of D, while at least one of the n independent vectors $v_1, \dots, v_n$ is not, say v_ν, and we can take all the X_i except X_ν to be 0 and $X_\nu = 1$.) This minor gives the polynomial $f_D \in \kappa_h[X_1, \dots, X_n]$.

Choose a field extension $\mathcal{F}$ of $\mathcal{K} = \text{frac}\,(R)$ that contains isomorphic copies of all of the κ_j. The product f of the f_D in $\mathcal{F}[x_1, \dots, x_n]$ as D varies through the $n-1$ element subsets of $v_1, \dots, v_{a-1}$ is then a nonzero polynomial in $\mathcal{F}[X_1, \dots, X_n]$, and so cannot vanish identically on the infinite domain R. Choose $r_1, \dots, r_n \in R$ so that $f(r_1, \dots, r_n) \neq 0$. Then every $f_D(r_1, \dots, r_n) \neq 0$ □

Lemma. *Let $g_1, \dots, g_n$ be elements of a Noetherian ring T and let J be an ideal of T of depth at least n such that $(g_1, \dots, g_n)T + J$ is a proper ideal of T. If $g_1, \dots, g_i$ is a* *regular sequence in T (i may be zero, i.e., we may be assuming nothing about $g_1, \ldots, g_n$) then there are elements $j_{i+1}, \ldots, j_n \in J$ such that*

$$g_1, \ldots, g_i, g_{i+1} + j_{i+1}, \ldots, g_n + j_n$$

is a regular sequence in T.

In particular, there are elements $j_1, \ldots, j_n \in J$ such that $g_1 + j_1, \ldots, g_n + j_n$ is a regular sequence.

Proof. The last sentence is the case $i = 0$. We proceed by induction on $n - i$. If $i = n$ there is nothing to prove. We may pass to $T/(g_1, \ldots, g_i)T$, and so reduce to the case where $i = 0$. The image J is the same as the image of $J' = J + (g_1, \ldots, g_i)$ modulo $(g_1, \ldots, g_i)$. J' is a proper ideal of depth at least n, and so killing a regular sequence of length i in J' poduces an ideal of depth at least $n - i > 0$. Thus, we may assume that $i = 0$.

It then suffices to choose $j = j_1$ such that $g_1 + j$ is not a zerodivisor, for we may apply the induction hypothesis to construct the rest of the sequence. But if this were not possible we would have that $g_1 + j$ is contained in the union of the associated primes of (0) in T, and this implies that J is contained in an associated prime of (0) in T by the Lemma on prime avoidance for cosets proved at the beginning of this Lecture. This is a contradiction, since the depth of J is positive. □

Theorem (existence of sufficiently many special sequences). *Let R be an infinite Cohen-Macaulay Noetherian domain and let S be a torsion-free generically étale R-algebra essentially of finite type over R. Let T be a localization of a polynomial ring in n variables over R that maps onto S, and let I be the kernel. Let $P_1, \ldots, P_r$ be the minimal primes of I in T. Then the Jacobian ideal $\mathcal{J}_{S/R}$ is generated by the images of elements* $\det(\partial g_j/\partial x_i)$ *such that $g_1, \ldots, g_n$ is a special sequence of elements of I, i.e., a regular sequence in I such that for every j, $1 \le j \le r$, $P_jT_{P_j} = (g_1, \ldots, g_n)T_{P_j}$.*

Proof. First choose generators $g_1, \ldots, g_N$ for I. Think of these generators as forming the entries of a $1 \times N$ matrix as in the Lemma on general position for generators. Each T_{P_j} is regular local of dimension n, so that each $P_jT_{P_j}/P_j^2T_{P_j}$ has dimension n. It follows from the Lemma cited that we may assume without loss of generality that every n element subset of the generators $g_1, \ldots, g_N$ generates every $P_jT_{P_j}$. We know that the size n minors of the $n \times N$ matrix $(\partial g_j/\partial x_i)$ generate $\mathcal{J}_{S/R}$. Fix one of these minors: by renumbering, we may assume that it corresponds to the first n columns. It will suffice to show that the image of this minor in S is the same as the image of a minor coming from a special sequence. We may apply the preceding Lemma to choose elements $h_1, \ldots, h_n \in J = I^2$ such that $g_1 + h_1, \ldots, g_n + h_n$ is a regular sequence. This sequence is special: since $J = I^2 \subseteq P_j^2$ for all j, the elements generate each $P_jT_{P_j}$, and it was chosen to be a regular sequence. Finally, by the Remark near the top of p. 2 of the Lecture Notes of February 1, the image of the Jacobian determinant of $g_1 + h_1, \ldots, g_n + h_n$ in S is the same as the image of the Jacobian determinant of $g_1, \ldots, g_n$, and the result follows. □

Lecture of February 13, 2019

Lemma (comparison of special sequences). *Let R be an infinite Cohen-Macaulay Noetherian domain and let S be a torsion-free generically étale R-algebra essentially of finite type over R. Let T be a localization of a polynomial ring in n variables over R that maps onto S, and let I be the kernel. Let $P_1, \ldots, P_r$ be the minimal primes of I in T. Assume, moreover, that S and T are local. Let $\underline{g} = g_1, \ldots, g_n$ and $\underline{h} = h_1, \ldots, h_n$ be two special sequences in I. Then there is a finite chain of special sequences joining $\underline{g}$ to $\underline{h}$ such that for any two consecutive special sequences occurring in this chain, the sequences of elements occuring differ in at most one spot.*

Proof. We first show that given two special sequences $g_1, \ldots, g_n$ and $h_1, \ldots, h_n$ and an integer i, $1 \leq i \leq n$, we can choose $u \in T$ such that $g_1, \ldots, g_n$ remains special when g_i is replaced by u and $h_1, \ldots, h_n$ remains special as well when h_i is replaced by u. Since regular sequences (and, hence, special sequences) are permutable in a local ring, we may assume without loss of generality that $i = n$. Our first objective is to choose u such that, for all j, both sequences generate each $P_jT_{P_j}$. Since $P_j \cap R = (0)$ for every j, we have for each j that $\mathcal{K} \subseteq T_{P_j}$. To solve the problem we shall first choose u with the required property in $\mathcal{K} \otimes_R T$. For every j let C_j denote the contraction of

$$\big((g_1, \ldots, g_{n-1}) + P_j^2\big)T_{P_j}$$

to $\mathcal{K} \otimes_R T$, and let D_j denote the contraction of

$$\big((h_1, \ldots, h_{n-1}) + P_j^2\big)T_{P_j}$$

to $\mathcal{K} \otimes_R T$. The C_j and D_j together constitute finally many vector spaces over the field $\mathcal{K}$. We claim that they do not cover $\mathcal{K} \otimes_R I \subseteq \mathcal{K} \otimes_R T$, for if they did then one of them would contain $\mathcal{K} \otimes_R I$ (see the first Proposition on p. 3 of the Lecture Notes of January 23), and this would contradict the existence of g_n if it were one of the C_j, or the existence of h_n if it were one of the D_j. Hence, we can choose $u \in \mathcal{K} \otimes_R I$ with the required property. After multiplying by a suitable element of $R - \{0\}$, we may assume that u is in I, and it will still have the required property, since the multiplier is a unit in every R_{P_j}. Finally, as in the proof of the Theorem on existence of sufficiently many special sequences (which is the last Theorem of the Lecture of February 11), we can choose $v \in I^2$ such that $u + v$ is not a zerodivisor modulo either $(g_1, \ldots, g_{n-1})T$ nor modulo $(h_1, \ldots, h_{n-1})T$: this comes down to the assertion that $u + I^2$ is not contained in the union of the associated primes of the two ideals, and by the Lemma on prime avoidance for cosets, it suffices to show that I^2 is not contained in any of them. But this is clear because all the associated primes have height $n - 1$ while I^2 has height n.

Finally, to prove the existence of the chain of special sequences we use induction on the number of terms in which the two sequences, counting from the beginning, agree. Suppose that $g_i = h_i$ for $i < j$ while sequences $g_j \neq h_j$ (j may be 0 here). Then by the result of the paragraph above we may choose u such that the sequences

$$g_1, \ldots, g_{j-1}, u, g_{j+1}, \ldots, g_n$$

and

$$g_1, \ldots, g_{j-1}, u, h_{j+1}, \ldots, h_n$$

are both special. The first differs from $g_1, \ldots, g_n$ in only the j th spot, and the second differs from $h_1, \ldots, h_n$ in only the j th spot as well. By the induction hypothesis there is a chain of the required form joining these two, and the result follows. □

The map Φ and the modules $W_{S/R}$.

Our next main goal is to construct the map Φ mentioned briefly in Step 3 of our Sketch of the proof the Jacobian theorem: see p. 4 of the Lecture Notes of February 8.

We first need a lemma whose proof involves universal modules of differentials or Kähler differentials.

In the next seven paragraphs, we assume only that $\mathcal{K}$ is a commutative ring and that T is $\mathcal{K}$-algebra. A *$\mathcal{K}$-derivation* of T into a T-module M is a map $D : T \to M$ such that

(1) D is a homomorphism of abelian groups

(2) For all $t_1, t_2 \in T$, $D(t_1t_2) = t_1D(t_2) + t_2D(t_1)$ and

(3) For all $c \in \mathcal{K}$, $D(c) = 0$.

Condition (2) implies that D is $\mathcal{K}$-linear, for $D(ct) = cD(t) + tD(c) = cD(t) + t(0) = cD(t)$. Note that $D(1 \cdot 1) = 1D(1) + 1D(1)$, i.e. $D(1) = D(1) + D(1)$, so that condition (2) implies that $D(1) = 0$. In the presence of the other conditions, (2) is equivalent to $\mathcal{K}$-linearity, for if the map is $\mathcal{K}$-linear then for all $c \in \mathcal{K}$, $D(c \cdot 1) = cD(1) = c(0) = 0$.

There is a *universal $\mathcal{K}$-derivation* from a given $\mathcal{K}$-algebra T into a specially constructed T-module $\Omega_{T/\mathcal{K}}$. This is obtained as follows. Let G denote the T-free module whose basis consists of elements b_t in bijective correspondence with the elements t of T. Consider the T-submodule H of G spanned by elements of the three forms:

(1) $b_{t_1+t_2} - b_{t_1} - b_{t_2}$ for all t_1, $t_2 \in T$;

(2) $b_{t_1t_2} - t_1b_{t_2} - t_2b_{t_1}$ for all t_1, $t_2 \in T$; and

(3) b_c for $c \in \mathcal{K}$.

We write $\Omega_{T/\mathcal{K}}$ for G/H. This is the *universal module of differentials* or the module of *Kähler differentials* for T over $\mathcal{K}$. Note that we have a map $d : T \to \Omega_{T/\mathcal{K}}$ that sends $t \mapsto b_t + H$, the class of b_t in G/H. The choice of elements that we killed (we took them as generators of H) precisely guarantees that d is a $\mathcal{K}$-derivation, the *universal $\mathcal{K}$-derivation* on T. It has the following universal property: given any T-module N and a $\mathcal{K}$-derivation $D : T \to N$, there is a unique T-linear map $L : M \to N$ such that $D = L \circ d$. To get the map L on G/H we define it on G so that the value on b_t is $D(t)$: this is forced if we are going to have $D = L \circ d$. One may check easily that H is killed, precisely because D is a $\mathcal{K}$-derivation, and this gives the required map. (It is also easy to see that the composition of d with any T-linear map *is* a $\mathcal{K}$-derivation.) Thus, for every T-module N, there is a bijection between the $\mathcal{K}$-derivatons of T into N and $\mathrm{Hom}_T(\Omega_{T/\mathcal{K}}, N)$.

Given generators t_i for T over $\mathcal{K}$, the elements dt_i (the index set may be infinite) span $\Omega_{T/\mathcal{K}}$. The value of d on a product of these generators is expressible in terms of the dt_i by iterated use of the product rule.

Given a polynomial ring $\mathcal{K}[X_i : i \in I]$ over $\mathcal{K}$, $\Omega_{T/\mathcal{K}}$ is the free T-module on the dX_i, and the universal derivation d is defined by the rule

$$dF = \sum_i \frac{\partial F}{\partial x_i} dX_i.$$

This formula is a consequence of the use of the iterated product rule, and it is straightforward to check that it really does give a derivation.

Note that if U is a multiplicative system in T, we have that $\Omega_{U^{-1}T/\mathcal{K}} \cong U^{-1}\Omega_{T/\mathcal{K}}$. Also observe that a $\mathcal{K}$-derivation $D : T \to M$ extends uniquely, via the rule $t/u \mapsto (uDt - tDu)/u^2$, to a $\mathcal{K}$-derivation $U^{-1}D : U^{-1}T \to U^{-1}M$ so that the diagram

$$\begin{tikzcd}
U^{-1}T \arrow[r, "U^{-1}D"] & U^{-1}M \\
T \arrow[u] \arrow[r, "D"] & M \arrow[u]
\end{tikzcd}$$

commutes.

The notations in the following Lemma are slightly different from those in our general setup.

Lemma. *Let $\mathcal{N}$ be a maximal ideal of $T = \mathcal{K}[X_1, \ldots, X_n]$, a polynomial ring over a field $\mathcal{K}$. Assume that $\mathcal{L} = \mathcal{K}[X_1, \ldots, X_n]/\mathcal{N}$ is separable field extension of $\mathcal{K}$. Then $g_1, \ldots, g_n \in \mathcal{N}T_{\mathcal{N}}$ generate $\mathcal{N}T_{\mathcal{N}}$ if and only if the image of $\det\bigl(\partial g_j/\partial x_i\bigr)$ in $\mathcal{L}$ is not 0.*

Proof. Consider the universal $\mathcal{K}$-derivation $d : \mathcal{K}[X] \to \Omega_{\mathcal{K}[X]/\mathcal{K}}$, the module of Kähler differentials, which, as noted above, is the free T-module generated by the elements $dX_1, \ldots, dX_n$. Of course, if $F \in \mathcal{K}[X]$ then $dF = \sum_{j=1}^n (\partial F/\partial x_j)\, dx_j$. The restriction of d to $\mathcal{N}$ gives a $\mathcal{K}$-linear map $\mathcal{N} \to \Omega_{\mathcal{K}[X]/\mathcal{K}}$, and, by the defining property of a derivation, it sends

$$\mathcal{N}^2 \to \mathcal{N}\Omega_{\mathcal{K}[X]/\mathcal{K}}.$$

Thus, there is an induced $\mathcal{K}$-linear map of $\mathcal{K}$-vector spaces

$$\delta : \mathcal{N}/\mathcal{N}^2 \to \mathcal{L} \otimes_T \Omega_{T/\mathcal{K}}.$$

Both modules are $\mathcal{L}$-vector spaces and it follows from the defining property of a derivation that δ is actually $\mathcal{L}$-linear (if $t \in T$ represents $\lambda \in \mathcal{L}$ and $u \in \mathcal{N}$, $d(tu) = tdu + udt$, and the second term will map to 0 in $\mathcal{L} \otimes_T \Omega_{T/\mathcal{K}}$). Since $T_{\mathcal{N}}$ is regular of dimension n, $\mathcal{N}/\mathcal{N}^2$ is an n-dimensional vector space over $\mathcal{L}$. The key point is that under the hypothesis that $\mathcal{L}$ is separable over $\mathcal{K}$, the map δ is an isomorphism of $\mathcal{L}$-vector spaces. To see this, observe that the map δ sends the elements represented by generators $g_1, \ldots, g_n$ for $\mathcal{N}T_{\mathcal{N}}$ to the elements represented by the dg_j, and so it has a matrix which is the image of the matrix $(\partial g_j/\partial x_i)$ after mapping the entries to $\mathcal{L}$. Thus, δ is an isomorphism if and only if the Jacobian determinant $\det(\partial g_j/\partial x_i)$ has nonzero image in $\mathcal{L}$. But this determinant generates $J_{\mathcal{L}/\mathcal{K}}$, and so δ is an isomorphism if and only if the Jacobian ideal of $\mathcal{L}$ over $\mathcal{K}$ is $\mathcal{L}$. But we may use any presentation of $\mathcal{L}$ over $\mathcal{K}$ to calculate $J_{\mathcal{L}/\mathcal{K}}$, and so we may instead use $\mathcal{L} \cong \mathcal{K}[Z]/\big(f(Z)\big)$ where Z here represents just one variable and where f is a single separable polynomial. The Jacobian determinant is then the value of $f'(Z)$ in $\mathcal{L}$, which is not zero by virtue of the separability.

Thus, δ is an $\mathcal{L}$-isomorphism. Moreover, we have already seen that if $g_1, \ldots, g_n$ are generators of $\mathcal{N}T_{\mathcal{N}}$ then the Jacobian determinant is not 0 in $\mathcal{L}$. But the converse is also clear, because if $g_1, \ldots, g_n$ are any elements of $\mathcal{N}T_{\mathcal{N}}$, they generate $\mathcal{N}T_{\mathcal{N}}$ if and only if their images in $\mathcal{N}T_{\mathcal{N}}/\mathcal{N}^2T_{\mathcal{N}} \cong \mathcal{N}/\mathcal{N}^2$ span this vector space over $\mathcal{L}$, by Nakayama's lemma, and this will be the case if and only if their further images in $\mathcal{L} \otimes_T \Omega_{T/\mathcal{K}}$ span that vector space over $\mathcal{L}$, since δ is an isomorphism. But that will be true if and only if the images of the dg_j span $\mathcal{L} \otimes_T \Omega_{T/\mathcal{K}}$, which is equivalent to the assertion that the images of the columns of the matrix $(\partial g_j/\partial x_i)$, after the entries are mapped to $\mathcal{L}$, span an n-dimensional space. This in turn is equivalent to the nonvanishing of $\det(\partial g_j/\partial x_i)$ in $\mathcal{L}$. □

We now return to our standard set of notations and assumptions, as in Step 2 of the Sketch of the proof of the Jacobian theorem from p. 3 of the Lecture Notes of February 8. Thus, T is a localization of $R[X_1, \ldots, X_n]$ that maps onto S with kernel I. U is the complement in T of the set of minimal primes $P_1, \ldots, P_r$ of of I in T, and $I = \bigcap_{i=1}^r P_i$. The P_i do not meet R and correspond to the minimal primes of $I(\mathcal{K} \otimes T)$. The expansion of P_i to $U^{-1}T$ is maximal ideal $\mathcal{M}_i$ corresponding to a maximal ideal $\mathcal{N}_i$ of $\mathcal{K}[X_1, \ldots, X_n]$, and has height n. Here, $T_{P_i} \cong \mathcal{K}[X_1, \ldots, X_n]_{\mathcal{N}_i}$.

Corollary. *Let $g_1, \ldots, g_n \in I$. If $g_1, \ldots, g_n$ is a special sequence in I, then the image γ of $\det\big(\partial g_j/\partial X_i\big)$ is not a zerodivisor in S, and so represents an invertible element of the total quotient ring $\mathcal{L}$ of S.*

Proof. We may view $\mathcal{L}$ as the product of the fields $\mathcal{L}_i$, where $\mathcal{L}_i$ is the fraction field of T/P_i but may also be identified with $\mathcal{K}[X_1, \ldots, X_n]/\mathcal{N}_i$. It suffices to show that γ does not map to 0 under $\mathcal{L} \twoheadrightarrow \mathcal{L}_i$ for any i. The fact that the image of γ is not 0 in $\mathcal{L}_i$ follows from the preceding Lemma, the separability of $\mathcal{L}_i$ over $\mathcal{K}$, and the fact that for every i, $g_1, \ldots, g_n$ generates $P_iT_{P_i}$, which we may identify with $\mathcal{N}_i\mathcal{K}[X_1, \ldots, X_n]_{\mathcal{N}_i}$. □

We continue the conventions in the paragraph preceding the statement of the Lemma, but because we shall let both S and its presentation vary we shall write θ for the map $T \to S$

and we shall denote by $\underline{g}$ a special sequence $g_1, \ldots, g_n$ in I. We may then temporarily define

$$\Phi_{\theta,\underline{g}}\colon \frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \to \mathcal{L}$$

by sending the class of u to $\overline{u}/\gamma$ where $\overline{u}$ is the image of u in $\mathcal{L}$, and γ is the image of $\det(\partial g_j/\partial x_i)$ in $\mathcal{L}$: the element γ is invertible in $\mathcal{L}$ by the Corollary just above. The map is well defined because the g_i vanish under the map to $\mathcal{L}$. We shall often write Φ when θ and $\underline{g}$ are understood. We shall soon show that the image of Φ is contained in $S :_{\mathcal{L}} J_{S/R}$. Once this is established we shall change the definition of Φ very slightly by restricting its range to be $S :_{\mathcal{L}} J_{S/R} \subseteq \mathcal{L}$.

We note that

$$\frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \cong \mathrm{Hom}_T\bigl(T/I,\, T/(g_1, \ldots, g_n)T\bigr).$$

We shall denote the image of $\Phi_{\theta,g}$ in $\mathcal{L}$ by $W_{S/R}(\theta, \underline{g})$. However, we shall see just below that it is independent of the choices of θ and $\underline{g}$, and once we know this we shall simply write it as $W_{S/R} \subseteq \mathcal{L}$.

Lemma. *With notation as above, $\Phi_{\theta,\underline{g}}$ is injective.*

Proof. Under the map $T \to \mathcal{L}$ the complement U of the union of the primes P_i becomes invertible. Because $\underline{g}$ is a regular sequence in T, every associated prime is minimal, and so no element of U is a zerodivisor on $T/(g_1, \ldots, g_n)T$. Thus,

$$\frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \hookrightarrow \frac{T}{(g_1, \ldots, g_n)T} \hookrightarrow \frac{U^{-1}T}{U^{-1}(g_1, \ldots, g_n)T} \cong \mathcal{L}.$$

The map $\Phi_{\theta,\underline{g}}$ is the composition of this composite injection with multiplication by the invertible element $1/\gamma$ in $\mathcal{L}$. $\square$

Lecture of February 15, 2019

We showed in the Lecture of February 13 that the map $\Phi_{\theta,\underline{g}}$ is injective. We next want to show that its image $W_{S/R}(\theta, \underline{g})$ is independent of the choice of the presentation θ and the choice of special sequence $\underline{g}$.

We first prove:

Lemma. *Let B be a ring, $J \subseteq B$ an ideal, and x, y elements of J that are nonzerodivisors in B. Then*

$$\frac{xB :_B J}{xB} \cong \frac{yB :_B J}{yB}$$

via the map that sends the class of $u \in xB :_B J$ to the class of an element $v \in yB :_B J$ such that $xv = yu$.

Proof. Given $u \in xB :_B J$, we have, since $y \in J$, that $yu \in xB$, and so $yu = xv$ with $v \in B$ (the choice of v is unique, since x is a nonzerodivisor in B). We first want to see that $v \in yB :_B J$, which means that if $a \in J$, then $av \in yB$. Since $a \in J$, $au = bx$ for $b \in B$. Then $auy = ybx$ and so $axv = ybx$. Since x is not a zerodivisor, this yields $av = yb$, as required. Next note that if we change the representative of the class of u, say to $u + xc$, then

$$y(u + xc) = yu + yxc = xv + yxc = x(v + yc).$$

Since v changes by a multiple of y, our map is well-defined. This establishes that we have a map

$$\frac{xB :_B J}{xB} \to \frac{yB :_B J}{yB}$$

of the form stated. By symmetry, there is a map

$$\frac{yB :_B J}{yB} \to \frac{xB :_B J}{xB}$$

of the same sort. By the symmetry of the condition $yu = xv$, if the class of u maps to the class of v then the class of v maps to the class of u, and vice versa. This shows that the two maps are mutually inverse. □

Theorem. *The image of the map $\Phi_{\theta,\underline{g}}$ in $\mathcal{L}$ is independent of the choice of $\underline{g}$, and of the choice of θ.*

Proof. To prove for a fixed presentation that the map is independent of the choice of special sequence suppose that we have two special sequences that yield maps with different images. We can preserve the fact that the images W, W' are different while localizing at a suitable prime or even maximal ideal of T: S is replaced by its localization at a corresponding prime. Simply choose the prime to be in the support of $(W + W')/(W \cap W')$. Thus, there is no loss of generality in assuming that T and S are local. The sequences in question remain special as we localize. But then, by the Lemma on comparison of special sequences from the beginning of the Lecture of February 13, we know that there exists a finite chain of special sequences joining the two that we are comparing such that any two consecutive sequences differ in at most one spot. Thus, we need only make the comparison when the two sequences differ in just one term, and since the sequences are permutable we may assume without loss of generality that one of them is $g_1 = g,\, g_2,\, \ldots\,,\, g_n$ and the other is $h,\, g_2,\, \ldots\,,\, g_n$, which we shall also denote $h_1,\, \ldots\,, h_n$.

We set up an isomorphism

$$\sigma\colon \frac{(g_1,\, \ldots\,, g_n)T :_T I}{(g_1,\, \ldots\,, g_n)T} \cong \frac{(h_1,\, \ldots\,, h_n)T :_T I}{(h_1,\, \ldots\,, h_n)T}$$

as follows. Let $B = R/(g_2, \ldots, g_n)$, let $J \subseteq B$ be the image of I, i.e., $I/(g_2, \ldots, g_n)$. Let x be the image of g and y the image of h. We now have the isomorphism by applying the Lemma proved just above.

To complete the proof of the independence of the image from the choice of special sequence we note that the following diagram commutes:

$$\begin{tikzcd}
\dfrac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \arrow[r, "\sigma"] \arrow[d, "\Phi_{\theta,\underline{g}}"'] & \dfrac{(h_1, \ldots, h_n)T :_T I}{(h_1, \ldots, h_n)T} \arrow[d, "\Phi_{\theta,\underline{h}}"] \\
\mathcal{L} \arrow[r, "\mathbf{1}_{\mathcal{L}}"'] & \mathcal{L}
\end{tikzcd}$$

To see this, one simply needs to see that if

$$(*) \qquad uh - vg = \sum_{j=2}^{n} t_j g_j$$

in T, then

$$(**) \qquad \frac{\overline{u}}{\gamma} = \frac{\overline{v}}{\eta}$$

in $\mathcal{L}$, where $\overline{u}$, $\overline{v}$ are the respective images of u and v in $\mathcal{L}$ and γ, η are the respective images of the determinants of the two Jacobian matrices in $\mathcal{L}$, i.e., that

$$u \det(\partial h_j/\partial X_i) \equiv v \det(\partial g_j/\partial X_i) \text{ modulo } I.$$

By differentiating $(*)$ with respect to each X_j in turn and using the fact that all the g, h and the g_j are in I, we see that, because the terms not shown coming from the product rule have a coefficient in I,

$$u\nabla h - v\nabla g \equiv \sum_{j=2}^{n} t_j \nabla g_j \quad \text{modulo } I.$$

Thus, the matrix whose columns are

$$u\nabla h,\ \nabla g_2, \ldots, \nabla g_n$$

and the matrix whose columns are

$$v\nabla g + \sum_{j=2}^{n} t_j \nabla g_j,\ \nabla g_2, \ldots, \nabla g_n$$

are equal mod I. By elementary column operations, we may drop the summation term from the first column of the second matrix when we calculate the determinant. Then we may factor u from the first column of the first matrix and v from the first column of the second matrix when we take determinants. This yields $\overline{u}\eta = \overline{v}\gamma$ in $\mathcal{L}$, and $(**)$ follows.

It remains only to prove that the image of $\Phi_{\theta,\underline{g}}$ is independent of the choice of $\theta\colon T \to S$ as well. We first consider the case of a finitely generated R-algebra S. The choice of a presentation is equivalent to the choice of a finite set of generators for S over R. We can compare the results from each of two different sets of generators with the result from their union, and so it suffices to see what happens when we enlarge a set of generators. By induction, it suffices to show that the image does not change when we enlarge a set of generators by one element, and so we may assume that we have $\theta : T = R[X_1, \ldots, X_n] \twoheadrightarrow S$ and an extension of θ, $\theta'\colon T[X_{n+1}] \twoheadrightarrow S$ by sending X_{n+1} to s. Let $T' = T[X_{n+1}]$. We can choose an element $F \in T$ such that F maps to s in S, and it follows easily that the kernel I' of θ' is $I + (X_{n+1} - F)$. It also follows easily that if $g = g_1, \ldots, g_n$ is special in I then $g' = g_1, \ldots, g_{n+1}$ with $g_{n+1} = X_{n+1} - F$ is a special sequence in I'. The larger (size $n+1$) Jacobian matrix has the same determinant γ as the size n Jacobian matrix of $g_1, \ldots, g_n$ with respect to $X_1, \ldots, X_n$, and it is easy to check that there is an isomorphism

$$\tau\colon \frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \cong \frac{(g_1, \ldots, g_{n+1})T' :_{T'} I'}{(g_1, \ldots, g_{n+1})T'}$$

which is induced by the inclusion $(g_1, \ldots, g_n)T :_T I \subseteq (g_1, \ldots, g_{n+1})T' :_{T'} I'$. Since the Jacobian determinants are the same we have a commutative diagram

$$\begin{tikzcd}
\frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} \arrow[r, "\tau"] \arrow[d, "\Phi_{\theta,g}"'] & \frac{(g_1, \ldots, g_{n+1})T' :_{T'} I'}{(g_1, \ldots, g_{n+1})T'} \arrow[d, "\Phi_{\theta',g'}"] \\
\mathcal{L} \arrow[r, "\mathbf{1}_{\mathcal{L}}"'] & \mathcal{L}
\end{tikzcd}$$

and this yields that the images are the same.

We have now justified the notation $W_{S/R}$ when S is finitely generated over R. We leave it to the reader as an exercise to verify that if s is a nonzerodivisor in S, then $W_{S[s^{-1}]/R} = (W_{S/R})_s$. Once we know this, by exactly the same argument we used to verify that the Jacobian ideal is independent of the choice of presentation for algebras essentially of finite type over R, it follows that $W_{S/R}(\theta)$ is independent of θ when S is essentially of finite type over R. □

For a given special sequence $\underline{g}$ it is obvious from the definition of $\Phi_{\theta,\underline{g}}$ that γ multiplies the image of $\Phi_{\theta,\underline{g}}$ into $S \subseteq \mathcal{L}$. Since the image is independent of the choice of special sequence and since, by the Theorem on the existence of sufficiently many special sequences at the end of the Lecture Notes of February 11, as the special sequence varies the values of γ generate $J_{S/R}$, we have:

Corollary. $W_{S/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$. □

The following result gives several properties of $W_{S/R}$ that we will want to exploit.

Proposition. *Let S be generically étale, torsion-free and essentially of finite type over the Noetherian domain R. Let $W = W_{S/R}$.*

(a) *For any multiplicative system U in S, $W_{U^{-1}S/R} = U^{-1}W$.*

(b) *W is torsion-free over S.*

(c) *For every prime ideal P of S, if u, v is part of a system of parameters for S_P then it is a regular sequence on W_P. (Thus, W is S_2.)*

(d) *If $W \subseteq W' \subseteq \mathcal{L}$ and $W_P = W'_P$ for all height one primes of S and for all minimal primes of S that are also maximal ideals, then $W = W'$.*

(e) *If $R \to S$ is a local homomorphism of regular local rings then $\mathcal{J}_{S/R}$ is principal and $W = S :_{\mathcal{L}} \mathcal{J}_{S/R}$.*

(f) *If S is normal and R_P is regular for every prime ideal P of R lying under a height one prime ideal Q of S, then $W = S :_{\mathcal{L}} \mathcal{J}_{S/R}$.*

Proof. Part (a) is essentially the last part of (4.3), while (b) is evident from the fact that $W \subseteq \mathcal{L}$, by definition.

To prove (c) note that by (a) we may assume that S is local and that u, v is part of a system of parameters. We may choose a presentation $\theta: T \twoheadrightarrow S$ and think of W as $\cong \big((g_1, \dots, g_n)T :_T I\big)/(g_1, \dots, g_n)T$, where the sequence $g_1, \dots, g_n$ is special. Let u_0, $v_0 \in T$ be representatives of u, v. Then $u_0 + I$ cannot be contained in the union of the minimal primes of $(g_1, \dots, g_n)$, or else it will be contained in one of them by the Lemma on prime avoidance for cosets. Since this will contain I, it will be a minimal prime of I, and contradicts the statement that u is part of a system of parameters in $S = T/I$. Thus, we can replace u_0 by an element u_1 representing u such that $g_1, \dots, g_n, u_1$ is part of a system of parameters for T. Similarly, $v_0 + I$ cannot be contained in the union of the minimal primes of $(g_1, \dots, g_n, u_1)T$, or else it is contained in one of them, say Q. Thinking modulo I, we see that Q is a minimal prime of u in T/I containing v, a contradiction. Thus, we may choose u_1, v_1 in T representing u, v respectively and such that $g_1, \dots, g_n, u_1, v_1$ is a regular sequence. Clearly, u_1, v_1 form a regular sequence on $T/(g_1, \dots, g_n)T$. We claim they also form a regular sequence on the set of elements killed by I. It is clear that u_1 remains not a zerodivisor on this set. Suppose that $v_1 z = u_1 y$ where z, y are killed by I. Then $z = u_1 x$, $y = -v_1 x$ where, *a priori*, $x \in T/(g_1, \dots, g_n)T$. But $Iz = 0$ and so $Iu_1 x = 0$, and since u_1 is not a zerodivisor on $T/(g_1, \dots, g_n)T$, it follows that $Ix = 0$ as well.

Part (d) is a consequence of the result we proved in (c). If $W \neq W'$ we can localize at a minimal prime of the support of W'/W and preserve the counterexample. By hypothesis, this prime cannot have height one (nor height 0, since, if a height 0 prime is not maximal then we can localize at it in two steps: first localize at a height one prime that contains it). Thus, we may assume that S is local of height two or more, and that W'/W is a nonzero module of finite length. It follows that we can choose an element $x \in W' - W$ and part of a system of parameters u, v for S such that uz and vz are in W. The relations $v(uz) = u(vz)$

over W together with part (c) show that $uz \in uW$, and it follows that $z \in W$ after all, a contradiction.

To prove (e) note that when R is regular so is T, and so $T \to S$ will be a surjection of local rings. The kernel of such a surjection must be generated by part of a minimal set of generators for the maximal ideal of T. It follows that I is a prime and we have $I = (g_1, \ldots, g_n)T$ is itself generated by a suitable special sequence. Then $\mathcal{J}_{S/R}$ is generated by

$$\gamma = \det(\partial g_j/\partial X_i),$$

and

$$\frac{(g_1, \ldots, g_n)T :_T I}{(g_1, \ldots, g_n)T} = \frac{I :_T I}{I} = \frac{T}{I} = S$$

and Φ sends 1 to $\dfrac{1}{\gamma}$, so that $W = S\dfrac{1}{\gamma}$, and one sees that $S :_{\mathcal{L}} J_{S/R} = S :_{\mathcal{L}} \gamma S = W$, as claimed.

To prove (f) it suffices by (d) to consider the problem after localizing at a height one or zero prime Q of S, and, without affecting the issue, one may also localize R at its contraction. If the prime of S has height 0, so does its contraction to R, and both rings become regular after localization. If the prime of S has height one, then, again, both rings become regular after localization, S because it is normal and R by hypothesis. In either case the result follows from part (e). □

Lecture of February 18, 2019

A critical Lemma and the final step in the proof.

The following result of Lipman and Sathaye is exactly what is needed to establish that $W_{S/R}$ decreases as S is increased by adjoining integral fractions.

Lemma. *Let T be a commutative ring, Y an indeterminate, and J an ideal of $T[Y]$ such that J contains a monic polynomial h in Y of degree d. Suppose also that J contains an element of the form $\alpha Y - \beta$ where $\alpha, \beta \in T$ are such that $J :_{T[Y]} \alpha T[Y] = J$, i.e., such that α is not a zerodivisor modulo J. Let $\mathfrak{G} \subseteq T$ be an ideal of T with $\mathfrak{G} \subseteq J$. Then for every element $v \in T[Y]$ such that $vJ \subseteq (h, \mathfrak{G})T[Y]$ there exists an element $u \in T$ such that $u(J \cap T) \subseteq \mathfrak{G}$ and such that*

$$v \equiv u\,\frac{\partial h}{\partial Y} \text{ modulo } J.$$

Proof. We may replace T by $T/\mathfrak{G}$ and J by $J/\mathfrak{G}T[Y]$ without affecting the problem. Thus, we may assume without loss of generality that $\mathfrak{G} = (0)$. By the division algorithm we may replace v by its remainder upon division by h, and so assume that $v = \sum_{i=1}^{d} u_i Y^{d-i}$, where the $u_i \in T$. We shall show that we may take $u = u_1$, and we drop the subscript from here on. First note that $u_i(J \cap T) = (0)$ for all i: in fact since $vJ \subseteq hT[Y]$ (recall that we killed $\mathfrak{G}$) we have that $v(J \cap T)$ consists of multiples of h that have degree smaller than d, and these must be zero. In particular, $u(J \cap T) = (0)$. Likewise, $v(\alpha Y - \beta) \in hT[Y]$. The left hand side has degree at most d and coefficient αu in degree d, and so we must have $v(\alpha Y - \beta) = \alpha uh$. Differentiating with respect to Y yields

$$\frac{\partial v}{\partial Y}(\alpha Y - \beta) + v\alpha = \alpha u \frac{\partial h}{\partial Y}$$

and since $\alpha Y - \beta \in J$, we have that

$$\alpha(v - u \frac{\partial h}{\partial Y}) \equiv 0 \text{ modulo } J.$$

Since α is not a zerodivisor modulo J, the required result follows. □

We now use this to prove:

Theorem. *If S_1 is obtained from S by adjoining finitely many integral fractions of $\mathcal{L}$, then $W_{S_1/R} \subseteq W_{S/R}$.*

Proof. By induction on the number of fractions adjoined, it is obviously sufficient to prove this when $S_1 = S[\lambda]$, where λ is a single element of $\mathcal{L}$. Choose a presentation $\theta\colon T \to S$ and a special sequence $g_1, \ldots, g_n$ in the kernel I. Let Y be a new indeterminate and extend θ to a map $T[Y] \twoheadrightarrow S[\lambda]$ by sending Y to λ. Since λ is integral over S there is a monic polynomial $h = h(Y) \in T[Y]$ of degree say, d, in the kernel J of $T[Y] \twoheadrightarrow S[\lambda]$. If $\lambda \in S$ there is nothing to prove so that we may assume that $d \geq 2$. Since λ is in $\mathcal{L}$ we may also choose α and β in T with α not a zerodivisor on J such that $\alpha Y - \beta$ is in the kernel. Consider the image of $h(Y)$ in $S[Y]$. There will be a certain subset of the minimal primes of S such that the image of λ is a multiple root of the image of h modulo those primes. If that set of primes is empty, we shall not alter h. If it is not empty choose an element of S that is not in any of those minimal primes but that is in the others, and represent it by an element $t \in T$. Then $h(Y) + t(\alpha Y - \beta)$ has the property that its image modulo any minimal prime of S has the image of λ as a simple root, and so we may assume, using this polynomial in place of the original choice of h, that h is a monic polynomial of degree $d \geq 2$ such that image of λ modulo every minimal prime of $\mathcal{L}$ is a simple root of the image of h.

Because h is monic in Y, the sequence $g_1, \ldots, g_n$, h is a regular sequence, and the Jacobian determinant with respect to $X_1, \ldots, X_n$, Y is $\gamma \frac{\partial h}{\partial Y}$, where γ is $\det(\partial g_j/\partial X_i)$. Our choice of h implies that $\frac{\partial h}{\partial Y}$ has image that is not in any minimal prime of $\mathcal{L}$, and it follows that $g_1, \ldots, g_n$, h is a special sequence in J and can be used to calculate $W_{S[\lambda]/R}$. Let $v \in (g_1, \ldots, g_n, h)T[Y] :_{T[Y]} J$. We may now apply the preceding Lemma with this

T, Y, J, v, α, β and h, while taking $\mathfrak{G} = (g_1, \, \dots \, , g_n)T$. Note that $J \cap T = I$. Observe as well that v gives rise to a typical element of the module $W_{S[\lambda]/R}$, namely the image of $v/(\gamma \, \dfrac{\partial h}{\partial Y})$ in $\mathcal{L}$, We want to show that this element is in $W_{S/R}$. Pick u as in the preceding Lemma. Then $u \in (g_1, \, \dots \, , g_n)T :_T I$ and since $v \equiv u \, \dfrac{\partial h}{\partial Y}$ modulo J, this image is the same as the image of $(u \, \dfrac{\partial h}{\partial Y})/(\gamma \, \dfrac{\partial h}{\partial Y}) = u/\gamma$, and so is in $W_{S/R}$, as required. □

The proof of the Jacobian theorem. We can now complete the proof of the theorem as already indicated in the Sketch of the proof of the Jacobian theorem in the Lecture of February 8. We know that S' is module-finite over S and can therefore be obtained from S by adjoining finitely many elements of the total quotient ring that are integral over S. We then have

$$S' :_{\mathcal{L}} \mathcal{J}_{S'/R} = W_{S'/R} \subseteq W_{S/R} \subseteq S :_{\mathcal{L}} \mathcal{J}_{S/R}$$

where the equality on the left follows from part (f) of the Proposition on p. 4 of the Lecture Notes of February 15, the middle inclusion follows from the Theorem above, and the inclusion on the right follows from the Corollary on p. 4 of the Lecture Notes of February 15. □

Lecture of February 20, 2019

If $I \subseteq J$ and J is integral over I, we call I a *reduction* of J. With this terminology, we have shown that if $(R, \, m, \, K)$ is local with K infinite, every ideal $I \subseteq m$ has a reduction with $\mathfrak{an}(I)$ generators, and one cannot do better than this whether K is infinite or not.

We have previously defined analytic spread for ideals of local rings. We can give a global definition as follows: if R is Noetherian and I is any ideal of R, let

$$\mathfrak{an}(I) = \sup\{P \in \mathrm{Spec}\,(R) : \mathfrak{an}(IR_P)\},$$

which is bounded by the the number of generators of I and also by the dimension of R.

The Briançon-Skoda theorem then gives at once:

Theorem. *Let R be regular and I an ideal. Let $n = \mathfrak{an}(I)$. Then for all $k \geq 1$, $\overline{I^{n+k-1}} \subseteq I^k$.*

Proof. If the two are not equal, this can be preserved while passing to a local ring of R. Thus, without loss of generality, we may assume that R is local. The result is unaffected by replacing R by $R(t)$, if necessary. Thus, we may assume that the residue class field of R is infinite. Then I has a reduction I_0 with n generators. From the form of the Briançon-Skoda theorem that we have already proved, we have that $\overline{I^{n+k-1}} = \overline{I_0^{n+k1}} \subseteq I_0^k \subseteq I$. □

The intersection of all ideals I_0 in I such that I is integral over I_0 is called the *core* of I. It is not immediately clear that the core is nonzero, but we have:

Theorem. *Let R be regular local with infinite residue class field, and let I be a proper ideal with $\mathfrak{an}(I) = n$. Then the core of I contains $\overline{I^n}$.*

Proof. If I is integral over I_0 then they have the same analytic spread, and I_0 has a reduction I_1 with n generators. Then $\overline{I^n} = \overline{I_0^n} = \overline{I_1^n} \subseteq I_1 \subseteq I_0$, and so $\overline{I^n}$ is contained in all such I_0. □

We next want to give a proof of the Briançon-Skoda theorem in characteristic p that is, in many ways, much simpler than the proof we have just given. The characteristic p result can be used to prove the equal characteristic 0 case as well.

Recall that when $x_1, \, \dots, x_d$ is a regular sequence on M, we require not only that x_i is a nonzerodivisor on $M/(x_1, \, \dots, x_{i-1})M$ for $1 \leq i \leq d$, but also that $(x_1, \, \dots, x_d)M \neq M$. If $(x_1, \, \dots, x_d)$ has radical m in the lcoal ring $(R, \, m, \, K)$, this is equivalent to the assertion $mM \neq M$, for otherwise we get that $m^tM = M$ for all t, and for large t, $m^t \subseteq (x_1, \, \dots, x_d)$.

Note that when $x_1, \, \dots, x_d$ is a regular sequence in a ring R and M is flat, we continue to have that x_i is a nonzerodivisor on $M/(x_1, \, \dots, x_{i-1})M$ for $1 \leq i \leq d$ (by induction on d this redues to the case where $d = 1$ and the fact that $x = x_1$ is a nonzerodivisor on R give an exact sequence

$$0 \to R \xrightarrow{\cdot x} R$$

which stays exact when we tensor with M over R). If M is faithfully flat, every regular sequence in R is a regular sequence on M. If R is regular, this characterizes faithful flatness:

Lemma. *Let (R, m, K) be local. Then M is faithfully flat over R if and only if every regular sequence in R is a regular sequence on M.*

Proof. By the preceding discussion, we need only prove the "if" part. It will suffice to prove that for every R-module N, $\mathrm{Tor}_i^R(N, M) = 0$ for all $i \geq 1$. Since N is a direct limit of finitely generated modules, it suffices to prove this when N is finitely generated. We use reverse induction on i. We have the result for $i > \dim(R)$ because $\dim(R)$ bounds the projective dimension of N. We assume the result for $i \geq k+1$, where $k \geq 1$, and prove it for $i = k$. Since N has a filtration by prime cyclic modules, it suffices to prove the vanishing when N is a prime cyclic module R/P. Let $x_1, \, \dots, x_d$ be a maximal regular sequene of R in P. Then P is a minimal prime of $(x_1, \, \dots, x_d)$, and, in particular, an associated prime. It follows that we have a short exact sequence

$$0 \to R/P \to R/(x_1, \, \dots, x_dR) \to C \to 0$$

for some module C. By the long exact sequence for Tor, we have

$$\cdots \to \mathrm{Tor}_{k+1}^R(C, \, M) \to \mathrm{Tor}_k^R(R/P, M) \to \mathrm{Tor}_k^R\big(R/(x_1, \, \dots, x_d)R, M\big) \to \cdots .$$

The leftmost term vanishes by the induction hypothesis and the rightmost term vanishes by problem 4 of Problem Set #3. □

We write F or F_R for the Frobenius endomorphism of a ring R of positive prime characteristic p. Thus $F(r) = r^p$. We write F^e or F^e_R for the eth iterate of F under composition. Thus, $F^e(r) = r^{p^e}$.

Corollary. *Let R be a regular Noetherian ring of positive prime characteristic p. Then $F^e : R \to R$ is faithfully flat.*

Proof. The issue is local on primes P of the first (left hand) copy of R. But when we localize at $R - P$ in the first copy, we find that for each element $u \in R - P$, u^{p^e} is invertible, and this means that u is invertible. Thus, when we local we get $F^e : R_P \to R_P$. Thus, it suffices to consider the local case. But if $x_1, \ldots , x_d$ is a regular sequence in R_P, it operates on the right hand copy as $x_1^{p^e}, \ldots , x_d^{p^e}$, which is regular in R_P. □

If I, $J \subseteq R$, we write $I :_R J$ for $\{r \in R : rJ \subseteq I\}$, which is an ideal of R.

Proposition. *Let I and J be ideals of the ring R such that J is finitely generated. Let S be a flat R-algebra. Then $(I :_R J)S = IS :_S JS$.*

Proof. Note that if $\mathfrak{A} \subseteq R$, $\mathfrak{A} \otimes_R S$ injects into S, since S is flat over R. But its image is $\mathfrak{A}S$. Thus, we may identify $\mathfrak{A} \otimes_R S$ with $\mathfrak{A}S$.

Let $J = (f_1, \ldots , f_h)R$. Then we have an exact sequece

$$0 \to I :_R J \to R \to (R/I)^{\oplus h}$$

where the rightmost map sends r to the image of $(rf_1, \ldots , rf_h)$ in $(R/I)^{\oplus h}$. This remains exact when we tensor with S over R, yielding an exact sequence:

$$0 \to (I :_R J)S \to S \to (S/IS)^{\oplus h}$$

where the rightmost map sends s to the image of $(sf_1, \ldots , sf_h)$ in $(S/IS)^{\oplus h}$. The kernel of the rightmost map is $IS :_S JS$, and so $(I :_R J)S = IS :_S JS$. □

When R has positive prime characteristic p, we frequently abbreviate $q = p^e$, and $I^{[q]}$ denotes the expansion of $I \subseteq R$ to $S = R$ where, however, the map $R \to R$ that gives the structural homomorphism of the algebra is F^e. Thus, $I^{[q]}$ is generated by the set of elements $\{i^q : i \in I\}$. Whenever we expand an ideal I, the images of generators for I generate the expansion. In particular, note that if $I = (f_1, \ldots , f_n)R$, then $I^{[q]} = (f_1^q, \ldots , f_n^q)R$. Note that it is *not* true $I^{[q]}$ consists only of qth powers of elements of I: one must take R-linear combinations of the qth powers. Observe also that $I^{[q]} \subseteq I^q$, but that I^q typically needs many more generators, namely all the monomials of degree q in the generators involving two or more generators.

Corollary. *Let R be a regular ring and let I and J be any two ideals. Then $(I :_R J)^{[q]} = I^{[q]} :_R J^{[q]}$.*

Proof. This is the special case of in which $S = R$ and the flat homomorphism is F^e. □

The following result is a criterion for membership in an ideal of a regular domain of characteristic $p > 0$ that is slightly weaker, *a priori*, than being an element of the ideal. This criterion turns out to be extraordinarily useful.

Theorem. *Let R be a regular domain and let $I \subseteq R$ be an ideal. Let $r \in R$ be any element. Let $c \in R - \{0\}$. Then $r \in I$ if and only if for all $e \gg 0$, $cr^{p^e} \in I^{[p^e]}$.*

Proof. The necessity of the second condition is obvious. To prove sufficiency, suppose that there is a counterexample. Then r satisfies the condition and is not in I, and we may localize at a prime in the support of $(I + rR)/I$. This give a counterexample in which $(R,\, m)$ is a regular local ring. Then $cx^{p^e} \in I^{[p^e]}$ for all $e \geq e_0$ implies that

$$c \in I^{[p^e]} :_R (xR)^{[p^e]} = (I :_R xR)^{[p^e]} \subseteq m^{[p^e]} \subseteq m^{p^e}$$

for all $e \geq e_0$, and so $c \in \bigcap_{e \geq e_0} m^{p^e}$. But this is 0, since the intersection of the powers of m is 0 in any local ring, contradicting that $c \neq 0$. □

We can now give a characteristic p proof of the Briançon-Skoda Theorem, which we restate:

Theorem (Briançon-Skoda). *Let R be a regular ring of positive prime characteristic p. Let I be an ideal generated by n elements. Then for every positive integer k, $\overline{I^{n+k-1}} \subseteq I^k$.*

Proof. If $n = 0$ then $I = (0)$ and there is nothing to prove. Assume $n \geq 1$. Suppose $u \in \overline{I^{n+k-1}} - I^k$. Then we can preserve this while localizing at some prime ideal, and so we may assume that R is a regular domain. By part (f) of theTheorem on the first page of the Lecture Notes of January 18, the fact that $u \in \overline{I^{n+k-1}}$ implies that there is an element $c \in R - \{0\}$ such that $cu^N \in (I^{n+k-1})^N$ for all N. In particular, this is true when $N = q = p^e$, a power of the characteristic. Let $I = (f_1, \, \ldots \, , f_n)$. We shall show that $(I^{n+k-1})^q \subseteq (I^k)^{[q]}$. A typical generator of $(I^{n+k-1})^q$ has the form $f_1^{a_1} \cdots f_n^{a_n}$ where $\sum_{i=1}^n a_i = (n + k - 1)q$. For every i, $1 \leq i \leq n$, we can use the division algorithm to write $a_i = b_i q + r_i$ where $b_i \in \mathbb{N}$ and $0 \leq r_i \leq q - 1$. Then

$$(n + k - 1)q = \sum_{i=1}^n a_i = (\sum_{i=1}^n b_i)q + \sum_{i=1}^n r_i \leq (\sum_{i=1}^n b_i)q + n(q - 1)$$

which yields

$$(\sum_{i=1}^n b_i)q \geq (n + k - 1)q - nq + n = (k - 1)q + n$$

and so $\sum_{i=1} b_i \geq k - 1 + \frac{n}{q} > k - 1$, and this shows that $\sum_{i=1}^n b_i \geq k$, as required □

Lecture of February 22, 2019

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. □

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 $z_i = \theta_i$, $1 \leq i \leq n$. 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. □

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. □

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. □

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. □

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 $d!\lim_{n\to\infty}\dfrac{\ell(N/m^{n+1}N)}{n^d} = 0$.*

(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 $M_n = I^nN \cap M$, 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 $I^{n+c}N \cap M \subseteq I^nM$, so that $I^{n+c}M \subseteq I^{n+c}N \cap M \subseteq I^nM$. 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 January 16. Then $e_J(M) = e_J(J^kM)$ by part (e) of the Proposition above, and so

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

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

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

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. □

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 $\dim(S) = \dim(S/xS) + 1 = \dim(R/xR) + 1 = \dim(R)$. □

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. □

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.

Lecture of February 25, 2019

One of our goals is to discuss what is known about the following conjecture of C. Lech, which has been an open question for over forty years.

Conjecture. *If $R \to S$ is a flat local map of local rings, then $e(R) \le e(S)$.*

This is open even in dimension three when S is module-finite and free over R. Note that one can immediately reduce to the case where both rings are complete.

Under mild conditions, a local ring R of multiplicity 1 is regular: it suffices if the completion $\widehat{R}$ has no associated prime P such that $\dim(\widehat{R}/P) < \dim(\widehat{R})$. Therefore, the following result is related to Lech's conjecture:

Theorem. *If S is faithfully flat over R and S is regular then R is regular. In particular, if $(R,\, m,\, K) \to (S,\, \mathfrak{n},\, L)$ is a flat local map of local rings and S is regular, then R is regular.*

Proof. The second statement implies the first, for if P is any prime of R then some prime Q of S lies over P, and we can apply the second statement to $R_P \to S_Q$ to conclude that R_P is regular.

To prove the second statement, let

$$(*) \quad \cdots \to G_n \to \cdots \to G_1 \to G_0 \to R \to R/m \to 0$$

be a minimal resolution of R/m over R. Then the matrix α_i of the map $G_i \to G_{i-1}$ has entries in m for all $i \ge 1$. Since S is R-flat, the complex obtained by applying $S \otimes_R \_$, namely

$$(**) \quad \cdots \to S \otimes_R G_n \to \cdots \to S \otimes_R G_1 \to S \otimes_R G_0 \to S/mS \to 0$$

gives an S-free resolution of S/mS over R. Moreover, the entries of the matrix of the map $S \otimes G_i \to S \otimes_R G_{i-1}$ are simply the images of the entries of the matrix α_i in S: these are in $\mathfrak{n}$, and so the complex given in $(**)$ is a *minimal* free resolution of S/mS over S. Thus, all of its terms are eventually 0, and this implies that all of the terms of $(*)$ are eventually 0. Hence, K has finite projective dimension over R, which implies that R is regular. □

Before treating Lech's conjecture itself, we want to give several other characterizations of $e_I(M)$ when I is generated by a system of parameters. There is a particularly simple characterization in the Cohen-Macaulay case. We first recall some facts about regular sequences. The results we state in the Proposition below are true for an arbitrary regular sequence on an arbitrary module. However, we only indicate proofs for the situation where R is local, M is a finitely generated R-module, and $x_1, \ldots, x_d$ are elements of the maximal ideal of R. The proofs are valid whenever we are in a situation where regular sequences are permutable, which makes the arguments much easier. (There is a treatment of the case where the regular sequence is not assumed to be permutable in the Extra Credit problems in Problem Sets #2 and #3 from Math 615, Winter, 2004. It is assumed that $M = R$ there, but the proofs are completely unchanged in the module case.) Recall that, in all cases, by virtue of the definition, the fact that $x_1, \ldots, x_d$ is a regular sequence on M implies that $(x_1, \ldots, x_d)M \neq M$.

Proposition. *Let $x_1, \ldots, x_d \in R$, let $I = (x_1, \ldots, x_d)R$, and let M be an R-module.*

(a) *Let $t_1, \ldots, t_d$ be nonnegative integers. Then $x_1, \ldots, x_d$ is a regular sequence if and only if $x_1^{t_1}, \ldots, x_d^{t_d}$ is a regular sequence on M.*

(b) *If $x_1, \ldots, x_d$ is a regular sequence on M, and $a_1, \ldots, a_d$ are nonnegative integers, then $x_1^{a_1} \cdots x_d^{a_d} w \in (x_1^{a_1+1}, \ldots, x_d^{a_d+1})M$ implies that $w \in (x_1, \ldots, x_d)M$.*

(c) *If $x_1, \ldots, x_d$ is a regular sequence on M, $\mu_1, \ldots, \mu_N$ are the monomials of degree n in $x_1, \ldots, x_d$, and $w_1, \ldots, w_N$ are elements of M such that $\sum_{j=1}^{N} \mu_j w_j \in I^{n+1}M$, then every $w_j \in IM$.*

(d) *If $x_1, \ldots, x_d$ is a regular sequence on M, then $\mathrm{gr}_I(M)$ may be identified with*

$$(M/IM) \otimes_{R/I} (R/I)[X_1, \ldots, X_d],$$

where the X_j are indeterminates and for nonnegative integers $a_1, \ldots, a_d$ such that $\sum_{j=1}^{d} a_j = n$, the image of $x_1^{a_1} \cdots x_d^{a_d} M$ in $I^n M/I^{n+1}M$ corresponds to

$$(M/IM)X_1^{a_1} \cdots X_d^{a_d}.$$

(e) *If $x_1, \ldots, x_d$ is a regular sequence on M, then $M/I^{n+1}M$ has a filtration in which the factors are $\binom{n+d}{d}$ copies of M/IM.*

Proof. (a) It suffices to prove the statement in the case where just one of t_i is different from 1: we can adjust the exponents on one element at a time. Since R-sequences are permutable, it suffices to do the case where only t_d is different from 1, and for this purpose we may work with $M/(x_1, \ldots, x_{d-1})M$. Thus, we may assume that $d = 1$, and the assertion we need is that x^t is a nonzerodivisor if and only if x is. Clearly, if $xw = 0$ then $x^t w = 0$, while if $x^t w = 0$ for t chosen as small as possible and $w \neq 0$ then $x(x^{t-1}w) = 0$.

(b) If all the a_i are zero then we are already done. If not, we use induction on the number of $a_i > 0$. Since we are assuming a situation in which R-sequences on a module are permutable we may assume that $a_d > 0$. Then

$$x_1^{a_1} \cdots x_d^{a_d} w = \sum_{j=1}^{d-1} x_j^{a_j+1} w_j + x_d^{a_d+1} w_d$$

for elements $w_1, \dots, w_d \in M$. Then

$$x_d^{a_d}(x_1^{a_1} \cdots x_{d-1}^{a_{d-1}} w - x_d w_d) \in (x_1^{a_1+1}, \dots, x_{d-1}^{a_{d-1}+1})M,$$

and since $x_1^{a_1+1}, \dots, x_{d-1}^{a_{d-1}}, x_d^{a_d}$ is also a regular sequence on M, we have that

$$x_1^{a_1} \cdots x_{d-1}^{a_{d-1}} w - x_d w_d \in (x_1^{a_1+1}, \dots, x_{d-1}^{a_{d-1}+1})M.$$

This yields that

$$x_1^{a_1} \cdots x_{d-1}^{a_{d-1}} w \in (x_1^{a_1+1}, \dots, x_{d-1}^{a_{d-1}+1}, x_d)M,$$

providing an example in which the number of $a_j > 0$ has decreased. This is a contradiction.

(c) Fix one of the $\mu_j = x_1^{a_1} \cdots x_d^{a_d}$. Then in every other μ_k and in every monomial of degree $n+1$, at least one x_i occurs with exponent a_i+1. Thus, $\mu_j w \in (x_1^{a_1+1}, \dots, x_d^{a_d+1})M$, and $w_j \in IM$ by part (b).

(d) For each monomial $\widetilde{\mu}$ in $X_1, \dots, X_d$ we write μ for the corresponding monomial in $x_1, \dots, x_d$. We define a map from

$$I^n M \to \bigoplus_{\deg(\widetilde{\mu})=n} (M/IM)\widetilde{\mu}$$

by sending $\sum_i \mu_j w_j \mapsto \sum_j \widetilde{\mu_j}\overline{w}_j$, where $\overline{w_j}$ is the image of $w_j \in M$ in M/IM. This map is well-defined by part (c), and is obviously surjective. The elements of $I^{n+1}M$ are precisely those elements of M which can be represented as $\sum_i \mu_j w_j$ with every $w_j \in IM$, and it follows at once that the kernel of the map is $I^{n+1}M$.

(e) This follows at once from part (d), since we can initially use a filtration with factors $I^k M/I^{k+1}M$, $0 \le k \le n$, and then refine it because each of these splits into a direct sum of copies of M/IM such that the number of copies is the same as the number of monomials of degree k in $X_1, \dots, X_d$. The number of monomials of degree at most d is $\binom{n+d}{d}$. □

We next note:

Theorem. *If (R, m, K) is local of dimension d, M is Cohen-Macaulay of dimension d over R, $x_1, \dots, x_d$ is a regular sequence on M, and $I = (x_1, \dots, x_d)$, then $e_I(M) = \ell\big(M/(x_1, \dots, x_d)M\big)$.*

Proof. By part (e) of the Lemma just above, we have that $M/I^{n+1}M$ has a filtration such that

(1) Every factor is $\cong M/IM$.

(2) The number of factors is $\binom{n+d}{d}$, i.e., is the same as the number of monomials of degree at most n in d indeterminates $X_1, \dots, X_d$.

This gives the result, for we then have

$$\ell(M/I^{n+1}M) = \binom{n+d}{d}\ell(M/IM),$$

and the leading term of $\binom{n+d}{d}$ is $\dfrac{n^d}{d!}$. □

Theorem. *Let $(R,\, m,\, K)$ be module-finite over a regular local ring A such that $x_1,\, \ldots\, , x_d$ is a regular system of parameters of A, and let M be an R-module of dimension d. Let $I = (x_1,\, \ldots\, , x_d)R$. Then $e_I(M)$ is the torsion-free rank of M over A.*

Proof. From the definition, it does not matter whether we think of M as an R-module, or whether we think of it as an A-module with maximal ideal $\mathfrak{n} = (x_1,\, \ldots\, , x_d)A$. In the latter case, if ρ is the torsion-free rank of M as an A-module, we have an exact sequence of A-modules

$$0 \to A^\rho \to M \to C \to 0$$

where C is a torsion A-module, so that $\dim(C) < d$. It follows that

$$e_I(M) = e_{\mathfrak{n}}(M) = re_{\mathfrak{n}}(A) + 0 = r\ell\bigl(A/(x_1,\, \ldots\, , x_d)A\bigr) = r \cdot 1 = r.$$

□

Discussion. If R is equicharacteristic, we can always reach the situation of the Theorem above. The mulltiplicity does not change if we replace R by $\widehat{R}$. But then we can choose a coefficient field K, and the structure theorems for complete local rings guarantee that R is module-finite over $A = K[[x_1,\, \ldots\, , x_d]] \subseteq \widehat{R}$.

More generally:

Theorem. *Let R be module-finite over a Cohen-Macaulay local ring B such that $x_1,\, \ldots\, , x_d$ is a system of parameters for B. Let M be an R-module of dimension d. Let $I = (x_1,\, \ldots\, , x_d)R$. If B is a domain, $e_I(M) = \ell(B/IB)\rho$, where ρ is the torsion-free rank of M over B. When B is not a domain, if there is a short exact sequence*

$$0 \to B^\rho \to M \to C \to 0$$

with $\dim(C) < d$, *then* $e_I(M) = \ell(B/IB)\rho$.

Proof. $\ell(M/I^{n+1})M$ is independent of whether one thinks of $x_1,\, \ldots\, , x_d$ as in B or in R. Thus, we can replace R by B. The result is then immediate from our results on additivity of multiplicity and the fact that when B is Cohen-Macaulay, $e_I(B) = \ell(B/I)$. □

We want to give a different characterization of multiplicities due to C. Lech. If $\underline{n} = n_1,\, \ldots\, , n_d$ is a d-tuple of nonnegative integers and f is a real-valued function of $\underline{n}$, we write $\lim\limits_{\underline{n}\to\infty} f(\underline{n}) = r$, where $r \in \mathbb{R}$, to mean that for all $\epsilon > 0$ there exists N such that for all $\underline{n} = n_1, \,\ldots\,, n_d$ satisfying $n_i \geq N$, $1 \leq i \leq d$, we have that $|f(\underline{n}) - r| < \epsilon$. One might also write $\lim\limits_{\min \underline{n}\to\infty} f(\underline{n}) = r$ with the same meaning. If $\underline{x} = x_1, \,\ldots\,, x_d$ is a system of parameters for R, we temporarily define the *Lech multiplicity* $e^{\mathrm{L}}_{\underline{x}}(M)$ to be

$$\lim_{\underline{n}\to\infty} \frac{\ell\bigl(M/(x_1^{n_1}, \,\ldots\,, x_d^{n_d})M\bigr)}{n_1 \cdots n_d}.$$

We shall show that the limit always exists, is 0 if $\dim(M) < d$, and, with $I = (x_1, \,\ldots\,, x_d)R$, is $e_I(M)$ when $\dim(M) = d$.

We first prove:

Lemma. *Let $\underline{x} = x_1, \,\ldots\,, x_d$, $d \geq 1$, be a system of parameters for a local ring (R, m, K) and let M', M, and M'' be finitely generated R-modules. Given $\underline{n} = n_1, \ldots, n_d$, let $I_{\underline{n}} = (x_1^{n_1}, \,\ldots\,, x_d^{n_d})R$, and let $\mathcal{L}_{\underline{n}}(M) = \ell(M/I_{\underline{n}}M)/n_1 \cdots n_d$.*

(a) *If*
$$0 \to M' \to M \to M'' \to 0$$
is exact, then for any m-primary ideal J,
$$\ell(M''/JM'') \leq \ell(M/JM) \leq \ell(M'/JM') + \ell(M''/JM''),$$
i.e.,
$$0 \leq \ell(M/JM) - \ell(M''/JM'') \leq \ell(M'/JM').$$
Hence, for all $\underline{n}$,
$$\mathcal{L}_{\underline{n}}(M'') \leq \mathcal{L}_{\underline{n}}(M) \leq \mathcal{L}_{\underline{n}}(M') + \mathcal{L}_{\underline{n}}(M''),$$
i.e.,
$$0 \leq \mathcal{L}_{\underline{n}}(M) - \mathcal{L}_{\underline{n}}(M'') \leq \mathcal{L}_{\underline{n}}(M').$$
Therefore, if the three limits exist,
$$e^{\mathrm{L}}_{\underline{x}}(M'') \leq e^{\mathrm{L}}_{\underline{x}}(M) \leq e^{\mathrm{L}}_{\underline{x}}(M') + e^{\mathrm{L}}_{\underline{x}}(M''),$$
If $e^{\mathrm{L}}_{\underline{x}}(M') = 0$ and $e^{\mathrm{L}}_{\underline{x}}(M'') = 0$, then $e^{\mathrm{L}}_{\underline{x}}(M) = 0$.

(b) *If M has a finite filtration with factors N_j we have that for any m-primary ideal J, $\ell(M/JM) \leq \sum_j \ell(N_j/JN_j)$. Hence, for all $\underline{n}$, $\mathcal{L}_{\underline{n}}(M) \leq \sum_j \mathcal{L}_{\underline{n}}(N_j)$, and $e^{\mathrm{L}}_{\underline{x}}(M) = 0$ whenever $e^{\mathrm{L}}_{\underline{x}}(N_j) = 0$ for all j.*

(c) *If $\dim(M) < d$ then $e^{\mathrm{L}}_{\underline{x}}(M) = 0$.*

(d) *If $0 \to M' \to M \to M'' \to 0$ is exact and $\dim(M') < d$, then $e^{\mathrm{L}}_{\underline{x}}(M)$ and $e^{\mathrm{L}}_{\underline{x}}(M'')$ exist or not alike, and if they exist they are equal.*

(e) *If each of M and M' embeds in the other so that the cokernel has dimension $< d$, then $e^{\mathrm{L}}_{\underline{x}}(M)$ and $e^{\mathrm{L}}_{\underline{x}}(M')$ exist or not alike, and they are equal.*

Proof. Part (a) follows because we have an exact sequence of finite length modules

$$0 \to M'/(JM \cap M') \to M/JM \to M''/JM \to 0 \to 0$$

and $JM \cap M' \supseteq JM'$, so that

$$\ell\bigl(M'/(JM \cap M')\bigr) \geq \ell(M'/JM').$$

The remaining statements in part (a) follow at once.

Part (b) follows from part (a) by a straightforward induction on the length of the filtration.

To prove (c) we may use induction on d. If $d = 1$ then $\dim(M) = 0$, so that $\ell(M/I_{\underline{n}}M) = \ell(M)$ is constant for all sufficiently large $\underline{n}$, while the denominator $n_1 \to \infty$. If $d > 1$ we first take a finite prime cyclic filtration of M. Thus, we may assume without loss of generality that M is a prime cyclic module. If $\dim(M) = 0$, we again have a constant numerator and a denominator that $\to \infty$, and so we may assume $\dim(M) > 0$. Since the x_i generate a primary ideal, some x_i does not kill $M = R/Q$, and so is a nonzerodivisor on M. By renumbering, we assume that $i = d$. Consider $\underline{n} = n_1, \, \ldots \, , n_d$ and let $\underline{n}^- = n_1, \, \ldots \, , n_{d-1}$, let $\underline{x}^- = x_1, \, \ldots \, , x_{d-1}$, and let $I_{\underline{n}^-} = (x_1^{n_1}, \, \ldots \, , \, x_{d-1}^{n_{d-1}})R$. Then

$$\frac{M}{I_{\underline{n}}M} = \frac{M}{(I_{\underline{n}^-} + x_d^{n_d})M} \cong \frac{M/x_d^{n_d}M}{I_{\underline{n}^-}(M/x_d^{n_d}M)}.$$

Note that $M/x_d^{n_d}M$ has a filtration with n_d factor modules N_j, $0 \leq j \leq n_d - 1$, where $N_j = x_d^jM/x_d^{j+1}M \cong M/x_dM$, and so with $\overline{M} = M/x_dM$, we have that $\ell(M/I_{\underline{n}}M) \leq n_d\ell(\overline{M}/I_{\underline{n}^-}\overline{M})$. It follows that

$$(*) \qquad \frac{\ell(M/I_{\underline{n}}M)}{n_1 \cdots n_d} \leq \frac{n_d\ell(\overline{M}/I_{\underline{n}^-}\overline{M})}{n_1 \cdots n_{d-1}n_d} = \frac{\ell(\overline{M}/I_{\underline{n}^-}\overline{M})}{n_1 \cdots n_{d-1}}.$$

We may view $\overline{M}$ as a module over $R/x_d^{n_d}R$, and

$$\dim(\overline{M}) < \dim(M) \leq \dim(R) - 1 = \dim(R/x_d^{n_d}).$$

By the induction hypothesis, $e^{\mathrm{L}}_{\underline{x}^-}(\overline{M}) = 0$ (working over $R/x_d^{n_d}R$), and it follows from $(*)$ that $e^{\mathrm{L}}_{\underline{x}}(M) = 0$ as well.

For part (d), note that (a) implies that $|\mathcal{L}_{\underline{n}}(M) - \mathcal{L}_{\underline{n}}(M'')| \leq \mathcal{L}_{\underline{n}}(M')$, and we are assuming that $\mathcal{L}_{\underline{n}}(M') \to 0$ as $\underline{n} \to \infty$.

Finally, for part (e), note that if we have short exact sequences

$$0 \to M' \to M \to C_1 \to 0 \quad \text{and} \quad 0 \to M \to M' \to C_2 \to 0$$

then from the first we have $\mathcal{L}_{\underline{n}}(M) - \mathcal{L}_{\underline{n}}(M') \leq \mathcal{L}_{\underline{n}}(C_1)$ and from the second we have $\mathcal{L}_{\underline{n}}(M') - \mathcal{L}_{\underline{n}}(M) \leq \mathcal{L}_{\underline{n}}(C_2)$. Hence, $|\mathcal{L}_{\underline{n}}(M) - \mathcal{L}_{\underline{n}}(M')| \leq \max\{\mathcal{L}_{\underline{n}}(C_1), \mathcal{L}_{\underline{n}}(C_2)\} \to 0$ as $\underline{n} \to \infty$. □

Lecture of February 27, 2019

Proposition. *Let M be an R-module. Let*

(a) *If M has a finite filtration with factors N_j, $1 \leq j \leq s$, and x is a nonzerodivisor on every N_j, then M/xM has a filtration with s factors N_j/xN_j, and M/x^nM has a filtration with ns factors: there are n copies of every N_j/xN_j, $1 \leq j \leq s$.*

(b) *If $x_1, \ldots, x_d$ is a regular sequence on M and $n_1, \ldots, n_d$ are nonnegative integers, then $M/(x_1^{n_1}, \ldots, x_d^{n_d})M$ has a filtration by $n_1 \cdots n_d$ copies of $M/(x_1, \ldots, x_d)M$.*

Proof. (a) By induction on the number of factors, this comes down to the case where there are two factors. That is, one has $0 \to N_1 \to M \to N_2 \to 0$. This has an isomorphic subcomplex $0 \to xN_1 \to xM \to xN_2 \to 0$, and the desired statement now follows from the exactness of the quotient complex. It follows as well that M/x^nM has a filtration by the modules N_j/x^nN_j, and each of these has a filtration with n factors, $x^kN_j/x^{k+1}N_j \cong N_j/xN_j$, $0 \leq k \leq n-1$.

For part (b) we use induction on d. The case $d = 1$ has already been handled in part (a). For the inductive step, we know that $M/(x_1^{n_1}, \ldots, x_{d-1}^{n_{d-1}})M$ has a filtration by $n_1 \cdots n_{d-1}$ copies of $M/(x_1, \ldots, x_{d-1})M$, and $x = x_d$ is a nonzerodivisor on each of these. The result now follows from the last statement in part (a), with $n = n_d$. □

We next observe:

Lemma. *Let R be a Noetherian ring and let M be a finitely generated R-module of dimension $d > 0$.*

(a) *M contains a maximum submodule N such that $\dim(N) < d$, and M/N has pure dimension d, i.e., for every $P \in \mathrm{Ass}\,(M/N)$, $\dim\,(R/P) = d$.*

(b) *Let W be a multiplicative system of R consisting of nonzerodivisors and suppose that M and M' are R-modules such that $W^{-1}M \cong W^{-1}M'$. Then there exist exact sequences $0 \to M' \to M \to C_1 \to 0$ and $0 \to M \to M' \to C_2 \to 0$ such that each of C_1 and C_2 is killed by a single element of W.*

(c) *Let (R, m, K) be a complete local ring of dimension d, and let M be a finitely generated faithful R-module of pure dimension d. Let $x_1, \ldots, x_d$ be a system of parameters for R. If R contains a field there is a coefficient field $K \subseteq R$ for R, and M is a torsion-free module over $A = K[[x_1, \ldots, x_d]]$, so that for some integer $\rho > 0$, M and A^ρ become isomorphic when we localize at $W = A - \{\{0\}$.*

In mixed characteristic, there exists Cohen-Macaulay ring $A \subseteq R$ containing $x_1, \dots, x_d$ as a system of parameters such that A has the form $B/(f)$ where B is regular and $f \neq 0$. Moreover, if W is the multiplicative system of nonzerodivisors in A then W consists of nonzero divisors of on M and $W^{-1}M$ is a finite direct sum of modules of the form $W^{-1}B/g_jB$ where each g_j is a divisor of f. In particular, $M' = \bigoplus_j B/g_jB$ is a Cohen-Macaulay module over A of pure dimension d such that $W^{-1}M$ and $W^{-1}M'$ are isomorphic as A-modules.

Proof. To prove (a), first note that since M has ACC on submodules, it has a maximal submodule N of dimension less than d: it may be 0. If N' is another submodule of M of dimension $< d$, then $d > \dim(N \oplus N') \geq \dim(N + N')$, and so $N + N' \subseteq M$ contradicts the maximality of N. Thus, N contains every submodule of M of dimension $< d$. If M/N had any nonzero submodule of dimension less than d, its inverse image in M would be strictly larger than N and of dimension less than d as well.

(b) Since $M \subseteq W^{-1}M \cong W^{-1}M'$, we have an injection $M \hookrightarrow W^{-1}M'$. Let $u_1, \dots, u_h$ be generators of M. Suppose that u_i maps to v_i/w_i, $1 \leq i \leq h$, where $v_i \in M'$ and $w_i \in W$. Let $w = w_1 \cdots w_h$. Then $M \cong wM \hookrightarrow \sum_i Rv_i \subseteq M'$. The map $W^{-1}M \to W^{-}M'$ that this induces is still an isomorphsim, since w is a unit in $W^{-1}R$. It follows that the cokernel C_1 of the map $M \to M'$ that we constructed is such that $W^{-1}C_1 = 0$. Since C_1 is finitely generated, there is a single element of W that kills C_1. An entirely similar argument yields $0 \to M' \to M \to C_2$ such that C_2 is killed by an element of W.

(c) Let $u_1, \dots, u_h$ generate M. Then the map $R \to M^{\oplus h}$ sending $r \mapsto (ru_1, \dots, ru_h)$ is injective. It follows that $\mathrm{Ass}\,(R) \subseteq \mathrm{Ass}\,(M^{\oplus h}) = \mathrm{Ass}\,(M)$, so that R is also of pure dimension d. Choose a field or discrete valuation ring V that maps onto a coefficient ring for R (so that the residue class field of V maps isomorphically to the residue class field of R), and let $X_1, \dots, X_d$ be formal indeterminates over V. Then the map $V \to R$ extends uniquely to a continuous map $B = V[[X_1, \dots, X_d]] \to R$ such that $X_i \mapsto x_i$, $1 \leq i \leq d$. Let M_B be the maximal ideal of B. Since the map $B \to R$ induces an isomorphism of residue class fields, and since R/m_BR has finite length over B (the x_i generate an m-primary ideal of R), R is module-finite over the image A of B in R. Moreover, we must have $\dim(A) = \dim(R)$.

In the equal characteristic case, where $V = K$ is a field, we must have $B \cong A = K[[x_1, \dots, x_d]]$. Moreover, M must be torision-free over A, since a nonzero torsion submodule would have dimension smaller than d. Hence M and A^ρ, where ρ is the torsion-free rank of M over A, become isomorphic when we localize at $A - \{0\}$.

We suppose henceforth that we are in the mixed characteristic case. We know that the ring A has pure dimension d. It follows that $A = B/J$, where J is an ideal all of whose associated primes in B have height one. Since B is regular, it is a UFD. Height one primes are principal, and any ideal primary to a height one prime has the form g^k, where g generates the prime and k is a nonnegative integer. It follows that $A = B/fB$, where $f = f_1^{k_1} \cdots f_h^{k_k}$ is the factorization of f into prime elements. Let W be the multiplicative system consisting of the complement of the union of the f_jB. The associated primes of

A are the $P_j = f_jA$, and these are also the associated primes of M. Then $W^{-1}A$ is an Artin ring and is the product of the local rings A_{Pj}: each of these may be thought of as obtained by killing $f_j^{k_j}$ in the DVR obtained by localizing B at the prime f_jB. M, as a B-module, is then a product of modules over the various A_{P_j}, each of which is a direct sum of cyclic modules of the form B/f_j^sB for $1 \leq s \leq k_j$. Each of these is Cohen-Macaulay of dimension d, and the images the x_i form a system of parameters, since each of these rings is a homomorphic image of A. □

We can now prove:

Theorem. *Let $(R,\, m,\, K)$ be a local ring of dimension d and let $x_1,\, \ldots\, , x_d$ be a system of parameters for R. Let $I = (x_1,\, \ldots\, , x_d)R$. Let M be a finitely generated R-module. Then $e^{\mathrm{L}}_{\underline{x}}(M) = 0$ if $\dim(M) < d$, and $e^{\mathrm{L}}_{\underline{x}}(M) = e_I(M)$ if $\dim(M) = d$.*

Proof. We have already proved that $e^{\mathrm{L}}_{\underline{x}}(M) = 0$ if $\dim(M) < d$: this is part (c) of the Lemma on p. 5 of the Lecture Notes from February 25. Now suppose that $\dim(M) = d$. We may complete R and M without changing either multiplicity. Let N be the maximum submodule of M of dimension smaller than d. Then we may replace M by M/N (cf. part (d) of the Lemma on p. 5 of the the Lecture Notes from February 25). Thus, we may assume that M has pure dimension d. We may replace R by R/Ann_RM and so assume that M is faithful. We view R as module-finite over A as in part (c) of the preceding Lemma. Since A contains $x_1,\, \ldots\, , x_d$, we may replace R by A and I by $(x_1,\, \ldots\, , x_d)A$. By parts (b) and (c) of the preceding Lemma, there is a Cohen-Macaulay A-module M' of dimension d such that each of M and M' embeds in the other with cokernel of dimension smaller than d. Thus, by part (e) of the Lemma on p. 5 of the Lecture Notes of February 25, we need only prove the result for M'. Hence, we may assume that M is Cohen-Macaulay. But it follows from the part (b) of the Proposition at the beginning of this lecture that $e^{\mathrm{L}}_{\underline{x}}(M) = \ell(M/IM)$ when M is Cohen-Macaulay, and we also know that $e_I(M) = \ell(M/M)$ in this case. □

We next review the definition and some basic properties of the Koszul complex

$$\mathcal{K}_\bullet(x_1,\, \ldots\, , x_n;\, M),$$

where $x_1,\, \ldots\, , x_n \in R$ and M is an R-module.

We first consider the case where $M = R$. We let $\mathcal{K}_1(x_1,\, \ldots\, , x_n;\, R)$ be the free module G with free basis $u_1,\, \ldots\, , u_n$. As a module, we let $\mathcal{K}_i(x_1,\, \ldots\, , x_n;\, R)$ be the free module $\bigwedge^i(G)$, which has a free basis with $\binom{n}{i}$ generators $u_{j_1} \wedge \cdots \wedge u_{j_i}$, $j_1 < \cdots < j_i$. The differential is such that $du_i = x_i$. More generally, the formula for the differential d is

$$(*) \quad d(u_{j_1} \wedge \cdots \wedge u_{j_i}) = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u_{j_1} \wedge \cdots \wedge u_{j_{t-1}} \wedge u_{j_{t+1}} \cdots \wedge u_{j_i}.$$

Consider an $\mathbb{N}$-graded skew-commutative R-algebra Λ. (This is an $\mathbb{N}$-graded associative algebra with identity such that for any two forms of degree f, g of degree h and k respectively, $gf = (-1)^{hk}gf$. That is, elements of even degree are in the center, and multiplying two elements of odd degree in reverse order reverses the sign on the product). An R-linear map d of Λ into itself that lowers degrees of homogeneous elements by one and satisfies

$$(\#) \quad d(uv) = (du)v + (-1)^{\deg(u)}u\,dv$$

when u is a form is called an *R-derivation* of Λ.

Then $\bigwedge^{\bullet}(G)$ is an N-graded skew-commutative R-algebra, and it is easy to verify that the differential is an R-derivation. By the R-bilinearity of both sides in u and v, it suffices to verify $(\#)$ when $u = u_{j_1} \wedge \cdots \wedge u_{j_h}$ and $v = u_{k_1} \wedge \cdots \wedge u_{k_i}$ with $j_1 < \cdots < j_h$ and $k_1 < \cdots < k_i$. It is easy to see that this reduces to the assertion $(**)$ that the formula $(*)$ above is correct even when the sequence $j_1, \ldots, j_i$ of integers in $\{1, 2, \ldots, n\}$ is allowed to contain repetitions and is not necessarily in ascending order: one then applies $(**)$ to $j_1, \ldots, j_h, k_1, \ldots, k_i$. To prove $(**)$, note that if we switch two consecutive terms in the sequence $j_1, \ldots, j_i$ every term on both sides of $(*)$ changes sign. If the $j_1, \ldots, j_i$ are mutually distinct this reduces the proof to the case where the elements are in the correct order, which we know from the definition of the differential. If the elements are not all distinct, we may reduce to the case where $j_t = j_{t+1}$ for some t. But then $u_{j_1} \wedge \cdots \wedge u_{j_i} = 0$, while all but two terms in the sum on the right contain $u_{j_t} \wedge u_{j_{t+1}} = 0$, and the remaining two terms have opposite sign.

Once we know that d is a derivation, we obtain by a straightforward induction on k that if $v_1, \ldots, v_k$ are forms of degrees $a_1, \ldots, a_k$, then

$$(* * *) \quad d(v_1 \wedge \cdots \wedge v_i) = \sum_{t=^i} (-1)^{a_1+\cdots+a_{t-1}} v_{j_1} \wedge \cdots \wedge v_{j_{t-1}} \wedge dv_{j_t} \wedge v_{j_{t+1}} \wedge \cdots \wedge v_{j_i}.$$

Note that the formula $(*)$ is a special case in which all the given forms have degree 1.

It follows that the differential on the Koszul complex is uniquely determined by what it does in degree 1, that is, by the map $G \to R$, where G is the free R-module $\mathcal{K}_1(\underline{x};\, R)$, together with the fact that it is a derivation on $\bigwedge(G)$. Any map $G \to R$ extends uniquely to a derivation: we can choose a free basis $u_1, \ldots, u_n$ for G, take the x_i to be the values of the map on the u_i, and then the differential on $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, R)$ gives the extension we want. Uniqueness follows because the derivation property forces $(* * *)$ to hold, and hence forces $(*)$ to hold, thereby determining the values of the derivation on an R-free basis.

Thus, instead of thinking of the Koszul complex $\mathcal{K}(x_1, \ldots, x_n;\, R)$ as arising from a sequence of elements $x_1, \ldots, x_n$ of R, we may think of it as arising from an R-linear map of a free module $\theta : G \to R$ (we might have written d_1 for θ), and we write $\mathcal{K}_\bullet(\theta;\, R)$ for the corresponding Koszul complex. The sequence of elements is hidden, but can be recovered by choosing a free basis for G, say $u_1, \ldots, u_n$, and taking $x_i = \theta(u_i)$, $1 \le i \le n$. The exterior algebra point of view makes it clear that the Koszul complex does not depend on the choice of the sequence of elements: only on the map of the free module $G \to R$. Different choices of basis produce Koszul complexes that look different from the "sequence of elements" point of view, but are obviously isomorphic. In particular, up to isomprphism, permuting the elements does not change the complex.

We write $\mathcal{K}_\bullet(x_1, \ldots, x_d;\, M)$, where M is an R-module, for $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, R) \otimes M$. The homology of this complex is denoted $H_\bullet(x_1, \ldots, x_n;\, M)$. Let $\underline{x} = x_1, \ldots, x_n$ and Let $I = (\underline{x})R$.

We have the following comments:

(1) The complex is finite: if M is not zero, it has length n. The i the term is the direct sum of $\binom{n}{i}$ copies of M. Both the complex and its homology are killed by $\mathrm{Ann}_R M$.

(2) The map from degree 1 to degree 0 is the map $M^n \to M$ sending

$$(u_1, \ldots, u_n) \mapsto x_1u_1 + \cdots x_nu_n.$$

The image of the map is IM, and so $H_0(x_1, \ldots, x_d;\, M) \cong M/IM$.

(3) The map from degree n to degree $n-1$ is the map $M \to M^n$ that sends

$$u \mapsto (x_1u_1,\, -x_2u_2, \cdots, \pm x_nu_n),$$

and so $H_n(x_1, \ldots, x_n;\, M) \cong \mathrm{Ann}_M I$.

(4) Given a short exact sequence of modules $0 \to M' \to M \to M'' \to 0$ we may tensor with the free complex $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, R)$ to obtain a short exact sequence of complexes

$$\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M') \to \mathcal{K}_\bullet(x_1, \ldots, x_n;\, M) \to \mathcal{K}_\bullet(x_1, \ldots, x_n;\, M'') \to 0.$$

The snake lemma then yields a long exact sequence of Koszul homology:

$$\cdots \to H_i(\underline{x};\, M') \to H_i(\underline{x};\, M) \to H_i(\underline{x};\, M'') \to H_{i-1}(\underline{x};\, M') \to \cdots$$

$$\to H_1(\underline{x};\, M') \to H_1(\underline{x};\, M) \to H_1(\underline{x};\, M'') \to M'/IM' \to M/IM \to M''/IM'' \to 0$$

(5) I kills $H_i(\underline{x};\, M)$ for every i and every R-module M. It suffices to see that x_d kills the homology: the argument for x_i is similar. Let $z \in \mathcal{K}_i(\underline{x};\, M)$, and consider $z \wedge u_n \in \mathcal{K}_{i+1}(\underline{x};\, M)$. Then

$$(*) \quad d(z \wedge u_n) = dz \wedge u_n + (-1)^i x_n z.$$

Hence, if z is a cycle, $d(z \wedge u_n) = (-1)^i x_n z$, which shows that $x_n z$ is a boundary.

(6) Let $\underline{x}^-$ denote $x_1, \ldots, x_{n-1}$. Let $G^- \subseteq G$ be the free module on the free basis $u_1, \ldots, u_{n-1}$. Then $\mathcal{K}_\bullet(\underline{x}^-;\, M)$ may be identified with

$$\bigwedge^{\bullet}(G^-) \otimes_R M \subseteq \bigwedge^{\bullet}(G) \otimes M = \mathcal{K}_\bullet(\underline{x};\, M).$$

This subcomplex is spanned by all terms that involve only $u_1, \ldots, u_{n-1}$. The quotient complex my be identified with $\mathcal{K}_\bullet(\underline{x}^-; M)$ as well: one lets $u_{j_1} \wedge \cdots \wedge u_{j_{i-1}} \wedge u_n \otimes w$ in degree i, where the $j_\nu < n$ and $w \in W$, correspond to $u_{j_1} \wedge \cdots \wedge u_{j_{i-1}} \otimes w$ in degree $i-1$. This gives a short exact sequence of complexes

$$0 \to \mathcal{K}_\bullet(\underline{x}^-;\, M) \to \mathcal{K}_\bullet(\underline{x};\, M) \to \mathcal{K}_{\bullet-1}(\underline{x}^-;\, M).$$

This in turn leads to a long exact sequence for homology:

$$\cdots \to H_i(\underline{x}^-;\, M) \to H_i(\underline{x}^-;\, M) \to H_i(\underline{x};\, M) \to H_{i-1}(\underline{x}^-;\, M) \to H_{i-1}(\underline{x}^-;\, M) \to \cdots .$$

The maps $\delta_i : H_i(\underline{x}^-;\, M) \to H_i(\underline{x}^-; M)$ and $\delta_{i-1} : H_{i-1}(\underline{x}^-;\, M) \to H_{i-1}(\underline{x}^-; M)$ are connecting homomorphisms. They may be computed as follows: a cycle z in the homology of the quotient complex $\mathcal{K}_\bullet(\underline{x}^-;\, M)$ in degree i can be lifted to $\mathcal{K}_{i+1}(\underline{x};\, M)$ as $z \wedge u_n$, and the differential takes this to $(-1)^i x_n z$ by the argument given in (5). Hence, δ_i is the endomorphism given by multiplication by $(-1)^i x_i$. It follows that we have short exact sequences:

$$0 \to \frac{H_i(\underline{x}^-;\, M)}{x_n H_i(\underline{x}^-;\, M)} \to H_i(\underline{x};\, M) \to \mathrm{Ann}_{H_{i-1}(\underline{x}^-;\, M)} x_n \to 0$$

for every i.

We next want to show that multiplicities with respect to a system of parameters can be computed using Koszul homology. Note that the matrices of the maps in the Koszul complex $\mathcal{K}_\bullet(\underline{x}; M)$ have entries in $I = (\underline{x})R$, so that for all every $\mathcal{K}_i(\underline{x};\, M)$ maps into $I\mathcal{K}_{i-1}(\underline{x};\, M)$ and for all s, $I^s\mathcal{K}_i(\underline{x};\, M)$ maps into $I^{s+1}\mathcal{K}_{i-1}(\underline{x};\, M)$.

Theorem. *Let M be a finitely generated module over a Noetherian ring R, let $\underline{x} = x_1, \ldots, x_n \in R$ and let $I = (\underline{x})R$. Then for all sufficiently large $h \gg n$, the subcomplex*

$$0 \to I^{h-n}\mathcal{K}_n(\underline{x};\, M) \to \cdots \to I^{h-i}\mathcal{K}_i(\underline{x};\, M) \to \cdots \to I^{h-1}\mathcal{K}_1(\underline{x};\, M) \to I^h\mathcal{K}_0(\underline{x};\, M) \to 0$$

of the Koszul complex $\mathcal{K}_\bullet(\underline{x};\, M)$ is exact (not just acyclic).

Proof. We abbreviate $\mathcal{K}_i = \mathcal{K}_i(\underline{x};\, M)$. Since there are only finitely many spots where the complex is nonzero, the assertion is equivalent to the statement that for fixed i, every cycle in $I^{k+1}\mathcal{K}_i$ is the boundary of an element in $I^k\mathcal{K}_{i+1}$ for all $k \gg 0$.

Let Z_i denote the module of cycles in $\mathcal{K}_i$. By the Artin-Rees lemma, there is a constant c_i such that for all $k \geq c_i$, $I^k\mathcal{K}_i \cap Z_i = I^{k-c_i}(I^{c_i}\mathcal{K}_i \cap Z_i)$. In particular, for all $k \geq c_i$, $I^{k+1}\mathcal{K}_i \cap Z_i = I(I^k\mathcal{K}_i \cap Z_i)$. For any k, the complex $I^k\mathcal{K}_\bullet(\underline{x};\, M)$., i.e.,

$$0 \to I^k\mathcal{K}_n(\underline{x};\, M) \to \cdots \to I^k\mathcal{K}_i(\underline{x};\, M) \to \cdots \to I^k\mathcal{K}_1(\underline{x};\, M) \to I^k\mathcal{K}_0(\underline{x};\, M) \to 0,$$

is the same as $\mathcal{K}_\bullet(\underline{x};\, I^kM)$, and so its homology is killed by I. Thus, a cycle in $I^k\mathcal{K}_i$, which is the same as an element of $I^k\mathcal{K}_i \cap Z_i$, when multiplied by any element of I, is a boundary. But for $k \gg 0$, $I^{k+1}\mathcal{K}_i \cap Z = I(I^k\mathcal{K} \cap Z)$, which is in the image of $I^k\mathcal{K}_{i+1}$, as required. □

Lecture of March 1, 2019

Discussion: the difference operator. Consider the ring $\mathbb{Q}[n]$ of polynomials in one variable n over the rational numbers. We define a $\mathbb{Q}$-linear function τ from this ring to itself by $\tau\bigl(P(n)\bigr) = P(n-1)$. Note that τ preserves degree and leading term. We write $\mathbf{1}$ for the identity map on $\mathbb{Q}[n]$, and Δ for the operator $\mathbf{1} - \tau$ that sends $P(n) \mapsto P(n) - P(n-1)$. Note that Δ lowers degree by one (if the degree is positive) and kills scalars. Moreover, if the leading term of $P(n)$ is an^d, where $a \in \mathbb{Q}$, the leading term of $\Delta\bigl(P(n)\bigr)$ is adn^{d-1}, which is similar to the behavior of the differentiation operator. In particular, if $P(n)$ has degree d, $\Delta^d P(n)$ is the scalar $d!a$, where a is the leading coefficient of $P(n)$. For each constant integer $c \geq 0$, $\tau^c\bigl(P(n)\bigr) = P(n-c)$. By the binomial theorem, for each k the operator

$$\Delta^k = (\mathbf{1} - \tau)^k = \mathbf{1} - \binom{k}{1}\tau + \binom{k}{2}\tau^2 - \cdots + (-1)^k\binom{k}{k}\tau^k$$

so that

$$(\#) \quad \Delta^k\bigl(P(n)\bigr) = P(n) - kP(n-1) + \cdots + (-1)^i\binom{k}{i}P(n-i) + \cdots + (-1)^k P(n-k).$$

We also note:

Lemma. *If $0 \to N_b \to \cdots \to N_a \to 0$ is a bounded complex of modules of finite length, the alternating sum of the lengths $\sum_{i=a}^b (-1)^i \ell(N_i)$ is the same as $\sum_{i=a}^b (-1)^i \ell\bigl(H_i(N_\bullet)\bigr)$.*

Proof. Let B_i be the image of N_{i+1} in N_i and Z_i the kernel of $N_i \to N_{i-1}$, so that $H_i = H_i(N_\bullet) = Z_i/B_i$. Then we have short exact sequences

$$0 \to Z_i \to N_i \to B_{i-1} \to 0 \quad \text{and} \quad 0 \to B_i \to Z_i \to H_i \to 0$$

for all i. It will be convenient to think of our summations as taken over all integers $i \in \mathbb{Z}$: this still makes sense since all but finitely many terms are zero, and will permit a convenient shift in the summation index. We then have:

$$\sum_i (-1)^i \ell(H_i) = \sum_i (-1)^i \bigl(\ell(Z_i) - \ell(B_i)\bigr) = \sum_i (-1)^i \ell(Z_i) + \sum_i (-1)^{i+1} \ell(B_i) =$$

$$\sum_i (-1)^i \ell(Z_i) + \sum_i (-1)^i \ell(B_{i-1}) = \sum_i (-1)^i \bigl(\ell(Z_i) + \ell(B_{i-1})\bigr) = \sum_i (-1)^i \ell(N_i).$$

□

If $(R,\, m,\, K)$ is local and $x_1, \ldots, x_d$ is a system of parameters, then for any finitely generated R-module M, all the modules $H_i(x_1, \ldots, x_d;\, M)$ have finite length: each is a finitely generated module killed by $(x_1, \ldots, x_d)R$.

Theorem (Serre). *Let $(R,\, m,\, K)$ be a local ring of Krull dimension d, and let M be a finitely generated R-module. Let $I = (x_1,\, \ldots\, , x_d)R$. Then*

$$\sum_{i=0}^{d}(-1)^i \ell\bigl(H_i(x_1,\, \ldots\, , x_d;\, M)\bigr)$$

is $e_I(M)$ if $\dim(M) = d$ and is 0 if $\dim(M) < d$.

Proof. By the Theorem at the end of the Lecture Notes of February 27, the subcomplex $\mathcal{A}_\bullet^{(n)}$ whose i th term is $I^{n-i}\mathcal{K}_i$, where $\mathcal{K}_i = \mathcal{K}_i(x_1,\, \ldots\, , x_d;\, M)$, is exact for all $n \gg 0$. Call the quotient complex $\mathcal{Q}_\bullet^{(n)}$. The long exact sequence of homology coming from the short exact sequence

$$0 \to \mathcal{A}_\bullet^{(n)} \to \mathcal{K}_\bullet \to \mathcal{Q}_\bullet^{(n)} \to 0$$

shows that $H_i(x_1,\, \ldots\, , x_d;\, M) \cong H_i(\mathcal{Q}_\bullet^{(n)})$ for all i if $n \gg 0$. Let $H(n)$ denote the Hilbert polynomial of M with respect to I, which agrees with $\ell(M/I^{n+1}M)$ for all $n \gg 0$. Then

$$\sum_i (-1)^i \ell\bigl(H_i(x_1,\, \ldots\, , x_d; M)\bigr)$$

is the same as

$$\sum_i (-1)^i \ell\bigl(H_i(\mathcal{Q}_\bullet^{(n+1)})\bigr)$$

for all $n \gg 0$, and this in turn equals

$$\sum_i (-1)^i \ell(\mathcal{Q}_i^{(n+1)})$$

by the Lemma just above. Since $\mathcal{Q}_i^{(n+1)}$ is the direct sum of $\binom{d}{i}$ copies of $M/I^{n+1-i}M$, for $n \gg 0$ this is

$$\sum_i (-1)^i \binom{d}{i} H(n-i),$$

which is $\Delta^d\bigl(H(n)\bigr)$ by the formula (#) in the Discussion at the beginning of this Lecture. By that same Discussion, this is also $d!$ times the leading coefficient of $H(n)$. □

Discussion: mapping cones. Let $\phi_\bullet : A_\bullet \to B_\bullet$ be a map of complexes of R-modules, so that we have a commutative diagram:

$$\begin{tikzcd}
\cdots \arrow[r, "d_{i+1}"] & B_i \arrow[r, "d_i"] & B_{i-1} \arrow[r, "d_{i-1}"] & \cdots \\
\cdots \arrow[r, "\delta_{i+1}"] & A_i \arrow[r, "\delta_i"] \arrow[u, "\phi_i"] & A_{i-1} \arrow[r, "\delta_{i-1}"] \arrow[u, "\phi_{i-1}"] & \cdots
\end{tikzcd}$$

We define the *mapping cone* $\mathcal{M}^\phi_\bullet$ to be the complex such that $\mathcal{M}^\phi_i = B_i \bigoplus A_{i-1}$, where the differential takes $b_i \oplus a_{i-1} \mapsto \big(d_i b_i + (-1)^{i-1}\phi_{i-1}(a_{i-1})\big) \oplus \delta_{i-1}(a_{i-1})$. It is easy to check that $\mathcal{M}^\phi_\bullet$ is a complex. Note that $B_\bullet$ is a subcomplex, and the quotient is $A_{\bullet-1}$ (the complex $A_\bullet$, but with the indices shifted so that the degree i term is A_{i-1}). It is straightforward to check that the mapping cone is a complex.

It is also straightforward to check that $\mathcal{K}_\bullet(x_1, \dots, x_d;\, M)$ is the mapping cone of the map

$$\phi_\bullet : \mathcal{K}_\bullet(x_1, \dots, x_{d-1};\, M) \to \mathcal{K}_\bullet(x_1, \dots, x_{d-1};\, M)$$

given by multiplication by x_d on each module.

We next observe that if

$$0 \to A_\bullet \xrightarrow{\phi} B_\bullet \to C_\bullet \to 0$$

is a short exact sequence of complexes, then the homology of the mapping cone $\mathcal{M}^\phi_\bullet$ of $A_\bullet \hookrightarrow B_\bullet$ is the same as $H_\bullet(C_\bullet)$. The isomorphism is induced by

$$\mathcal{M}^\phi_i = B_i \oplus A_{i-1} \twoheadrightarrow B_i \twoheadrightarrow C_i.$$

For a suitable choice of ±, $u \oplus v$ is a cycle in $\mathcal{M}^\phi_n$ iff $du = \pm\phi(v)$. Note that we automatically have $\delta(v) = 0$, since $\phi(\delta(v)) = d(\phi(v)) = \pm ddu = 0$, and ϕ is injective. The cycle is completely determined by u, and u occurs in a cycle iff its image represents a cycle in C_i. The module of boundaries is $d(B_{i+1}) + \phi(A_i) \subseteq B_i$, and obviously maps onto the module of boundaries in C_i. □

Corollary. *If x_d is not a zerodivisor on M, then*

$$H_i(x_1, \dots, x_d;\, M) \cong H_i(x_1, \dots, x_{d-1};\, M/x_dM)$$

for all i.

Proof. We apply the discussion of mapping cones when the map ϕ is injective with $A_\bullet = B_\bullet = \mathcal{K}_\bullet(x_1, \dots, x_{d-1}, M)$, and $\phi = \cdot x_n$. The fact that x_n is not a zerodivisor on M implies that the map ϕ is injective. Note that $C_\bullet \cong \mathcal{K}_\bullet(x_1, \dots, x_{d-1}; M/x_nM)$. The stated result is immediate.

Theorem. *Let (R, m, K) be local of dimension d and let $x \in m$ be part of a system of parameters generating a reduction of m. Suppose that x is not a zerodivisor on M. Then $e(M) = e(M/xM)$, where M/xM is viewed as a module over R/xR.*

Proof. Let $x_1, \dots, x_d$ be a system of parameters generating a reduction I of m, where $x = x_n$. Then the images of $x_1, \dots, x_{d-1}$ generate a reduction J for m/xR in R/xR. Thus, $e(M) = e_I(M)$, and $e(M/xM) = e_J(M/xM)$, and we may compute each of these as an alternating sum of lengths of Koszul homology. But the correspondingly indexed Koszul homology modules are isomorphic by the preceding Corollary. □

Our next goal is to prove that, under mild conditions, rings of multiplicity 1 are regular. We first need:

Lemma (Hironaka). *Let (R, m, K) be a local domain and let $x \in R - \{0\}$ be such that xR has a unique minimal prime P. Suppose that R/P is normal and that R_P is a discrete valuation ring in which x generates the maximal ideal PR_P. Suppose also that the normalization S of R is module-finite over R (which is true when R is complete) and that every minimal prime Q of xS lies over P (which is true if R is universally catenary). Then R is normal, and $P = xR$.*

Proof. Note that if R is universally catenary, and Q is any minimal prime of xS in S, if P' is the contraction of Q to R, the height of P' must be one by the dimension formula: R and S have the same fraction field, and $R/P' \hookrightarrow S/Q$ is module-finite, so that the extension or residue class fields $R_{P'} \to S_Q$ is algebraic. Since P' contains x, we must have $P' = P$.

Since R_P is a discrete valuation ring, it is normal and so $S \subseteq R_P$. Hence, $S_P = R_P$ is already local of dimension one, and S_Q is a further localization of dimension one. It follows that $S_Q = R_P$, and that $QS_Q = PR_P$. Moreover, since $QS_Q \cap S = Q$, we have that $PR_P \cap S = Q$, and so only one prime Q of S lies over P.

We have that S/Q is contained in the fraction field of R/P, and it is an integral extension. Since R/P is normal, we must have that $S/Q = R/P$, and so every residue class in S/Q can be represented by an element of R. This implies that $S = Q + R$. We can also see that $xS = Q$: we have that $xS \subseteq Q$, and to check $Q \subseteq xS$ it suffices to show that this is true after localization at each minimal prime of xS, since S is normal. Q is the only such prime, and $QS_Q = PR_P = xR_P = xS_Q$. Since $S = Q + R$, we now have that $S = xS + R$. By Nakayama's lemma, this implies that $S = R$, so that R is normal. Then $P = Q$, and $Q = xS = xR$. □

We shall say that a module M over a Noetherian ring R *has pure dimension d* (M may be equal to R) if for every associated prime P of M, $\dim(R/P) = d$. An equivalent condition is that every nonzero submodule of M has dimension d.

Theorem. *Let (R, m, K) by a local ring. The R is regular if and only if R has multiplicity 1 and suppose $\widehat{R}$ has pure dimension.*

Proof. If R is regular, it is Cohen-Macaulay and its multiplicity is the length when w we kill a regular system of parameters, which is 1. Moreover, $\widehat{(R)}$ is again regular, and so is a domain. We therefore only need to show the "If" part: we assume that R has multiplicity 1 and $\widehat{R}$ is of pure dimension, and we need to prove that R is regular.

We use induction on $\dim(R)$. If $\dim(R) = 0$, then $e(R) = \ell(R) = 1$, so that R must be a field and is regular.

We may replace R by $\widehat{R}$ without affecting any relevant issue. Then

$$(*) \quad e(R) = \sum_P \ell(R_P)e(R/P)$$

where P runs through all the associated primes of R, each of which is minimal and such that $\dim(R/P) = \dim(R)$, by hypothesis. It follows that there is only one associated prime, necessarily minimal, and that R_P has length one, and so is a field. This implies that R is a domain.

If the residue field of R is infinite, we can complete the argument as follows. Choose $x \in R$ so that it is part of system of parameters that generates a reduction of m. If $\dim(R) = 1$, the $e(R) = \ell(R/xR) = 1$, so that R/xR is a field and $m = xR$, which shows that R is regular.

If $\dim(R) \geq 2$, then we still have $e(R/xR) = e(R) = 1$. Thus, applying $(*)$ of the second paragraph to R/xR, we find that xR has a unique minimal prime P in R (*a priori*, xR may have embedded primes), that $(R/xR)_P$ is a field, so that $PR_P = xR_P$, and that $e(R/P) = 1$. By the induction hypothesis, R/P is regular, and, therefore, normal. R is universally catenary (complete local rings are homomorphic images of regular rings) and and has a module-finite normalization. Hence, we are in the situation of Hironaka's Lemma, and $P = xR$. Since R/xR is regular, so is R.

If the residue field of R is finite, we may replace R by $R(t)$. The theory of excellent rings then implies that if we complete again, the hypothesis we need on associated primes is preserved: the completion of a ring of ring or module of pure dimension has pure dimension in the excellent case. (One can reduce this to studying the situation when R is an excellent local domain. The theory of excellent rings then yields that the completion is reduced, and is such that all minimal primes have quotients of the same dimension.)

An alternative is to take an irreducible polynomial f of large degree over the residue field K of R, lift it to a monic polynomial g over R, and replace R by $R_1 = R[x]/(g)$. This ring is still complete, and it is module-finite and free over R, so that it has pure dimension. Killing m gives $L = K[x]/(f)$, which is a field. Therefore the new ring still has multiplicity one. Once the cardinality of L is sufficiently large, there will exist a system of parameters of R_1 that gives a reduction of the maximal ideal of R_1, and we can proceed as above. $\square$

Lecture of March 11, 2019

Examples. Let $R = K[[x,\, y]]/(x^2, xy)$. This ring has a unique minimal prime, xR, and $m = (x,\, y)R$ is embedded. The image $\overline{x}$ of x in the ring generates a submodule isomorphic to R/m, which has lower dimension. Then $e(R) = e(R/xR) = e(K[[y]]) = 1$.

Likewise, if $R = K[[x,\, y,\, z]]/\big((x,y)\cap(z)\big)$, then R has two minimal primes, $(x,y)R$ and zR. Thus, $\dim(R) = \dim(R/zR) = \dim(K[[x,\, y]]$, while the module $zR \cong R/(x,y) \cong K[[z]]$ is one-dimensional. Thus, $e(R) = e(R/zR) = e(K[[x,\, y]]) = 1$.

These examples illustrate that a local ring of multiplicity 1 need not be regular. In the first example, R_{red} is a domain. In the second, R is reduced, but not equidimensional.

Finally, consider $R = K[[u,\, v,\, x,\, y,\, z]]/\big((u,v)\cap(x,y)\cap z\big)$. This ring is reduced but not equidimensional. It has dimension 4 (when we kill zR we get $K[[u,\, v,\, x,\, y]]$), but has two minimal primes with quotients of dimension 3. Consider the ring obtained when we localize at $P = (u,\, v,\, x,\, y)$. The localization S of $T = K[[u,\, v,\, x\,y,\, z]]$ at $(u,\, v,\, x,\, y)T$ is regular of dimension 4, and $u,\, v,\, x,\, y$ is a regular system of parameters. Thus, $R_P = S/\bigl((u,\, v) \cap (x,\, y)\bigr)$ has two minimal primes with quotients that are regular of dimension 2. It follows that $e(R) = 1$ while $e(R_P) = 2$. The problem here is that we "localized away" the relevant minimal prime of R that governed its multiplicitiy.

Discussion: localization. One expects that under mild conditions, $e(R_P) \leq e(R)$. But we only expect this for primes P such that $\dim(R_P) + \dim(R_P) = \dim(R)$. (We always have $\dim(R/P) + \dim(R_P) \leq \dim(R)$. The condition of equality means that P is part of a chain of primes of maximum length, $\dim(R)$, in R.) It is conjectured that in all local rings, whenever $\dim(R_P) + \dim(R_P) = \dim(R)$, one has that $e(R_P) \leq e(R)$.

In studying this problem, one is naturally led to Lech's Conjecture. The result on localization is true if R is excellent (and under various weaker hypotheses), but, so far as I know, remains open in the general case. It would follow, however, from a proof of Lech's Conjecture, which permits a reduction to the case where the ring is complete.

First note:

Lemma. *Let P be a prime ideal of a local ring R. Then:*

(a) *For every minimal prime Q of $P\widehat{R}$,* $\mathrm{height}\,(Q) = \mathrm{height}\,(P)$*.*

(b) *If* $\dim(R/P) + \dim(R_P) = \dim(R)$*, then there exists a minimal prime Q of PR such that* $\dim(\widehat{R}/Q) + \dim(\widehat{R}_Q) = \dim(\widehat{R})$.

(c) *If $\widehat{R/P}$ is reduced, then with Q as in part (b) we have that $e(R_P) = e(\widehat{R}_Q)$.*

Proof. (a) $R_P \to \widehat{R}_Q$ is faithfully flat, so that $\dim(\widehat{R}_Q) \geq \dim(R_P)$. The minimality of Q implies that PR_P expands to a $Q\widehat{R}_Q$-primary ideal in $\widehat{R}_Q$, so that a system of parameters for R_P will be a system of parameters for $\widehat{R}_Q$ as well.

For (b), note that the completion of R/P, which is $\widehat{R}/P\widehat{R}$, has the same dimension as R/P, and so has a minimal prime, say $Q/P\widehat{R}$, where Q is prime in $\widehat{R}$, such that $\dim(\widehat{R}/Q) = \dim(\widehat{R}/P\widehat{R} = \dim(R/P)$. By part (a), $\dim(\widehat{R}_Q = \dim(R_P)$ as well.

To prove (c), observe that if $\widehat{R/P}$ is reduced, then so is $\widehat{R}_Q/P\widehat{R}_Q$, which means that PR_P expands to the maximal ideal in $\widehat{R}_Q$. The equality of multiplicities then follows from the Proposition on p. 6 of the Lecture Notes of February 22. □

Our next objective, which will take a while, is to prove the following:

Theorem (localization theorem for multiplicities). *If P is a prime ideal of a complete local ring R such that* $\dim(R/P) + \dim(R_P) = \dim(R)$*, then $e(R_P) \leq e(R)$.*

Assuming this for the moment, we have several corollaries.

Corollary. *If P is a prime of a local ring R such that* $\dim(R/P) + \dim(R_P) = \dim(R)$ *and the completion of R/P is reduced,*[4] *then $e(R_P) \leq e(R)$.*

Proof. Choose a minimal prime Q of $P\widehat{R}$ such that $\dim(\widehat{R}/Q) + \dim(\widehat{R}_Q) = \dim(\widehat{R})$, as in part (b) of the Lemma. Then by part (c),

$$e(R_P) = e(\widehat{R}_Q) \leq e(\widehat{R}) = e(R).$$

Corollary. *If Lech's conjecture holds, then for every prime P of a local ring R such that* $\dim(R/P) + \dim(R_P) = \dim(R)$*, $e(R_P) \leq e(R)$.*

Proof. Choose Q as in part (b) of the Lemma. Then $R_P \to \widehat{R}_Q$ is flat local, and so by Lech's conjecture

$$e(R_P) \leq e(\widehat{R}_Q) \leq e(\widehat{R}) = e(R). \qquad \square$$

We also get corresponding results for modules.

Corollary. *If R is a local ring, M a finitely generated R-module, and P is a prime of the support of M such that* $\dim(R/P) + \dim(M_P) = \dim(M)$*, then:*

(a) *If the completion of R/P is reduced, then $e(M_P) \leq e(M)$.*

(b) *If Lech's conjecture holds, then $e(M_P) \leq e(M)$.*

Proof. Note that we can replace R by $R/\mathrm{Ann}_R M$, so that we may assume that M is faithful and $\dim(R) = \dim(M) = d$, say. Note that M is faithful if and only if for some (equivalently, every) finite set of generators $u_1, \ldots, u_h$ for M, the map $R \to M^{\oplus h}$ such that $r \mapsto (ru_1, \ldots, ru_h)$ is injective. This condition is obviously preserved by localization. Now,

$$(*) \quad e(M) = \sum_{1 \leq i \leq h,\, \dim(R/P_i) = d} \ell_{R_{P_i}}(M_{P_i}) e(R/P_i).$$

Note that once we have that M is faithful, $\dim(R/P) + \dim(M_P) = \dim(M)$ is equivalent to $\dim(R/P) + \dim(R_P) = \dim(R)$, since M_P is faithful over R_P. The minimal primes of M and R are the same, and so are the minimal primes of M_P and R_P: the latter correspond to the minimal primes of R that are contained in P. There is a formula like $(*)$ for $e(M_P)$, where the summation is extended over minimal primes $\mathfrak{p}$ of the support of M_P, i.e., of R_P, such that $\dim(R_P)/\mathfrak{p} = \dim(M_P)$, which is $\dim(R_P)$. Let $\mathfrak{p}$ be such a minimal prime. Then there is a chain of primes from $\mathfrak{p}$ to P of length height (P), and this can be concatenated with a chain of primes of length $\dim(R/P)$ from P to m, producing a chain of length $\dim(R)$. It follows that $\dim(R/\mathfrak{p}) \geq d$, and the other inequality is obvious. Therefore, $\mathfrak{p}$ is one of the P_i. Moreover, in R/P_i, we still have

$$\dim\big((R/P_i)/(P/P_i)\big) + \text{height}\,\big((R/P_i)_{P/P_i}\big) = \dim(R/P_i) = d.$$

[4] This is always true if R is excellent: the completion of an excellent reduced local ring is reduced.

Thus, the terms in the formula corresponding to $(*)$ for M_P correspond to a subset of the the terms occurring in $(*)$, but have the form

$$\ell_{R_{P_i}}(M_{P_i})e(R_P/P_iR_P).$$

Note that each P_i occurring is contained in P, and localizing first at P and then at P_iR_P produces the same result as localizing at P_i. Using either (a) or (b), whichever holds, we have that every $e\big((R/P_i)_P\big) \leq e(R/P_i)$. □

We next want to understand multiplicities in the hypersurface case.

Theorem. *Let (R, m, K) be a regular local ring of dimension d and let $f \in m$. Let $S = R/fR$. The $e(S)$ is the m-adic order of f, i.e., the unique integer k such that $f \in m^k - m^{k+1}$.*

Proof. We use induction on $\dim(R)$. If $\dim(R) = 1$ the result is obvious. Suppose $\dim(R) > 1$. We replace R by $R(t)$ if necessary so that we may assume the residue class field is infinite. Choose a regular system of parameters $x_1, \ldots, x_d$ for R. By replacing these by linearly independent linear combinatons we may assume that x_1 is such that

(1) x_1 does not divide f, so that the image of x_1 is not a zerodivisor in S.

(2) The image of x_1 in m/m^2 does not divide the leading form of f in $\mathrm{gr}_m(R)$.

(3) The image of x_1 in S is part of a minimal set of generators for a minimal reduction of m/fR, the maximal ideal of S.

Let $\overline{x}$ be the image of x_1 in S. Then $e(S) = e(S/\overline{x}S)$, and this is the quotient of the regular ring R/x_1R by the image of f. Moreover, the (m/x_1R)-adic order of the image of f in R/x_1R is the same as the m-adic order of f in R. The result now follows from the induction hypothesis applied to the image of f in R/x_1R. □

We next want to reduce the problem of proving the localization result for complete local domains to proving the following statement:

Theorem (symbolic powers in regular rings). *Let $P \subseteq Q$ be prime ideals of a regular ring R. Then $P^{(n)} \subseteq Q^{(n)}$ for every positive integer n.*

We postpone the proof for the moment. Note, however, that one can reduce at once to the local case, where Q is the maximal ideal, by working with (R_Q, QR_Q) instead of R.

Discussion: the symbolic power theorem for regular rings implies that multiplciities do not increase under localization. Let R be complete local, and let P be a prime ideal of R such that $\dim(R/P) + \mathrm{height}(R_P) = \dim(R)$. We want to show that $e(R_P) \leq e(R)$. Exactly as in the discussion of the module case in the proof of the Corollary, one can reduce to the case where R is a domain. As usual, one may assume without loss of generality that the residue field is sufficiently large for R to have a system of parameters $x_1, \ldots, x_d$ that generates a minimal reduction of m. Then in the equicharacteristic case (respectively, the mixed characteristic case), we can map $K[[X_1, \dots, X_d]] \to R$ (respectively, $V[[X_1, \dots, X_d]] \to R$), where $K \subseteq R$ (respectively $V \subseteq R$) is a coefficient field (respectively, a complete DVR that is a coefficient ring) and so that $X_i \mapsto x_i$, $1 \le i \le d$. In both cases, R is module-finite over the image A: in the equicharacteristic case, $A = K[[x_1, \dots, x_d]]$ is regular, while in mixed characteristic the kernel of $V[[X_1, \dots, X_d]] \to R$ must be a height one prime, and therefore principle, so that $A \cong V[[x_1, \dots, x_d]]/(f)$. Since the maximal ideal of R is integral over $(x_1, \dots, x_d)R$ and R is module-finite over A, the maximal ideal of A is also integral over $(x_1, \dots, x_d)A$. Let ρ denote the torsion-free rank of R as an A-module, which is the same as the degree of the extension of fraction fields. Suppose that P is a prime of R and let $\mathfrak{p}$ be its contraction to A. Let I be the ideal $(x_1, \dots, x_d)A$. Then $e(R) = e_{IR}(R)$, which is the same as $e_I(R)$ with R thought of as an A-module. This is $\rho\, e_I(A) = \rho\, e(A)$. The result on symbolic powers gives the result on localization of multiplicities for $A = T/(f)$, when T is regular: one multiplicity is the order of f in T with respect to the maximal ideal, while the other is the order of f in a localization of T. (In the equicharacteristic case, both A and its localization are regular, and both multiplicities are 1.) Thus, $\rho\, e(A_{\mathfrak{p}}) \le \rho\, e(A) = e(R)$. But we shall see in the sequel that $e(R_P) \le e_{\mathfrak{p}}(R_{\mathfrak{p}})$, with $R_{\mathfrak{p}}$ is viewed as an $A_{\mathfrak{p}}$ module. Since R is module-finite over A, $R_{\mathfrak{p}}$ is module-finite over $A_{\mathfrak{p}}$, and $R_{\mathfrak{p}}/\mathfrak{p}^n R_{\mathfrak{p}}$ is an Artin ring, and is a product of local rings one of which is $R_P/(\mathfrak{p}^n R_P)$. Then

$$\ell_{A_{\mathfrak{p}}}(R_{\mathfrak{p}}/\mathfrak{p}^n R_{\mathfrak{p}}) \ge \ell_{A_{\mathfrak{p}}}(R_P/\mathfrak{p}^n R_P) \ge \ell_{A_{\mathfrak{p}}}(R_P/P^n R_P) \ge \ell_{R_P}(R_P/P^n R_P)$$

for all n, so that the multiplicity of $R_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module is greater than or equal to $e(R_P)$. But then

$$e(R_P) \le e_{\mathfrak{p}}(R_{\mathfrak{p}}) = \rho\, e(A_{\mathfrak{p}}) \le \rho\, e(A) = e(R),$$

as required. $\square$

Thus, all that remains is to prove the theorem on symbolic powers in regular rings.

Lecture of March 13, 2019

Before attacking the problem of comparing symbolic powers of primes, we want to discuss some techniques that will be needed. One is connected with enlarging the residue class field of a local ring.

Proposition. *Let (R, m, K) be a local ring, and let θ be an element of the algebraic closure of K with minimal monic irreducible polynomial $f(x) \in K[x]$. Let $F(x)$ be a monic polynomial of the same degree d as f that lifts F to $R[x]$. Let $S = R[x]/(F)$. Then S is module-finite, free of rank d, and local over R. Hence, S is R-flat. The residue field of S is isomorphic with $L = K[\theta]$, and S has maximal ideal mS.*

Proof. S is module-finite and free of rank d over R by the division algorithm. Hence, every maximal ideal of S must lie over m, and the maximal ideals of S correspond bijectively to those of $S/mS = R[x]/(mR[x] + FR[x]) \cong K[x]/fK[x] \cong K[\theta]$, which shows that mS is maximal and that it is the only maximal ideal of S. This also shows that $S/mS \cong K[\theta]$. □

Discussion: getting reductions such that the number of generators is the analytic spread. Let $(R,\, m,\, K)$ be local and I an ideal with analytic spread h. One way of enlarging the residue field so as to guarantee the existence of a reduction of I with h generators is to replace R by $R(t)$, so that the residue class field becomes infinite. For this purpose, it is not necessary to enlarge R so that K becomes infinite. One only needs that K have sufficiently large cardinality. When K is finite, one can choose a primitive element θ for a larger finite field extension L: the cardinality of the finite field L may be taken a large as one likes, and a primitive element exists because the extension is separable. Recall that the issue is to give one-forms of $B = K \otimes_R \mathrm{gr}_I(R)$ that are a homogeneous system of parameters. After making the type of extension in the Proposition, one has, because mS is the maximal ideal of S, that

$$L \otimes_S \mathrm{gr}_{IS}(S) \cong L \otimes_S \big(S \otimes_R \mathrm{gr}_I(R)\big) \cong L \otimes_R \mathrm{gr}_I(R) \cong L \otimes_K \big(K \otimes_R \mathrm{gr}_I(R)\big).$$

If one makes a base change to $\overline{K} \otimes_K B$, where $\overline{K}$ is the algebraic closure of K, one certainly has a linear homogeneous system of parameters. The coefficients will lie in L for any sufficiently large choice of finite field L.

Proposition. *Let $(R,\, m,\, K)$ be any complete local ring. Then R has a faithfully flat extension $(S, \mathfrak{n}, L)$ such that $\mathfrak{n} = mS$ and L is the algebraic closure of K. If R is regular, then S is regular.*

Proof. We may take R to be a homomorphic image of $T = K[[x_1,\, \ldots\, , x_d]]$, where K is a field, or of $T = V[[x_1,\, \ldots\, , x_d]]$, where $(V,\, \pi V, K)$ is a complete DVR such that the induced map of residue class fields is an isomorphism. In the first case, let L be the algebraic closure of K. Then $T_1 = L[[x_1,\, \ldots\, , x_n]]$ is faithfully flat over T, and the expansion of $(x_1,\, \ldots\, , x_d)T$ to T_1 is the maximal ideal of T_1. Here , faithful flatness follows using the Lemma on p. 2 of the Lecture Notes of February 20, becasuse every system of parameters for T is a system of parameters for T_1, and so a regular sequence on T_1, since T_1 is Cohen-Macaulay. Then $S = T_1 \otimes_T R$ is faithfully flat over R, has residue class field L, and m expands to the maximal ideal.

We can solve the problem in the same way in mixed characteristic provided that we can solve the problem for V: if $(W, \pi W, L)$ is a complete DVR that is a local extension of V with residue class field L, then $T_1 = W[[x_1,\, \ldots\, , x_d]]$ will solve the problem for T, and $T_1 \otimes_T R$ will solve the problem for R, just as above.

We have therefore reduced to studying the case where the ring is a complete DVR V. Furthermore, if $(W,\, \pi W,\, L)$ solves the problem but is not necessarily complete, we may use $\widehat{W}$ to give a solution that is a complete DVR.

Next note that if $(V_\lambda, \pi V_\lambda,\, K_\lambda)$ is a direct limit system of DVRs, all with the same generator π for their maximal ideals, such that the maps are local and injective, then

$\varinjlim_\lambda V_\lambda$ is DVR with maximal ideal generated by π. It is then clear that the residue class field is $\varinjlim_\lambda K_\lambda$. The reason is that every nonzero element of the direct limit may be viewed as arising from some V_λ, and in that ring it may be written as a unit times a power of π. Thus, every nonzero element of the direct limit is a unit times a power of π.

We now construct the required DVR as a direct limit of DVRs, where the index set is given by a well-ordering of the field L, the algebraic closure of K, in which 0 is the least element. We shall construct the family $\{(V_\lambda,\, \pi, ,K_\lambda)\}_{\lambda \in L}$ in such a way that for every $\lambda \in L$,

$$\{\mu \in L : \mu \leq \lambda\} \subseteq K_\lambda \subseteq L.$$

This will complete the proof, since the direct limit of the family will be the required DVR with residue class field L.

Take $V_0 = V$. If $\lambda \in L$ and V_μ has been constructed for $\mu < \lambda$ such that for all $\mu < \lambda$,

$$\{\nu \in L : \nu \leq \mu\} \subseteq K_\mu \subseteq L,$$

then we proceed as follows to construct V_λ. There are two cases.

(1) If λ has an immediate predecessor μ and $\lambda \in K_\mu$ we simply let $V_\lambda = V_\mu$, while if $\lambda \notin K_\mu$, we take $\theta = \lambda$ in the first Proposition to construct V_λ.

(2) If λ is a limit ordinal, we first let $(V',\, \pi V',\, K') = \varinjlim_{\mu<\lambda} V_\mu$. If λ is in the residue class field of V', we let $V_\lambda = V'$. If not, we use the first Proposition to extend V' so that its residue class field is $K'[\lambda]$. □

To prove the theorem on comparison of symbolic powers in regular rings, we shall also need some results on valuation domains that are not necessarily Noetherian. In particular, we need the following method of constructing such valuation domains.

Proposition. *Let $(V,\, \mathfrak{n}, L)$ be a valuation domain with fraction field $\mathcal{K}$ and let $(W, m,\, K)$ be a valuation domain with fraction field L. Let $g : V \twoheadrightarrow L$ be the quotient map. Then $T = \{v \in V : g(v) \in W\} \subseteq V$ is a valuation domain with fraction field $\mathcal{K}$. Its maximal ideal is $\{v \in V : g(v) \in m\}$. Its residue class field is K, and it contains a prime ideal $\mathfrak{q}$ which may be described as $\mathfrak{n} \cap T$. Moreover $T/\mathfrak{q} = W$, while $T_\mathfrak{q} = V$.*

Proof. Let $f \in \mathcal{K}$ be nonzero. If $f \notin V$ then $1/f$ is not only in V: it must be in $\mathfrak{n}$, and so has image 0 in L. Thus, $1/f \in T$. If $f \in V - \mathfrak{n}$ then $1/f \in V - \mathfrak{n}$ as well. The images of these two elements are reciprocals in $W/\mathfrak{n} = K$, and so at least one of the two is in W. Thus, either f or $1/f$ is in V. Finally, if $f \in \mathfrak{n}$ then $g(f) = 0 \in W$, and so $f \in T$. This shows that V is a valuation domain with fraction field $\mathcal{K}$.

The restriction of g to T clearly maps T onto K. This means that the kernel of this map must be the unique maximal ideal of T, and that the residue class field is K. The prime $\mathfrak{q}$ is clearly the kernel of the surjection $T \twoheadrightarrow W$ obtained by restricting g to T, whence $T/\mathfrak{q} = W$. Since $\mathfrak{n}$ lies over $\mathfrak{q}$, we have an induced local map $T_\mathfrak{q} \to V$ of valuation domains of $\mathcal{K}$. This map must be the identity by the third Remark on p. 1 of the Lecture Notes of Ferbruary 5. □

The valuation domain T is called the *composite* of V and W.

Corollary. *Let R be a domain with fraction field $\mathcal{K}$, and*

$$P_0 \subseteq P_1 \subseteq \cdots \subseteq P_k$$

a chain of prime ideals of R. Then there exists a valuation domain V with $R \subseteq V \subseteq \mathcal{K}$ and a chain of prime ideals

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_k$$

of V such that $\mathfrak{q}_i \cap R = P_i$, $1 \leq i \leq k$. Morevover, we may assume that $\mathfrak{q}_k$ is the maximal ideal of V.

Proof. If $n = 0$, we simply want to find V a valuation domain with maximal ideal $\mathfrak{q}$ lying over $P = P_0$. We may replace R by R_P and apply the Corollary on p. 2 of the Lecture Notes of January 14 with $I = PR_P$ and $L = \mathcal{K}$.

Now suppose that V_{k-1} together with

$$\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_{k-1}$$

solve the problem for

$$P_0 \subseteq \cdots \subseteq P_{k-1}.$$

If $P_k = P_{k-1}$ take $V = V_{k-1}$ and $\mathfrak{q}_k = \mathfrak{q}_{k-1}$. If $P_{k-1} \subset P_k$ is strict, we can choose a valuation domain W of the fraction field of R/P_{k-1} containing R/P_{k-1} and whose maximal ideal lies over P_k/P_{k-1}. Take V to be the composite of V_{k-1} and W. □

Lecture of March 15, 2019

To finish our comparison of symbolic powers in a regular ring, we shall make use of quadratic transforms (also called *quadratic transformations* or *quadratic dilatations*) in a more general context than in the proof of the Lipman-Sathaye Jacobian Theorem.

Let (R, m, K) be a local domain with $R \subseteq (V, \mathfrak{n})$ a local map, where V is a not necessarily Noetherian valuation domain. The *first quadratic transform* of R along V is the localization (R_1, m_1) of $R[m/x]$ at the contraction of $\mathfrak{n}$, where x is any element of m such that $xV = mV$. This ring is again a local ring with a local map $R_1 \to V$.

The quadratic transform is independent of the choice of the element x. To see this, suppose that $xV = yV$, where $y, x \in m$. Then $y/x \in R[m/x]$ is a unit in V, so its inverse $x/y \in R_1$. Since $m/y = (m/x)(x/y)$, it follows that $R[m, y] \subseteq R_1$. Moreover, each element of $R[m/y]$ that is invertible in V has an inverse in R_1, so that if Q is the contraction of $\mathfrak{n}$ to $R[m/y]$ we have an induced inclusion map $R[m/y]_Q \to R_1$. An exactly symmetric argument gives the opposite inclusion.

As in our earlier situation, we may take iterated quadratic transforms

$$R \subseteq R_1 \subseteq \cdots \subseteq R_k \subseteq \cdots \subseteq V.$$

Note that if $m = x_1, \ldots, x_h$, then $mV = (x_1, \ldots, x_h)V$, so that x may be chosen from among the x_i. Putting this together with the Lemma on p. 2 of the Lecture Notes of February 4, we have:

Proposition. *Let (R, m, K) be regular local with $x_1, \ldots, x_d$ a regular system of parameters and suppose that $R \subseteq (V, \mathfrak{n})$ is local where V is a valuation domain. If the x_i are numbered so that $x_jV \subseteq x_1V$ for all $j > 1$, then the quadratic transform R_1 is a localization of the ring $S = R[x_2/x_1, \ldots, x_d/x_1]$, which is regular of dimension d. In particular, R_1 has dimension at most d. Moreover, $S/x_1S \cong K[X_2, \ldots, X_d]$, where X_i is the image of x_i/x_1, $2 \leq i \leq d$.* □

Here is another important example:

Theorem. *Let R be a one dimensional local domain whose integral closure $(V, \mathfrak{n})$ is local and module-finite over R. (This is always the case if R is a complete one-dimensional local domain.) Let*

$$R \subseteq R_1 \subseteq \cdots \subseteq R_k \subseteq \cdots \subseteq V$$

be the sequence of iterated quadratic transforms. Then for all sufficiently large k, $R_k = V$.

Proof. Since V is module-finite over R, it cannot have an infinite ascending chain of R-submodules. It follows that the chain R_i is eventually stable. But if the maximal ideal of R_i is not principal and has minimal generators $y_1, \ldots, y_h$ with y_1 of least order in V, then for some $j > 1$, $y_j/y_1 \in V - R_i$, and $y_j/y_1 \in R_{i+1}$. Therefore, for sufficiently large i, the maximal ideal of R_i is prinicpal. But then R_i is a DVR, and is a normal ring inside the fraction field of R and containing R. It follows that $R_i = V$. □

We also note:

Theorem. *Let (R, m, K) be a local domain with $R \subseteq (V, \mathfrak{n})$ a local inclusion, where V is a valuation domain of the fraction field of R. Let $\mathfrak{q}$ be a prime ideal of V lying over $P \neq m$ in R. Let*

$$R \subseteq R_1 \subseteq R_2 \subseteq \cdots \subseteq R_k \subseteq \cdots \subseteq V$$

be the sequence of quadratic trransforms of R along V. Let P_i be the contraction of P to R_i. Then

$$R/P \subseteq R_1/P_1 \subseteq R_2/P_2 \subseteq \cdots \subseteq R_k/P_k \subseteq \cdots \subseteq V/\mathfrak{q}$$

is the sequence of quadratic transforms of $R/P \subseteq V/\mathfrak{q}$ along $V/\mathfrak{q}$.

Proof. By induction on k, it suffices to see this when $k = 1$. Let $x_1, \ldots, x_h$ generate the maximal ideal m of R with $x_1V = mV$. Some $x \in m$ is not in $\mathfrak{n}$, and since $xV \subseteq mV = x_1V$, $x_1 \notin \mathfrak{q}$ and so $x_1 \notin P$. Moreover, $x_1(V/\mathfrak{q}) = (m/P)(V/\mathfrak{q})$. It follows that the quadratic transform of R/P along $V/\mathfrak{q}$ is the localization at the contraction of $\mathfrak{n}$ of $(R/P)[\widetilde{m}/\overline{x}_1]$, where $\widetilde{m}$ is m/P and $\overline{x}_1$ is the image of x_1 in R/P. The stated result follows at once. Note that we again have $P_1 \neq m_1$, the maximal ideal of R_1, since $x_1 \in m_1 - P_1$. □

We next observe:

Lemma. *Let $(R,\,m,\,K)$ be a regular local ring with algebraically closed residue class field, and suppose $R \subseteq (V, \mathfrak{n})$ is local, where V is a valuation domain and $R/m \to Vn$ is an isomorphism. Then there is a regular system of parameters $x_1, \ldots, x_d$ for R such that the first quadratic transform is the localization of $R[x_2/x_1, \ldots, x_d/x_1]$ at the height d maximal ideal generated by $x_1, x_2/x_1, \ldots, x_d/x_1$, so that these elements are a regular system of parameters in the first quadratic transform.*

Proof. Let $x_1,\, y_2, \ldots, y_d$ be one regular system of parameters for R such that $x_1V = mV$. $\mathfrak{n}$ contains x_1, and so $\mathfrak{n}$ lies over a prime ideal of R containing x_1. Hence, the quotient of $R[m/x_1]$ by the contraction of $\mathfrak{n}$ is also a quotient of $K[Y_2, \ldots, Y_d]$, where Y_i is the image of y_i/x_1, $2 \leq i \leq d$. The resulting quotient domain imbeds embeds K-isomorphically in $K = V/\mathfrak{n}$, and so is equal to K. It follows that the contraction of $\mathfrak{n}$ corresponds to a maximal ideal of $K[Y_2, \ldots, Y_d]$, which must have the form $(Y_2 - c_2, \ldots, Y_d - c_d)$ for elements $c_2, \ldots, c_d \in K$. Therefore we may let $x_i = y_i - c_i x_1$ for each i, $2 \leq i \leq d$. □

Proof of the theorem on comparison of symbolic powers. We want to show that if R is regular and $P \subseteq Q$ are prime, then $P^{(n)} \subseteq Q^{(n)}$ for all n. By considering a saturated chain of primes joining P to Q we immediately reduce to the case where the height if Q/P in R/P is one. We may replace R by R_Q, and so we may assume that Q is m in the regular local ring (R, m) and that $\dim(R/P) = 1$.

Suppose that $(R,\,m,\,K) \to S$ is a flat local map, where S is regular with maximal ideal mS. Then it suffices to prove the theorem for S, for if P_1 in S lies over P and we know the theorem for S, we have

$$P^{(n)} \subseteq P_1^{(n)} \subseteq (mS)^n = m^n S,$$

and then

$$P^{(n)} \subseteq m^n S \cap R = m^n,$$

because S is faithfully flat over R. We may therefore replace R first by its completion, and then by a complete regular local ring with an algebraically closed residue field. Hence, from now on, we shall assume that R is complete with residue class field K that is algebraically closed, as well as that $\dim(R/P) = 1$.

We now introduce valuations. Let V_1 be a valuation domain of the fraction field of R whose maximal ideal contracts to P: we may use, for example, order with respect to powers of PR_P to construct V_1. Let W be the integral closure of R/P, which will be a discrete valuation ring because R/P is a complete local domain of dimension one. Since K is algebraically closed, the residue class field of W is K. Let $(V, \mathfrak{n})$ be the composite valuation. Then $\mathfrak{n}$ lies over m, and $V/\mathfrak{n} = K$. Moreover, V has a prime [q] lying over P. Now consider the sequence of quadratic transforms

$$(R,\, m,\, K) \subseteq (R,\, m_1,\, K) \subseteq (R,\, m_2,\, K) \subseteq \cdots \subseteq (R_k,\, m_k,\, K) \subseteq \cdots \subseteq (V,\, \mathfrak{n},\, K).$$

Each R_i has a prime P_i that is the contraction of $\mathfrak{q}$. Now R/P_k is the kth quadratic transform of R/P, by the Theorem above, and so for large k is the DVR W, by the earlier Theorem. Then R_k/P_k is regular, and so P_k is generated by part of a regular system of parameters. We shall see in the sequel that $P_k^{(n} = P_k^n \subseteq m^n$ in this case. Assuming this, to complete the proof it suffices to show that if a given R_i provides a counterexample (where $R_0 = R$), then so does its quadratic transform.

We might as well work with R and

$$R_1 = R[x_2/x_1,\, \ldots\, ,\, x_d]_{\mathcal{M}},$$

where $\mathcal{M}$ is the maximal ideal $(x_1,\, x_2/x_1,\, \ldots\, , x_d/x_1)R[m/x_1]$. Suppose $f \in R$ has m-adic order n, but order at least $n+1$ in R_P. Since $m^n/x_1^n \subseteq R[m/x_1]$, we have that $f/x_1^n \in R[m/x_1]$. Since $x_1 \notin P_1$, f_n/x_1^n has the same order as f in $(R_1)_{P_1}$, and since P_1 lies over P this will be at least $n+1$. It therefore will suffice to show that f/x_1^n has m_1-adic order at most n in R_1. Since $R_1/\mathcal{M}^{n+1}$ already local, it suffices to show that $f/x_1^n \notin \mathcal{M}^{n+1}$. Suppose otherwise. The ideal $\mathcal{M}^{n+1}$ is generated by elements μ/x_1^{n+1} where μ is a monomial of degree $n+1$ in $x_1^2, x_2, \ldots\, , x_n$, and

$$R[m/x_1] = \bigcup_t m^t/x_1^t.$$

Therefore, for some t, we have

$$f/x_1^n \in (1/x_1^{n+1})(x_1^2, x_2, \ldots\, , x_d)^{n+1} m^t/x_1^t$$

and so

$$x_1^{t+1} f \in (x_1^2, x_2, \ldots\, , x_d)^{n+1} m^t.$$

Each of the obvious generators obtained by expanding the product on the right that involves x_1^2 has degree at least $n+t+2$. Hence, in the degree $n+t+1$ part of $\mathrm{gr}_m(R) = K[X_1,\, \ldots\, , X_d]$, we have that

$$X_1^{t+1} F \in (X_2,\, \ldots\, ,\, X_d)^{n+1} (X_1,\, \ldots\, , X_d)^t,$$

where F is the image of f in m^n/m^{n+1}, and is supposedly not 0. By taking homogeneous components in degree $n+t+1$ we see that $x_1^{t+1}F$ must be in the K-vector space span of the obvious monomial generators of

$$(X_2,\, \ldots\, ,\, X_d)^{n+1} (X_1,\, \ldots\, , X_d)^t.$$

But this is clearly impossible with $F \neq 0$, since none of these monomials is divisible by X_1^{t+1}.

This completes the proof, once we have shown that for primes generated by a regular sequence, symbolic powers are the same as ordinary powers.

Lecture of March 18, 2019

We have completed the proof of the theorem on comparison of symbolic powers of prime ideals in regular rings as soon as we have established:

Lemma. *Let P be a prime ideal of the ring R that is generated by a regular sequence, $x_1, \ldots, x_k$. Then $P^{(n)} = P^n$ for every integer n.*

Proof. Let $u \in R - P$. We need only show that u is not a zerodivsor on P^n. Suppose $ur \in P^n$ with $r \notin P^n$. Choose h, which may be 0, such that $r \in P^h - P^{h+1}$: evidently, $h < n$. Then $ur \in P^n \subseteq P^{h+1}$. This implies that the image of u in R/P is a zerodivisor on P^h/P^{h+1}. But by part (d) of the Proposition on p. 2 of the Lecture Notes of February 25, P^h/P^{h+1} is a free R/P-module with a free basis in bijective correspondence with monomials of degree h in variables $X_1, \ldots, X_k$. $\square$

Before proceeding further, we want to record an import result on flatness. We first note:

Lemma. *Let M be an R-module with a finite filtration such that $x \in R$ is not a zerodivisor on any factor. Then x is not a zerodivisor on M.*

Proof. By induction on the number of factors, it suffices to consider that case of two factors, i.e., where one has a short exact sequence $0 \to N_1 \to M \to N_2 \to 0$. If $u \in M$ is such that $xu = 0$, then the image of u in N_2 must be 0, or else x will be a zerodivisor on N_2. But then $u \in N_1$, and so $xu = 0$ implies that $u = 0$. $\square$

Next note that when $(R, m, K) \to (S, \mathfrak{n}, L)$ is local and M is an S-module, M/mM is called the *closed fiber* of M (because it is the fiber over the unique closed point m of $\mathrm{Spec}\,(R)$). In this case, if we make a base change to R/I, where $I \subseteq m$ is an ideal of R, R, S, and M become R/I, S/IS, and M/IM, respectively, but the closed fiber does not change: $(M/IM)/m(M/IM) \cong M/mM$.

In the result that follows, the most important case is when $M = S$.

Theorem. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a local homomorphism of local rings and let M be an S-module that is R-flat. Then:*

(a) $\dim(M) = \dim(R) + \dim(M/mM)$.

(b) *If $y \in \mathfrak{n}$ is a nonzerodivisor on M/mM, then it is a nonzerodivisor on M and on M/IM for every ideal $I \subseteq m$ of R. Moreover, if $y \in \mathfrak{n}$ is a nonzerodivisor on M/mM, then M/yM is again flat over R.*

If $\operatorname{depth}_m R = 0$*, then $y \in \mathfrak{n}$ is a nonzerodivisor on M if and only if it is a nonzerodivisor on M/mM.*

(c) $\operatorname{depth}_{\mathfrak{n}} M = \operatorname{depth}_m nR + \operatorname{depth}_{\mathfrak{n}} M/mM$.

Proof. For part (a), we proceed by induction on $\dim(R)$. If $\dim(R) = 0$ then m is nilpotent, and (a) holds even without the assumption that M is R-flat. If $\dim(R) \geq 1$, let $\mathfrak{A}$ be the ideal of nilpotent elements in R, and make a base change to $R/\mathfrak{A}$. The dimensions of R and M do not change, and the closed fiber does not change. Thus, we may assume that R is reduced. But then m contains a nonzerodivisor x, which is consequently also a nonzerodivisor on M because M is R-flat. Make a base change to R/xR. By the induction hypothesis, $\dim(M/xM) = \dim(R/xR) + \dim(M/mM)$. Since $\dim(M/xM) = \dim(M) - 1$ and $\dim(R/xR) = \dim(R) - 1$, the result follows.

For part (b), suppose that y is not a zerodivisor on M/mM. We want to show that y is not a zerodivisor on M/IM. Suppose y kills a nonzero element u of M/IM. We can choose $N \gg 0$ so large that $u \notin m^N(M/IM)$. It follows that y kills the nonzero image of u in $(M/IM)/m^N(M/IM) \cong M/(I + m^N)M$, and so there is no loss of generality in assuming that I is m-primary. In this case, R/I has a finite filtration in which every factor is copy of $K = R/m$. When we apply $M \otimes_R \_$, the fact that M is R-flat implies that M/IM has a finite filtration in which every factor is a copy of $M \otimes R/m \cong M/mM$. By the Lemma above, since y is not a zerodivisor on any of these factors, it is not a zerodivisor on M/IM, as required.

To prove that M' is R-flat, it suffices to show that $\operatorname{Tor}_1^R(N, M') = 0$ for every finitely generated R-module N, since every R-module is a direct limit of finitely generated R-modules. Since a finitely generated R-module N has a finite filtration with cyclic factors, it follows that it suffices to prove that $\operatorname{Tor}^R(R/I, M') = 0$ for every ideal I of R. Let $M' = M/yM$. Starting with the short exact sequence

$$0 \to M \xrightarrow{y} M \to M/yM \to 0$$

we may apply $R/I \otimes_R \_$ to get a long exact sequence part of which is

$$\to \operatorname{Tor}_1^R(R/I, M) \to \operatorname{Tor}_1^R(R/I, M/yM) \to M/IM \xrightarrow{y\cdot} M/IM \to \cdots .$$

Since M is R-flat, the leftmost term is 0, and since we have already shown that y is not a zerodivisor on M/IM, it follows that $\operatorname{Tor}_1^R(R/I, M/yM) = 0$ for all I, as required.

We next consider the case where $\operatorname{depth}_m(R) = 0$. Then we can choose a nonzero element $z \in R$ such that $zm = 0$, i.e.,

$$0 \to m \to R \xrightarrow{z\cdot} R$$

is exact. Applying $\_ \otimes_R M$, we have that

$$0 \to m \otimes_R M \to M \xrightarrow{z\cdot} M$$

is exact. This shows both that $m \otimes_R M$ may be identified with its image, which is mM, and that $\mathrm{Ann}_M z = mM$. We have already shown that if y is a nonzerodivisor on M/mM then it is a nonzerodivisor on M. For the converse, suppose $u \in M$ is such that $yu \in mM$. We must show that $u \in mM$. But $zyu \in zmM = 0$, and so $zu = 0$, i.e., $u \in \mathrm{Ann}_M z$, which we have already shown is mM, as required.

To prove part (c), let $x_1, \dots, x_h \in m$ be a maximal regular sequence in R. Since M is flat, we may make a base change to $R/(x_1, \dots, x_h)R$, $M/(x_1, \dots, x_h)M$. Both sides of the equality we are trying to prove decrease by h, since the closed fiber is unchanged. Thus, we may assume without loss of generality that $\mathrm{depth}_m(R) = 0$. We complete the argument by induction on $\dim(M/mM)$. Since $y \in \mathfrak{n}$ is a nonzerodivisor on M/mM if and only if it is a nonzerodivisor on M, if one of these two modules has depth 0 on $\mathfrak{n}$ then so does the other. Therefore, we may assume that $\mathrm{depth}_{\mathfrak{n}} M/mM > 0$. Choose $y \in \mathfrak{n}$ that is a nonzerodivisor on M/mM. Then y is also a nonzerodivisor on M, and M/yM is again R-flat. Let $M/mM = \overline{M}$. We may apply the induction hypothesis to M/yM to conclude that

$$\mathrm{depth}_{\mathfrak{n}}(M/yM) = \mathrm{depth}_{\mathfrak{n}}(\overline{M}/y\overline{M}) + \mathrm{depth}_m(R),$$

since $\overline{M}/y\overline{M}$ may be identified with the closed fiber of M/yM. Since

$$\mathrm{depth}_n(M/yM) = \mathrm{depth}_{\mathfrak{n}}(M) - 1$$

and

$$\mathrm{depth}_{\mathfrak{n}}(\overline{M}/y\overline{M}) = \mathrm{depth}_{\mathfrak{n}}(M/mM) - 1,$$

the result follows. $\square$

Lemma. *Let $(R,\, m,\, K)$ to $(S, \mathfrak{n},\, L)$ be a flat local map of local rings.*

(a) *$R(t) \to S(t)$ is flat, where t is an indeterminate.*

(b) *$\widehat{R} \to \widehat{S}$ is flat.*

Proof. For (a), $R \otimes_{\mathbb{Z}} \mathbb{Z}[t] \to S \otimes_{\mathbb{Z}} \mathbb{Z}[t]$ is flat by base change, so that $R[t] \to S[t]$ is flat, and $S[t] \to S(t)$ is a localization, and so flat. Hence, $S(t)$ is flat over $R[t]$, and the map factors $R[t] \to R(t) \to S(t)$. Whenver B is flat over A and the map factors $A \to W^{-1}A \to T$, T is also flat over $W^{-1}A$. This follows form the fact that for $(W^{-1}A)$-modules $0 \to N \hookrightarrow M$, the map $T \otimes_{W^{-1}A} N \to T \otimes_{W^{-1}A} N$ may be identified with $T \otimes_A N \to T \otimes_A M$. To see this, note that we have a map $T \otimes_A M \to T \otimes_{W^{-1}A} M$, and the kernel is spanned by elements of the form $w^{-1}u \otimes v - u \otimes w^{-1}v$. But since w in invertible in T, we can prove that this is 0 by multiplying by w^2, which yields $wu \otimes v - u \otimes wv = 0$. This proves (a).

To prove (b), note that it suffices to prove that $0 \to N \hookrightarrow M$, a map of $\widehat{R}$-modules, remains injective after applying $\widehat{S} \otimes_{\widehat{R}} \_$ in the case where N and M are finitely generated.

Given a counterexample, we can choose $u \in \widehat{S}\otimes_{\widehat{R}} N$ that is not 0 and is killed when mapped into $\widehat{S} \otimes_{\widehat{R}} M$. We can choose k so large that $u \notin m^k(\widehat{S} \otimes_{\widehat{R}} N)$, and, by the Artin-Rees lemma, we can choose n so large that $m^n M \cap N \subseteq m^k N$. Then there is a commutative diagram

$$\begin{tikzcd}
N \arrow[r, hook] \arrow[d, two heads] & M \arrow[d, two heads] \\
N/(m^n M \cap N) \arrow[r, hook] & M/m^n M
\end{tikzcd}$$

and we may apply $\widehat{S} \otimes_{\widehat{R}} \_$ to see that the image of u in $\widehat{S} \otimes_{\widehat{R}} \bigl(N/(m^n M \cap N)\bigr)$ is nonzero (even if we map further to $\widehat{S} \otimes_{\widehat{R}} (N/m^k M)$), but maps to 0 in $\widehat{S} \otimes_{\widehat{R}} (M/m^n M)$. When applied to maps of finite length $\widehat{R}$-modules, the functor $\widehat{S} \otimes_{\widehat{R}} \_$ preserves injectivity because $R \to S \to \widehat{S}$ is flat, and $\widehat{S} \otimes_{\widehat{R}} \_$ and $\widehat{S} \otimes_R \_$ are the same functor on finite length $\widehat{R}$-modules V: we have that $\widehat{R} \otimes_R V \cong V$ since V is killed by m^s for some s and $\widehat{R}/m^s\widehat{R} \cong R/m^s$, and so, by the associativity of tensor,

$$\widehat{S} \otimes_{\widehat{R}} V \cong \widehat{S} \otimes_{\widehat{R}} (\widehat{R} \otimes_R V) \cong \widehat{S} \otimes_R V. \qquad \square$$

We can now make several reductions in studying Lech's conjecture.

Theorem. *In order to prove Lech's conjecture that $e(R) \leq e(S)$ when $(R, m, K) \to (S, \mathfrak{n}, L)$ is flat local and R has dimension d, it suffices to prove the case where* $\dim(S) = \dim(R) = d$, *R and S are both complete with infinite residue class field, S has algebraically closed residue class field, R is a domain, and S has pure dimension.*

Proof. By the Lemma above and the final Proposition in the Lecture Notes of February 22, we can replace R and S by $R(t)$ and $S(t)$ and so assume that the residue class fields are infinite. Likewise, we can replace R and S by their completions. We can choose a minimal prime Q of mS such that $\dim(S/Q) = \dim(S/mS)$. By the Lemma on p. 1 of the Lecture Notes of March 11, we have that $\mathrm{height}\,(Q) = \mathrm{height}\,(m) = \dim(R)$. Since $\dim(S) = \dim(S/mS) + \dim(R)$, we have that $\dim(S) = \dim(S/Q) + \mathrm{height}\,(Q)$. By the Theorem on behavior of multiplicities under localization in complete local rings, we then have $e(S_Q) \leq e(S)$. Thus, if $e(R) \leq e(S_Q)$ we have $e(R) \leq e(S)$ as well. It follows that we may replace S by S_Q and so we may assume that $\dim(S) = \dim(R) = d$. We may have lost completeness, but we may complete again. By the second Proposition on p. 1 of the Lecture Notes of March 13, we can give a local flat map $(S, \mathfrak{n}, L) \to (S', \mathfrak{n}', L')$ such that S' is complete, $\mathfrak{n}' = \mathfrak{n}S'$ and L' is algebraically closed. Thus, we may assume that S has an algebraically closed residue class field.

We can give a filtration of R by prime cyclic modules R/P_i, $1 \leq i \leq h$. Then $e(R)$ is the sum of the $e(R/P_i)$ for those i such that $\dim(R/P_i) = \dim(R)$. Tensoring with S over R gives a corresponding filtration of S by modules S/P_iS, and $e(S)$ is the sum of the $e(S/P_iS)$ for those i such that $\dim(S/P_iS) = \dim(S)$. Since $\dim(S) = \dim(R) + \dim(S/mS)$ and, for each i, $\dim(S/P_iS) = \dim(R/P_i) + \dim(S/mS)$, the values of i such that $\dim(R/P_i) =$

$\dim(R)$ are precisely those such that $\dim(S/P_iS) = \dim(S)$. Thus, it suffices to consider the case where R is a complete local domain.

If $\dim(R) = \dim(S)$ and R is a complete local domain, then it follows that S has pure dimension. We use induction on the dimension. If $\dim(R) = 0$ then $\dim(S) = 0$ and the result is clear. Let R' be the normalization of R. $R' \otimes_R S$ is faithfully flat over R' and still local (the maximal ideal of R' is nilpotent modulo the maximal ideal of R). Moreover, $S \subseteq R' \otimes_R S$, so that we may assume that R is normal. Suppose that S contains an S-submodule of dimension smaller than S, say J, and choose J maximum, so that S/J has pure dimension d. Then R does not meet J, and so injects into S/J. Choose $x \in m - \{0\}$. Then x is a nonzerodivisor in R, and, hence a nonzerodivisor on S and on J. It is also a nonzerodivisor on S/J, for any submodule killed by x would be a module over S/xS, and hence of smaller dimension. It follows that

$$0 \to xJ \to xS \to x(S/J) \to 0$$

is exact, and we get that

$$0 \to J/xJ \to S/xS \to (S/J)/x(S/J) \to 0$$

is exact. Then

$$\dim(J/xJ) \leq \dim(J) - 1 < \dim(S) - 1 = \dim(S/xS).$$

Therefore, S/xS does not have pure dimension. Because all associated primes of xR have height one, R/xR has a filtration whose factors are torsion-free modules over rings R/P_i of dimension $\dim(R) - 1$, where the P_i are the minimal primes of x. By the induction hypothesis, every S/P_iS has pure dimension. Since a finitely generated torsion-free module over R/P_i embeds in a finitely generated free module over R/P_i, the tensor product of a finitely generated torsion-free module over R/P_i with S also has pure dimension. Thus, S/xS has a filtration whose factors are modules of pure dimension, and so has pure dimension itself. This contradiction establishes the result. □

One approach to obtaining a class of local rings R for which Lech's conjecture holds for every flat local map $R \to S$ is via the notion of a *linear maximal Cohen-Macaulay module.* Recall that over a local ring $(R,\, m,\, K)$, a module M is a Cohen-Macaulay module if it is finitely generated, nonzero, and $\mathrm{depth}_m M = \dim(M)$. In particular, M is Cohen-Macaulay module over R if and only if it is Cohen-Macaulay module over R/I, where $I = \mathrm{Ann}_R M$. E.g., the residue class field $K = R/m$ is always Cohen-Macaulay module over R. By a maximal Cohen-Macaulay module we mean a Cohen-Macaulay module module whose dimension is equal to $\dim(R)$. It is not known whether every excellent local ring has a maximal Cohen-Macaulay module: this is an open question in dimension 3 in all characteristics.

We write $\nu(M)$ for the least number of generators of the R-module M. If M is finitely generated over a local (or quasi-local) ring $(R,\, m,\, K)$, Nakayama's lemma implies that $\nu(M) = \dim_K(M/mM)$.

Note the following fact, which has proved useful in studying Lech's conjecture:

Proposition. *Let $(R,\, m,\, K)$ be local and let M be a maximal Cohen-Macaulay module. Then $e(M) \geq \nu(M)$.*

Proof. We may replace R by $R(t)$ and M by $R(t) \otimes_R M$ if necessary and so assume that the residue class field of R is infinite. Let $I = (x_1,\, \ldots\,, x_d)$ be a minimal reduction of m, where $d = \dim(R)$. Then $e(M) = \ell(M/IM) \geq \ell(M/mM) = \nu(M)$. □

We shall call M a *linear maximal Cohen-Macaulay module* over the local ring $(R,\, m,\, K)$ if it is a maximal Cohen-Macaulay module and $e(M) = \nu(M)$. Because of the inequality in the Proposition just above, the term *maximally generated* maximal Cohen-Macaulay module is also used in the literature, as well as *top-heavy* maximal Cohen-Macaulay module and *Ulrich* maximal Cohen-Macaulay module. The idea of the proof of the Proposition above also yields:

Proposition. *Suppose that M is a maximal Cohen-Macaulay module over a local ring $(R,\, m,\, K)$ and that K is infinite or, at least, the m has a minimal reduction I generated by a system of parameters $x_1,\, \ldots\,, x_d$. Then:*

(a) *M is a linear maximal Cohen-Macaulay module if and only if $mM = IM$.*

(b) *If M is a linear maximal Cohen-Macaulay module then $m^nM = I^nM$ for all $n \in \mathbb{N}$.*

(c) *If M is a linear maximal Cohen-Macaulay module then $\mathrm{gr}_m(M)$ is a Cohen-Macaulay module over $\mathrm{gr}_m(R)$.*

Proof. (a) Since $IM \subseteq mM \subseteq M$ we have that

$$e(M) = \ell(M/IM) = \ell(M/mM) + \ell(mM/IM) = \nu(M) + \ell(mM/IM).$$

Hence, $e(M) = \nu(M)$ if and only if $\ell(mM/IM) = 0$, i.e., if and only if $mM = IM$.

Part (b) follows by induction on n: if $m^nM = I^nM$ then

$$m^{n+1}M = m^n mM = m^n(IM) = I(m^nM) = I(I^nM) = I^{n+1}M.$$

For part (c), observe that $\mathrm{gr}_m M = \mathrm{gr}_I M$, by part (b), and the result is then immediate from part (d) of the Proposition on p. 2 of the Lecture Notes of February 25, which identifies $\mathrm{gr}_I(M)$ with

$$(M/IM) \otimes_{R/I} (R/I)[X_1,\, \ldots\,, X_d],$$

where X_i is the image of x_i in I/I^2, $1 \leq i \leq d$, and $X_1,\, \ldots\,, X_d$ are algebraically independent over R/I. □

□

Lecture of March 20, 2019

Before proceeding further with our study of Lech's conjecture, we want to discuss a result known as the *associativity* of multiplicities whose proof uses Lech's theorem on computing multiplicities using ideals generated by powers of parameters.

Before we prove this result, we want to make some remarks on the behavior of limits of real-valued functions of two integer variables: these might as well be positive, since we will be taking limits as the variables approach $+\infty$ either jointly or independently. Let $G(m,\, n)$ be such a function, and suppose that

$$\lim_{(m,n)\to\infty} G(m,\, n)$$

exists, and also that the iterated limit

$$\lim_{m\to\infty}\bigl(\lim_{n\to\infty} G(m,\, n)\bigr)$$

exists as well. Then they are equal. If the joint limit is L, then, given $\epsilon > 0$ there exists N such that for all $m,\, n \geq N$, $|L - G(m,\, n)| < \epsilon$. It follows that each for $m \geq n$, $L_m = \lim\limits_{n\to\infty} G(m,\, n)$, which we are assuming exists, is such that $|L - L_m| \leq \epsilon$, since all of the values of $G(m,\, n)$ are at distance at most ϵ from L for all $m \geq N$. It also follows that the iterated limit must have a value that is at distance at most ϵ from L. Since this is true for all $\epsilon > 0$, the iterated limit must be L.

Note however, that when the joint limit exists, it is possible that neither iterated limit exists. E.g., for $m,\, n \geq 1$ we can let

$$G(m,n) = 1/\min\{m,\, n\}$$

if $m+n$ is even and 0 if $m+n$ is odd. For any fixed m, the function takes on the values $1/m$ and 0 alternately for large n, and the iterated limit does not exist.

On the other hand, observe that we can define $G(m,n) = 1$ if $m \geq n$ and $G(m,n) = 0$ if $m < n$. The iterated limits both exist, but are different, and the joint limit does not exist. If, alternatively, we define $G(m,\, n) = 0$ when $m = n$ and $G(m,\, n) = 1$ when $m \neq n$, both iterated limits exist and are equal, but the joint limit does not.

Note that the Corollary on p. 5 of the Lecture Notes of February 22 is a special case of the following Theorem, namely the case where $r = 0$. It is also used in the proof.

Theorem (associativity of multiplicities). *Let M be a module of dimenson d over a local ring R of dimension d. Let $x_1,\, \ldots\, , x_d$ be a system of parameters for R, and let $I = (x_1,\, \ldots\, , x_d)R$. Let $r,\, s$ be nonnegative integers such that $r+s = d$. Let $\mathfrak{A} = (x_1,\, \ldots\, , x_r)R$ and $\mathfrak{B} = (x_{r+1},\, \ldots\, ,\, x_d)R$. Let $\mathcal{P}$ be the set of minimal primes of $x_1,\, \ldots\, , x_r$ such that* $\dim M_P + \dim\,(R/P) = d$. *Then*

$$e_I(M) = \sum_{P\in\mathcal{P}} e_{\mathfrak{B}}(R/P)e_{\mathfrak{A}}(M_P).$$

Proof. Let $\mathfrak{A}_m = (x_1^m, \dots, x_r^m)R$ and $\mathfrak{B}_n = (x_{r+1}^n, \dots, x_d^n)R$. Consequently, by Lech's result on calculation of multiplicities, which is the Theorem on p. 3 of the Lecture Notes of February 27,

$$e_I(M) = \lim_{m,n\to\infty} \frac{\ell\big(M/(\mathfrak{A}_m + \mathfrak{B}_n)M\big)}{m^r n^s}.$$

In this instance we know that the joint limit exists. The iterated limit exists as well, since we have

$$\lim_{m\to\infty} \big(\frac{1}{m^r} \lim_{n\to\infty} \frac{\ell\big(M/(\mathfrak{A}_m + \mathfrak{B}_n)M\big)}{n^s}\big) = \lim_{m\to\infty} \frac{e_{\mathfrak{B}}(M/\mathfrak{A}_m M)}{m^r}.$$

Since M and R have dimension d and $x_1, \dots, x_d$ is a system of parameters, so is $x_1^m, \dots, x_r^m, x_{r+1}^n, \dots, x_d^n$, and $M/\mathfrak{A}_m M$ will have dimension s. P will be a (necessarily minimal) prime of the support of $M/\mathfrak{A}_m M$ such that $\dim(R/P) = \dim(M/\mathfrak{A}M)$ if and only if P contains $\mathfrak{A}$, P contains $\operatorname{Supp}(M)$, and $\dim(R/P) = s$. Since $\dim(R/\mathfrak{A}) = s$, P must be a minimal prime of $\mathfrak{A}$. Let $\mathcal{Q}$ denote the set of minimal primes of $\mathfrak{A}$ such that $\dim(R/P) = s$. By the Corollary on p. 5 of the Lecture Notes of February 21,

$$e_{\mathfrak{B}}(M/\mathfrak{A}_m M) = \sum_{P\in\mathcal{Q}} e_{\mathfrak{B}}(R/P)\ell_{R_P}(M_P/\mathfrak{A}_m M_P).$$

Note that since P is a minimal prime of $\mathfrak{A}$, $\mathfrak{A}$ expands to an ideal primary to the maximal ideal in R_P. Consequently,

$$\lim_{m\to\infty} \frac{e_{\mathfrak{B}}(M/\mathfrak{A}_m M)}{m^r} = \sum_{P\in\mathcal{Q}} e_{\mathfrak{B}}(R/P) \lim_{m\to\infty} \frac{\ell_{R_P}(M_P/\mathfrak{A}_m M_P)}{m^r}.$$

We now see that the iterated limit exists. Note that

$$\lim_{m\to\infty} \frac{\ell_{R_P}(M_P/\mathfrak{A}_m M_P)}{m^r}$$

is 0 if $\dim(M_P) < r$, and $e_{\mathfrak{A}}(M_P)$ otherwise. Therefore we need only sum over those minimal primes P of $\mathfrak{A}$ in $\operatorname{Supp}(M)$ such that $\dim(M_P) = r$ and $\dim(R/P) = s$. The latter two conditions are equivalent to the condition $\dim(M_P) + \dim(R/P) = d$ given that $P \in \operatorname{Supp}(M)$ contains $\mathfrak{A}$, since $\dim(M_P) \le \dim(R_P) \le r$ and $\dim(R/P) \le \dim(M/\mathfrak{A}M) = s$.

However, if P is a minimal prime of $\mathfrak{A}$, we do not need to require that $P \in \operatorname{Supp}(M)$, for if not $M_P = 0$ and the term corresponding to P does not affect the sum. Therefore, the value does not change if we sum over primes $P \in \mathcal{P}$, and this yields

$$e_I(M) = \sum_{P\in\mathcal{P}} e_{\mathfrak{B}}(R/P)e_{\mathfrak{A}}(M_P),$$

as required. □

Our next objective is to obtain some classes of local rings R such that Lech's conjecture always holds for flat local maps $R \to S$. Lech proved the result for the case where $\dim(R) \leq 2$. However, we shall first focus on cases that are given by the existence of linear maximal Cohen-Macaulay modules and related ideas.

We shall say that an R-module M has *rank* ρ if there is a short exact sequence

$$0 \to R^\rho \to M \to C \to 0$$

such that $\dim(C) < \dim(R)$. If M has rank ρ for some ρ, we shall say that M is an R-module *with rank.* When R is a domain, M always has rank equal to the maximum number of elements of M linearly independent over R. When R has a module M of rank ρ, $e(M) = \rho e(R)$, by the additivity of multiplicities.

The following result is very easy, but very important from our point of view.

Theorem. *Let (R, m, K) be a local ring that has a linear maximal Cohen-Macaulay module of rank ρ. Then for every flat local map $(R, m, K) \to (S, \mathfrak{n}, L)$, $e(R) \leq e(S)$.*

Proof. As observed earlier, we may assume that mR is $\mathfrak{n}$-primary. It follows that $S \otimes M$ is Cohen-Macaulay over S, and also has rank ρ. Then

$$e(R) = e(M) = \frac{1}{\rho}\,\nu(M) = \frac{1}{\rho}\,\nu(S \otimes_R M) \leq \frac{1}{\rho}\,e(S \otimes M) = e(S). \qquad \square$$

Therefore, Lech's conjecture holds for any ring R that admits a maximal Cohen-Macaulay module M such that $e(M) = \nu(M)$. Consequently, we shall focus for a while on the problem of constructing linear maximal Cohen-Macaulay modules.

However, we first want to point out the following idea, which has also been used to settle Lech's conjecture in important cases. Suppose that R and S are as in the statement of the Theorem just above, and that M is any Cohen-Macaulay module with rank, say ρ. Then

$$e(S) = \frac{1}{\rho}\,e(S \otimes_R M) \geq \frac{1}{\rho}\,\nu(S \otimes_R M) = \frac{1}{\rho}\,\nu(M) = \frac{1}{\rho}\,e(M)\,\frac{\nu(M)}{e(M)} = \frac{\nu(M)}{e(M)}\,e(R).$$

Hence:

Theorem. *Let (R, m, K) be a local ring that has a sequence of Cohen-Macaulay modules $\{M_n\}$ with rank such that*

$$\lim_{n\to\infty} \frac{\nu(M)}{e(M)} = 1.$$

Then for every flat local map $(R, m, K) \to (S, \mathfrak{n}, L)$, $e(R) \leq e(S)$. $\square$

Remark. In fact, it suffices if there is any Cohen-Macaulay module M with rank such that $\dfrac{\nu(M)}{e(M)} > \dfrac{e(R) - 1}{e(R)}$.

Lech's conjecture is easy in dimension 0: it reduces to the case where R is a local domain, and therefore a field. Thus, $e(R) = 1 \le e(S)$.

In dimension one, we need only consider the case of a local domain.

Theorem. *Let $(R,\, m,\, K)$ be a local domain with an infinite residue class field. Then m^k is a linear maximal Cohen-Macaulay module for all sufficiently large $k \gg 0$*

Therefore Lech's conjecture holds for all local rings R of dimension at most one.

Proof. Since the Hilbert polynomial $\ell(R/m^{n+1}$ is $e(R)n + c$ for some constant c, it follows that $\ell(m^k/m^{k+1}) = e(R)$ for all $k \gg 0$. But this is also $\nu(m^k)$. Since R is a one-dimensional domain, any nonzero torsion-free module is Cohen-Macaulay. □

Remark. When the residue field is infinite, we can argue alternatively that m has a reduction xR, and then for sufficiently large k, $m^{k+1} = xm^k$.

We shall eventually prove that if $(R,\, m,\, K)$ is local such that R has a linear maximal Cohen-Macaulay module, and $f \in m$ is such that the leading form of f in $\mathrm{gr}_m(R)$ is a nonzerodivisor, then R/fR has a linear maximal Cohen-Macaulay module. It will follow that if R is a *strict complete intersection*, i.e., has the form $T/(f_1,\, \ldots\,, f_h)$ where $(T, \mathcal{M})$ is regular and the leading forms of the f_j form a regular sequence in $\mathrm{gr}_{\mathcal{M}}T$, then R has a linear maximal Cohen-Macaulay module. This will take a considerable effort.

Lecture of March 22, 2019

We are going to use certain matrix factorizations to construct linear maximal Cohen-Macaulay modules over hypersurfaces.

Discussion: Cohen-Macaulay modules over hypersurfaces R/fR of finite projective dimension over R. In order to illustrate the connection, we first consider the following relatively simple situation. Let $(R,\, m,\, K)$ be a Cohen-Macaulay local ring of dimension n, let $f \in m$ be a nonzerodivisor, and suppose that we want to study maximal Cohen-Macaulay modules over R/fR that have finite projective dimension over R. Such a module M has depth $n-1$, and so $\mathrm{pd}_R M = 1$. Thus, there is a minimal free resolution

$$0 \to R^h \to R^s \to M \to 0$$

of M over R. If we localize at f, since $M_f = 0$, we see that $h = s$, and so M is given as the cokernel of an $s \times s$ matrix α. Let e_i be the ith standard basis vector for R^s, written as a column. Then for every i, $1 \le i \le s$, we have, since $fM = 0$, that fe_i is in the column space of α, which means that there is a column vector B_i such that $\alpha B_i = fe_i$. If we form the $s \times s$ matrix β whose columns are $B_1, \, \ldots\,, B_n$, we have that $\alpha\beta = f\boldsymbol{I}_s$, where $\boldsymbol{I}_s$ is the $s \times s$ identity matrix. Over the ring $R_f \supseteq R$, $\beta = f\alpha^{-1}$, which implies that α and β commute, i.e., $\alpha\beta = \beta\alpha = f\boldsymbol{I}_s$.

Let $^{-}$ indicate images in R/fR. We claim that the complex

$$\cdots \xrightarrow{\overline{\beta}} \overline{R}^s \xrightarrow{\overline{\alpha}} \overline{R}^s \xrightarrow{\overline{\beta}} \overline{R}^s \xrightarrow{\overline{\alpha}} \overline{R}^s \to 0,$$

whose augmentation is M, is acyclic. Suppose $v \in R^s$ represents a vector in the kernel of α (the argument for β is identical). Then $\alpha(v)$ vanishes mod fR^s, and so $\alpha(v) = fu$. Then $\beta\alpha(v) = \beta(fu) = f\beta(u)$, but $\beta\alpha = f\boldsymbol{I}_s$, and so we have $fv = f\beta(u)$. Since f is not a zerodivisor, $v = \beta(u)$, and exactness follows.

Given M, we obtain a matrix factorization. Conversely, given a matrix factorization of $f\boldsymbol{I}_s$, the argument we just gave shows that the complex

$$\cdots \xrightarrow{\overline{\beta}} \overline{R}^s \xrightarrow{\overline{\alpha}} \overline{R}^s \xrightarrow{\overline{\beta}} \overline{R}^s \xrightarrow{\overline{\alpha}} \overline{R}^s \to 0,$$

is exact over $\overline{R} = R/fR$. Call the augmentation M. Then $M = \operatorname{Coker}(\alpha)$ is its own k th module of syzygies for arbitarily large k. This implies that $\operatorname{depth}_m(M) = n - 1$: over a Cohen-Macaulay ring, if a module has depth b smaller than that of the ring, its first module of syzygies has depth $b + 1$. Once the module has depth equal to that of the ring, the modules of syzygies, if nonzero, continue to have depth equal to that of the ring (in the case of R/fR, the eventual depth is $n - 1$). We have therefore established a correspondence between matrix factorizations of f into two factors and Cohen-Macaulay modules over R/fR that have finite projective dimension over R.

In our eventual construction of linear maximal Cohen-Macaulay modules over hypersurfaces, we shall make use of matrix factorizations with large numbers of factors.

By a *matrix factorization* of $f \in R$ over R of *size* s with d *factors* we mean a d-tuple of matrices $\alpha = (\alpha_1, \ldots, \alpha_d)$ over R such that

$$f\boldsymbol{I}_s = \alpha_1 \cdots \alpha_d$$

and satisfying the additional condition that for all i,

$$f\boldsymbol{I}_s = \alpha_i\alpha_{i+1} \cdots \alpha_d\alpha_1\alpha_2 \cdots \alpha_{i-1}$$

as well. Here, it will be convenient to interpret the subscripts mod d. Note that the weak commutativity condition is automatic if f is a nonzerodivisor in R, for then

$$(\alpha_1 \cdots \alpha_{i-1})^{-1} = f\alpha_i\alpha_{i+1} \cdots \alpha_d$$

for all i, which implies that $\alpha_1 \cdots \alpha_{i-1}$ and $\alpha_i\alpha_{i+1} \cdots \alpha_d$ commute for all i. If α is either a matrix or a d-tuple of matrices, $I(\alpha) = I_1(\alpha)$ denotes the ideal generated by the entries of α or by the entries of all of the matrices occurring in α.

We define two matrix factorizations of size s with d factors, say $\alpha = (\alpha_1, \ldots, \alpha_d)$ and $\beta = (\beta_1, \ldots, \beta_d)$, to be *equivalent* if there are invertible $s \times s$ matrices $\gamma_0, \gamma_1, \ldots, \gamma_d$ over R such that $\gamma_0 = \gamma_d$ and for all i, $1 \leq i \leq d$, we have $\beta_i = \gamma_{i-1}\alpha_i\gamma_i^{-1}$.

Our goal is to prove that if $I \subseteq R$ and $f \in I^d$ for $d \geq 2$ then f has a matrix factorization $\alpha = (\alpha_1, \ldots, \alpha_d)$ of some size s with d factors such that $I(\alpha) = I$. Moreover, we shall see that by increasing s this can even be done in such a way that all of the matrices α_i are the same, and $I(\alpha_i) = I$ for all i.

The argument will involve solving the problem for a "generic form" of degree s in indeterminates over $\mathbb{Z}$, and then specializing.

We shall use the theory of Clifford algebras and Clifford modules over a field K to prove the existence of matrix factorizations.

Discussion: the definition of Clifford algebras. Let K be a field, let L be the vector space spanned by n variables $X_1, \ldots, X_n$, and let $V = L^* = \mathrm{Hom}_K(V, K)$ be the space of linear functionals on L with dual basis $e_1, \ldots, e_n$. Let f be a form of degree d in $X_1, \ldots, X_d$ such that f does not vanish identically on K^d. This is automatic when K is infinite. Our main interest is in the case where $K = \mathbb{Q}$.

The *Clifford algebra* over K corresponding to f, which we denote $C(f)$, is defined as follows. Let $\mathcal{T}(V)$ denote the tensor algebra of V over K, which is an $\mathbb{N}$-graded associative algebra over K such that $[\mathcal{T}(V)]_h$ is the h-fold tensor product $V \otimes_K V \otimes_K \cdots \otimes_K V$, where there are h copies of V. We may alternatively write $[\mathcal{T}(V)]_h = V^{\otimes h}$. Note that $\mathcal{T}(V)]_0 = K$, and $[\mathcal{T}(V)]_1 = V$, which generates $\mathcal{T}(V)$ over K. The multiplication is such that

$$(v_1 \otimes \cdots \otimes v_a)(w_1 \otimes \cdots \otimes w_b) = (v_1 \otimes \cdots \otimes v_a \otimes w_1 \otimes \cdots \otimes w_b).$$

$C(f)$ is defined as the quotient of $\mathcal{T}(V)$ by the two-sided ideal generated by all elements of the form

$$(c_1e_1 + \cdots + c_ne_n)^d - f(c_1, \ldots, c_n)$$

for all $(c_1, \ldots, c_n) \in K^n$. Thus, $\mathcal{T}(f)$ is universal with respect to the property the dth power of every linear form is a scalar whose value is determined by applying f to the coefficients of the form.

The most common use of these algebras is in the case where $d = 2$, but it will be very important to consider larger values of d here.

We note that the the Clifford algebra $C(f)$ is $\mathbb{Z}_d$-graded: this follows from the fact that every homogeneous component of every generator has degree 0 or d. When C is a $\mathbb{Z}_d$-graded algebra or module, and i is an integer, we may write either $[C]_i$ or $[C]_{[i]}$ for the component of C in degree $[i]$, where $[i]$ is the class of i modulo d.

By a *Clifford module* over a Clifford algebra $C(f)$ we mean a $\mathbb{Z}_d$-graded $C(f)$-module M such that M is a nonzero finite-dimensional K-vector space. It is not at all clear whether a Clifford algebra has a Clifford module. The following result makes a strong connection with matrix factorization. We may write either $[M]_i$ or M_i for the graded component in degree i.

Proposition. *Let K be an field, let L be the vector space spanned over K by n indeterminates $X_1, \dots, X_n$, let f be a form of degree $d \geq 2$ that does not vanish identically on K^n, which is always the case when f is nonzero and K is infinite, let $V = L^*$, and let $C(f)$ be the Clifford algebra of f over K.*

(a) *If M is a Clifford module, then all the M_i have the same$K$-vector space dimension, say s.*

(b) *If K is infinite, then there is a bijective correspondence between isomorphism classes of Clifford modules M over $C(f)$ such that every M_i has dimension $s \geq 1$ over K and equivalence classes of of matrix factorizations of f over K.*

Proof. For part (a), suppose $F(c_1, \dots, c_n) \neq 0$ and let $v = c_1e_1 + \cdots + c_ne_n \in V$. Multiplication by v gives a K-linear map $M_i \to M_{i+1}$ for every i. The composition of all of these maps is multiplication by v^n, which is the same as multiplication by $f(c_1, \dots, c_n) = a \in K - \{0\}$. Since v^n is an automorphism of M, each map $M_i \to M_{i+1}$ given by multiplication by v is a K-linear bijection.

We now prove (b). Fix a K-basis for every M_i. Let η_{ij} be the matrix of multiplication by $e_j \in V$ as a map $M_i \to M_{i+1}$ with respect to the fixed bases. Let $\underline{c} = c_1, \dots, c_n$ be any elements of K. Then the matrix of multiplication by $v = c_1e_1 + \cdots c_ne_n$ mapping $M_i \to M_{i+1}$ is $\theta_i(\underline{c}) = c_1\eta_{i1} + \cdots + c_n\eta_{in}$. For all choices of $\underline{c}$, the composition of maps

$$\big(M_{i+d-1} \xrightarrow{\theta_{i+d-1}(\underline{c})} M_{i+d}\big) \circ \cdots \circ \big(M_{i+1} \xrightarrow{\theta_{i+1}(\underline{c})} M_{i+2}\big) \circ \big(M_i \xrightarrow{\theta_i(\underline{c})} M_{i+1}\big)$$

is multiplication by $f(c_1, \dots, c_n)$, i.e.,

$$(*) \qquad f\big((\underline{c})\big)\boldsymbol{I}_s = \theta_i(\underline{c})\theta_{i+1}(\underline{c}) \cdots \theta_{i+d-1}(\underline{c}).$$

Keep in mind here that $M_{i+d} = M_i$. Since K is infinite, it follows that $(*)$ holds when we replace the elements c_i by indeterminates. Thus, if for every i we let

$$\alpha'_i = X_1\eta_{i1} + \cdots + X_n\eta_{in},$$

which is a matrix of linear forms in the X_j over K, then we must have

$$(**) \qquad f\big(X_1, \dots, X_n\big)\boldsymbol{I}_s = \alpha'_{i-1}(X_1, \dots, X_n)\alpha'_{i-2}(X_1, \dots, X_n) \cdots \alpha'_i(X_1, \dots, X_n)$$

for all i. Thus gives a matrx factorization except that the matrices are numbered in reverse. If we let $\alpha_i = \alpha'_{d+1-i}$ we have a matrix factorization

Conversely, given a matrix factorization of size s, we may construct a Clifford module M with all components M_i isomorphic to K^s by letting the multiplication by the linear form

$$v = c_1e_1 + \cdots + c_ne_n$$

from the i th component to the $i+1$ st component be the map whose matrix is obtained by the substitution $X_1 = c_1, \ldots, X_n = c_n$ in the matrix α_{d+1-i}.

The statement about isomorphism now follows from the fact that if $\gamma_1, \ldots, \gamma_d$ are change of basis matrices for the various $M_{d+1-i} = K^s$, the matrices α_i change to $\gamma_{i-1}\alpha_i\gamma_i^{-1}$. □

Let C and C' be two $\mathbb{Z}_d$-graded associative K-algebras (this statement includes the hypothesis that K is in the center of each). Let $\Psi_d(t) \in \mathbb{Z}[t]$ denote the d th cyclotomic polynomial (we discuss these further later) over $\mathbb{Q}$, which is the minimal polynomial over $\mathbb{Q}$ of a primitive d th root of unity in $\mathbb{C}$. Assume that K contains a root ξ of $\Psi_d(t)$, which will, of course, be a d th root of unity, since $\Psi(t)$ divides $t^d - 1$ even in $\mathbb{Z}[t]$. K can always be enlarged by a finite algebraic extension to contain such an element ξ. If K has characteristic 0, ξ is simply a primitive d th root of unity.

We then define the *twisted* tensor product $C \otimes_K C'$ to be the $\mathbb{Z}_d$-graded K-algebra which, as a K-vector space, is simply $C \otimes_K C'$, graded so that

$$[C \otimes_K C']_i = \bigoplus_{j+k=i} [C]_i \otimes_K [C']_j$$

where i, j, and k are in $\mathbb{Z}_d$, and with multiplication such that, if $u, v \in C$ are forms and $u', v' \in C'$ are forms, then

$$(\#) \qquad (u \otimes u')(v \otimes v') = \xi^{\deg(u')\deg(v)}(uv) \otimes (u'v').$$

It is easy to check that multiplication is associative for triples of elements each of which is a tensor product of two forms, and the general case follows readily. Notice in particular that if u and u' are 1-forms, then

$$(1 \otimes u')(u \otimes 1) = \xi(u \otimes 1)(1 \otimes u').$$

Quite similarly, we can give essentially the same definition for the *twisted tensor product* $M \otimes_K M'$ of a $\mathbb{Z}_d$-graded C-module M and a $\mathbb{Z}_d$-graded C'-module M', which will be a $\mathbb{Z}_d$-graded module over $C \otimes_K C'$. One has to give the action of $C \otimes_K C'$ on $M \otimes_K M'$. The formula is the same as given in (#), but now $u \in C$, $u \in C'$, $v \in M$ and $v' \in M'$ are forms.

Lecture of March 25, 2019

We want to establish that in the twisted tensor product of two $\mathbb{Z}_d$-graded K-algebras, $C \otimes_K C'$, one has that if $u \in C$ and $v \in C'$ are forms of degree 1, then

$$(u \otimes 1 + 1 \otimes v)^d = u^d \otimes 1 + 1 \otimes v^d,$$

a property reminiscent of the behavior of the Frobenius endomorphism in the commuative case. In order to prove this, we need to develop a "twisted" binomial theorem.

To this end, let $\widetilde{q}$, $\widetilde{U}$, and $\widetilde{V}$ be non-commuting indeterminates over $\mathbb{Z}$ and form the free algebra they generate modulo the relations

(1) $\widetilde{q}\widetilde{U} = \widetilde{U}\widetilde{q}$

(2) $\widetilde{q}\widetilde{V} = \widetilde{V}\widetilde{q}$

(3) $\widetilde{V}\widetilde{U} = \widetilde{q}\widetilde{U}\widetilde{V}$

We denote the images of $\widetilde{q}$, $\widetilde{U}$, and $\widetilde{V}$ by q, U, and V, respectively. Thus, q is in the center of quotient ring $\mathcal{A}$. While U and V do not commute, it is clear that every monomial in U and V may be rewritten in the form $q^iU^jV^k$, with i, j, $k \in \mathbb{N}$, in this ring. In fact, $\mathcal{A}$ is the free $\mathbb{Z}$-module spanned by these monomials, with the multiplication

$$(q^iU^jV^k)(q^{i'}U^{j'}V^{k'}) = q^{i+i'+kj'}U^{j+j'}V^{k+k'}.$$

This is forced by iterated use of the relations (1), (2), and (3), and one can check easily that this gives an associative multiplication on the free $\mathbb{Z}$-module on the monomials $q^iU^jV^k$.

In this algebra, one may calculate $(U+V)^d$ and write it as a linear combination of monomials U^iV^j each of whose coefficients is a polynomial in $\mathbb{Z}[q]$. When q is specialized to 1, the coefficients simply become ordinary binomial coefficients. We want to investigate these coefficients, which are called *Gaussian polynomials*, *Gaussian coefficients*, or *q-binomial coefficients*. We shall denote the coefficient of U^kV^{d-k}, $0 \le i \le d$, as $\begin{bmatrix} d \\ k \end{bmatrix}_q$. For example,

$$(U+V)^2 = V^2 + UV + VU + U^2 = V^2 + (q+1)UV + V^2,$$

and so $\begin{bmatrix} 2 \\ 0 \end{bmatrix}_q = \begin{bmatrix} 2 \\ 2 \end{bmatrix}_q = 1$ while $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = q+1$.

Theorem (twisted binomial theorem). *Let notation be as above.*

(a) *The coefficient polynomials* $\begin{bmatrix} d \\ k \end{bmatrix}_q$ *are determined recursively by the rules*

(1) $\begin{bmatrix} d \\ 0 \end{bmatrix}_q = \begin{bmatrix} d \\ d \end{bmatrix}_q = 1$ *and*

(2) $\begin{bmatrix} d+1 \\ k+1 \end{bmatrix}_q = \begin{bmatrix} d \\ k \end{bmatrix}_q + q^{k+1}\begin{bmatrix} d \\ k+1 \end{bmatrix}_q.$

(b) *For all d and k,* $\begin{bmatrix} d \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{1-q^{d-i}}{1-q^{i+1}}.$

(c) *Let λ, u, and v be elements of any associative ring $\mathcal{R}$ with identity such that λ commutes with u and v and $vu = \lambda uv$. Let $\begin{bmatrix} d \\ k \end{bmatrix}_q(\lambda)$ denote the element of $\mathcal{R}$ that is the image of $\begin{bmatrix} k \\ d \end{bmatrix}_q$ under the map $\mathbb{Z}[q] \to \mathcal{R}$ that sends $q \mapsto \lambda$. Then*

$$(u+v)^d = \sum_{k=0}^{d} \begin{bmatrix} d \\ k \end{bmatrix}_q(\lambda) u^k v^{d-k}.$$

Proof. For part (a), first note that is it is evident that the coefficients of V^d and U^d in the expansion of $(U+V)^d$ are both 1. Now $(U+V)^{d+1} = (U+V)(U+V)^d$, and it is clear that there are two terms in the expansion that contribute to the coefficient of $U^{k+1}V^{d-k}$: one is the product of U with the U^kV^{d-k} term in $(U+V)^{d-k}$, which gives $\begin{bmatrix} d \\ k \end{bmatrix}_q U^{k+1}V^{d-k}$, and the other is the product of V with the $U^{k+1}V^{d-k-1}$ term, which gives $\begin{bmatrix} d \\ k+1 \end{bmatrix}_q VU^{k+1}V^{d-k-1}$. Since $VU^{k+1} = q^{k+1}U^{k+1}V$, the result follows.

For part (b), it will suffice to show that the proposed expressions for the $\begin{bmatrix} d \\ k \end{bmatrix}_q$ satisfy the recursion in part (a), that is:

$$\prod_{i=0}^{k} \frac{1-q^{d+1-i}}{1-q^{i+1}} = \prod_{i=0}^{k-1} \frac{1-q^{d-i}}{1-q^{i+1}} + q^{k+1} \prod_{i=0}^{k} \frac{1-q^{d-i}}{1-q^{i+1}}.$$

We can clear denominators by multiplying by the denominator of the left hand term to get the equivalent statement:

$$(*) \quad \prod_{i=0}^{k}(1-q^{d+1-i}) = (1-q^{k+1}) \prod_{i=0}^{k-1}(1-q^{d-i}) + q^{k+1} \prod_{i=0}^{k}(1-q^{d-i}).$$

The left hand term may be rewritten as

$$\prod_{j=-1}^{k-1}(1-q^{d-j}) = (1-q^{d+1}) \prod_{i=0}^{k-1}(1-q^{d-i}).$$

We may divide both sides of $(*)$ by

$$\prod_{i=0}^{k-1}(1-q^{d-i})$$

to see that $(*)$ is equivalent to

$$1 - q^{d+1} = 1 - q^{k+1} + q^{k+1}(1 - q^{d-k}),$$

which is true.

Part (c) follows at once, for there is a homomorphism of $\mathcal{A} = \mathbb{Z}[q, U, V] \to \mathcal{R}$ such that $q \mapsto \lambda$, $U \mapsto u$ and $V \mapsto v$. □

Recall that the dth cylcotomic polynomial $\Psi_d(t)$, $d \geq 1$, is the minimal polynomial of a primitive dth root of unity over $\mathbb{Q}$. It is a monic polynomial with coefficients in $\mathbb{Z}$ and irreducible over $\mathbb{Z}$ and $\mathbb{Q}$. The degree of $\Psi_d(t)$ is the Euler function $\Phi(d)$, whose value is the number of units in $\mathbb{Z}_d$. If $d = p_1^{k_1} \cdots p_h^{k_h}$ is the prime factorization of d, where the p_i are mutually distinct, then

$$\Phi(d) = \prod_{j=1}^{h} (p^{k_j} - p^{k_j - 1}).$$

The polynomials $\Psi_d(t)$ may be found recursively, using the fact that

$$t^d - 1 = \prod_{a|d} \Psi_a(t),$$

where a runs through the positive integer divisors of d. We next observe:

Corollary. *For every d and $1 \leq k \leq d-1$, $\Psi_d(q)$ divides $\begin{bmatrix} d \\ k \end{bmatrix}_q$ in $\mathbb{Z}[q]$.*

Proof. Let ξ be a primitive dth root of unity in $\mathbb{C}$. It suffices to show that $\begin{bmatrix} d \\ k \end{bmatrix}_q (\xi) = 0$. This is immediate from the formula in part (b) of the Theorem, since one of the factors in the numerator, corresponding to $i = 0$, is $q^d - 1$, which vanishes when $q = \xi$, while the exponents on q in the factors in the denominator vary between 1 and $k < d$, and so the denominator does not vanish when we substitute $q = \xi$. □

Corollary. *In the twisted tensor product $C \otimes C'$ of two $\mathbb{Z}_d$-graded K-algebras, if u is any form of degree 1 in C and v is any form of degree 1 in C', then $(u \otimes 1 + 1 \otimes v)^d = u^d \otimes 1 + 1 \otimes_d v^d$.*

Proof. By the preceding Corollary, all the q-binomial coefficients of the terms involving both $u \otimes 1$ and $1 \otimes v$ vanish. □

Theorem. *Let f and g be forms of degree d over a field K in disjoint sets of variables, say $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_m$. Then there is a surjective $\mathbb{Z}_d$-graded K-algebra homomorphism $C(f+g) \twoheadrightarrow C(f) \otimes_K C(g)$. Hence, if M is a Clifford module over $C(f)$ and*

N is a Clifford module over $C(g)$, then the twisted tensor product $M \otimes_K N$ is a Clifford module over $C(f+g)$.

Proof. Let V be the dual of the K-span of $X_1, \ldots, X_n$, with dual K-basis $e_1, \ldots, e_n$, and let V' the dual of the K-span of $Y_1, \ldots, Y_m$, with dual basis $e'_1, \ldots, e'_m$. Then $C(f+g)$ is the quotient of $\mathcal{T}(V \oplus V')$ by the two-sided ideal generated by all relations of the the form

$$(*) \quad (c_1e_1 + \cdots + c_ne_n + c'_1e'_1 + \cdots + c'_me'_m)^d - f(c_1, \ldots, c_n) - g(c'_1, \ldots, c'_m),$$

where $\underline{c} = c_1, \ldots, c_n \in K$ and $\underline{c'} = c'_1, \ldots, c'_m \in K$. The maps $\mathcal{T}(V) \twoheadrightarrow C(f)$ and $\mathcal{T}(V') \twoheadrightarrow C(g)$ will induce a map $C(f+g) \twoheadrightarrow C(f) \otimes_K C(g)$ provided that each of the relations $(*)$ maps to 0 in $C(f) \otimes_K C(g)$. With

$$u = c_1e_1 + \cdots + c_ne_n$$

and

$$v = c'_1e'_1 + \cdots + c'_me'_m,$$

we have that

$$(v \otimes 1)(u \otimes 1) = \xi\,(u \otimes 1)(1 \otimes v)$$

in the twisted tensor product, and so $(u+v)^d$ maps to $u^d \otimes 1 + 1 \otimes v^d$. Thus, the element displayed in $(*)$ maps to

$$u^d \otimes 1 + 1 \otimes v^d - f(\underline{c})(1 \otimes 1) - g(\underline{c'})(1 \otimes 1) = \big(u^d - f(\underline{c})\big) \otimes 1 + 1 \otimes \big(v^d - g(\underline{c'})\big) = 0 + 0 = 0,$$

as required. □

We now use these ideas to get a matrix factorization for a generic form. In a sense, we carry this out over the field $Q[\xi]$, but we observe that the entries of the matrices are actually in $\mathbb{Z}[\xi]$. We then embed $\mathbb{Z}[\xi]$ in a ring of matrices over $\mathbb{Z}$ to get a solution over $\mathbb{Z}$. This result gives the a version of the theorem over any ring, by applying a suitable homomorphism.

We first introduce two notations. If $\alpha_1, \ldots, \alpha_d$ are square matrices, then $\mathrm{diag}(a_1, \ldots, a_d)$ denotes the square matrix whose size is the sum of the sizes of the $\alpha_1, \ldots, \alpha_d$, and whose block form is

$$\begin{pmatrix} \alpha_1 & 0 & 0 & \cdots & 0 \\ 0 & \alpha_2 & 0 & \cdots & 0 \\ 0 & 0 & \alpha_3 & \cdots & 0 \\ & & \cdots & & \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & \alpha_d \end{pmatrix}$$

This matrix corresponds to the direct sum of the maps represented by the $\alpha_1, \ldots, \alpha_d$.

When $\alpha_1, \ldots, \alpha_d$ are square matrices of the same size, say s, we write $\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)$ for the matrix whose block form is

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & \alpha_1 \\ \alpha_d & 0 & 0 & \cdots & 0 & 0 \\ 0 & \alpha_{d-1} & 0 & \cdots & 0 & 0 \\ & & & \cdots & & \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & \alpha_2 & 0 \end{pmatrix}$$

Here "cyc" stands for "cyclic." One may think about this matrix as follows. Suppose that the α_i are thought of as linear transformations on a vector space V of dimension s over K. Let $V_i = V$, $1 \le i \le d$, and let $W = V^{\oplus d}$ thought of as $V_1 \oplus \cdots \oplus V_d$. Then $\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)$ corresponds to the linear transformation of V whose restriction to V_i is given by $\alpha_{d+1-i} : V_i \to V_{i+1}$. The subscript i should be read modulo d, so that the restriction to V_d is $\alpha_1 : V_d \to V_1$. Thus, $\big(\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)\big)^d$, when restricted to V_i, is the composite

$$(V_{i-1} \xrightarrow{\alpha_{d+1-(i-1)}} V_i) \circ \cdots \circ (V_{i+1} \xrightarrow{\alpha_{d-i}} V_{i+2}) \circ (V_i \xrightarrow{\alpha_{d+1-i}} V_{i+1}),$$

i.e.,

$$\alpha_{d+2-i}\alpha_{d+3-i} \cdots \alpha_d \alpha_1 \cdots \alpha_{d-i}\alpha_{d+1-i}.$$

Hence, if $\alpha_1, \ldots, \alpha_d$ is a matrix factorization of f of size s, one also has a matrix factorization of f of size ds with d factors all of which are equal to $\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)$.

Theorem. *Let $d \ge 2$ and $s \ge 1$ be integers, and let f denote the degree d linear form over $\mathbb{Z}$ in sd variables given as*

$$f = X_{1,1}X_{1,2} \cdots X_{1,d} + \cdots + X_{s,1}X_{s,2} \cdots X_{s,d}.$$

Note that f is the sum of s products of d variables, where all of the variables that occur are distinct. Let ξ be a primitive d th root of unity. Then f has a matrix factorization $f\boldsymbol{I}_{d^{s-1}} = \alpha_1 \cdots \alpha_d$ over

$$R = \mathbb{Z}[\xi][X_{ij} : 1 \le i \le s,\ 1 \le j \le d]$$

of size s^{d-1} such that $I(\alpha) = (X_{ij} : 1 \le i \le s,\ 1 \le j \le d)R$. Moreover, every entry of every matrix is either 0 or of the form $\xi^k X_{ij}$.

Proof. We use induction on s. We construct the factorization over $\mathbb{Q}[\xi]$, but show as we do so that the entries of the matrices constructed are in $\mathbb{Z}[\xi]$.

If $s = 1$ we have that

$$(x_{1,1}x_{1,2} \cdots x_{1,d}) = (x_{1,1})(x_{1,2}) \cdots (x_{1,d}).$$

By part (b) of the Proposition on p. 3 of the Lecture Notes of March 22, we have a corresponding Clifford module.

Now suppose that we have constructed a matrix factorization $\beta_1, \ldots, \beta_d$ of size d^{s-1} for

$$f_1 = X_{11}X_{12}\cdots X_{1d} + \cdots + X_{s-1,1}X_{s2}\cdots X_{s-1,d}$$

that satisfies the conditions of the theorem. Let M be the corresponding Clifford module. We also have a factorization for $g = x_{s,1}\cdots x_{s_d}$, namely

$$(x_{s,1}x_{s,2}\cdots x_{s,d}) = (x_{s,1})(x_{s,2})\cdots(x_{s,d}).$$

Since the two sets of variables occurring in f_1 and g respectively are disjoint, the twisted tensor product $M \otimes_K N$, where $K = \mathbb{Q}[\xi]$, of the corresponding Clifford modules is a Clifford module Q over $C(f_1 + g) = C(f)$, by the Theorem at the top of p. 4 of today's Lecture Notes. Note that each N_j has dimension 1, and that

$$(*) \quad Q_i = M_{i-1} \otimes_K N_1 \oplus M_{i-2} \otimes_K N_2 \oplus \cdots \oplus M_i \otimes_K N_d$$

has dimension s^{d-1}. Then Q gives a matrix factorization of $f = f_1 + g$ of size d^{s-1} over $\mathbb{Q}[\xi]$.

However, we shall give explicit bases for the Q_i and show that the matrices that occur have entries of the form specified in the statement of the theorem, which shows that one has a matrix factorization over $Z[\xi]$. We use all the tensors of pairs of basis elements, one from one of the M_i and one from one of the N_j but order the basis for Q_i as indicated in the direct sum displayed in $(*)$ above. The result is that the map from $Q_i \to Q_{i+1}$ that comes from multiplication by $c_{1,1}e_{1,1} + \cdots + c_{s-1,d}e_{s-1,d}$ (the indexing on the scalars $c_{i,j}$ corresponds to the indexing on the variables $X_{i,j}$) has as its matrix the result obtained by substituting the $c_{i,j}$ for the $X_{i,j}$ in $\mathrm{diag}(\beta_{d+1-i-1}, \beta_{d+1-i-2}, \cdots, \beta_{d+1-i})$, for the map is the direct sum of the maps $M_{i-j} \otimes_K N_j \to M_{i-j+1} \otimes_K N_j$ induced by the maps $M_{i-j} \to M_{i-j+1}$.

On the other hand, the map from $Q_i \to Q_{i+1}$ given by multiplication by $c'_1e'_1 + \cdots c'_de'_d$ maps the j th term $M_{i-j} \otimes_K N_j$ to the $j+1$ st term $M_{i-j} \otimes_K N_{j+1}$, and corresponds to multiplication by $\xi^{i-j}X_{s,d+1-j}$ evaluated at $(\underline{c}')$ on the summand $M_{i-j} \otimes_K N_j$, which has K-vector space dimension d^{s-2}. The result γ_{d+1-i} is the matrix

$$\mathrm{cyc}(\xi^{i-d}X_{s,1}\boldsymbol{I}_{d^{s-2}},\, \xi^{i-(d-1)}X_{s,2}\boldsymbol{I}_{d^{s-2}},\, \ldots,\, \xi^{i-1}X_{s,1}\boldsymbol{I}_{d^{s-2}}),$$

Therefore, we get a matrix factorization of f with d factors of size d^{s-1} in which

$$\alpha_i = \mathrm{diag}(\beta_{i-1}, \beta_{i-2}, \cdots, \beta_i) + \gamma_i.$$

Since all of the coefficients needed are 0 or powers of ξ, this is a factorization over $\mathbb{Z}[\xi]$. All of the variables occur, possibly with coefficient ξ^k, but ξ is a unit in $\mathbb{Z}[\xi]$, and so all of the conditions of the theorem are satisfied. $\square$

Lecture of March 27, 2019

Our next objective is to give a matrix factorization of a generic form over $\mathbb{Z}$ instead of $\mathbb{Z}[\xi]$. The idea is to replace the ring $\mathbb{Z}[\xi]$ by a ring of matrices over $\mathbb{Z}$.

Discussion: block form. Let R be any associative ring with identity, and let $\mathcal{M}_n(R)$ denote the ring of $n \times n$ matrices with entries of R, which we may identify, as usual, with the ring of R-linear edomorphisms of R^n, thought of as $n \times 1$ column vectors over R. The matrix η acts on the column γ by mapping it to $\eta\gamma$. The observation we want to make is that we may identify $\mathcal{M}_{kh}(R) \cong \mathcal{M}_k(\mathcal{M}_h(R))$. The naive way to make the identification is to partition each $kh \times kh$ matrix into a $k \times k$ array of $h \times h$ blocks. More conceptually, we may think of the domain of an R-linear map $R^{kh} \to R^{kh}$ as the direct sum of k copies of R^h, i.e., as $(R^h)^{\oplus k}$, and we may think of the target of the map as $(R^h)^k$, the product of k copies of R^h. Then the map is determined by its restrictions to the k direct summands R^h of the domain, and the map from a particular summand $R^h \to (R^h)^k$ corresponds to giving k R-linear maps $R^h \to R^h$, one for each factor of the target module.

Discussion: polynomials in commuting variables over a matrix ring. . Let $X_1, \ldots, X_k$ denote indeterminates both over R and over each matrix ring over R such that the X_i commute with one another, with elements of R, and with matrices over R. Then we may identify the rings

$$\mathcal{M}_n(R[X_1, \ldots, X_k]) \cong \mathcal{M}_n(R)[X_1, \ldots, X_k].$$

Given a finite linear combination $\sum_h \eta^{(h)}\mu_h$ where each $\eta^{(h)} = \bigl(r_{ij}^{(h)}\bigr) \in \mathcal{M}_n(R)$ and each μ_h is a monomial in the X_i, we let it correspond to the matrix $\bigl(\sum_h r_{ij}^{(h)}\mu_h\bigr)$.

Let ξ be a primitive dth root of unity. Recall that its minimal polynomial is denoted $\Psi_d(t)$: suppose that $\delta = \Phi(d)$, which is the degree of Ψ_d, and that

$$\Psi_d(z) = z^\delta + c_{\delta-1}z^{\delta-1} + \cdots + c_0,$$

where the $c_j \in \mathbb{Z}$. If we take $1, \xi, \xi^2, \ldots, \xi^{\delta-1}$ as a basis for $\mathbb{Z}[\xi]$, then the matrix of multiplication by ξ on $Z[\xi]$ is

$$\theta = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ & & & \cdots & & \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & -c_{\delta-1} \end{pmatrix},$$

the *companion* matrix of $\Psi_d(t)$, and $\mathbb{Z}[\xi] \cong \mathbb{Z}[\theta] \subseteq \mathcal{M}_\delta(\mathbb{Z})$. Notice that each of the powers $\boldsymbol{I}_\delta, \theta, \theta^2, \ldots, \theta^{d-1}$ has an entry equal to 1, because θ^i maps the basis element 1 to the basis element θ^i, $0 \le i \le d-1$.

We then have:

Theorem. *Let $d \geq 2$ and $s \geq 1$ be integers, and let f denote the degree d linear form over $\mathbb{Z}$ in sd variables given as*

$$f = X_{1,1}X_{1,2}\cdots X_{1,d} + \cdots + X_{s,1}X_{s,2}\cdots X_{s,d}.$$

Let $\delta = \Phi(d)$. Then f has a matrix factorization $f\boldsymbol{I}_{\delta d^{s-1}} = \alpha_1 \cdots \alpha_d$ over

$$R = \mathbb{Z}[X_{i,j} : 1 \leq i \leq s,\ 1 \leq j \leq d]$$

of size δs^{d-1} such that $I(\alpha) = (X_{i,j} : 1 \leq i \leq s,\ 1 \leq j \leq d)R$.

Proof. We begin with the matrix factorization over $R[\xi]$ which has size d^{s-1} given in the Theorem on p. 5 of the Lecture Notes of March 25. We write $\underline{X}$ for the collection of variables $X_{i,j}$, $1 \leq i \leq s$, $1 \leq j \leq d$. By the Discussions above, we have an embedding of

$$\mathbb{Z}[\xi][\underline{X}] \hookrightarrow \mathcal{M}_\delta(\mathbb{Z})[\underline{X}] \cong \mathcal{M}_\delta(\mathbb{Z}[\underline{X}])$$

which will give a matrix factorization of $(f\boldsymbol{I}_\delta)\boldsymbol{I}_{d^{s-1}}$ with d factors in $\mathcal{M}_{d^{s-1}}\big(\mathcal{M}_\delta(R)\big)$. Under the identification $\mathcal{M}_{d^{s-1}}\big(\mathcal{M}_\delta(R)\big) \cong \mathcal{M}_{\delta d^{s-1}}(R)$ this yields a matrix factorization for $f\boldsymbol{I}_{\delta d^{s-1}}$ whose entries are $\mathbb{Z}$-linear forms in the variables $\underline{X}$. In the factorization given in the previous Theorem, every $X_{i,j}$ occurred, possibly with a coefficient ξ^k, $0 \leq k \leq \delta - 1$. In the new factorization $\xi^k X_{i,j}$ is replaced by a block corresponding to $\theta^k X_{i,j}$. Since θ^k has an entry equal to 1, the variable $X_{i,j}$ occurs as an entry. $\square$

Now that we have dealt with the generic case, we can immediately get a corresponding result for any finitely generated ideal in any ring.

Theorem. *Let I be a finitely generated ideal of a ring R, and let $f \in I^d$, where $d \geq 2$. Then for some integer N there exists a matrix factorization $f\boldsymbol{I}_N = \alpha_1 \cdots \alpha_d$ such that $I(\alpha) = I$. In fact, there exists such a factorization in which $\alpha_1 = \alpha_2 = \cdots = \alpha_d$, and $I(\alpha_i) = I$, $1 \leq i \leq d$.*

Proof. Since $f \in I^d$, for some choice of elements $u_{ij} \in I$ we can write

$$f = u_{1,i} \cdots u_{1,d} + \cdots + u_{s,1} \cdots u_{s,d}$$

with all of the $u_{i,j} \in I$. We may assume all of the finitely many generators of I occur among the $u_{i,j}$ by including some extra terms in which one of the factors is 0. We may then map $\mathbb{Z}[X_{i,j} : 1 \leq i \leq s, 1 \leq j \leq d] \to R$ so that $X_{i,j} \mapsto u_{i,j}$. Applying the homomorphism to the factorization for the generic form given in the preceding Theorem, we obtain a factorization of f satisfying all but one of the conditions needed: it need not satisfy the condition that

$$\alpha_1 = \alpha_2 = \cdots = \alpha_d.$$

But we may satisfy the additional condition by increasing the size by a factor of d and taking all of the matrices to be $\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)$: see the discussion on p. 5 of the Lecture Notes of March 25. $\square$

The following result will play an important role in our construction of linear maximal Cohen-Macaulay modules over hypersurfaces.

Theorem. *Let $(R,\, m,\, K)$ be a local ring, and let $f \in m^d$ be a nonzerodivisor, where $d \geq 2$. Then for some s there is a matrix factorization $f\boldsymbol{I}_s = \alpha_1 \cdots \alpha_d$ such that $I(\alpha_i) = m$ for $1 \leq i \leq d$. Let $G = G_0 = R^s$, and let G_i be the image of $\psi_i = \alpha_1\alpha_2 \cdots \alpha_i$, so that $G_i \subseteq R^s$ as well, and $G_d = fR^s$. Let $M_i = G_i/G_{i+1}$, $1 \leq i \leq d$. Then all of the modules G_i/G_d, G/G_{i+1} and M_i, $0 \leq i \leq d-1$, are maximal Cohen-Macaulay modules over $\overline{R} = R/fR$, and all of them have finite projective dimension, necessarily 1, over R. Moreover, $\nu(M_i) = s$, $0 \leq i \leq d-1$.*

Proof. Since $f\boldsymbol{I}_s = \psi_i\psi'_i$, where $\psi'_i = \alpha_{i+1} \cdots \alpha_d$, we have from the Discussion on the first page of the Lecture Notes of March 21 concerning Cohen-Macaulay modules over hypersurfaces that if $\overline{}$ indicates images after applying $\overline{R} \otimes_R \_$, then

$$\cdots \xrightarrow{\overline{\psi'_i}} \overline{R}^s \xrightarrow{\overline{\psi_i}} \overline{R}^s \xrightarrow{\overline{\psi'_i}} \overline{R}^s \xrightarrow{\overline{\psi_i}} \overline{R}^s \to 0$$

is acyclic, and that

$$\operatorname{Ker} \overline{\psi'_i} = \operatorname{Im} \overline{\psi_i} \cong \operatorname{Coker} \overline{\psi'_i} \cong \operatorname{Coker} \psi'_i,$$

and the same holds with the roles of ψ_i and ψ'_i interchanged. The image of ψ_i contains fR^s, which is the image of $\psi_i\psi'_i$, i.e., $fR^s \subseteq G_i \subseteq R^s$, and $G_i/fR^s = G_i/G_d$ may be identified with $\operatorname{Im} \overline{\psi_i}$. Thus, every G_i/G_d is a maximal Cohen-Macaulay module over $\overline{R}$ of finite projective dimension over R. Note as well that $R^d/G_i = \operatorname{Coker} \psi_i$ is a maximal Cohen-Macaulay module over $\overline{R}$ of finite projective dimension over R.

We have that $G_{i+1} = \operatorname{Im} \psi_{i+1} = \operatorname{Im} \psi_i\alpha_{i+1} \subseteq \psi_i(mR^s)$, since $I(\alpha_{i+1}) = m$, and this is contained in $m\psi_i(R_s) = mG_i$. Hence, $M_i = G_i/G_{i+1}$ is minimally generated over $\overline{R}$ by s elements, and the short exact sequences

$$0 \to M_i \to R^s/G_{i+1} \to R^s/G_i \to 0$$

show that every M_i is a maximal Cohen-Macaulay over $\overline{R}$ of finite projective dimension over R as well.

A maximal Cohen-Macaulay module over $\overline{R}$ that has finite projective dimension over R must have projective dimension 1 over R, since its depth is $d-1$. □

Proposition. *Let $(R,\, m,\, K)$ be local and $f \in m^d - m^{d+1}$. Let $\mathcal{L}(f)$ denote the leading form of f, i.e., the image of f in $m^d/m^{d+1} = [\mathrm{gr}_m(R)]_d$. Suppose that N is a finitely generated R-module ($N = R$ is the most important case) and that $\mathcal{L}(f)$ is a nonzerodivisor on $\mathrm{gr}_m(N)$. Let $\overline{R} = R/fR$, which has maximal ideal $\overline{m} = m/fR$, and let $\overline{N} = N/fN$. Then*

(a) *f is a nonzerodivisor on N.*

(b) *For every integer $n \geq 0$, $fN \cap m^nN = fm^{n-d}N$.*

(c) *For every $u \in N - \{0\}$, $\mathcal{L}(fg) = \mathcal{L}(f)\mathcal{L}(u)$, and the m-adic order of fu is the sum of the m-adic orders of f and u.*

(d) $\mathrm{gr}_{\overline{m}}(\overline{N}) \cong \mathrm{gr}_m(N)/\mathcal{L}(f)\mathrm{gr}_m(N)$.

Proof. We first prove (c). If $u \neq 0$, say $u \in m^h N - m^{h+1}N$, then it follows that $fu \notin m^{d+h+1}N$, i.e., that $fu \in m^{d+h}N - m^{d+h+1}N$, or else $\mathcal{L}(f)\mathcal{L}(u) = 0$, a contradiction. This proves both that $\mathrm{ord}\,(fu) = d + h$ and that $\mathcal{L}(fu) = \mathcal{L}(f)\mathcal{L}(u)$. Part (a) follows as well, for if $fu = 0$, then $\mathcal{L}(f)\mathcal{L}(u) = 0$.

To prove (b), note that if $fu \in m^n N$, then $d + \mathrm{ord}\,(u) \geq n$, and so $\mathrm{ord}\,(u) \geq n - d$, which shows that $u \in m^{n-d}N$.

Finally, to prove (d), note that

$$\overline{m}^n\overline{N}/\overline{m}^{n+1}\overline{N} \cong (m^nN + fN)/(m^{n+1}N + fN) \cong m^nN/\big(m^nN \cap (m^{n+1}N + fN)\big).$$

Now if $u_n = u_{n+1} + fv$ with $u_n \in m^nN$ and $u_{n+1} \in m^{n+1}N$, then $fv = u_n - u_{n+1} \in m^nN$, and so $v \in m^{n-d}N$ by part (b). Then

$$\begin{aligned}\overline{m}^n\overline{N}/\overline{m}^{n+1}\overline{N} &\cong m^nN/(m^{n+1}N + fm^{n-d}N)\\ &\cong [\mathrm{gr}_m(N)]/\mathcal{L}(f)[\mathrm{gr}_m(N)]_{n-d} \cong [\mathrm{gr}_m(N)/\mathcal{L}(f)\mathrm{gr}_m(N)]_n,\end{aligned}$$

as required. □

Discussion. To calculate the multiplicity of a local ring (R, m, K) or of an R-module M one may work alternatively with the Hilbert function of $\mathrm{gr}_m(R)$ or the Hilbert function of $\mathrm{gr}_m(M)$: the lattter, for example, is defined as $\dim_K[\mathrm{gr}_m(M)]_n$, and is eventually a polynomial of degree $\dim(M) - 1$. This function is the first difference of the Hilbert function. If the Hilbert function of M has leading term $\frac{e}{r!}n^r$, where $r = \dim(M)$, then the leading term of the Hilbert function of $\mathrm{gr}_m(M)$ will be

$$\frac{e}{r!}rn^{r-1} = \frac{e}{(r-1)!}n^{r-1}.$$

Corollary. *Let (R, m, K) be local and let $f \in m$ be such that its leading form $\mathcal{L}(f)$ has degree d.*

(a) *If $\mathcal{L}(f)$ is a nonzerodivisor in $\mathrm{gr}_m(R)$, then $e(R/fR) = de(R)$.*

(b) *If N is a finitely generated R-module and $\mathcal{L}(f)$ is a nonzerodivisor on $\mathrm{gr}_m(N)$, then $e(N) = de(N/fN)$.*

Proof. It suffices to prove (b), which is more general. In the notation of the preceding proposition. $e(\overline{N})$ may be calculated from the Hilbert function of $\mathrm{gr}_{\overline{m}}(\overline{N})$, which is $\mathrm{gr}(N)/\mathcal{L}(f)\mathrm{gr}(N)$. If the Hilbert function of $\mathrm{gr}_m(N)$ is $H(n)$, the Hilbert function for $\mathrm{gr}(N)/\mathcal{L}(f)\mathrm{gr}(N)$ will be $H(n) - H(n - d)$. If the leading term of the polynomial corresponding to $H(n)$ is $\frac{e}{(r-1)!}n^{r-1}$, the new leading term is $\frac{de}{(r-2)!}n^{r-2}$, since the polynomial $cn^{r-1} - c(n - d)^{r-1}$ has leading term $cd(r - 1)n^{r-2}$ for any constant c. □

In order to prove the result we want on existence of linear maximal Cohen-Macaulay modules, we need to generalize the Theorem on p. 3 to a situation in which we have tensored with a linear maximal Cohen-Macaulay module N over R.

Lecture of March 29, 2019

The following result can be deduced easily from the Buchsbaum-Eisenbud acyclicity criterion, but we give a short, self-contained argument.

Proposition. *Let (R, m, K) be a local ring and N a maximal Cohen-Macaulay module over R. If M is a finitely generated R-module of finite projective dimension over R, then $\mathrm{Tor}_i^R(M, N) = 0$ for all $i \geq 1$.*

Proof. For any prime ideal P in $\mathrm{Supp}\,(N)$, N_P is again a maximal Cohen-Macaulay module over R_P. (This is clear if $\mathrm{height}\,(P) = 0$. If $\mathrm{height}\,(P) > 0$, choose $x \in P$ not in any minimal prime of R. Then x is not a zerodivisor on N, and the result follows by Noetherian induction, since N/xN will be a maximal Cohen-Macaulay module for R/xR.) Let $\mathrm{pd}_R(M) = h$. Then $\mathrm{Tor}_i^R(M,\, N) = 0$ for $i > h$. If we have a a counterexample, we can localize at a minimal prime P of $\bigoplus_{i=1}^h \mathrm{Tor}_i^R(M,\, N)$. Thus, we may assume without loss of generality that all of the non-vanishing $\mathrm{Tor}_i^R(M,\, N)$ for $i \geq 1$ have finite length, and we can choose i as large as possible for which one of these Tor modules is not 0. If

$$0 \to G_h \to \cdots \to G_0 \to 0$$

is a minimal free resolution of M over R, the modules $\mathrm{Tor}_i^R(M,\, N)$ are the homology modules of the complex

$$0 \to G_h \otimes_R N \to \cdots \to G_0 \otimes_R N \to 0.$$

Let d_j denote the map

$$G_j \otimes_R N \to G_{j-1} \otimes_R N.$$

Let $Z_j = \mathrm{Ker}\,(d_j)$ and let $B_j = \mathrm{Im}\,(d_{j+1})$. Thus, $Z_j = B_j$ for $j > i$. Note that we cannot have $\dim\,(R) = 0$, for then $\mathrm{pd}_R M \leq \mathrm{depth}_m(R) = 0$, and M is free. Thus, we may assume $\dim\,(R) \geq 1$. Also note that we cannot have $i = h$, because $\mathrm{Tor}_R^h(M,\, N) \subseteq G_h \otimes_R N$, a finite direct sum of copies of N, and has no submodule of finite length, since $\mathrm{depth}_m N = \dim\,(R) > 0$. Then we have a short exact sequence

$$0 \to B_i \to Z_i \to \mathrm{Tor}_i^R(M,\, N) \to 0$$

and an exact sequence

$$0 \to G_h \otimes_R N \to \cdots \to G_{i+1} \otimes_R N \to B_i \to 0.$$

Since $\mathrm{Tor}_i^R(M,\,N)$ is a nonzero module of depth 0, $Z_i \neq 0$, and $Z_i \subseteq G_i \otimes N$ has depth at least one. It follows that $\mathrm{depth}_m(B_i) = 1$. The exact sequences

$$0 \to B_j \to G_j \otimes_R N \to B_{j-i} \to 0$$

for $j > i$ enable us to see successively that $\mathrm{depth}_m B_{i+1} = 2$, $\mathrm{depth}_m B_{i+2} = 3$ and, eventually, $\mathrm{depth}_m B_{h-1} = (h-1) - (i-1) = h - i$. But $B_{h-1} = G_h \otimes_R N$ has depth $\dim(R) \geq \mathrm{depth}_m R \geq h > h - i$, since $i \geq 1$, a contradiction. □

We next observe the following result related to the final Corollary of the Lecture of March 27.

Lemma. *Let $(R,\,m,\,K)$ be local, and $f \in m^d - m^{d+1}$ be such that $\mathcal{L}(f)$ is part of a homogeneous system of parameters for $\mathrm{gr}_m(R)$. Let N be a linear maximal Cohen-Macaulay module. Then $e(N/fN) = de(N)$.*

Proof. Without loss of generality we may replace R by $R(t)$ and N by $R(t) \otimes_R N$, and so assume that we have an infinite residue class field. Let $\dim(R) = r$, and let $x_1,\,\ldots\,,x_r$ be a minimal reduction of m. Then $\mathrm{gr}_N \cong (N/mN) \otimes_K K[X_1,\,\ldots\,,X_r]$ is Cohen-Macaulay of depth r over $\mathrm{gr}_m(R)$: the images of the x_j in m/m^2 form a regular sequence. It follows that $\mathcal{L}(f)$, which has degree d, is a nonzerodivisor on $\mathrm{gr}_m(N)$, and we may apply part (b) of the final Corollary of the Lecture of March 27. □

We are now ready to prove the result we are aiming for (cf. [J. Herzog, B. Ulrich, and J. Backelin, *Linear maximal Cohen-Macaulay modules over strict complete intersections*, Journal of Pure and Applied Algebra **71** (1991) 187–202.]

Theorem (Herzog, Ulrich, and Backelin). *Let $(R,\,m,\,K)$ be a Cohen-Macaulay local ring that has a linear maximal Cohen-Macaulay module N. Let $f \in m^d - m^{d+1}$ be a nonzerodivisor such that its leading form $\mathcal{L}(f) \in \mathrm{gr}_m(R)$ is part of a homogeneous system of parameters for $\mathrm{gr}_m(R)$. Then R/fR has a linear maximal Cohen-Macaulay module.*

Proof. We adopt the notation of the Theorem on p. 3 of the Lecture of March 27, so that we have a chain

$$R^s = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_d = fR^s$$

as in the statement of that Theorem. Thus, the modules

$$0 \subseteq G_{d-1}/G_d \subseteq \cdots \subseteq G_i/G_d \subseteq \cdots \subseteq G_0/G_d$$

give an ascending filtration of $G_0/G_d \cong R^s/fR^s$ in which every factor module M_i is a maximal Cohen-Macaulay module over $\overline{R} = R/fR$ that is minimally generated by s elements and such that all of the modules G_i/G_d, G_0/G_i, and $M_i = G_i/G_{i+1}$ have finite projective dimension over R.

We shall show that the modules $G_i/G_d \otimes N$ give an ascending filtration of N^s/fN^s such that each factor $M_i \otimes_R N$ is a maximal Cohen-Macaulay module over $\overline{R}$. We then prove that at least one of $M_i \otimes_R N$ is a linear maximal Cohen-Macaulay module over $\overline{R}$.

First, we have short exact sequences

$$0 \to G_i/G_d \to G_0/G_d \to G_0/G_i \to 0,$$

$0 \leq i \leq d-1$ (this is the range for i throughout). These remain exact when we apply $\_ \otimes_R N$, since G_0/G_i has finite projective dimension over R and N is a maximal Cohen-Macaulay module: $\mathrm{Tor}_1(G_0/G_i,\, N) = 0$. This shows that each $(G_i/G_d) \otimes_R N$ embeds in

$$G_0/G_d \otimes_R N \cong \overline{R}^s \otimes_R N \cong (N/fN)^{\oplus s}.$$

The short exact sequences

$$0 \to G_{i+1}/G_d \to G_i/G_d \to M_i \to 0$$

likewise remain exact when we apply $\_ \otimes_R N$, and so it follows that the factors are the modules $M_i \otimes_R N$.

We want to prove that each $M_i \otimes_R N$ is a maximal Cohen-Macaulay module over $\overline{R}$. We use the notation of the proof of the Theorem on p. 3 of the Lecture Notes of March 27. Recall that the complex

$$\cdots \xrightarrow{\overline{\psi}_i'} \overline{R}^s \xrightarrow{\overline{\psi}_i} \overline{R}^s \xrightarrow{\overline{\psi}_i'} \overline{R}^s \xrightarrow{\overline{\psi}_i} \overline{R}^s \to 0$$

is acyclic, and that $\mathrm{Coker}\, \psi_i = R^s/G_i$, which is also $\mathrm{Coker}\, \overline{\psi_i}$. Moreover, we have that $\mathrm{Im}\, \overline{\psi_i} \cong G_i/G_d$. Therefore we have short exact sequences:

$$0 \to R^s/G_i \to \overline{R}^s \to G_i/G_d \to 0 \qquad \text{and} \qquad 0 \to G_i/G_d \to \overline{R}^s \to R^s/G_i \to 0$$

for all i, $0 \leq i \leq d-1$. Since these modules have finite projective dimension over R, both sequences remain exact when we apply $\_ \otimes_R N$, yielding

$$(*) \quad 0 \to (R^s/G_i) \otimes_R N \to \overline{N}^s \to (G_i/G_d) \otimes_R N \to 0$$

and

$$(**) \quad 0 \to (G_i/G_d) \otimes_R N \to \overline{N}^s \to (R^s/G_i) \otimes_R N \to 0.$$

If

$$k = \mathrm{depth}_m\big((G_i/G_d) \otimes_R N\big) < \dim(\overline{R}) = \mathrm{depth}_m \overline{N},$$

then (*) shows that

$$\mathrm{depth}_m\big((R^s/G_i) \otimes_R N\big) = k+1,$$

and then (**) shows that

$$\mathrm{depth}_m\big(G_i/G_d) \otimes_R N\big) \geq k+1 > k,$$

a contradiction. If

$$\operatorname{depth}_m\big((R^s/G_i)\otimes_R N\big) < \dim(\overline{R}) - 1,$$

we get an entirely similar contradiction by first using $(**)$ and then $(*)$.

The exact sequences

$$0 \to M_i \to R^s/G_{i+1} \to R^s/G_i \to 0$$

likewise remain exact when we apply $\_ \otimes_R N$, yielding exact sequences

$$0 \to M_i \otimes_R N \to (R^s/G_{i+1}) \otimes_R N \to (R^s/G_i) \otimes_R N \to 0.$$

Since the modules in the middle and on the right are maximal Cohen-Macaulay modules over $\overline{R}$, so is $M_i \otimes_R N$, $0 \le i \le d-1$.

Since these d modules are the factors in a filtration of $(N/fN)^s$, we have that

$$e\big((N/fN)^s\big) = \sum_{i=0}^{d-1} e(M_i \otimes_R N).$$

The left hand side is $se(N/fN)$, which is $sde(N)$ by the preceding Lemma. Since there are d terms in the sum, there is at least one choice of i such that $e(M_i \otimes_R N) \le se(N)$. But

$$\nu(M_i \otimes N) = \dim{}_K\big(K \otimes_R (M_i \otimes_N N)\big) = \dim{}_K\big((K \otimes_R K) \otimes_R (M_i \otimes_R N)\big)$$

$$= \dim{}_K\big((K \otimes_R M_i) \otimes_K (K \otimes_R N) = \nu(M_i)\nu(N) = s\nu(N) = se(N),$$

since N is a linear maximal Cohen-Macaulay module over R. Thus, there is at least one i such that $e(M_i \otimes_R N) \le \nu(M_i \otimes_R N)$. Since the opposite inequality is automatic, for this choice of i we have that $M_i \otimes_R N$ is a linear maximal Cohen-Macaulay module over $\overline{R}$. □

Corollary. *Let $(R,\, m,\, K)$ be a local ring that is a* strict *complete intersection, i.e., the quotient of a regular ring $(T, \mathfrak{n})$ by a sequence of elements $f_1, \, \ldots\, , f_k$ whose leading forms constitute a regular sequence in $\mathrm{gr}_{\mathfrak{n}}T$. Then R has a linear maximal Cohen-Macaulay module.* □

Remark. In [J. Herzog, B. Ulrich, and J. Backelin, *Linear maximal Cohen-Macaulay modules over strict complete intersections*, Journal of Pure and Applied Algebra **71** (1991) 187–202], a converse to the Theorem on p. 3 of the Lecture Notes of March 27 is obtained, showing that flitrations of R^s/fR^s like the one given by the $G_i/G)d$ all come from matrix factorizatons. Also, the authors use the fact that $I(\alpha) = I$ to prove, in certain cases, that there are infinitely many mutually non-isomorphic maximal Cohen-Macaulay modules M satisfying certain restrictions on $e(M)$ and $\nu(M)$ and, in particular, on the ratio $\dfrac{\nu(M)}{e(M)}$.

We next want to show that linear maximal Cohen-Macaulay modules exist for certain determinantal rings and for certain Segre products when both factors have linear maximal Cohen-Macaulay modules. We recall that if R and S are two finitely generated $\mathbb{N}$-graded K-algebras, the *Segre product* of R and S, which we shall denote $R \circledS_K S$, is defined as

$$\bigoplus_n R_n \otimes_K S_n,$$

which is $\mathbb{N}$-graded so that $[R \circledS_K S]_n = R_n \otimes_K S_n$. This is a K-subalgebra of the tensor product $R \otimes_K S$, which has an $\mathbb{N}^2$-grading in which

$$[R \otimes_K S]_{h,k} = R_h \otimes_K S_k.$$

Note that $R \circledS_K S$ is a direct summand of $R \otimes_K S$: an $R \circledS_K S$-module complement is

$$\bigoplus_{h \neq k} R_h \otimes_K S_k.$$

For example, if $R = K[x_1, \dots, x_r]$ and $S = K[y_1, \dots, y_s]$ are polynomial rings,

$$T = R \otimes_K S = K[x_1, \dots, x_r, y_1, \dots, y_s],$$

a polynomial ring, and $R \circledS_K S = K[x_i y_j : 1 \le i \le r,\ 1 \le j \le s] \subseteq T$. If $Z = \bigl(z_{ij}\bigr)$ is an $r \times s$ matrix of new indeterminates, the K-algebra map

$$K[z_{ij} : 1 \le i \le r,\ 1 \le j \le s] \twoheadrightarrow R \circledS_K S$$

sending $z_{ij} \mapsto x_i y_j$ can be shown to have kernel $I_2(Z)$, so that

$$K[z_{ij} : 1 \le i \le r, 1 \le j \le s]/I_2(Z) \cong R \circledS_K S.$$

See Problem 5 of Problem set #5.

We shall see eventually that the Segre product of two Cohen-Macaulay rings need not be Cohen-Macaulay in general.

Lecture of April 1, 2019

Our next objective is to exhibit linear maximal Cohen-Macaulay modules for rings defined by the vanishing of the minors of a matrix of indeterminates in two special cases: one is the case of maximal minors, and the other the case of 2×2 minors. We shall solve the second problem in two different ways, one of which generalizes to the case of Segre products of standard graded K-algebras each of which has a linear maximal Cohen-Macaulay module.

Discussion: rings defined by the vanishing of the minors of a generic matrix. Let K be a field and let $X = \bigl(X_{ij}\bigr)$ denote an $r \times s$ matrix of indeterminates over K, where $1 \le r \le s$. Let $K[X]$ denote the polynomial ring in the rs variables X_{ij}. The ideal generated by the size t minors, $I_t(X)$, is known to be prime: in fact, $K[X]/I_t(X)$ is known to be a Cohen-Macaulay normal domain. This was first proved in [M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971), 1020–1058], and was treated by two methods in the Lecture Notes from Math 711, Winter 2006: one is the method of principal radical systems, adapted from the paper just cited, and the other is via the method of Hodge algebras. We shall assume the fact that these ideals are prime here. An argument for the case $t = 2$ is given in Problem 5 of Problem Set #5, in which the isomorphism of $K[X]/I_2(X)$ with the Segre product of two polynomial rings over K, one in r variables and one in s variables, is established.

We note that it is easy to see that when K is algebraically closed, the algebriac set $V\bigl(I_t(X)\bigr) \subseteq \mathbb{A}^{rs}_K$ is irreducible: this is the algebraic set of $r \times s$ matrices of rank at most $t-1$. For any such matrix α, the map $K^s \to K^r$ that it represents factors through K^{t-1}, e.g., through a $(t-1)$-dimensional subspace of K^r containing the image of α, and the factorization

$$K^s \to K^{t-1} \to K^r$$

enables us to write $\alpha = \beta\gamma$ where β is $r \times (t-1)$ and γ is $(t-1) \times s$. Any matrix that factors this way has column space contained in the column space of β, which shows that we have a surjection

$$\mathbb{A}^{r(t-1)}_K \times \mathbb{A}^{(t-1)s} \twoheadrightarrow V\bigl(I_t(X)\bigr).$$

This proves the irreducibility, since the image of an irreducible algebraic set is irreducible, and shows, at least, that $\mathrm{Rad}\,\bigl(I_t(X)\bigr)$ is prime.

It is also easy to calculate the dimension of $V\bigl(I_t(X)\bigr)$ and, hence, of $K[X]/I_t(X)$. Let $\rho = t-1$. Consider the open set in $W \subseteq X$ such that the first ρ rows of X are linearly independent. The open set U of choices γ for these rows (we may think of points $\gamma \in U$ as $\rho \times s$ matrices of maximal rank) has dimension ρs. Each remaining row is a unique linear combination of the rows of γ using ρ coefficients, so that the last $r-\rho$ rows of the matrix can be written uniquely in the form $\eta\gamma$, where η is an arbitrary $(r-\rho) \times \rho$ matrix. This gives a bijective map of $\mathbb{A}^{(r-\rho)\rho} \times U$ onto the dense open $W \subseteq X$, and so the dimension of $V\bigl(I_t(X)\bigr)$, which is the same as $\dim(W)$, is $(r-\rho)\rho + \rho s = \rho(r+s-\rho)$, where $\rho = t-1$. It also follows that the height of $I_t(X)$ is $rs - \rho(r+s-\rho) = (r-\rho)(s-\rho)$.

If $t = r$, the case of maximal minors, the height is

$$rs - (r-1)(s+1) = rs - (rs - s + r - 1) = s - r + 1.$$

If $t = 2$, the dimension is $r + s - 1$.

Discussion: linear maximal Cohen-Macaulay modules over a standard graded ring. Let K be a field. Recall that a *standard* graded K-algebra is a finitely generated $\mathbb{N}$-graded

K-algebra R such that $R_0 = K$ and $R = K[R_1]$, i.e., R is generated over K by its forms of degree 1. In dealing with the existence of linear maximal Cohen-Macaulay modules over the local ring R_m of a standard graded K-algebra at its homogeneous maximal ideal $m = \bigoplus_{n=1}^{\infty} R_n$, it is convenient to work entirely in the graded case.

Note that $\mathrm{gr}_{mR_m} R_m \cong \mathrm{gr}_m(R) \cong R$, so that each of the local ring and the graded ring determines the other. If N is a linear maximal Cohen-Macaulay module over a local ring $(S, \mathfrak{n}, K)$, then $M = \mathrm{gr}_{\mathfrak{n}} N$ is a maximal Cohen-Macaulay module over $R = \mathrm{gr}_{\mathfrak{n}} S$, and R is a standard graded K-algebra. To check this it suffices to to do so after replacing S by $S(t)$, so that the residue class field is infinite. R is replaced by $K(t) \otimes_K R$, and M by $K(t) \otimes_K M$, which does not affect the Cohen-Macaulay property. But when the residue class field is infinite, we can choose a minimal reduction $I = (x_1, \ldots, x_r)S$ for m, where $r = \dim(R) = \dim(S)$ and $x_1, \ldots, x_r$ is a system of paramters, and then

$$\mathrm{gr}_{\mathfrak{n}}(N) = \mathrm{gr}_I(N) \cong (N/IN) \otimes_K K[X_1, \ldots, X_r],$$

where $K[X_1, \ldots, X_r]$ is a polynomial ring. Note that $M = \mathrm{gr}_{\mathfrak{n}}(N)$ is generated in degree 0: $M_0 = N/IN = N/mN$.

Conversely, if M is an $\mathbb{N}$-graded maximal Cohen-Macaulay module over the standard graded K-algebra R, and M is generated by elements of equal (necessarily smallest) degree, we shall refer to M as a *linear maximal Cohen-Macaulay module in the graded sense* over R if $e(M) = \nu(M)$, where $e(M)$ is defined as the integer e such that $\dfrac{e}{(r-1)!} n^{r-1}$ agrees with the leading term of the Hilbert polynomial of M (by which we mean the polynomial that agrees with $\dim_K(M_n)$ for all $n \gg 0$). Note that we can shift the grading on such an M so that it is generated in degree 0. This does not affect $\nu(M)$ nor $e(M)$. This is precisely the condition for M_m to be a linear maximal Cohen-Macaulay module over R.

In fact, if we have a finitely generated graded module M over standard graded K-algebra R, then

$$\nu(M_m) = \dim_K(M_m/mM_m) = \dim_K(M/mM) = \nu(M),$$

and a minimal set of generators of M as a module may be taken to consist of homogeneous elements. Under the condition that M is generated in degree 0, $\mathrm{gr}_{mR_m} M_m \cong M$, and $e_{R_m}(M_m)$ may be calculated from the Hilbert function of the associated graded module, which yields that $e_{R_m}(M_m) = e(M)$. If R has a system of parameters $x_1, \ldots, x_r$ consisting of linear forms, which is automatic when K is infinite, then we again have $mM = (x_1, \ldots, x_r)M$ in the graded case, since $e(M) = \ell\big(M/(x_1, \ldots, x_r)M\big)$ and $\nu(M) = \ell(M/mM)$.

Discussion: a linear homogeneous system of parameters for the maximal minors. Consider an $r \times s$ matrix X of indeterminates $X_{i,j}$, over K, where $r \leq s$. We can give a linear homogeneous system of parameters for $K[X]/I_r(X)$. as follows. Let D_j be the diagonal whose entries are $X_{1,j}, X_{2,j+1}, \ldots, X_{r,j+r-1}$, where $1 \leq i \leq s - r + 1$. The linear homogeneous system of parameters consists of the elements below these diagonals (there are $r(r-1)/2$

such elements), the differences $X_{k+1,j+k}-X_{j,1}$ (these are all on the diagonal D_j) as j varies, $1 \leq j \leq s-r+1$, and the elements above all the diagonals (again, there are $r(r-1)/2$ such elements). The total number of elements is $r(r-1)+(s-r-1)(r-1)=(r-1)(s-1)$, which is the dimension of the ring $K[X]/I_r(X)$. To check that the elements specified form a system of parameters, it suffices to check that the the maximal ideal is nilpotent in the quotient. Note that, because all elements below D_1 are 0 and the image of D_1 in the quotient has all entries equal to, say, x_1 (the image of X_{11}), we find from the vanishing of the leftmost $r \times r$ minor that $x_1^r = 0$, so that x_1 is nilpotent. We can then prove by induction on j that all the elements on the diagonal that is the image of D_j (these are all equal) are nilpotent. If we know this for all variables below the diagonal D_j by the induction hypothesis, and x_j, the image of $X_{1,j}$, is the common image of the elements on D_j, then the x_j^r is nilpotent, from the vanishing of the minor consisting of r consecutive columns beginning with the j th.

In fact, the quotient of $K[X]/I_r(X)$ by this linear homogeneous system of parameters turns out to be isomorphic with $K[x_1, \, \ldots \, , x_{s-r+1}]/\mathcal{M}^r$, where the numerator is a polynomial ring and $\mathcal{M} = (x_1, \, \ldots \, , x_{s-r+1})$. This is left as an exercise: see Problem 2. in Problem Set #5 . It follows that the multiplicity of the ring $K[X]/I_r(X)$ is the number of monomials of degree at most $r-1$ in $s-r+1$ variables, which is $\displaystyle\binom{s}{r-1}$.

We can now show:

Theorem. *With notation as above, the ideal P generated by the $r-1$ size minors of the first $r-1$ rows of X is a linear maximal Cohen-Macaulay module for $R = K[X]/I_r(X)$ in the graded sense.*

Proof. The generators of P have equal degree, and since P has rank one, $e(P) = e(R)$. Clearly, $\nu(P) = \displaystyle\binom{s}{r-1} = e(P)$. Thus, we need only see that P is maximal Cohen-Macaulay when considered as an R-module. The key point is that P is a height one prime in R: its inverse image in the polynomial ring has height $s-(r-1)+1 = s-r+2$, one more than the height of $I_r(X)$. Moreover, the quotient R/P is Cohen-Macaulay: it is a polynomial ring over a ring obtained by killing minors of an $(r-1) \times s$ matrix of indeterminates, and so its depth on the homogeneous maximal ideal of R is $\dim(R)-1$. The short exact sequence

$$0 \to P \to R \to R/P \to 0$$

now implies that P has depth equal to $\dim(R)$ as an R-module. □

We next want to give a calculation of the multiplicity of the ring $R = K[X]/I_2(X)$ when $X = \bigl(X_{ij}\bigr)$ is a matrix of indeterminates. We already know from Problem 5 of Problem Set #5 and Problem 6 of Problem Set #4 that the answer is $\displaystyle\binom{r+s-2}{r-1}$. We give an alternative proof of this by a completely different method. The idea of this method is the same as the idea of the proof that these rings are Cohen-Macaulay via the technique of principal radical systems.

If $r = 1$ the ring is a polynomial ring in s variables and the multiplicity is 1, which is correctly given by the formula. We prove that the multiplicity is $\binom{r+s-2}{r-1}$ by induction on the number of variables. The idea is to kill one of the entries of the matrix, say $x = x_{11}$. Since the ring is a domain x_{11} is not a zerodivisor, and the resulting ring has the same multiplicity as R. In this ring, $x_{1j}x_{i1} = x_{11}x_{ij} = 0$ in R for $i,\, j \geq 1$, and so every prime ideal contains either all of the elements x_{1j} or all of the elements x_{i1}. Since $P = (x_{1j} : 1 \leq j \leq s)$ is a prime, and $Q = (x_{i1} : 1 \leq i \leq r)$ is a prime, P and Q are precisely the minimal primes of $x_{11}R$ in R. If we localize at P the elements x_{i1}, $i \geq 2$ become invertible, and the resulting ring is easily checked to be a field (localizing at x_{i2} produces a localization of a polynomial ring over K). The situation is the same if we localize at Q. Thus, $e(R) = e(R/P) + e(R/Q)$. The former is the ring obtained by killing the 2×2 minors of an $(r-1) \times s$ matrix of indeterminates, and the latter by killing the 2×2 minors of an $r \times (s-1)$ matrix of indeterminates. The result now follows form the identity

$$\binom{r+s-2}{r-1} = \binom{r-1+s-2}{r-1-1} + \binom{r+s-1-2}{r-1}.$$

Discussion: linear maximal Cohen-Macaulay modules for $K[X]/I_2(X)$. Our first proof uses the fact that the ring $K[X]/I_2(X)$ has, for $t \geq 1$, and endomorphism reminiscent of the Frobenius endomorphism. To wit, the K-algebra endomorphism $K[X] \to K[X]$ that sends $X_{ij} \mapsto X_{ij}^t$ for all i and j maps $I_2(X)$ into itself:

$$x_{ij}x_{hk} - x_{ik}x_{hj} \mapsto x_{ij}^t x_{hk}^t - x_{ik}^t x_{hj}^t.$$

and the latter element is a multiplie of the former element.

If we think of

$$R = K[X]/I_2(X) \cong K[Y_1,\, \dots\,, Y_r] \circledS_K K[Z_1,\, \dots\,, Z_s]$$

this endomorphism is induced by the K-endomorphism of the polynomial ring

$$K[Y_1,\, \dots\,, Y_r,\, Z_1,\, \dots\,, Z_s]$$

such that $Y_i \mapsto Y_i^t$ and $Z_j \mapsto Z_j^t$. This is clearly an injective endomorphism. We can restrict this endomorphism to the Segre product. We then have $X_iY_j \mapsto (X_iY_j)^t$. From this point of view, it is clear that this endomorphism θ_t of R is injective. We write ${}^tR$ for R viewed as an R-module via θ_t. The map $R \to {}^tR$ is module-finite, since every x_i^t is in the image $\theta_t(R)$. A homogeneous system of parameters in R maps to a homogeneous system of parameters in ${}^tR$, which is Cohen-Macaulay, since R is. That is, ${}^tR$ is a maximal Cohen-Macaulay module over R.

We can now decompose ${}^tR$ into a large number of R-modules. It will follow that each of these, if nonzero, is a maximal Cohen-Macaulay R-module. This decomposition proceeds as follows.

We can think of ${}^tR$ as R and the image of R as the subring S spanned by all monomials

$$Y_1^{a_1} \cdots Y_r^{a_r} Z_1^{b_1} \cdots Z_s^{b_s}$$

such that

$$a_1 + \cdots + a_r = b_1 + \cdots + b_s$$

and t divides every a_i and every b_j. Fix elements $\underline{\alpha} = \alpha_1, \, \dots \, , \alpha_r$ and $\underline{\beta} = \beta_1, \, \dots \, , \beta_s$ in $\mathbb{Z}/t\mathbb{Z}$ such that

$$\alpha_1 + \cdots + \alpha_r = \beta_1 + \cdots + \beta_s$$

in $\mathbb{Z}/t\mathbb{Z}$. Let $M_{\underline{\alpha}, \underline{\beta}}$ be the K-span of all monomials $Y_1^{a_1} \cdots Y_r^{a_r} Z_1^{b_1} \cdots Z_s^{b_s}$ such that $a_i \cong \alpha_i$ mod $t\mathbb{Z}$, $1 \leq i \leq r$ and $b_j \cong \beta_j$ mod $t\mathbb{Z}$, $1 \leq j \leq s$. It is easy to see that $M_{\underline{\alpha}, \underline{\beta}}$ is an S-module.

We claim that for all $t \geq r$, the choice $t-1, \, t-1, \, \dots \, , t-1$ for α and $0, 0, \dots \, , 0, t-r$ for β produces a linear maximal Cohen-Macaulay module , namely $M_{\underline{\alpha}, \underline{\beta}}$, in the graded sense. This module has rank one, because multiplication by $Y_1 \cdots Y_r Z_s^r$ produces an ideal in S. Hence, the multiplicity is the same as for S, i.e., $\begin{pmatrix} r+s-2 \\ r-1 \end{pmatrix}$. It is easy to see that this module is generated minimally by all monomials of the form

$$Y_1^{t-1} \cdots Y_r^{t-1} Z_1^{a_1 t} \cdots Z_{s-1}^{a_{s-1} t} Z_s^{t-r},$$

where the a_i are nonnegative and

$$a_1 + \cdots + a_{s-1} = r - 1.$$

These generators all have the same degree, and the number of generators is the same as the number of monomials of degree $r-1$ is $s-1$ variables, which is $\begin{pmatrix} r+s-2 \\ r-1 \end{pmatrix}$, as required. □

Lecture of April 3, 2019

Before giving a second proof of the existence of linear maximal Cohen-Macaulay modules for $K[X]/I_2(X)$ and the extension of this result to the case of more general Segre products, we want to note that the Segre product of two Cohen-Macaulay rings need not be Cohen-Macaulay, even when one of them is a normal hypersurface and the other is a polynomial ring.

In fact, let K be any field whose characteristic is different from 3, and let

$$R = K[X,\, Y,\, Z]/(X^3 + Y^3 + Z^3) = K[x,\, y,\, z]$$

and $S = K[s,\, t]$ where X, Y, Z, s, and t are indeterminates over K. We shall show that $T = R \,\textcircled{s}_K\, S$ is a three-dimensional domain that is not Cohen-Macaulay.

We have that

$$T = K[xs,\, ys,\, zs,\, xt,\, yt,\, zt] \subseteq K[x,\, y,\, z,\, s,\, t].$$

The equations

$$(zs)^3 + \bigl((xs)^3 + (ys)^3\bigr) = 0 \quad \text{and} \quad (zt)^3 + \bigl((xt)^3 + (yt)^3\bigr) = 0$$

show that zs and zt are both integral over $D = K[xs,\, ys,\, xt,\, zt] \subseteq T$. The elements x, y, s, and t are algebraically independent, and the fraction field of D is $K[xs,\, ys,\, t/s]$, so that $\dim(D) = 3$, and

$$D \cong K[X_{11},\, X_{12},\, X_{21},\, X_{22}]/(X_{11}X_{22} - X_{12}X_{21})$$

with X_{11}, X_{12}, X_{21}, X_{22} mapping to xs, ys, xt, yt respectively.

It is then easy to see that ys, xt, $xs - yt$ is a homogeneous system of parameters for D, and, consequently, for T as well. The relation

$$(zs)(zt)(xs - yt) = (zs)^2(xt) - (zt)^2(ys)$$

now shows that T is *not* Cohen-Macaulay, for $(zs)(zt) \notin (xt,\, ys)T$. To see this, suppose otherwise. The map

$$K[x,\, y,\, z,\, s,\, t] \to K[x,\, y,\, z]$$

that fixes $K[x,\, y,\, z]$ while sending $s \mapsto 1$ and $t \mapsto 1$ restricts to give a K-algebra map

$$K[xs,\, ys,\, zs,\, xt,\, yt,\, zt] \to K[x,\, y,\, z].$$

If $(zs)(zt) \in (xt,\, ys)T$, applying this map gives $z^2 \in (x,\, y)K[x,\, y,\, z]$, which is false — in fact, $K[x,\, y,\, z]/(x,\, y) \cong K[z]/(z^3)$. □

Segre products do have good properties that are important. It was already noted that $R \,\textcircled{s}_K\, S$ is a direct summand of $R \otimes_K S$. This implies that every ideal of $R \,\textcircled{s}_K\, S$ is contracted from $R \otimes_K S$. In particular, $R \,\textcircled{s}_K\, S$ is Noetherian and, since it is $\mathbb{N}$-graded, finitely generated over K. This is quite obvious when R and S are standard, since it is then generated by the products of elements in a basis for R_1 with elements in a basis for S_1. When $R \otimes_K S$ is normal, so is $R \,\textcircled{s}_K\, S$. In particular, this is true of the ring in the example above. $R = K[X,\, Y,\, Z]/(X^3 + Y^3 + Z^3)$ is normal, since it is Cohen-Macaulay and the singular locus is the origin (the partial derivatives of $X^3 + Y^3 + Z^3$ vanish simultaneously only at the origin), and $R \otimes_K S = R[s, t]$.

Discussion: the dimension of the Segre product. For any finitely generated N-graded K-algebras R and S with $R_0 = K = S_0$, we have that

$$\dim (R \circledS_K S) = \dim (R) + \dim (S) - 1.$$

Each of R and S has a homogeneous system of parameters. After raising the elments to powers, we find that R is module-finite over $A = K[F_1, \ldots, F_r]$, where $F_1, \ldots, F_r$ form a homogeneous system of parameters of degree k, and S is module-finite over $B = K[G_1, \ldots, G_s]$ where $G_1, \ldots, G_s$ is a homogeneous system of parameters of degree k as well. If K is infinite and R and S are standard, we may even assume that $k = 1$ here. Then $A \circledS_K B \cong K[X]/I_2(X)$ where X is an $r \times s$ matrix of indeterminates over K, and so has dimension $r + s - 1$. The result now follows because $R \circledS_K S$ is module-finite over $A \circledS_K B$. To see this, choose $h \gg 0$ so that homogenous generators for R over A and for S over B have degree $\leq h$. Let V_k be a K-basis for R_k for $k \leq h$ and let W_k be a K-basis for S_k for $k \leq h$. Then the finite set $\mathcal{S}$ of elements of the form $v \otimes w$, where $v \in V_k$ and $W \in w_k$ for some $k \leq h$, generate $R \circledS_K S$ *as a module* over $A \circledS_K B$. To see this, let $F \in R_t$ and $G \in S_t$ be given. Then F is an A-linear combination of elements in a fixed V_k with coefficients in A_{t-k}, and G is a B-linear combination of elements in a fixed W_k with coefficients in B_{t-k}. Here, if $t \leq h$ one may take $k = t$, and if $t \geq h$, one may take $k = h$. It follows that every element of the form $F \otimes G$ is in the $A \circledS_K B$-span of $\mathcal{S}$, as claimed, and elements of this form span $R \circledS_K S$ over K. □

Our next objective is to give a different proof that $R = K[X]/I_2(X)$ has a linear maximal Cohen-Macaulay module. Again, we consider the isomorphism

$$K[X]/I_2(X) \cong S = K[Y_1, \ldots, Y_r] \circledS_K K[Z_1, \ldots, Z_s] \subseteq KY_1, \ldots, Y_r, Z_1, \ldots, Z_s] = T.$$

For every $\delta \in \mathbb{Z}$, let T_δ denote the K-span of the monomials $\mu \in T$ such that

$$\deg_Y(\mu) - \deg_Z(\mu) = \delta,$$

where $\deg_Y(\mu)$ denotes the total degree of μ in the variables $Y_1, \ldots, Y_r$ and $\deg_Z \mu$ denotes the total degree of μ in the variables $Z_1, \ldots, Z_s$. Then T_δ is obviously an S-module, and $T = \bigoplus_{\delta \in \mathbb{Z}} T_\delta$.

The following result is proved in [S. Goto and K.-i. Watanabe, *On graded rings*, I, Journal of the Mathematical Society of Japan **30** (1978) 179–213].

Theorem. *With the above notation, T_δ is a maximal Cohen-Macaulay module of torsion-free rank one over the Segre product*

$$K[Y_1, \ldots, Y_r] \circledS_K K[Z_1, \ldots, Z_s] = S \cong R = K[X]/I_2(X)$$

for $s > \delta > -r$.

Proof. The case where $\delta = 0$ is the statement that $T_0 = S$ is Cohen-Macaulay, which we are assuming here. We assume that $\delta \geq 0$ and proceed by induction on s. The case where $0 \geq \delta > -r$ then follows by interchanging the roles of $Y_1, \ldots, Y_r$ and $Z_1, \ldots, Z_s$.

The case where $s = 1$ is obvious. Note that $T_\delta \cong Z_1^\delta T_\delta$, and that $Z_1^\delta T_\delta$ is the ideal generated by the monomials of degree δ in $Y_1Z_1, \ldots, Y_rZ_1$, which is P^δ, where $P = (Y_1Z_1, \ldots, Y_rZ_1)$. P corresponds to the prime ideal of R generated by the variables in the first column. The quotient is $K[X^-]/I_2(X^-)$, where X^- is the $r \times (s-1)$ matrix obtained by omitting the first column of X: this ring has dimension $r+(s-1)-1 = r+s-2$, from which it follows that P is a height one prime of S. To complete the proof, it will suffice to show that for $1 \le \delta < s$, S/P^δ is Cohen-Macaulay: the short exact sequence

$$0 \to P^\delta \to S \to S/p^\delta \to 0$$

then shows that

$$\mathrm{depth}_m P^\delta = \mathrm{depth}_m (S/P^\delta) + 1 = \dim(S).$$

We filter S/P^δ by the modules P^k/P^{k+1}, $0 \le k < \delta$. Each of these is a module over S/P, and it suffices to show that each is a maximal Cohen-Macaulay module over S/P. We already know this when $k = 0$, and so we may assume that $1 \le k < \delta$.

We make use of the fact for every $k \in \mathbb{N}$, $P^k = Z_1^kT \cap S$. This gives an injection of

$$P^k/P^{k+1} \hookrightarrow Z_1^kT/Z_1^{k+1}T \cong T/Z_1T \cong K[Y_1, \ldots, Y_r, Z_2, \ldots, Z_s] = T^-.$$

If we identify P^k/P^{k+1} as a submodule of T^- in this way, the action of S/P is obtained by identifying $S/P \cong K[Y_1, \ldots, Y_r] \circledS_K K[Z_2, \ldots, Z_s] \subseteq T^-$. The generators of P^k map to the monomials of degree k in $Y_1, \ldots, Y_r$. Thus, we may identify P^k/P^{k+1} with T_k^-. Since s has been decreased by 1 and $k < \delta \le s-1$, the result follows from the induction hypothesis. □

Corollary. *With notation as in the Theorem above, T_{s-1} is a linear maximal Cohen-Macaulay module over $S \cong R$.*

Proof. The generators of T_{s-1} have the same degree, and since T_{s-1} is rank one,

$$e(T_{s-1}) = e(T_0) = \binom{r+s-2}{r-1},$$

which is the same as the number of monomials of degree $s-1$ in $Y_1, \ldots, Y_r$. □

We can now prove:

Theorem (D. Hanes). *Let K be an infinite field. Let R and S be standard graded K-algebras that possess linear maximal Cohen-Macaulay modules in the graded sense. Then so does $R \circledS_K S$.*

Proof. We may assume that M and N are the linear maximal Cohen-Macaulay modules over R and S respectively and that they are generated in degree 0. Let $Y_1, \ldots, Y_r$ be a homogeneous linear system of parameters for R, where $r = \dim(R)$, and let $Z_1, \ldots, Z_s$

be a homogenous linear system of parameters for S, where $s = \dim(S)$. Let m and $\mathfrak{n}$ be the respective homogeneous maximal ideals in R and S.

Then R is module-finite over $A = K[Y_1, \ldots, Y_r]$, and S is module-finite over $B = K[Z_1, \ldots, Z_s]$. Moreover, $R \otimes_K S$ is module-finite over $A \otimes_K B$, and $R \circledS_K S$ is module-finite over $A \circledS_K B$, by the Discussion on the dimension of Segre products. Since M is Cohen-Macaulay it is A-free, and its rank $c = e(M)$. Similarly, N is B-free of rank $d = e(N)$. Note that $mM = (Y_1, \ldots, Y_r)M$ and that $\mathfrak{n}N = (Z_1, \ldots, Z_s)N$.

The action of any degree one form F of R on $M \cong A^c$ is an A-linear map and can be thought of as being given by a $c \times c$ matrix over A. Since multiplication by F increases degrees by one, the entries of each such matrix must be degree one forms of A. Similarly, the action of any degree one form $G \in S$ on N is given by a $d \times d$ matrix of linear forms over B.

Consider the $R \otimes_K S$ module $M \otimes_K N$. We can consider it as

$$A^c \otimes_K B^d \cong T^{cd},$$

where

$$T = K[Y_1, \ldots, Y_r] \otimes_K K[Z_1, \ldots, Z_s].$$

For $\delta \in \mathbb{Z}$, we can define $(M \otimes_K N)_\delta$ as $(T_\delta)^{cd}$. Because the action of forms of R and forms of S preserves the bigrading on T^{cd} coming from the Y-grading and the Z-grading on T, every $(M \otimes_K N)_\delta$ is a module over $R \circledS_K S$. Since $(M \otimes_K N)_\delta$ is finitely generated even as a module over

$$T_0 = A \circledS_K B \subseteq R \circledS_K S,$$

it is finitely generated over $R \circledS_S$. For $s > \delta > -r$ it is maximal Cohen-Macaulay over $R \circledS_K S$, since $R \circledS_K S$ is module-finite over $A \circledS_K B$, and we know that it is maximal Cohen-Macaulay over $A \circledS_K B$.

To complete the proof, we shall show that $W = (M \otimes_K N)_{s-1}$ is a linear maximal Cohen-Macaulay module over $R \circledS_K S$. It is maximal Cohen-Macaulay and generated by elements of equal degree. To complete the argument, we shall prove that

$$\nu(W) = cd \binom{r+s-2}{r-1} = e(W).$$

Include $Y_1, \ldots, Y_r$ in a set of one-forms $F_1, \ldots, F_h$ that generate m, and include $Z_1, \ldots, Z_s$ in a set of one-forms $G_1, \ldots, G_k$ that generate $\mathfrak{n}$. Let $\mathcal{M}$ be the maximal ideal of $R \circledS_K S$, which is generated by the products $F_i G_j$. Let $\mathcal{Q}$ be the maximal ideal of $A \circledS_K B$, which is generated by the products $Y_i Z_j$. Then for every integer $n \geq 0$,

$$\mathcal{M}^n(M \otimes_K N) = (F_i G_j : 1 \leq i \leq h,\, 1 \leq j \leq k)^n (M \otimes_K N) =$$

$$(F_i : 1 \leq i \leq r)^n (G_j : 1 \leq j \leq s)^n (M \otimes_K N) =$$

$$\begin{aligned}&\bigl((F_i : 1 \leq i \leq h)^n M\bigr) \otimes_K \bigl((G_j : 1 \leq j \leq k)^n N\bigr) =\\ &m^n M \otimes_K \mathfrak{n}^n N = \bigl((Y_i : 1 \leq i \leq r)^n M\bigr) \otimes_K \bigl((Z_j : 1 \leq j \leq s)^n N\bigr) =\\ &\bigl((Y_i : 1 \leq i \leq r)(Z_j : 1 \leq j \leq s)\bigr)^n (M \otimes_K N\bigr) = \mathcal{Q}^n(M \otimes_K N).\end{aligned}$$

Since $M \otimes_K N$ splits into

$$\bigoplus_{\delta \in \mathbb{Z}} (M \otimes_K N)_\delta$$

as $R \circledS_K S$-modules, we also have that

$$\mathcal{M}^n(M \otimes_K N)_\delta = \mathcal{Q}^n(M \otimes_K N)_\delta$$

for every δ. In particular, $\mathcal{M}^n W = \mathcal{Q}^n W$ for all n. Consequently, we have that $\nu(W) = \ell(W/\mathcal{M}W) = \ell(W/\mathcal{Q}W)$, which is the number of generators of W as a module over $A \circledS_K B$. Since W is the direct sum of cd copies of $(A \circledS_K B)_{s-1}$, this is $cd\binom{s+r-2}{r-1}$, as required. Similarly,

$$\dim_K(\mathcal{M}^n W/\mathcal{M}^{n+1}W) = \dim_K(\mathcal{Q}^n W/\mathcal{Q}^{n+1}W),$$

and this is cd times the Hilbert function of $(A \circledS_K B)_{s-1}$ with respect to $\mathcal{Q}$. The multiplicity is therefore

$$cd\, e_{\mathcal{Q}}\bigl((A \circledS_K B)_{s-1}\bigr) = cd\binom{r+s-2}{r-1}. \qquad \square$$

Lecture of April 5, 2019

We aim to prove the following result of Paul Monsky, following his paper [P. Monsky, *The Hilbert-Kunz function*, Mathematische Annalen **263** (1983) 43–49].

Theorem (Monsky). *Let (R, m, K) be local where R has prime characteristic $p > 0$, let $\mathfrak{A}$ be an m-primary ideal, and let M be a finitely generated R-module of Krull dimension d. Then*

$$\lim_{n \to \infty} \frac{\ell(M/\mathfrak{A}^{[p^n]}M)}{p^{nd}}$$

exists, and is a positive real number.

The function whose value on n is $\ell(M/\mathfrak{A}^{[p^n]}M)$ is called the *Hilbert-Kunz function* of M with respect to $\mathfrak{A}$ and we denote its value on n by $\mathcal{F}_{HK}(\mathfrak{A}, M)(n)$. If $\mathfrak{A} = m$, we may simply write $\mathcal{F}_{HK}(M)(n)$.

The limit, which we have not yet proved exists, is called the *Hilbert-Kunz multiplicity* of M with respect to $\mathfrak{A}$. We denote it by $e_{HK}(\mathfrak{A},\, M)$. If $\mathfrak{A} = m$, we write simply $e_{HK}(M)$.

Example. Let

$$R = K[[X,\, Y,\, Z]]/(XY - Z^d) = K[[x,\, y,\, z]],$$

where K is a field and X, Y, Z are formal indeterminates. Here, $m = (x,\, y,\, z)R$. Note that R is a normal hypersurface, and

$$R \cong S = K[[U^d,\, V^d, UV]] \subseteq K[[U,\, V]],$$

the formal power series ring in two variables. We shall show that $e_{HK}(R) = 2 - \dfrac{1}{d}$.

Every element of R can be written uniquely in the form $x^iy^jz^k$ where $0 \le k \le d-1$. The quotient ring $R/(x^q,\, y^q)R$, where $q = p^n$, has a K-basis consisting of the elements $x^iy^jz^k$, $0 \le i \le q-1$, $0 \le j \le q-1$, and $0 \le k \le d-1$. We can write $q = p^n = a_nd + r_n$ where $a_n \in \mathbb{N}$ and $0 \le r_n \le d-1$. Then $z^q = z^{a_nd}z^{r_n} = (xy)^{a_n}z^{r_n}$. As we multiply by z, z^2, $\ldots$ we obtain as multiples all the elements $x^{a_n}y^{a_n}z^s$ for $1 \le s \le d-1$. Multiplying by z one more time yields $x^{a_n+1}y^{a_n+1}$. Of course, once we see that $x^iy^jz^k$ is 0 mod $(x^q,\, y^q,\, z^q)$, this also follows for $x^{i'}y^{j'}z^{k'}$ whenever $i' \ge i$, $j' \ \ge j$, and $k' \ge k$. From this we see that a K-basis for the quotient $R/m^{[q]} = R/(x^q,\, y^q,\, z^q)R$ consists of all monomials $x^iy^jz^k$ such that either

(1) $0 \le i \le a_n - 1$, $0 \le j \le q-1$, and $0 \le k \le d-1$ or

(2) $0 \le i \le q-1$, $0 \le j \le a_n - 1$, and $0 \le k \le d-1$ or

(3) $i = j = a_n$ and $0 \le k < r_n$.

The number monomials satisfying (1) or (2) is $a_nqd + qa_nd$ while the number satisfying both conditions is a_n^2d. The number satisfying condition (3) is r_n. Hence, $\ell(R/m^{[q]}) = 2a_n^d - a_n^2d + r_n$. Note that since a_n is the integer part of q/d, it lies between $(q/d) - 1$ and q/d, and so $a_n/q \to 1/d$ as $n \to \infty$. Moreover, $0 \le r_n < d$ shows that $r_n/q^2 \to 0$ (for that matter, $r_n/q \to 0$) as $n \to \infty$. Hence,

$$\lim_{n \to infty} \frac{\ell(R/m^{[q]})}{q^2} = \frac{2d}{d} - \frac{d}{d^2} + 0 = 2 - \frac{1}{d}.$$

We next make some elementary observations:

Lemma. *Let $(R,\, m,\, K)$ be local where R has prime characteristic $p > 0$, let $\mathfrak{A}$ be an m-primary ideal, and let M be a finitely generated R-module of dimension d.*

(a) *The values of the Hilbert Kunz function of M with respect to $\mathfrak{A}$ are independent of whether we regard the base ring as R, or as R/Ann_RM. Hence, the question of whether the Hilbert-Kunz multiplicity exists is independent of which ring is regarded as the base ring.*

(b) *Let $(R,\, m,\, K) \to (S,\, \mathfrak{n},\, L)$ be flat local such that $\mathfrak{n} = mS$. Then for all n,*

$$\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) = \mathcal{F}_{HK}(\mathfrak{A},\, S \otimes_R M)(n),$$

and so the question of whether the Hilbert-Kunz multiplicity exists is not affected by base change from R to S. In particular, we may make a base change from R to $\widehat{R}$.

(c) *There exist positive real constants C and C' such that for all n,*

$$Cp^{nd} < \mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \leq C'p^{nd}.$$

(d) *If $\mathfrak{A}$ is generated by part of a system of parameters for $R/\mathrm{Ann}_R M$, then $e_{HK}(\mathfrak{A},\, M) = e_{\mathfrak{A}}(M)$.*

(e) *If $\mathfrak{A} \subseteq \mathfrak{B}$, then $\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \geq \mathcal{F}_{HK}(\mathfrak{B},\, M)(n)$ for all n, Hence, $e_{HK}(\mathfrak{A},\, M) \geq e_{HK}(\mathfrak{B},\, M)$ whenever they exist.*

(f) *Whenever it exists, $e_{HK}(\mathfrak{A},\, M) \leq e_{\mathfrak{A}}(M)$.*

Proof. Part (a) is obvvious. Part (b) follows from the fact that for any fnite length module N over R, $\ell_S(S \otimes_K N) = \ell_R(N)$ (if N has a finite filtration whose factors are h copies of $K = R/m$, then $S \otimes_K N$ has a filtration whose factors are h copies of $S \otimes_R K = S/mS = S/\mathfrak{n} = L$). One may apply this to each $N = M/\mathfrak{A}^{[q]}M$, noting that

$$S \otimes N \cong (S \otimes_R M)/(\mathfrak{A}S)^{[q]}(S \otimes_R M).$$

For part (c), note that if $\mathfrak{A}$ has k generators then $\mathfrak{A}^{kq} \subseteq \mathfrak{A}^{[q]} \subseteq \mathfrak{A}^q$, since a monomial in k elements of degree kq must have at least one individual exponent that is at least q. Hence,

$$(*) \quad \ell(M/(\mathfrak{A}^k)^q M) \geq \ell(M/\mathfrak{A}^{[q]}M) \geq \ell(M/\mathfrak{A}^q M).$$

The Hilbert polynomial of M with respect to $\mathfrak{A}$ has leading coefficient cn^d for a suitable positive real constant c. It follows that the upper bound in $(*)$ is asymptotic to $c(kq)^d = ck^q(q^d)$, while the lower bound is asymptotic cq^d, and the result follows.

Part (d) is immediate from the definition and Lech's formula for multiplicities with respect to parameter ideals.

Part (e) is obvious from the definition.

For part (f), first note that we can replace R by $R(t)$ as in part (b), and so assume that the residue class field is infinite. Second, we replace R by $R/\mathrm{Ann}_R M$ as in part (a). Let $x_1, \,\dots\,, x_d$ by a system of parameters generating an ideal I that is a reduction of $\mathfrak{A}$. Then

$$e_{\mathfrak{A}}(M) = e_I(M) = e_{HK}(I,\, M) \geq e_{HK}(\mathfrak{A},\, M)$$

by part (e). $\square$

From part (b) of this Lemma, the problem of proving the existence of Hilbert-Kunz multiplicities reduces to the case where the local ring is complete. By the Proposition near the bottom of p. 1 of the Lecture Notes of March 13, we know that there is a flat local map from the complete ring $(R,\, m,\, K)$ to a local ring $(S, \mathfrak{n},\, L)$ such that $\mathfrak{n} = mS$ and L is algebraically closed. Therefore, we may also assume without loss of generality that K is algebraically closed. We shall see that this implies that $F : R \to R$ is module-finite.

Given $e \in \mathbb{N}$ and an R-module M we write ${}^eM$ for M viewed as an R-module via restriction of scalars via the map $F^e : R \to R$. Thus, with $u \in {}^eM$, $r \cdot u = r^{p^e}u$. When $F : R \to R$ is module-finite, so are its iterations F^e, and it follows that if M is finitely generated as an R-module, so is ${}^eM$. Moreover, $M \mapsto {}^eM$ is an exact functor from R-modules to R-modules: neither the underlying abelian groups nor the maps change when we apply this functor.

When K is perfect and N is a finite length R-module, ${}^eN$ is also a finite length R-module and, in fact, $\ell({}^eN) = \ell(N)$. To see this, suppose that N has a filtration by h copies of K. Then ${}^eN$ has a filtration by h copies of ${}^eK$, by the exactness of restriction of scalars. The action of m on ${}^eK$ is 0, and, although the action of K on ${}^eK$ is via the iterated Frobenius endomorphism F^e, $F^e : K \to K$ is an isomorphism, and so ${}^eK$ is a one-dimensional vector space over K, i.e., it is isomorphic with K. Note also that if $\mathfrak{B}$ is any ideal of R, then $\mathfrak{B}({}^eM)$, under the abelian group identification of ${}^eM$ with M, becomes $\mathfrak{B}^{[p^e]}M$. Thus,

$${}^eM/(\mathfrak{B}\,{}^eM) = {}^e(M/\mathfrak{B}^{[p^e]}M).$$

From these remarks we obtain:

Proposition. *Let $(R,\, m,\, K)$ be local of prime characteristic $p > 0$ such that $F : R \to R$ is module-finite. Suppose also that K is pefect. Let $\mathfrak{A} \subseteq m$ be any m-primary ideal. Let M be a finitely generated R-module of dimension d. Then for every nonnegative integer n, $\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n) = \mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)$, and so if $e_{HK}(\mathfrak{A},\, {}^eM)$ exists, so does $e_{HK}(\mathfrak{A},\, M)$, and $e_{HK}(\mathfrak{A},\, {}^eM) = p^{ed}e_{HK}(\mathfrak{A},\, M)$.*

Proof. We have that

$$\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n) = \ell\big({}^eM/(\mathfrak{A}^{[p^n]})\,{}^eM\big) = \ell(M/(\mathfrak{A}^{[p^n]})^{[p^e]}M)$$

$$= \ell(M/\mathfrak{A}^{[p^{n+e}]}M) = \mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)$$

for all n, and so

$$e_{HK}(\mathfrak{A},\, M) = \lim_{n\to\infty} \frac{\mathcal{F}_{HK}(\mathfrak{A},\, M)(n+e)}{p^{(n+e)d}} = \frac{1}{p^{ed}} \lim_{n\to\infty} \frac{\mathcal{F}_{HK}(\mathfrak{A},\, {}^eM)(n)}{p^{nd}} = \frac{1}{p^{ed}} e_{HK}(\mathfrak{A},\, {}^eM),$$

as required. □

We also have:

Lemma. *Let $(R,\, m,\, K)$ be local of prime characteristic $p > 0$, let M be a finitely generated R-module of dimension d, and let $\mathfrak{A} \subseteq M$ be m-primary.*

(a) *If $N \subseteq M$ is such that* $\dim(N) < \dim(M)$, *then for all $n \geq 0$*

$$\mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n) + Cp^{(d-1)n}.$$

Hence,

$$|\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) - \mathcal{F}_{HK}(\mathfrak{A},\, M/N)(n)| \leq Cp^{(d-1)n},$$

and so $e_{HK}(\mathfrak{A},\, M/N)$ and $e_{HK}(\mathfrak{A},\, M)$ exist or not alike, and, if they exist, are equal.

(b) *Let M' be another finitely generated R-module of dimension d, and let W be a multiplicative system in R consisting of nonzerodivisors on M and on M'. If $W^{-1}M = W^{-1}M'$, then there exists a positivive constant C such that for all $n \geq 0$,*

$$|\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) - \mathcal{F}_{HK}(\mathfrak{A},\, M')(n)| \leq Cp^{(d-1)n}.$$

Hence, $e_{HK}(\mathfrak{A},\, M')$ and $e_{HK}(\mathfrak{A},\, M)$ exist or not alike, and, if they exist, are equal.

Proof. For part (a), note that for every $q = p^n$ we have, with $\overline{M} = M/N$, the exact sequence

$$N/\mathfrak{A}^{[q]}N \to M/\mathfrak{A}^{[q]}M \to \overline{M}/\mathfrak{A}^{[q]}\overline{M} \to 0,$$

and while the first map need not be injective, we still have that the length of the module in the middle is at most the sum of the lengths of the other two modules. The inequality on the right is exactly this statement, while the inequality on the left is immediate from the surjectivity of the map on the right. The bound on the absolute value of the difference follows at once, and so does the final statement once we divide by q^d.

To prove part (b), note that we have a map $M \hookrightarrow W^{-1}M'$ that becomes an isomorphism when we localize at W. Choose $w \in W$ to be the product of the denominators of the images of a finite set of generators for M. Then the injection maps $wM \hookrightarrow M'$, and since $M \cong wM$ we have an injection $M \hookrightarrow M'$ whose cokernel Q is killed by an element of W, which implies that $\dim(Q) \leq \dim(M)$. The short exact sequences

$$M/\mathfrak{A}^{[q]}M \to M/\mathfrak{A}^{[q]}M' \to Q/\mathfrak{A}^{[q]}Q \to 0$$

yield inequalities

$$\mathcal{F}_{HK}(\mathfrak{A},\, M')(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M)(n) + C_1p^{nd}$$

for some real constant C_1 and for all n, using part (a). In an exactly similar way, there is a short exact sequence

$$0 \to M' \to M \to Q' \to 0$$

with $\dim(Q') < d$, and we obtain

$$\mathcal{F}_{HK}(\mathfrak{A},\, M)(n) \leq \mathcal{F}_{HK}(\mathfrak{A},\, M')(n) + C_2p^{nd}$$

for all n. The inequality we need now follows with $C = \max\{C_1, C_2\}$, and the final statement is obvious. $\square$

Discussion: the existence of Hilbert-Kunz multiplicities reduces to the case of complete local domains with perfect residue class field. We have already seen that the existence of Hilbert-Kunz multiplicities reduces to the case where the ring is complete local with algebraically closed residue class field. In particular, the residue class field may be assumed to be perfect. By part (a) of the Lemma above, we may reduce to the case where M has pure dimension. We may replace R by $R/\mathrm{Ann}_R M$ and therefore suppose that M is faithful, and so that M and R have the same minimal primes, which are also the associated primes of M.

Let W be the multiplicative system of elements not in any minimal prime of R, which consists of nonzerodivisors on M. Then $W^{-1}M$ is a module over $W^{-1}R$, which is a semilocal Artin ring, and so is the product of its localizations at the various minimal primes P_i, $1 \leq i \leq h$, of R. Hence,

$$W^{-1}M \cong \prod_{i=1}^{h} M_{P_i} = \bigoplus_{i=1}^{h} M_{P_i}.$$

Choose a power of P_i that kills M_{P_i}, say $P_i^{N_i}$, and let $M_i = \mathrm{Ann}_M P_i^{N_i}$. Every element of M_{P_i} can be multiplied into the image of M by an element of $R - P_i$, and, if we multiply further by an element of $R - P_i$, we obtain a multiple in M_i. Thus, $(M_i)_{P_i} = M_{P_i}$. The M_i are mutually disjoint, however: a nonzero element of M cannot be killed by both a power of P_i and a power of P_j for $i \neq j$, or else M will have an associated prime containing both P_i and P_j. Thus,

$$M_1 \oplus M_2 \oplus \cdots \oplus M_h \subseteq M$$

and the two become equal when we localize at W. Therefore, to show that the Hilbert-Kunz multiplicity of M exists, it suffices to show this for every M_i.

We can therefore reduce to the case where $\mathrm{Ass}\,(M)$ contains a unique associated prime P. Replacing R by $R/\mathrm{Ann}_R M$, we may also assume that R has a unique minimal prime P. Choose e so large that $P^{[p^e]} = 0$. To show that the Hilbert-Kunz multiplicity of M exists, it suffices to prove this for ${}^eM$ instead. But P kills ${}^eM$, which is consequently a module over R/P. We have therefore reduced to the case where R is a complete local domain with perfect residue class field and $\dim(M) = \dim(R)$. Moreover, M has no nonzero submodule of smaller dimension, which implies that M is torsion-free over R. Now choose $R^\rho \subseteq M$ such that ρ is the torsion-free rank of M over R. Then M/R^ρ is torsion, and so we have reduced to considering the case where $M = R^\rho$. But then we have reduced to the case where $M = R$, as required. $\square$

It remains to prove the case where $M = R$ is a complete local domain with perfect residue class field. This is the most interesting part of the argument.

Lecture of April 8, 2019

Recall the if R is a Noetherian ring of prime characteristic $p > 0$, R is called F-*finite* if $F : R \to R$ makes R into a module-finite algebra over

$$F(R) = \{r^p : r \in R\},$$

a subring of R that is also denoted R^p. When R is F-finite, the composition $F^e : R \to R$ also makes R into a finite module over

$$F^e(R) = \{r^{p^e} : r \in R\},$$

a subring of R that is alternatively denoted R^{p^e}.

If R is F-finite, it is trivial that every homomorphic image of R is F-finite. The same holds for each localization $W^{-1}R$, because inverting the elements in W^p has the effect of inverting the elements of W. If R is F-finite, so is $R[x]$: if $r_1, \, \ldots \,, r_h$ span R over $F(R)$, then the elements $r_i x_j$, $1 \leq i \leq h$, $0 \leq j < p$ span $R[x]$ over $F(R[x]) = F(R)[x^p]$. By induction, any finitely generated algebra over an F-finite ring is F-finite, and it is likewise true that any algebra essentially of finite type over an F-finite ring is F-finite.

A perfect field is obviously F-finite, and so a field that is finitely generated as a field over a perfect field is F-finite: it is a localization of a finitely generated algebra over a perfect field. Thus, if K is perfect, each of the fields $K(t_1, \, \ldots \,, t_n)$ is F-finite, where $t_1, \, t_2, \, \ldots \,, \, t_n, \, \ldots$ are indeterminates over K, but the field $K(t_1, \, \ldots \,, t_n, \, \ldots)$ where we adjoin infinitely many indeterminates, is not. We note:

Proposition. *A complete local ring $(R, \, m, \, K)$ of prime characteristic $p > 0$ is F-finite if and only if its residue class field K is F-finite.*

Proof. Since $K = R/m$, if R is F-finite then K is. Suppose that K is F-finite, and let $c_1, \, \ldots \,, c_h$ be a basis for K over $F(K)$. Then R is a homomorphic image of a formal power series ring $S = K[[x_1, \, \ldots \,, x_d]]$, and it suffices to show that S is F-finite. But the set of elements

$$\{c_j x_1^{a_1} \cdots x_d^{a_d} : 0 \leq j \leq h, \; 0 \leq a_i < p \text{ for } 0 \leq i \leq d\}$$

spans S over $F(S) = F(K)[[x_1^p, \, \ldots \,, \, x_d^p]]$. $\square$

This justifies the assertion in the Lecture Notes of April 5 that a complete local ring with perfect residue class field is F-finite.

We next want to understand the behavior of the rank of ${}^eR$ when R is a complete local domain with a perfect residue class field.

Note that when R is reduced of prime characteristic $p > 0$, the three maps $F^e : R \to R$, $R^{p^e} \subseteq R$, and $R \subseteq R^{1/p^e}$ are isomorphic. The isomorphism of $F^e : R \to R$ with $R^{p^e} \subseteq R$ follows from the fact that, for a reduced ring R, F^e is injective and $F^e(R) = R^{p^e}$. To understand the third map, we need to define the ring R^{1/p^e}. When R is a domain, there we may take this to be the subring of an algebraic closure of the fraction field of R that consists of all the elements of the for r^{1/p^e} for $r \in R$. In the general case, one can show that there is an extension S of R, unique up to canonical isomorphism, such that the map $R = \{s^{p^e} : s \in S\}$. In fact, since $R \cong R^{p^e}$ via the map $r \mapsto r^{p^e}$, we "think of" R^{p^e} as R, and take S to be R.

This means that when R is reduced, we may think of ${}^eR$ as R^{1/p^e}.

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring of Krull dimension d such that K is perfect. Then for every $e \in \mathbb{N}$, the torsion-free rank of ${}^eR$ over R is p^{de}.*

Proof. By the structure theory of complete local rings, R is module finite over $A = K[[x_1,\, \ldots\,, x_d]]$. Let $\mathrm{frac}\,(R) = \mathcal{L}$ and $\mathrm{frac}\,(A) = \mathcal{K}$. The torsion free rank of R^{1/p^e} over R is the same as $[\mathcal{L}^{1/p^e} : \mathcal{L}]$. We have that

$$[\mathcal{L}^{1/p^e} : \mathcal{K}] = [\mathcal{L}^{1/p^e} : \mathcal{K}^{1/p^e}]\,[\mathcal{K}^{1/p^e} : \mathcal{K}]$$

and also

$$[\mathcal{L}^{1/p^e} : \mathcal{K}] = [\mathcal{L}^{1/p^e} : \mathcal{L}]\,[\mathcal{L} : \mathcal{K}],$$

so that

$$(*) \quad [\mathcal{L}^{1/p^e} : \mathcal{K}^{1/p^e}]\,[\mathcal{K}^{1/p^e} : \mathcal{K}] = [\mathcal{L}^{1/p^e} : \mathcal{L}]\,[\mathcal{L} : \mathcal{K}].$$

The map $u \to u^{1/p^e}$ gives an isomorphism of the inclusion $\mathcal{K} \subseteq \mathcal{L}$ with the inclusion $\mathcal{K}^{1/p^e} \subseteq \mathcal{L}^{1/p^e}$, so that

$$[\mathcal{L}^{1/p^e} : \mathcal{K}^{1/p^e}] = [\mathcal{L} : \mathcal{K}].$$

But then $(*)$ implies that

$$[\mathcal{L}^{1/p^e} : \mathcal{L}] = [\mathcal{K}^{1/p^e} : \mathcal{K}],$$

and the latter is the same as the torsion-free rank over A of

$$B = A^{1/p^e} \cong K[[x_1^{1/p^e},\, \ldots\,,\, x_d^{1/p^e}]].$$

Let $y_i = x_i^{1/p^e}$, $1 \leq i \leq d$. Then B is free over A on the basis consisting of all monomials $y_1^{a_1} \cdots y_d^{a_d}$ with $0 \leq a_i < p^e$ for $1 \leq i \leq d$. This free basis has cardinality $(p^e)^d = p^{de}$, as required. □

We are now ready to prove the existence of Hilbert-Kunz multiplicities: the result is stated on the first page of the Lecture Notes of April 5, but we repeat the statement.

Theorem (Monsky). *Let M be a finitely generated module of dimension d over $(R,\, m,\, K)$, where R has prime characteristic $p > 0$, and let $\mathfrak{A} \subseteq m$ be m-primary. Then the Hilbert-Kunz multiplicity $e_{HK}(\mathfrak{A},\, M)$ of M with respect to $\mathfrak{A}$ exists, and is a positive real number.*

Proof. By the results of the Lecture of April 5, it suffices to prove this when $M = (R,\, m,\, K)$ is a complete local domain with a perfect residue class field. Let

$$\gamma_n = \frac{\ell(R/\mathfrak{A}^{[p^n]})}{p^{nd}}.$$

We shall prove that the sequence $\{\gamma_n\}_n$ is a Cauchy sequence. This will prove that the sequence has a limit. The fact that the limit is positive then follows from the lower bound in part (c) of the Lemma on p. 2 of the Lecture Notes of April 5.

The first key point is that ${}^1R \cong R^{1/p}$ has torsion-free rank p^d as an R-module. Thus, ${}^1R$ and $R^{\oplus p^d}$ become isomorphic after localization at a nonzero element of the domain R. By part (b) of the Lemma on p. 4 of the Lecture Notes of April 5, there is a positive real constant C such that

$$(*) \quad |\mathcal{F}_{HK}(\mathfrak{A},\, R^{\oplus p^d})(n) - \mathcal{F}_{HK}(\mathfrak{A},\, {}^1R)(n)| \leq C/p^{(d-1)n}$$

for all $n \in \mathbb{N}$. The leftmost term is $p^d\mathcal{F}_{HK}(\mathfrak{A},\, R)(n)$. By the Proposition at the top of p. 4 of the Lecture Notes of April 5,

$$\mathcal{F}_{HK}(\mathfrak{A},\, {}^1R)(n) = \mathcal{F}_{HK}(\mathfrak{A},\, R)(n+1).$$

Thus, $(*)$ becomes

$$(**) \quad |p^d\mathcal{F}_{HK}(\mathfrak{A},\, R)(n) - \mathcal{F}_{HK}(\mathfrak{A},\, R)(n+1)| \leq Cp^{(d-1)n}.$$

We may divide both sides by $p^{(n+1)d}$ to obtain

$$(***) \quad |\gamma_n - \gamma_{n+1}| \leq C/p^{dn-n-dn-d} = \frac{Cp^{-d}}{p^n}.$$

Hence, for all $N \geq n$,

$$|\gamma_n - \gamma_N| \leq |\gamma_n - \gamma_{n+1}| + |\gamma_{n+1} - \gamma_{n+2}| + \cdots + |\gamma_{N-1} - \gamma_N|$$

$$\leq \frac{Cp^{-d}}{p^n}(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots) \leq \frac{Cp^{-d}(1-1/p)^{-1}}{p^n},$$

which shows that $\{\gamma_n\}_n$ is a Cauchy sequence, as claimed. □

The proof of the Theorem of Monsky can be easily adapted to show more.

Theorem. *Let $(R,\, m,\, K)$ by a local ring of prime characteristic $p > 0$, let M be a finitely generated R-module, and let $\mathfrak{A} \subseteq m$ be an m-primary ideal. Then the Hilbert-Kunz multiplicity with respect to $\mathfrak{A}$ is additive in the sense that if one has a finite filtration of M with factors N_i, $e_{HK}(\mathfrak{A},\, M)$ is the sum of the values of $e_{HK}(\mathfrak{A},\, N_i)$ for those N_i of the same dimension as M.*

Equivalently, if $\mathcal{P}$ is the set of (necessarily minimal) primes in the support of M such that $\dim(R/P) = \dim(M)$, *then*

$$(*) \quad e_{HK}(\mathfrak{A},\, M) = \sum_{P \in \mathcal{P}} \ell_{R_P}(M_P) e_{HK}(\mathfrak{A},\, R/P).$$

Proof. Additivity implies the formula $(*)$ because if one takes a prime cyclic filtration of M, the only terms that contribute to the value of $e_{HK}(\mathfrak{A},\, M)$ are those R/P with $P \in \mathcal{P}$, and the number of factors equal to R/P is the same as $\ell_{R_P}(M_P)$. On the other hand, it is easy to see that if one has $(*)$, then additivity follows because for every $P \in \mathcal{P}$, $\ell_{R_P}(N_P)$ is additive in N for modules N whose support is contained in $\mathrm{Supp}\,(M)$.

It will suffice to prove additivity after applying $S \otimes_R \_$, where $(S,\, \mathfrak{n},\, L)$ is complete local with L algebraically closed, $R \to S$ is flat local, and $\mathfrak{n} = mS$. Hence, we may assume without loss of generality that R is complete local with algebraically closed residue class field, and it suffices to prove that $(*)$ holds in this case.

We may replace M by M/N where N is a maximal submodule of smaller dimension without affecting the issue. Thus, we may assume without loss of generality that M is of pure dimension. We may replace R by $R/\mathrm{Ann}_R M$ without affecting any relevant issue, so that the minimal primes of the support of M are those of R.

Let W be the multiplicative system that is the complement of the union of the minimal primes of R. Exactly as in the argument on pages 5 and 6 of the Lecture Notes of April 5, we have $M_1 \oplus \cdots \oplus M_h \subseteq M$ such that each M_i has a unique minimal prime $P_i \in \mathcal{P}$ in its support and localization at W induces an isomorphism. We then have that

$$\ell_{R_{P_i}}(M_{P_i}) = \ell_{R_{P_i}}\big((M_i)_{P_i}\big)$$

for every i while $(M_i)_{P_j} = 0$ if $j \neq i$. We then have that

$$e_{HK}(\mathfrak{A},\, M) = e_{HK}(\mathfrak{A},\, M_1 \oplus \cdots \oplus M_h) = \sum_{i=1}^{h} e_{HK}(\mathfrak{A},\, M_i),$$

and the formula $(*)$ will follow if we can show that it holds for all of the M_i. We have thus reduced to the case where M has a unique minimal prime P in its support.

If we repalce M by ${}^eM$, the Hilbert-Kunz multiplicity with respect to $\mathfrak{A}$ is multiplied by p^{de}, by the Proposition on p. 4 of the Lecture Notes of April 5. The same is true for $\ell_{R_P}(M)$: if M_P has a filtration by k copies of $\kappa = R_P/PR_P$, $({}^eM)_P$ has a filtration by k copies of ${}^e\kappa$, and the dimension of ${}^e\kappa$ over κ is the same as the torsion-free rank of ${}^e(R/P)$ over R/P, which is p^{de}, as required, by the first Theorem on p. 2 of today's Lecture Notes.

Thus, we may replace M by ${}^eM$ for $e \gg 0$, and so reduce to the case where $R/\mathrm{Ann}_R M$ is a domain. Hence, we can reduce to the case where R is a domain and M is torsion-free over R. If M has torsion-free rank ρ over R, we have already seen that $e_{HK}(\mathfrak{A},\, M) = \rho\, e_{HK}(\mathfrak{A},\, R)$, which is just what we need. $\square$

Example. To illustrate how complicated the behavior of Hilbert-Kunz multiplicities can be in relatively simple examples, we consider

$$R = \mathbb{Z}_5[[X_1,\, X_2,\, X_3,\, X_4]](X_1^4 + X_2^4 + X_3^4 + X_4^4]].$$

It is proved in [C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, that

$$\mathcal{F}_{HK}(R)(n) = \frac{168}{61}(5^n)^3 - \frac{107}{61}3^n.$$

In particular, $e_{HK}(R) = \dfrac{168}{61}$.

Discussion. Hilbert-Kunz multiplicities can be used to characterize tight closure in complete local domains. This characterizes tight closure many instances. If R is essentially of finite type over an excellent local ring, $r \in R$ is in the tight closure of the ideal I if and only if for every complete local domain D to which R maps, the image of r is in the tight closure of ID. See Theorem (2.1) of [M. Hochster, *Tight closure in equal characteristic, big Cohen-Macaulay algebras, and solid closure*, in Commutative Algebra: Syzygies, Multiplicities and Birational Algebra, Contemp. Math. **159**, Amer. Math. Soc., Providence, R. I., 1994, 173–196], which gives a summary of many properties of tight closure. Moreover, in an excellent local ring $(R,\, m,\, K)$, $r \in R$ is in the tight closure of I if and only if it is in the tight closure of every m-primary ideal containing I.[5]

Therefore, much of the theory can be developed from a criterion for when an element $r \in R$ is in the tight closure of an m-primary ideal I in a complete local domain R. In this situation, one such criterion is the following: for a proof see Theorem (8.17) of [M. Hochster and C. Huneke, *Tight closure, invariant theory, and the generic perfection of determinantal loci*, Journal of the Amer. Math. Soc. **3** (1990) 31–116].

Theorem. *Let $(R,\, m,\, K)$ be a complete local domain of prime characteristic $p > 0$, let I be an m-primary ideal of R, let $r \in m$, and let $J = I + rR$. Then r is in the tight closure of I in R if and only $e_{HK}(I,\, R) = e_{HK}(J,\, R)$.*

Time permitting, we still aim to prove two results of Lech: one is that his conjecture holds when the base ring has dimension 2, and the other is that it holds in equal characteristic when the closed fiber S/mS of the map $(R,\, m,\, K) \to (S,\, \mathfrak{n},\, L)$ is a complete intersection. Cf. [C. Lech, *Note on multiplicities of ideals*, Arkiv for Mathemtik **4** (1960) 63–86].

However, we shall first focus on some results of D. Hanes in positive characteristic, including the fact that Lech's conjecture holds for graded rings of dimension 3 with a perfect

[5] Necessity is obvious. For sufficiency, one may pass to the reduced case and then R has a test element c (see Theorem (6.1) of [M. Hochster and C. Huneke, *F-regularity, test elements, and smooth base change*, Trans. Amer. Math. Soc. **346** (1994) 1–62]). If $cu^q \notin I^{[q]}$, we can choose N so large that $cu^q \notin I^{[q]} + m^N$. Then $cu^q \notin (I + m^N)^{[q]}$, and so u is not in the tight closure of $I + m^N$. $\square$

residue class field, which is proved by means of the construction of "approximately" linear maximal Cohen-Macaulay modules.

Lecture of April 10, 2019

The next two results suggest that characteristic p techniques may be helpful in proving the existence of linear maximal Cohen-Macaulay modules.

Let R be a ring of prime characteristic $p > 0$. The *Frobenius closure* I^{F} of an ideal $I \subseteq R$ is

$$\{r \in R : \text{for some } e \in \mathbb{N},\ r^{p^e} \in I^{[p^e]}\}.$$

Note that once this holds for one value of e, it also holds for all larger values. Alternatively, I^{F} is the union of contractions of I to R under the maps $F^e : R \to R$ as e varies: the union is increasing. Note that $I \subseteq I^{\mathrm{F}}$. When R is Noetherian, the contractions of I under the various F^e are the same for all $e \gg 0$. Thus, if $J = I^{\mathrm{F}}$, we can choose $e \gg 0$ such that $J^{[p^e]} \subseteq I^{[p^e]}$. But since $I \subseteq J$, the opposite inclusion is obvious. Hence, for all $e \gg 0$, $(I^{\mathrm{F}})^{[p^e]} = I^{[p^e]}$. Notice that when $r \in I^{\mathrm{F}}$, we have that $1 \cdot r^{p^e} \in I^{[p^e]}$ for all $e \gg 0$, so that $I^{\mathrm{F}} \subseteq I^*$, the tight closure of I in R.

Theorem (D. Hanes). *Let (R, m, K) be an F-finite Cohen-Macaulay local ring of prime characterisitc $p > 0$. Suppose that there exists an ideal $I \subseteq m$ generated by a system of parameters such that $I^{\mathrm{F}} = m$. Then for all sufficiently large e, ${}^eR$ is a linear maximal Cohen-Macaulay module over R.*

Proof. Choose any e such that $m^{[p^e]} = I^{[p^e]}$. Since R is F-finite, ${}^eR$ is a finitely generated module over R, and, obviously a maximal Cohen-Macaulay module: if $x_1, \ldots, x_d$ is a system of parameters in R, they form an R-sequence on ${}^eR$ because $x_1^{p^e}, \ldots, x_d^{p^e}$ is a regular sequence on R. Note that under the identification of ${}^eR$ with R, $I\,{}^eR$ becomes $I^{[p^e]}$ and $m\,{}^eR$ becomes $m^{[p^e]}$. Since $I^{[p^e]} = m^{[p^e]}$, we have that $I\,{}^eR = m\,{}^eR$, as required. □

Theorem. *Let (R, m, K) be any F-finite Cohen-Macaulay ring of prime characteristic $p > 0$. Then R has a free extension S such that $R \to S$ is local, the induced map of residue class fields is an isomorphism, and S has a linear maximal Cohen-Macaulay module.*

Proof. Let $x_1, \ldots, x_d$ be any system of parameters for R. Then for any sufficiently large integer $e \in \mathbb{N}$, we have that $m^{[p^e]} \subseteq I$. Let $Z_1, \ldots, Z_d$ be indeterminates over R, let $T = R[Z_1, \ldots, Z_d]$, and let $S = T/J$, where J is generated by the elements $Z_i^{p^e} - x_i$, $1 \leq i \leq d$. Evidently, S is module-finite over R, and so its maximal ideals all lie over m. But

$$S/mS \cong T/(Z_i^{p^e} : 1 \leq i \leq d)T,$$

a zero-dimensional local ring with residue class field isomorphic with K. Thus, S is local with residue class field K. Evidently, S is free over R on the basis consisting of the images of all monomials $Z_1^{a_1} \cdots Z_d^{a_d}$ with $0 \leq a_i \leq p^e$ for $1 \leq i \leq d$. Thus, S satisfies all of the requirements of the Theorem, provided that we can show that it has a linear maximal Cohen-Macaulay module.

Let $z_1, \ldots, z_d$ be the images of $Z_1, \ldots, Z_d$, respectively, in S. Clearly, $z_1, \ldots, z_d$ is a system of parameters for S, since killing them produces $R/(x_1, \ldots, x_d)R$. Since S is free over the Cohen-Macaulay ring R, it is Cohen-Macaulay. It will therefore suffice to show that it satisfies the hypothesis of the preceding Theorem. In fact, the maximal ideal $\mathfrak{n}$ of S is the Frobenious closure of $(z_1, \ldots, z_d)S$. The ideal $\mathfrak{n}$ is generated by m and the z_i. But

$$m^{[p^e]} \subseteq (x_1, \ldots, x_d) \subseteq (z_1, \ldots, z_d)^{[p^e]}$$

since $x_i = z_i^{p^e}$ in S, while it is obvious that every $z_i^{p^e} \in (z_1, \ldots, z_d)^{[p^e]}$. □

We next want to discuss some results concerning the existence of linear maximal Cohen-Macaulay modules over Veronese subrings of polynomial rings.

This problem may seem rather special, but the ideas used to solve the problem in dimension three, for example, can be used to prove the existence of "approximately linear" maximal Cohen-Macaulay modules for standard graded domains over a perfect field of positive characteristic in dimension 3, and this circle of ideas has provided a substantial body of results on Lech's conjecture for standard graded algebras.

Let K be field and let S be a standard graded K-algebra. By the tth Veronese subring $S^{(t)}$ of S we mean

$$\bigoplus_{i=0}^{\infty} S_{it},$$

which may also be described as the K-algebra $K[S_t]$ generated by S_t. Clearly, S is module-finite over $S^{(t)}$, since for every homogeneous element F of S, $F^t \in S^{(t)}$.

Both Segre products and Veronese subrings arise naturally in projective geometry. Let $\mathrm{Proj}(R)$ denote the projective scheme associated with a standard graded K-algebra R. (This scheme is covered by open affines of the form $\mathrm{Spec}\,\big([R_F]_0\big)$, where F is a form of positive degree in R. To get an open cover it suffices to use finitely many F: any set of homgeneous generators F_j of an ideal primary to the homogeneous maximal ideal wil provide such a cover, and we may take the F_j to be one-forms.) An important reason for studying Segre products is that

$$\mathrm{Proj}(R \circledS_K S) \cong \mathrm{Proj}(R) \times \mathrm{Proj}(S).$$

The Veronese subrings of S have the property that

$$\mathrm{Proj}(S^{(t)}) = \mathrm{Proj}(S)$$

for all t. A specific homogeneous coordinate ring S for a projective scheme X over K (which means that $X = \mathrm{Proj}(S)$) gives an embedding of X in $\mathbb{P}^n_K$ by taking a degree-preserving mapping of a polynomial ring $K[X_0, \dots, X_n]$ onto R so as to give an isomorphism of vector spaces in degree 1. The Veronese subrings of R turn out to give a family of different embeddings of X into projective spaces. Although this is an important motivation for studying Veronese subrings, we shall not need to take this point of view in the sequel.

If M is any finitely generated $\mathbb{Z}$-graded S-module (there will be only finitely many nonzero negatively graded components), for every $i \in \mathbb{Z}_t$ we define

$$M_{i,t} = \bigoplus_{j \equiv i \bmod t\mathbb{Z}} M_j.$$

We then have that every $M_{i,t}$ is an $S^{(t)}$-module, and that

$$M = \bigoplus_{i \in \mathbb{Z}_t} M_{i,t}.$$

We may apply this notational convention to $M = S$ itself, to obtain a splitting of S into t modules over $S^{(t)}$. Then $S_{0,t} = S^{(t)}$.

We now want to consider the case where $S = K[X_1, \dots, X_d]$ is a polynomial ring. In this case $S^{(t)}$ is generated over K by all monomials of degree t in $x_1, \dots, x_d$. The elements $x_1^t, \dots, x_d^t$ form a system of parameters in S and, hence, in $R = S^{(t)}$. The other generators of the the maximal ideal of R are integral over the ideal $(x_1^t, \dots, x_d^t)S^{(t)}$, and so this parameter ideal is a minimal reduction of the maximal ideal of $S^{(t)}$. Note that any nonzero monomial of degree $t-i$, $0 \le i \le t-1$, multiplies $S_{i,t}$ into $S_{0,t} = S^{(t)}$. Therefore, every $S_{i,t}$ has rank one as an $S^{(t)}$-module.

It follows that the rank of S over $S^{(t)}$ is t, since S is the direct sum of t modules over $S^{(t)}$, each of which has torsion-free rank one.

Since $x_1^t, \dots, x_d^t$ generates a minimal reduction of the maximal ideal of $S^{(t)}$ which is a parameter ideal, we have that $e(S^{(t)})$ is the torsion-free rank of $S^{(t)}$ over $B = K[x_1^t, \dots, x_d^t]$. Clearly, the torsion-free rank of S over B is t^d, and we have just seen that the torsion free-rank of S over $R = S^{(t)}$ is t. It follows that

$$e(R) = t^d/t = t^{d-1}.$$

(In the case of composite extensions of domains, torsion-free rank multiplies: one may pass to the fraction fields, and then the torsion-free rank is the same as the degree of the corresponding field extension.)

We next want to classify all the graded Cohen-Macaulay modules over $S^{(t)}$ when S is the polynomial ring in two variables. We shall use this classification to show that there is a unique graded linear maximal Cohen-Macaulay module that is indecomposable, i.e., not a direct sum.

In the case of the polynomial ring in three variables, we shall, at least, exhibit a graded module that is a linear maximal Cohen-Macaulay module.

Lecture of April 12, 2019

We can now analyze all graded maximal Cohen-Macaulay modules for a Veronese subring of the polynomial ring in two variables, and show, as a corollary, that there is a unique indecomposable linear maximal Cohen-Macaulay module up to shifts in grading. Recall that if M is a $\mathbb{Z}$-graded module and $h \in \mathbb{Z}$, $M(h)$ denotes the same module, graded so that $[M(h)]_n = [M]_{h+n}$ for all n. We also need:

Discussion: reflexive modules over normal domains of dimension 2. Let M and W be any R-modules. Then there is a natural canonical map

$$M \to \mathrm{Hom}_R\bigl(\mathrm{Hom}_R(M,\,W),\,W\bigr)$$

whose value on $u \in M$ is the map θ_u defined by

$$\theta_u(f) = f(u).$$

Recall that an R-module M is *reflexive* if the natural map

$$M \to \mathrm{Hom}_R\bigl(\mathrm{Hom}_R(M,\,R),\,R\bigr)$$

is an isomorphism.

Notice that if $x,\,y \in R$ form a regular sequence on W, they form a regular sequence on $V = \mathrm{Hom}_R(M,\,W)$ whenever $V \neq 0$. First note that if $f \in V$, then $xf = 0$ if and only if x kills all values of f, and this implies that $f = 0$, since x is not a zerodivisor W. Second, if $xf = yg$ then for all u in M, $xf(u) = yg(u)$, and this implies that $g(u)$ is, in a unique way, a multiple of x, i.e., there exists a unique element of W, which we may denote $h(u)$, such that $g(u) = xh(u)$. It is easy to check that h is an R-linear map from $M \to W$, and so $g = xh$. We have shown that $x,\,y$ is a regular sequence on $\mathrm{Hom}_R(M,\,W)$.

This helps explain the following fact, which is a particular case of the Theorem on p. 2 of the Lecture Note from Math 615, March 29, 2004.

Theorem. *A finitely generated module over a Noetherian normal domain of dimension two is maximal Cohen-Macaulay if and only if it is reflexive.*

We also note:

Lemma. *Let M be a finitely generated $\mathbb{Z}$-graded module over the polynomial ring $S = K[X_1,\,\ldots\,,X_d]$. Then M has depth d on the maximal ideal of S if and only if M is S-free.*

Proof. This is a graded version of a special case of the Auslander-Buchsbaum theorem, but we give an elementary proof. The "if" part is obvious. Suppose that the depth is

d. Let $u_1, \ldots, u_h$ be forms of M whose images in $M/(x_1, \ldots, x_d)M$ form a K-basis for $M/(x_1, \ldots, x_d)M$. It will suffice to show that $u_1, \ldots, u_h$ is a free basis for M over S. The case where $d = 0$ is obvious, and we use induction on d. The depth condition implies that $x_1, \ldots, x_d$ is a regular sequence on M, and the induction hypothesis implies that M/x_1M is free on the images of the u_j over $K[x_2, \ldots, x_d]$. The homogeneous Nakayama Lemma implies that $u_1, \ldots, u_h$ span M. We must show that there is no nonzero relation on the u_j. If there is a relation

$$\sum_{j=1}^{h} F_j u_j = 0$$

with some $F_j \neq 0$, by taking homogeneous components we may assume that $\deg F_j + \deg u_j$ is constant, say δ, and we may choose δ as small as possible for a nonzero homogeneous relation. Consider the relation modulo x_1S. By the induction hypothesis, it must vanish, so that every F_j can be written x_1G_j, and then we have

$$x_1(\sum_{j=1}^{h} G_j u_j = 0).$$

Since x_1 is not a zerodivisor on M, we have that

$$\sum_{j=1}^{h} G_j u_j = 0,$$

which gives a relation of lower degree, a contradiction. □

Theorem. *Let M be a graded maximal Cohen-Macaulay module over $R = S^{(t)}$, where $S = K[X, Y]$ is a polynomial ring in two variables over a field K. Then M is a finite direct sum of modules $S(h)_{j,t}$, each of which is a maximal Cohen-Macaulay module.*

Proof. Let M be any maximal $\mathbb{Z}$-graded Cohen-Macaulay module over R. Since S is Cohen-Macaulay, it is a maximal Cohen-Macaulay R-module, and, hence, each of the modules $S_{j,t}$ is a maximal Cohen-Macaulay R-module.

Because $R \to S$ splits, we obtain an R-split embedding $M \hookrightarrow S \otimes_R M$ as R-modules. The $\mathbb{Z}_t$-indexed splitting of S as an R-module induces such a splitting on $S \otimes_R M$, where the degree 0 component is M. Then we have

$$\mathrm{Hom}_R\bigl(\mathrm{Hom}_R(M, R)\, R\bigr) \hookrightarrow \mathrm{Hom}_R\bigl(\mathrm{Hom}_R(S \otimes_R M, R), R\bigr)$$

where the module on the right continues to have both a graded S-modoule structure and a $\mathbb{Z}_t$-indexed splitting into R-modules. It has depth two as an R-module, since R does, and so it has depth two as a graded S-module. Thus, by the Lemma, the module is a finite direct sum of modules $S(h_\nu)$ with h_ν varying.

The module on the left is a split direct summand and is, in fact, the index 0 summand of the module on the right in the splitting indexed by $\mathbb{Z}_t$. However, since M is maximal Cohen-Macaulay and R is normal of dimension two, we have that

$$M \to \mathrm{Hom}_R\bigl(\mathrm{Hom}_R(M,\, R)\, R\bigr)$$

is an isomorphism. The stated conclusion follows at once. □

Corollary. *Let $R = S^{(t)}$, where $S = K[X,\, Y]$ is a polynomial ring in two variables over a field K. Then a graded R-module M is a linear maximal Cohen-Macaulay module over R if and only if M is a direct sum of copies of modules $S(h)_{t-1,t}$. Thus, M is an indecomposable linear maximal Cohen-Macaulay module if and only if it is, up to a shift in grading, $S_{t-1,t}$.*

Proof. A direct sum of modules is maximal Cohen-Macaulay if and only if each summand is, and both $\nu(\_)$ and $e(\_)$ are additive over direct sums. It follows that a direct sum of nonzero modules is a linear maximal Cohen-Macaulay module if and only if every summand is a linear maximal Cohen-Macaulay module. Since all of the $S_{j,t}$ are maximal Cohen-Macaulay modules of torsion-free rank one, each of them has multiplicity t. The result now follows because $S_{j,t}$ is minimally generated by the monomials of degree j, namely

$$X^j,\, X^{j-1}Y,\, ,\dots,\, XY^{j-1},\, Y^j,$$

in X and Y, and so $\nu(S_{j,t}) = j+1$, $0 \le j \le t-1$. Obviously, $S_{j,t}$ is a linear maximal Cohen-Macaulay module if and only if $j = t-1$. □

We next want to show that when $S = K[X,\, Y,\, Z]$, the polynomial ring in three variables over the field K, one can construct linear maximal Cohen-Macaulay modules over $R = S^{(t)}$ for all $t \ge 1$. We first note:

Lemma. *Let A be an $r \times s$ matrix over an arbitrary ring R and let Q be the cokernel of the map $A : R^s \to R^r$; Q is also the quotient of R^r by the column space of A. Then $I_r(A)$ kills Q, i.e., $I_r(A)R^r \subseteq Im\,(A)$.*

Proof. Let D denote the determinant of an $r \times r$ minor of A. By permuting the columns, we might as well assume that D corresponds to the first r columns of A. It suffices to show that the product of D with every standard basis vector for R^r, written as a column, is in the column space of A, and so it certainly suffices to prove that it is in the R-span of the first r columns. Therefore, we might as well replace A by the submatrix formed from its first r columns. We change notation, so that A is now an $r \times r$ matrix. Let B denote the classical adjoint of A, which is the $r \times r$ matrix that is the transpose of the matrix of cofactors of A. Then $AB = D\boldsymbol{I}_r$. Since each column of AB is the product of A with a column of B, and since the columns of $D\boldsymbol{I}_r$ are precisely the products of D with the standard basis for R^r, the result follows. □

We are now ready to construct a linear maximal Cohen-Macaulay module over $R = S^{(t)}$. To this end, let A denote the $t-1 \times t+1$ matrix

$$\begin{pmatrix} X & Y & Z & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & X & Y & Z & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & X & Y & Z & \cdots & 0 & 0 & 0 \\ & & & & \cdots & & & & \\ & & & & \cdots & & & & \\ & & & & \cdots & & & & \\ 0 & 0 & 0 & 0 & 0 & \cdots & X & Y & Z \end{pmatrix}$$

where the i th row has entries X, Y, and Z in the i th, $i{+}1$ st, and $i{+}2$ nd spots, respectively, and 0 everywhere else, $1 \leq i \leq t-1$. We have an exact sequence:

$$(*) \quad 0 \to N \to S(-1)^{\oplus t+1} \xrightarrow{A} S^{\oplus t-1}.$$

Theorem. *Let notation be as above, so that $S = K[X,\,Y,\,Z]$ is the polynomial ring in three variables over a field K, $R = S^{(t)}$ for a positive integer t, and $N \subseteq S(-1)^{\oplus t+1}$ is the kernel of the matrix A defined above. Then the module $M = N_{t-1,t} \subseteq N$ is a linear maximal Cohen-Macaulay module over R of torsion-free rank 2, with minimal generators all of the same degree.*

Proof. Using the splitting indexed by $\mathbb{Z}_t$, the sequence $(*)$ displayed above yields

$$(**) \quad 0 \to M \to S_{t-2,t}^{\oplus t+1} \xrightarrow{A} S_{t-1,t}^{\oplus t-1}$$

where the map on the right is the restriction of the linear map with matrix A. By the Lemma above, the image of $A : S(-1)^{\oplus t+1} \to S^{\oplus t-1}$ contains $I_{r-1}(A)S^{\oplus t-1}$. By Problem 2. of Problem Set #5,

$$I_{r-1}(A) = (X,\,Y,\,Z)^{t-1}S.$$

But $[(X,\,Y,\,Z)^{t-1}S]_{t-1,t} = S_{t-1,t}$, and it follows that the restricted map induced by A in $(**)$ is surjective, i.e., that

$$0 \to M \to S_{t-2,t}^{\oplus t+1} \xrightarrow{A} S_{t-1,t}^{\oplus t-1} \to 0$$

is exact. Since the modules in the middle and on the right are maximal Cohen-Macaulay modules, so is M. Since the rank of every $S_{j,t}$ is one, the module in the middle has rank $t+1$, and the module on the right has rank $t-1$. It follows that M has rank 2, and so $e(M) = 2\,e(R) = 2t^2$.

To complete the proof, it will suffice to show that $\nu(M) = 2t^2$ as well. If we think of $M \subseteq S_{t-2,t}^{\oplus t+1}$, the least degree (using degree in S for every component) in which there might be nonzero elements of M is $t-2$. Now,

$$\dim\big([S]_n = \binom{n+2}{2},$$

and so the dimension of the piece of M that lies in $S_{t-2,t}^{\oplus t+1}$ is

$$(t+1)\binom{t}{2} - (t-1)\binom{t+1}{2} = \frac{(t+1)t(t-1)}{2} - \frac{(t-1)(t+1)t}{2} = 0$$

The next possible degree in which M might be nonzero is $t+t-2 = 2t-2$, and here we get

$$(t+1)\binom{2t}{2} - (t-1)\binom{2t+1}{2} = \frac{(t+1)(2t)(2t-1)}{2} - \frac{(t-1)(2t+1)2t}{2} = 2t^2.$$

Clearly, one needs $2t^2$ minimal generators in this degree, and these elements must generate, since $\nu(M) \leq e(M)$ always.

We give an alternative argument. First note that if $y_1, \ldots, y_h$ is a regular sequence on all of the modules in the short exact sequence

$$(\#) \quad 0 \to M \to M' \to M'' \to 0$$

then it is easy to see by induction on h that

$$(\#\#) \quad 0 \to M/(y_1, \ldots, y_h)M \to M'/(y_1, \ldots, y_h)M' \to M''/(y_1, \ldots, y_h)M'' \to 0$$

is exact, and since the short exact sequence (#) maps onto the short exact sequence (##) the nine lemma implies that the sequence of kernels

$$0 \to (y_1, \ldots, y_h)M \to (y_1, \ldots, y_h)M' \to (y_1, \ldots, y_h)M'' \to 0$$

is exact as well.

We know, as in the first argument, know that there are no elements of $M \subseteq S_{t-2,t}^{\oplus t+1}$ in degree $t-2$. Every element of M, thought of a submodule of $S^{\oplus t+1}$, has degree $2t-2$ or more. If m is the maximal ideal of R, which is generated by the monomials of degree t in X, Y, Z, we have that all elements of mM have degree $3t-2$ or greater, and every monomial of degree $3t-2$ or more in X, Y, Z must involve X^t or Y^t or Z^t. Hence, $mM \subseteq (X^t, Y^t, Z^t)S^{\oplus t+1}$, and it follows that $mM \subseteq (X^t, Y^t, Z^t)S_{t-2,t}^{\oplus t+1}$. Since all three of the modules M, $S_{t-2,t}^{\oplus t+1}$, and $S_{t-1,t}^{\oplus t-1}$ are maximal Cohen-Macaulay modules over the ring R, we have that $X^t, Y^t, Z^t \in R$ is a regular sequence on all of them, and so we see that

$$0 \to (X^t, Y^t, Z^t)M \to (X^t, Y^t, Z^t)S_{t-2,t}^{\oplus t+1} \to (X^t, Y^t, Z^t)S_{t-1,t}^{\oplus t-1} \to 0$$

is exact. It follows that $mM \subseteq (X^t, Y^t, Z^t)M$, and so they are equal, which is what we need for M to be linear. □