FOUNDATIONS OF TIGHT CLOSURE THEORY

by Melvin Hochster

These notes give an introduction to tight closure theory based on Lectures given in Math 711 in Fall, 2007, at the University of Michigan. In the current version, only the positive characteristic theory is covered. There are several novel aspects to this treatment. One is that the theory for all modules, not just finitely generated modules, is developed systematically. It is shown that all the known methods of proving the existence of test elements yield completely stable test elements that can be used in testing tight closure for all pairs of modules. The notion of strong F-regularity is developed without the hypothesis that the ring be F-finite. The definition is simply that every submodule of every module is closed, without the hypothesis of finite generation. This agrees with the usual definition in the F-finite case, which is developed first in these notes. A great deal of revision and expansion are planned.

The structure of the individual lectures has been preserved. References often refer to a result as, say, "the Theorem on p. k of the Lecture of ...". The page numbering meant is internal to the lecture and is not shown explicitly. Thus, if the Lecture begins on p. n, the result specified would be on page $n + k - 1$.

I have not tried to give complete references. When references are given, they occur in full in the text where they are cited. At this time there is no separate list.

Subsidiary material has been included in the notes that was not covered in detail in the lectures. Such material has usually been indicated by enclosing it in special brackets. This paragraph is an example of the use of these indicators.

There are five problem sets interspersed, with solutions given at the end.

The author would like to thank Karl Schwede and Kevin Tucker for their very helpful comments.

The author would also like to thank the National Science Foundation for its support through grant DMS0400633.

Contents

Math 711: Lecture of September 5, 2007

Throughout these lecture notes all given rings are assumed commutative, associative, with identity and modules are assumed unital. Homomorphisms are assumed to preserve the identity. With a few exceptions that will be noted as they occur, given rings are assumed to be Noetherian. However, we usually include this hypothesis, especially in formal statements of theorems.

Our objective is to discuss tight closure closure theory and its connection with the existence of big Cohen-Macaulay algebras, as well as the applications that each of these have: they have many in common.

At certain points in these notes we will include material not covered in class that we want to assume. We indicate where such digressions begin and end with double bars before and after, just as we have done for these two paragraphs. On first perusal, the reader may wish to read only the unfamiliar definitions and the statements of theorems given, and come back to the proofs later.

In particular, the write-up of this first lecture is much longer than will be usual, since a substantial amount of prerequisite material is explained, often in detail, in this manner.

By a *quasilocal ring* (R, m, K) we mean a ring with a unique maximal ideal m: in this notation, $K = R/m$. A quasilocal ring is called *local* if it is Noetherian. A homomorphism $h : R \to S$ from a quasilocal ring (R, m, K) to a quasilocal ring (S, m_S, K_S) is called *local* if $h(m) \subseteq m_S$, and then h induces a map of residue fields $K \to K_S$.

If $x_1, \ldots, x_n \in R$ and M is an R-module, the sequence $x_1, \ldots, x_n$ is called a *possibly improper* regular sequence on M if x_1 is not a zerodivisor on M and for all i, $0 \le i \le n-1$, x_{i+1} is not a zerodivisor on $M/(x_1, \ldots, x_i)M$. A possibly improper regular sequence is called a *regular sequence* on M if, in addition, $(*)$ $\quad (x_1, \ldots, x_n)M \neq M$. When $(*)$ fails, the regular sequence is called *improper*. When $(*)$ holds we may say that the regular sequence is *proper* for emphasis, but this use of the word "proper" is not necessary.

Note that every sequence of elements is an improper regular sequence on the 0 module, and that a sequence of any length consisting of the element 1 (or units of the ring) is an improper regular sequence on every module.

If $x_1, \ldots, x_n \in m$, the maximal ideal of a local ring (R, m, K), and M is a nonzero finitely generated R-module, then it is automatic that if $x_1, \ldots, x_n$ is a possibly improper regular sequence on M then $x_1, \ldots, x_n$ is a regular sequence on M: we know that $mM \neq M$ by Nakayama's Lemma.

If $x_1, \dots, x_n \in R$ is a possibly improper regular sequence on M and and S is any flat R-algebra, then the images of $x_1, \dots, x_n$ in S form a possibly improper regular sequence on $S \otimes_R M$. By a straightforward induction on n, this reduces to the case where $n = 1$, where it follows from the observation that if $0 \to M \to M$ is exact, where the map is given by multiplication by x, this remains true when we apply $S \otimes_R \_$. In particular, this holds when S is a localization of R.

If $x_1, \dots, x_n$ is a regular sequence on M and S is flat over R, it remains a regular sequence provided that $S \otimes_R \big(M/(x_1, \dots, x_n)M\big) \neq 0$, which is always the case when S is faithfully flat over R.

Nakayama's Lemma, including the homogeneous case

Recall that in Nakayama's Lemma one has a *finitely generated module* M over a quasilocal ring (R, m, K). The lemma states that if $M = mM$ then $M = 0$. (In fact, if $u_1, \dots, u_h$ is a set of generators of M with h minimum, the fact that $M = mM$ implies that $M = mu_1 + \cdots mu_h$. In particular, $u_h = f_1u_1 + \cdots + f_hu_h$, and so $(1 - f_h)u_h = f_1u_1 + \cdots + f_{h-1}u_{h-1}$ (or 0 if $h = 1$). Since $1 - f_h$ is a unit, u_h is not needed as a generator, a contradiction unless $h = 0$.)

By applying this 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. □

In general, regular sequences are not permutable: in the polynomial ring $R = K[x, y, z]$ over the field K, $x - 1, xy, xz$ is a regular sequence but $xy, xz, x - 1$ is not. However, if M is a finitely generated nonzero module over a local ring (R, m, K), a regular sequence on M is permutable. This is also true if R is $\mathbb{N}$-graded, M is $\mathbb{Z}$-graded but nonzero in only finitely many negative degrees, and the elements of the regular sequence in R have positive degree.

To see why, note that we get all permutations if we can transpose two consecutive terms of a regular sequence. If we kill the ideal generated by the preceding terms times the module, we come down to the case where we are transposing the first two terms. Since the ideal generated by these two terms does not depend on their order, it suffices to consider the case of regular sequences x, y of length 2. The key point is to prove that y is not a zerodivisor on M. Let $N \subseteq M$ by the annihilator of y. If $u \in N$, $yu = 0 \in xM$ implies that $u \in xM$, so that $u = xv$. Then $y(xv) = 0$, and x is not a zerodivsior on M, so that $yv = 0$, and $v \in N$. This shows that $N = xN$, contradicting Nakayama's Lemma (the local version or the homogeneous version, whichever is appropriate).

The next part of the argument does not need the local or graded hypothesis: it works quite generally. We need to show that x is a nonzerodivisor on M/yM. Suppose that $xu = yv$. Since y is a nonzerodivisor on xM, we have that $v = xw$, and $xu = yxw$. Thus $x(u - yw) = 0$. Since x is a nonzerodivisor on M, we have that $u = yw$, as required. □

The Krull dimension of a ring R may be characterized as the supremum of lengths of chains of prime ideals of R, where the length of the strictly ascending chain

$$P_0 \subset P_1 \subset \cdots \subset P_n$$

is n. The Krull dimension of the local ring (R, m, K) may also be characterized as the least integer n such that there exists a sequence $x_1, \ldots, x_n \in m$ such that $m =$

Rad $\big((x_1, \dots, x_n)R\big)$ (equivalently, such that $\overline{R} = R/(x_1, \dots, x_n)R$ is a zero-dimensional local ring, which means that $\overline{R}$ is an Artinian local ring).

Such a sequence is called a *system of parameters* for R.

One can always construct a system of parameters for the local ring (R, m, K) as follows. If $\dim(R) = 0$ the system is empty. Otherwise, the maximal ideal cannot be contained in the union of the minimal primes of R. Choose $x_1 \in m$ not in any minimal prime of R. In fact, it suffices to choose x_1 not in any minimal primes P such that $\dim(R/P) = \dim(R)$. Once $x_1, \dots, x_k$ have been chosen so that $x_1, \dots, x_k$ is part of a system of parameters (equivalently, such that $\dim\big(R/(x_1, \dots, x_k)R\big) = \dim(R) - k)$), if $k < \dim(R)$ the minimal primes of $(x_1, \dots, x_k)R$ cannot cover m. It follows that we can choose x_{k+1} not in any such minimal prime, and then $x_1, \dots, x_{k+1}$ is part of a system of parameters. By induction, we eventually reach a system of parameters for R. Notices that in choosing x_{k+1}, it actually suffices to avoid only those minimal primes Q of $(x_1, \dots, x_k)R$ such that $\dim(R/Q) = \dim\big(R/(x_1, \dots, x_k)R\big)$ (which is $\dim(R) - k$).

A local ring is called *Cohen-Macaulay* if some (equivalently, every) system of parameters is a regular sequence on R. These include regular local rings: if one has a minimal set of generators of the maximal ideal, the quotient by each in turn is again regular and so is a domain, and hence every element is a nonzerodivisor modulo the ideal generated by its predecessors. Moreover, *local complete intersections*, i.e., local rings of the form $R/(f_1, \dots, f_h)$ where R is regular and $f_1, \dots, f_h$ is part of a system of parameters for R, are Cohen-Macaulay. It is quite easy to see that if R is Cohen-Macaulay, so is R/I whenever I is generated by a regular sequence.

If R is a Cohen-Macaulay local ring, the localization of R at any prime ideal is Cohen-Macaulay. We define an arbitrary Noetherian ring to be *Cohen-Macaulay* if all of its local rings at maximal ideals (equivalently, at prime ideals) are Cohen-Macaulay.

Cohen-Macaulay rings in the graded and local cases

We want to put special emphasis on the graded case for several reasons. One is its importance in projective geometry. Beyond that, there are many theorems about the graded case that make it easier both to understand and to do calculations. Moreover, many of the most important examples of Cohen-Macaulay rings are graded.

We first 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. 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 K be a field and let R be a finitely generated $\mathbb{N}$-graded K-algebra with $R_0 = K$. Let $\mathcal{M} = \bigoplus_{d=1}^{\infty} R_j$ be the homogeneous maximal ideal of R. Then* $\dim(R) = \mathrm{height}(\mathcal{M}) = \dim(R_{\mathcal{M}})$.

Proof. The dimension of R will be equal to the dimension of R/P for one of the minimal primes P of R. Since P is minimal, it is an associated prime and therefore is homogenous. Hence, $P \subseteq \mathcal{M}$. The domain R/P is finitely generated over K, and therefore its dimension is equal to the height of every maximal ideal including, in particular, $\mathcal{M}/P$. Thus,

$$\dim(R) = \dim(R/P) = \dim\big((R/P)_{\mathcal{M}}\big) \leq \dim R_{\mathcal{M}} \leq \dim(R),$$

and so equality holds throughout, as required. □

Proposition (homogeneous prime avoidance). *Let R be an $\mathbb{N}$-graded algebra, and let I be a homogeneous ideal of R whose homogeneous elements have positive degree. Let $P_1, \ldots, P_k$ be prime ideals of R. Suppose that every homogeneous element $f \in I$ is in $\bigcup_{i=1}^{k} P_i$. Then $I \subseteq P_j$ for some j, $1 \leq j \leq k$.*

Proof. We have that the set H of homogeneous elements of I is contained in $\bigcup_{i=1}^{k} P_k$. If $k = 1$ we can conclude that $I \subseteq P_1$. We use induction on k. Without loss of generality, we may assume that H is not contained in the union of any $k - 1$ if the P_j. Hence, for every i there is a homogeous element $g_i \in I$ that is not in any of the P_j for $j \neq i$, and so it must be in P_i. We shall show that if $k > 1$ we have a contradiction. By raising the g_i to suitable positive powers we may assume that they all have the same degree. Then $g_1^{k-1} + g_2 \cdots g_k \in I$ is a homogeneous element of I that is not in any of the P_j: g_1 is not in P_j for $j > 1$ but is in P_1, and $g_2 \cdots g_k$ is in each of $P_2, \ldots, P_k$ but is not in P_1. □

Now suppose that R is a finitely generated $\mathbb{N}$-graded algebra over $R_0 = K$, where K is a field. By a *homogenous system of parameters* for R we mean a sequence of homogeneous elements $F_1, \ldots, F_n$ of positive degree in R such that $n = \dim(R)$ and $R/F_1, \ldots, F_n)$ has Krull dimension 0. When R is a such a graded ring, a homogeneous system of parameters always exists. By homogeneous prime avoidance, there is a form F_1 that is not in the union of the minimal primes of R. Then $\dim(R/F_1) = \dim(R) - 1$. For the inductive step, choose forms of positive degree $F_2, \ldots, F_n$ whose images in R/F_1R are a homogeneous system of parameters for R/F_1R. Then $F_1, \ldots, F_n$ is a homogeneous system of parameters for R. □

Moreover, we have:

Theorem. *Let R be a finitely generated $\mathbb{N}$-graded K-algebra with $R_0 = K$ such that $\dim(R) = n$. A homogeneous system of parameters $F_1, \ldots, F_n$ for R always exists. Moreover, if $F_1, \ldots, F_n$ is a sequence of homogeneous elements of positive degree, then the following statements are equivalent.*

(1) *$F_1, \ldots, F_n$ is a homogeneous system of parameters.*

(2) *m is nilpotent modulo $(F_1, \ldots, F_n)R$.*

(3) *$R/(F_1, \ldots, F_n)R$ is finite-dimensional as a K-vector space.*

(4) *R is module-finite over the subring $K[F_1, \ldots, F_n]$.*

Moreover, when these conditions hold, $F_1, \ldots, F_n$ are algebraically independent over K, so that $K[F_1, \ldots, F_n]$ is a polynomial ring.

Proof. We have already shown existence.

(1) ⇒ (2). If $F_1, \ldots, F_n$ is a homogeneous system of parameters, we have that

$$\dim\big(R/F_1, \ldots, F_n)\big) = 0.$$

We then know that all prime ideals are maximal. But we know as well that the maximal ideals are also minimal primes, and so must be homogeneous. Since there is only one homogenous maximal ideal, it must be $m/(F_1, \ldots, F_n)R$, and it follows that m is nilpotent on $(F_1, \ldots, F_n)R$.

(2) ⇒ (3). If m is nilpotent modulo $(F_1, \ldots, F_n)R$, then the homogeneous maximal ideal of $\overline{R} = R/(F_1, \ldots, F_n)R$ is nilpotent, and it follows that $[\overline{R}]_d = 0$ for all $d \gg 0$. Since each $\overline{R}_d$ is a finite dimensional vector space over K, it follows that $\overline{R}$ itself is finite-dimensional as a K-vector space.

(3) ⇒ (4). This is immediate from the homogeneous form of Nakayama's Lemma: a finite set of homogeneous elements of R whose images in $\overline{R}$ are a K-vector space basis will span R over $K[F_1, \ldots, F_n]$, since the homogenous maximal ideal of $K[F_1, \ldots, F_n]$ is generated by $F_1, \ldots, F_n$.

(4) ⇒ (1). If R is module-finite over $K[F_1, \ldots, F_n]$, this is preserved mod $(F_1, \ldots, F_n)$, so that $R/(F_1, \ldots, F_n)$ is module-finite over K, and therefore zero-dimensional as a ring.

Finally, when R is a module-finite extension of $K[F_1, \ldots, F_n]$, the two rings have the same dimension. Since $K[F_1, \ldots, F_n]$ has dimension n, the elements $F_1, \ldots, F_n$ must be algebraically independent. □

The technique described in the discussion that follows is very useful both in the local and graded cases.

Discussion: making a transition from one system of parameters to another. Let R be a Noetherian ring of Krull dimension n, and assume that one of the two situations described below holds.

(1) (R, m, K) is local and $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$ are two systems of parameters.

(2) R is finitely generated $\mathbb{N}$-graded over $R_0 = K$, a field, m is the homogeneous maximal ideal, and $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$ are two homogeneous systems of parameters for R.

We want to observe that in this situation there is a finite sequence of systems of parameters (respectively, homogeneous systems of parameters in case (2)) starting with $f_1, \ldots, f_n$ and ending with $g_1, \ldots, g_n$ such that any two consecutive elements of the sequence agree in all but one element (i.e., after reordering, only the i th terms are possibly different for a single value of i, $1 \leq i \leq n$). We can see this by induction on n. If $n = 1$ there is nothing to prove. If $n > 1$, first note that we can choose h (homogeneous of positive degree in the graded case) so as to avoid all minimal primes of $(f_2, \ldots, f_n)R$ and all minimal primes of $(g_2, \ldots, g_n)R$. Then it suffices to get a sequence from $h, f_2, \ldots, f_n$ to $h, g_2, \ldots, g_n$, since the former differs from $f_1, \ldots, f_n$ in only one term and the latter differs from $g_1, \ldots, g_n$ in only one term. But this problem can be solved by working in R/hR and getting a sequence from the images of $f_2, \ldots, f_n$ to the images of $g_2, \ldots, g_n$, which we can do by the induction hypothesis. We lift all of the systems of parameters back to R by taking, for each one, h and inverse images of the elements in the sequence in R (taking a homogeneous inverse image in the graded case), and always taking the same inverse image for each element of R/hR that occurs. □

The following result now justifies several assertions about Cohen-Macaulay rings made without proof earlier.

Note that a regular sequence in the maximal ideal of a local ring (R, m, K) is always part of a system of parameters: each element is not in any associated prime of the ideal generated by its predecessors, and so cannot be any minimal primes of that ideal. It follows that as we kill successive elements of the sequence, the dimension of the quotient drops by one at every step.

Corollary. *Let (R, m, K) be a local ring. There exists a system of parameters that is a regular sequence if and only if every system of parameters is a regular sequence. In this case, for every prime ideal I of R of height k, there is a regular sequence of length k in I.*

Moreover, for every prime ideal P of R, R_P also has the property that every system of parameters is a regular sequence.

Proof. For the first statement, we can choose a chain as in the comparison statement just above. Thus, we can reduce to the case where the two systems of parameters differ in only one element. Because systems of parameters are permutable and regular sequences are permutable in the local case, we may assume that the two systems agree except possibly for the last element. We may therefore kill the first $\dim(R) - 1$ elements, and so reduce to the case where x and y are one element systems of parameters in a local ring R of dimension 1. Then x has a power that is a multiple of y, say $x^h = uy$, and y has a power that is a multiple of x. If x is not a zerodivisor, neither is x^h, and it follows that y is not a zerodivisor. The converse is exactly similar.

Now suppose that I is any ideal of height h. Choose a maximal sequence of elements (it might be empty) of I that is part of a system of parameters, say $x_1, \ldots, x_k$. If $k < h$, then I cannot be contained in the union of the minimal primes of $(x_1, \ldots, x_k)$: otherwise, it will be contained in one of them, say Q, and the height of Q is bounded by k. Chose $x_{k+1} \in I$ not in any minimal prime of $(x_1, \ldots, x_k)R$. Then $x_1, \ldots, x_{k+1}$ is part of a system of parameters for R, contradicting the maximality of the sequence $x_1, \ldots, x_k$.

Finally, consider the case where $I = P$ is prime. Then P contains a regular sequence $x_1, \ldots, x_k$, which must also be regular in R_P, and, hence, part of a system of parameters. Since $\dim(R_P) = k$, it must be a system of parameters. □

Lemma. *Let K be a field and assume either that*

(1) *R is a regular local ring of dimension n and $x_1, \ldots, x_n$ is a system of parameters*

or

(2) *$R = K[x_1, \ldots, x_n]$ is a graded polynomial ring over K in which each of the x_i is a form of positive degree.*

Let M be a nonzero finitely generated R-module which is $\mathbb{Z}$-graded in case (2). Then M is free if and only if $x_1, \ldots, x_n$ is a regular sequence on M.

Proof. The "only if" part is clear, since $x_1, \ldots, x_n$ is a regular sequence on R and M is a direct sum of copies of R. Let $m = (x_1, \ldots, x_n)R$. Then $V = M/mM$ is a finite-dimensional K-vector space that is graded in case (2). Choose a K-vector space basis for V consisting of homogeneous elements in case (2), and let $u_1, \ldots, u_h \in M$ be elements of M that lift these basis elements and are homogeneous in case (2). Then the u_j span M by the relevant form of Nakayama's Lemma, and it suffices to prove that they have no nonzero relations over R. We use induction on n. The result is clear if $n = 0$.

Assume $n > 0$ and let $N = \{(r_1, \ldots, r_h) \in R^h : r_1u_1 + \cdots + r_hu_h = 0\}$. By the induction hypothesis, the images of the u_j in M/x_1M are a free basis for M/x_1M. It follow that if $\rho = (r_1, \ldots, r_h) \in N$, then every r_j is 0 in R/x_1R, i.e., that we can write $r_j = x_1s_j$ for all j. Then $x_1(s_1u_1 + \cdots + s_hu_h) = 0$, and since x_1 is not a zerodivisor on M, we have that $s_1u_1 + \cdots + s_hu_h = 0$, i.e., that $\sigma = (s_1, \ldots, s_h) \in N$. Then $\rho = x_1\sigma \in x_1N$, which shows that $N = x_1N$. Thus, $N = 0$ by the appropriate form of Nakayama's Lemma. □

We next observe:

Theorem. *Let R be a finitely generated graded algebra of dimension n over $R_0 = K$, a field. Let m denote the homogeneous maximal ideal of R. The following conditions are equivalent.*

(1) *Some homogeneous system of parameters is a regular sequence.*

(2) *Every homogeneous system of parameters is a regular sequence.*

(3) *For some homogeneous system of parameters $F_1, \dots, F_n$, R is a free-module over $K[F_1, \dots, F_n]$.*

(4) *For every homogeneous system of parameters $F_1, \dots, F_n$, R is a free-module over $K[F_1, \dots, F_n]$.*

(5) *R_m is Cohen-Macaulay.*

(6) *R is Cohen-Macaulay.*

Proof. The proof of the equivalence of (1) and (2) is the same as for the local case, already given above.

The preceding Lemma yields the equivalence of (1) and (3), as well as the equivalence of (2) and (4). Thus, (1) through (4) are equivalent.

It is clear that (6) $\Rightarrow$ (5). To see that (5) $\Rightarrow$ (2) consider a homogeneous system of parameters in R. It generates an ideal whose radical is m, and so it is also a system of parameters for R_m. Thus, the sequence is a regular sequence in R_m. We claim that it is also a regular sequence in R. If not, x_{k+1} is contained in an associated prime of $(x_1, \dots, x_k)$ for some k, $0 \leq k \leq n-1$. Since the associated primes of a homogeneous ideal are homogeneous, this situation is preserved when we localize at m, which gives a contradiction.

To complete the proof, it will suffice to show that (1) $\Rightarrow$ (6). Let $F_1, \dots, F_n$ be a homogeneous system of parameters for R. Then R is a free module over $A = K[F_1, \dots, F_n]$, a polynomial ring. Let Q be any maximal ideal of R and let P denote its contraction to A, which will be maximal. These both have height n. Then $A_P \to R_Q$ is faithfully flat. Since A is regular, A_P is Cohen-Macaulay. Choose a system of parameters for A_P. These form a regular sequence in A_P, and, hence, in the faithfully flat extension R_Q. It follows that R_Q is Cohen-Macaulay. $\square$

From part (2) of the Lemma on p. 8 we also have:

Theorem. *Let R be a module-finite local extension of a regular local ring A. Then R is Cohen-Macaulay if and only if R is A-free.*

It it is not always the case that a local ring (R, m, K) is module-finite over a regular local ring in this way. But it does happen frequently in the complete case. Notice that the property of being a regular sequence is preserved by completion, since the completion $\widehat{R}$ of a local ring is faithfully flat over R, and so is the property of being a system of parameters. Hence, R is Cohen-Macaulay if and only if $\widehat{R}$ is Cohen-Macaulay.

If R is complete and contains a field, then there is a coefficient field for R, i.e., a field $K \subseteq R$ that maps isomorphically onto the residue class field K of R. Then, if $x_1, \ldots, x_n$ is a system of parameters, R turns out to be module-finite over the formal power series ring $K[[x_1, \ldots, x_n]]$ in a natural way. Thus, in the complete equicharacteristic local case, we can always find a regular ring $A \subseteq R$ such that R is module-finite over A, and think of the Cohen-Macaulay property as in the Theorem above.

The structure theory of complete local rings is discussed in detail in the Lecture Notes from Math 615, Winter 2007: see the Lectures of March 21, 23, 26, 28, and 30 as well as the Lectures of April 2 and April 4.

Cohen-Macaulay modules

All of what we have said about Cohen-Macaulay rings generalizes to a theory of Cohen-Macaulay modules. We give a few of the basic definitions and results here: the proofs are very similar to the ring case, and are left to the reader.

If M is a module over a ring R, the *Krull dimension* of M is the Krull dimension of $R/\mathrm{Ann}_R(I)$. If (R, m, K) is local and $M \neq 0$ is finitely generated of Krull dimension d, a *system of parameters* for M is a sequence of elements $x_1, \ldots, x_d \in m$ such that, equivalently:

(1) $\dim\bigl(M/(x_1, \ldots, x_d)M\bigr) = 0$.

(2) The images of $x_1, \ldots, x_d$ form a system of parameters in $R/\mathrm{Ann}_R M$.

In this local situation, M is *Cohen-Macaulay* if one (equivalently, every) system of parameters for M is a regular sequence on M. If J is an ideal of $R/\mathrm{Ann}_R M$ of height h, then it contains part of a system of parameters for $R/\mathrm{Ann}_R M$ of height h, and this will be a regular sequence on M. It follows that the Cohen-Macaulay property for M passes to M_P for every prime P in the support of M. The arguments are all essentially the same as in the ring case.

If R is any Noetherian ring $M \neq 0$ is any finitely generated R-module, M is called *Cohen-Macaulay* if all of its localizations at maximal (equivalently, at prime) ideals in its support are Cohen-Macaulay.

The Cohen-Macaulay condition is increasingly restrictive as the Krull dimension increases. In dimension 0, every local ring is Cohen-Macaulay. In dimension one, it is sufficient, but not necessary, that the ring be reduced: the precise characterization in dimension one is that the maximal ideal not be an embbeded prime ideal of (0). Note that

$K[[x,y]]/(x^2)$ *is* Cohen-Macaulay, while $K[[x,y]]/(x^2, xy)$ is not. Also observe that all one-dimensional domains are Cohen-Macaulay.

In dimension 2, it suffices, but is not necessary, that the ring R be normal, i.e., integrally closed in its ring of fractions. Note that a normal Noetherian ring is a finite product of normal domains. If (R, m, K) is local and normal, then it is a doman. The associated primes of a principal ideal are minimal if R is normal. Hence, if x, y is a system of parameters, y is not in any associated prime of xR, i.e., it is not in any associated prime of the module R/xR, and so y is not a zerodivisor modulo xR.

The two dimensional domains $K[[x^2,\, x^2,\, y, xy]]$ and $K[x^4,\, x^3y,\, xy^3,\, y^4]]$ (one may also use single brackets) are not Cohen-Macaulay: as an exercise, the reader may try to see that y is a zerodivisor mod x^2 in the first, and that y^4 is a zerodivisor mod x^4 in the second. On the other hand, while $K[[x^2,\, x^3, y^2,\, y^3]]$ is not normal, it is Cohen-Macaulay.

Direct summands of rings

Let $R \subseteq S$ be rings. We want to discuss the consequences of the hypothesis that the inclusion $R \hookrightarrow S$ splits as a map of R-modules. When this occurs, we shall simply say that R is a *direct summand* of S. When we have such a splitting, we have an R-linear map $\rho : S \to R$ that is the identity on R. Here are some facts.

Proposition. *Let R be a direct summand of S. Then:*

(a) *For every ideal I of R, $IS \cap R = I$.*

(b) *If S is Noetherian, then R is Noetherian.*

(c) *If R is an $\mathbb{N}$-graded ring with $R_0 = A$ and S is Noetherian , then R is finitely generated over A.*

(d) *If S is a normal domain, then R is normal.*

Proof. Let ρ be a splitting.

(a) If $r \in R$ is such that $r = \sum_{i=1}^{h} f_i s_i$ with the $f_i \in I$ and the $s_i \in S$, so that r is a typical element of $IS \cap R$, then $r = \rho(r) = \sum_{i=1}^{n} f_i \rho(s_i)$, since the $f_i \in R$. Since each $\rho(s_i) \in R$, we have that $r \in I$.

(b) If $\{I_n\}_n$ is a nondecreasing chain of ideals of R, we have that the chain $\{I_nS\}_n$ is stable from some point on, say $I_tS = I_NS$ for all $t \geq N$. We may then apply (a) to obtain that $I_t = I_tS \cap R = I_NS \cap R = I_N$ for all $t \geq N$.

(c) From part (b), R is Noetherian, and so the ideal J spanned by all forms of positive degree is finitely generated, say by forms $F_1, \dots, F_n$ of positive degree. Then $R = A[F_1, \dots, F_n]$: otherwise, choose a form G of least degree that is in R and not in $A[F_1, \dots, F_n]$. Then $G \in J$, and so we can write G as a sum of terms H_jF_j where every

H_j is a nonzero form such that $\deg(H_j) + \deg(F_j) = \deg(G)$. Since $\deg(H_j) < \deg(G)$, every $H_j \in A[F_1, \ldots, F_n]$, and the result follows.

(d) Let $a, b \in R$ with $b \neq 0$ such that a/b is integral over R. Then a/b is an element of $\mathrm{frac}\,(S)$ integral over S as well, and so $a/b \in S$. Thus, $a \in bS \cap R = bR$ by part (a). and so $a = br$ with $r \in R$. This shows that $r = a/b \in R$. $\square$

Segre products

Let R and S be finitely generated $\mathbb{N}$-graded K-algebras with $R_0 = S_0 = K$. We define the *Segre product* $R \circledS_K S$ of R and S over K to be the ring

$$\bigoplus_{n=1}^{\infty} R_n \otimes_K S_n,$$

which is a subring of $R \otimes_K S$. In fact, $R \otimes_K S$ has a grading by $\mathbb{N} \times \mathbb{N}$ whose (m, n) component is $R_m \otimes_K S_n$. (There is no completely standard notation for Segre products: the one used here is only one possbility.) The vector space

$$\bigoplus_{m \neq n} R_m \otimes_K S_n \subseteq R \otimes_K S$$

is an $R \circledS_K S$-submodule of $R \otimes_K S$ that is an $R \circledS_K S$-module complement for $R \circledS_K S$. That is, $R \circledS_K S$ is a direct summand of $R \otimes_K S$ when the latter is regarded as an $R \circledS_K S$-module. It follows that $R \circledS_K S$ is Noetherian and, hence, finitely generated over K. Moreover, if $R \otimes_K S$ is normal then so is $R \circledS_K S$. In particular, if R is normal and S is a polynomial ring over K then $R \circledS_K S$ is normal.

Let $S = K[X, Y, Z]/(X^3 + Y^3 + Z^3) = K[x, y, z]$, where K is a field of characteristic different from 3: this is a homogeneous coordinate ring of an elliptic curve C, and is often referred to as a *cubical cone*. Let $T = K[s, t]$, a polynomial ring, which is a homogeneous coordinate ring for the projective line $\mathbb{P}^1 = \mathbb{P}^1_K$. The Segre product of these two rings is $R = K[xs, ys, zs, xt, yt, zt] \subseteq S[s, t]$, which is a homogeneous coordinate ring for the smooth projective variety $C \times \mathbb{P}^1$. This ring is a normal domain with an isolated singularity at the origin: that is, its localization at any prime ideal except the homogeneous maximal ideal m is regular. R and R_m are normal but not Cohen-Macaulay.

We give a proof that R is not Cohen-Macaulay. The equations

$$(zs)^3 + \big((xs)^3 + (ys)^3\big) = 0 \quad \text{and} \quad (zt)^3 + \big((xt)^3 + (yt)^3\big) = 0$$

show that zs and zt are both integral over $D = K[xs,\, ys,\, xt,\, zt] \subseteq R$. 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 R as well. The relation

$$(zs)(zt)(xs - yt) = (zs)^2(xt) - (zt)^2(ys)$$

now shows that R is *not* Cohen-Macaulay, for $(zs)(zt) \notin (xt,\, ys)R$. 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 $(zs)(zt) \in (xt,\, ys)R$, applying this map gives $z^2 \in (x,\, y)K[x,\, y,\, z]$, which is false — in fact, $K[x,\, y,\, z]/(x,\, y) \cong K[z]/(z^3)$. $\square$

Cohen-Macaulay rings are wonderfully well-behaved in many ways: we shall discuss this at considerable length later. Of course, regular rings are even better.

One of the main objectives in these lectures is to discuss two ways of dealing with rings in which the Cohen-Macaulay property fails. One is the development of a tight closure theory. The other is to prove the existence of "lots" of big Cohen-Macaulay algebras. These two methods are closely related, and we shall explore that relationship. In any case, one conclusion that one may reach is that rings that do not have the Cohen-Macaulay property nonetheless have better behavior than one might at first expect.

The situation right now is that there are relatively satisfactory results for both of these techniques for Noetherian rings containing a field. There are also results for local rings of mixed characteristic in dimension at most 3. (For a mixed characteristic local domain, the characteristic of the residue class field is a positive prime p while the characteristic of the fraction field is 0. The p-adic integers give an example, as well as module-finite extensions of formal power series rings over the p-adic integers.)

The integral closure of an ideal

The Briançon-Skoda theorem discussed in (2) below refers to the *integral closure* $\overline{I}$ of an ideal I. We make the following comments: for proofs, see the Lecture Notes from Math 711, Fall 2006, September 13 and September 15 (those notes also give a detailed treatment of the Lipman-Sathaye proof of the Briançon-Skoda theorem). If $I \subseteq R$ and $u \in R$ then $u \in \overline{I}$ precisely if for some n, u satisfies a monic polynomial

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0$$

with $r_j \in I^j$, $1 \leq j \leq n$.

Alternatively, if one forms the *Rees ring*

$$R[It] = R + It + I^2t^2 + I^3t^3 + \cdots + I^nt^n + \cdots \subseteq R[t],$$

where t is an indeterminate, the integral closure of $R[It]$ in $R[t]$ has the form

$$R + J_1t + J_2t^2 + J_3t^3 + \cdots + J_nt^n + \cdots$$

where every $J_n \subseteq R$ is an ideal. It turns out that $J_1 = \overline{I}$, and, in fact, $J_n = \overline{I^n}$ for all $n \geq 1$.

It turns out as well that for $u \in R$, one has that $u \in \overline{I}$ if and only if $u \in IV$ for every map from R to a valuation domain V. When R is Noetherian, it suffices to consider maps to Noetherian discrete valuation domains (we refer to such a domain as a DVR: this is the same as a regular local ring of Krull dimension 1) such that the kernel of the map is a minimal prime of R. In particular, if R is a Noetherian domain, it suffices to consider injective maps of R into a DVR.

If R is a Noetherian domain, yet another characterization of $\overline{I}$ is as follows: $u \in \overline{I}$ if and only if there is an element $c \in R - \{0\}$ such that $cu^n \in I^n$ for all $n \in \mathbb{N}$ (it suffices if $cu^n \in I^n$ for infinitely many values of $n \in \mathbb{N}$).

Here are some of the results that can be proved using tight closure theory, which we shall present even though we have not yet discussed what tight closure is.

(1) If $R \subseteq T$ are rings such that T is regular and R is a direct summand of T as an R-module, then R is Cohen-Macaulay. (This is known in the equal characteristic case: it is an open question in general.)

(2) If $I = (f_1, \ldots, f_n)$ is an ideal of a regular ring R, then $\overline{I^n} \subseteq I$. (The case where R is regular is known even in mixed characteristic. In the case where R is equicharacteristic, it is known that $\overline{I^n}$ is contained in the tight closure of I, with no restriction on the Noetherian ring R.)

(3) If $I \subseteq R$ is an ideal and S is module-finite extension of R, then $IS \cap R$ is contained in the tight closure of I in equal characteristic. (That is, tight closure "controls" how large the contracted expansion of an ideal to a module-finite extension ring can be.)

(4) Tight closure can be used to prove that if R is regular, then R is a direct summand of every module-finite extension ring. More generally, in equal characteristic, every ring such that every ideal is tightly closed is a direct summand of every module-finite extension ring. Whether the converse holds is an open question.

Whether every regular ring is a direct summand of every module-finite extension remains an important open question in mixed characteristic, where it is known in dimension at most 3. The proof in dimension 3, due to Ray Heitmann, is very difficult. We shall discuss Heitmann's work further.

(5) Tight closure can be used to prove theorems controlling the behavior of symbolic powers of prime ideals in regular rings. (We shall give more details about this in the next lecture.)

(6) Tight closure can be used in the proof of several subtle statements about homological properties of local rings. These statements are known as "the local homological conjectures." Some are now theorems in equal characteristc but open in mixed characteristic. Others are now known in general. Some remain open in every characteristic. We shall discuss these in more detail later.

By a *big Cohen-Macaulay* module for a local ring $(R,\, m,\, K)$ we mean a not necessarily finitely generated R-module M such that every system of parameters of R is a regular sequence on M. It is not sufficient for one system of parameters to be a regular sequence, but if one system of parameters is a regular sequence then the m-adic completion of M has the property that every system of parameters is a regular sequence. Some authors use the term "big Cohen-Macaulay module" when one system of parameters is a regular sequence, and call the big Cohen-Macaulay module "balanced" if every system of parameters is a regular sequence.

An R-algebra S is called a *big Cohen-Macaulay* algebra over R if it is a big Cohen-Macaulay module as well as an R-algebra.

The existence of big Cohen-Macaulay algebras is known if the local ring R contains a field. The proof in equal characteristic 0 depends on reduction to characteristic $p > 0$. In mixed characteristic, it is easy in dimension at most 2 and follows from difficult results of Heitmann in dimension 3. We shall discuss all this at considerable length later.

Big Cohen-Macaulay algebras can be used to prove results like those mentioned in (1), (4), and (6) for tight closure. I conjecture that the existence of a tight closure theory with sufficiently good properties in mixed characteristic is equivalent to the existence of sufficiently many big Cohen-Macaulay algebras in mixed characteristic. This is a somewhat vague statement, in that I am not being precise about the meaning of the word "sufficiently" in either half, but it is a point of view that forms one of the themes of these lectures, and will be developed further.

Math 711: Lecture of September 7, 2007

Symbolic powers

We want to make a number of comments about the behavior of symbolic powers of prime ideals in Noetherian rings, and to give at least one example of the kind of theorem one can prove about symbolic powers of primes in regular rings: there was a reference to such theorems in (5) on p. 15 of the notes from the first lecture.

Let P be a prime ideal in any ring. We define the n th *symbolic power* $P^{(n)}$ of P as

$$\{r \in R : \text{for some } s \in R - P, sr \in P^n\}.$$

Alternatively, we may define $P^{(n)}$ as the contraction of $P^n R_P$ to R. It is the smallest P-primary ideal containing P^n. If R is Noetherian, it may be described as the P-primary component of P^n in its primary decomposition.

While $P^{(1)} = P$, and $P^{(n)} = P^n$ when P is a *maximal* ideal, in general $P^{(n)}$ is larger than P^n, even when the ring is regular. Here is one example. Let x, y, z, and t denote indeterminates over a field K. Grade $R = K[x,\, y,\, z]$ so that x, y, and z have degrees 3, 4, and 5, respectively. Then there is a degree preserving K-algebra surjection

$$R \twoheadrightarrow K[t^3,\, t^4,\, t^5] \subseteq K[t]$$

that sends x, y, and z to t^3, t^4, and t^5, respectively. Note that the matrix

$$X = \begin{pmatrix} x & y & z \\ y & z & x^2 \end{pmatrix}$$

is sent to the matrix

$$\begin{pmatrix} t^3 & t^4 & t^5 \\ t^4 & t^5 & t^6 \end{pmatrix}.$$

The second matrix has rank 1, and so the 2×2 minors of X are contained in the kernel P of the surjection $R \twoheadrightarrow K[t^3,\, t^4,\, t^5]$. Call these minors $f = xz - y^2$, $g = x^3 - yz$, and $h = yx^2 - z^2$. It is not difficult to prove that these three minors generate P, i.e., $P = (f,\, g,\, h)$. We shall exhibit an element of $P^{(2)} - P$. Note that f, g, and h are homogeneous of degrees 8, 9, and 10, respectively.

Next observe that $g^2 - fh$ vanishes mod xR: it becomes $(-yz)^2 - (-y^2)(-z^2) = 0$. Therefore, $g^2 - fh = xu$. g^2 has an x^6 term which is not canceled by any term in fh, so that $u \neq 0$. (Of course, we could check this by writing out what u is in a completely explicit calculation.) The element $g^2 - fh \in P^2$ is homogeneous of degree 18 and x has degree 3. Therefore, u has degree 15. Since $x \notin P$ and $xu \in P^2$, we have that $u \in P^{(2)}$.

But since the generators of P all have degree at least 8, the generators of P^2 all have degree at least 16. Since $\deg(u) = 15$, we have that $u \notin P^2$, as required.

Understanding symbolic powers is difficult. For example, it is true that if $P \subseteq Q$ are primes of a regular ring then $P^{(n)} \subseteq Q^{(n)}$: but this is somewhat difficult to prove! See the Lectures of October 20 and November 1, 6, and 8 of the Lecture Notes from Math 711, Fall, 2006.

This statement about inclusions fails in simple examples where the ring is not regular. For example, consider the ring

$$R = K[U,\, V,\, W,\, X,\, Y,\, Z]/(UX + VY + WZ) = K[u,\, v,\, w,\, x,\, y,\, z]$$

where the numerator is a polynomial ring. Then R is a hypersurface: it is Cohen-Macaulay, normal, with an isolated singularity. It can even be shown to be a UFD. Let Q be the maximal ideal generated by the images of all of the variables, and let P be the prime ideal $(v,\, w,\, x,\, y,\, z)R$. Here, $R/P \cong K[U]$. Then $P \subseteq Q$ but it is not true that $P^{(2)} \subseteq Q^{(2)}$. In fact, since $-ux = yy + wz \in P^2$ and $u \notin P$, we have that $x \in P^{(2)}$, while $x \notin Q^{(2)}$, which is simply Q^2 since Q is maximal.

The following example, due to Rees, shows that behavior of symbolic powers can be quite bad, even in low dimension.

Let P be a prime ideal in a Noetherian ring R. Let t be an indeterminate over R. When I is an ideal of R, a very standard construction is to form the Rees ring

$$R[It] = R + It + \cdots + I^n t^n + \cdots \subseteq R[t],$$

which is finitely generated over R: if $f_1,\, \ldots\,,\, f_h$ generate the ideal I, then

$$R[It] = R[f_1 t,\, \ldots\,,\, f_h t].$$

An analogous construction when $I = P$ is prime is the *symbolic power algebra*

$$R + Pt + P^{(2)}t^2 + \cdots + P^{(n)}t^n + \cdots \subseteq R[t].$$

We already know that this algebra is larger than $R[Pt]$, but one might still hope that it is finitely generated. Roughly speaking, this would say that the elements in $P^{(n)} - P^n$ for sufficiently large n arise a consequence of elements in $P^{(k)} - P^k$ for finitely many values of k.

However, this is false. Let

$$R = \mathbb{C}[X,\, Y,\, Z]/(X^3 + Y^3 + Z^3),$$

where $\mathbb{C}$ is the field of complex numbers. This is a two-dimensional normal surface: it has an isolated singularity. It is known that there are height one homogeneous primes P that have infinite order in the divisor class group: this simply means that no symbolic power of P is principal. David Rees proved that the symbolic power algebra of such a prime P is not finitely generated over R. This was one of the early indications that Hilbert's Fourteenth Problem might have a negative solution, i.e., that the ring of invariants of a linear action of a group of invertible matrices on a polynomial ring over a field K may have a ring of invariants that is not finitely generated over K. M. Nagata gave examples to show that this can happen in 1958.

Analytic spread

In order to give a proof of the result of Rees described above, we introduce the notion of analytic spread. Let (R, m, K) be local and $I \subseteq m$ an ideal. When K is infinite, the following two integers coincide:

(1) The least integer n such that I is integral over an ideal $J \subseteq I$ that is generated by n elements.

(2) The Krull dimension of the ring $K \otimes_R R[It]$.

The integer defined in (2) is called the *analytic spread* of I, and we shall denote it $\mathfrak{an}(I)$. See the Lecture Notes of September 15 and 18 from Math 711, Fall 2006 for a more detailed treatment.

The ring in (2) may be written as

$$S = K \oplus I/mI \oplus I^2/mI^2 \oplus \cdots \oplus I^n/mI^n \oplus \cdots$$

Note that if we define the *associated graded ring* $\mathrm{gr}_I(R)$ of R with respect to I as

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

which may also be thought of as $R[It]/IR[It]$, then it is also true that $S \cong K \otimes_R \mathrm{gr}_I(R)$.

The idea underlying the proof that when K is infinite and $h = \mathfrak{an}(I)$, one can find $f_1, \ldots, f_h \in I$ such that I is integral over $J = (f_1, \ldots, f_h)R$ is as follows. The K-algebras S is generated by its one-forms. If K is infinite, one can choose a homogeneous system of parameters for S consisting of one-forms: these are elements of I/mI, and are represented by elements $f_1, \ldots, f_h$ of I. Let J be the ideal generated by $f_1, \ldots, f_h$ in R. The S is module-finite over the image of $K \otimes R[Jt]$, and using this fact and Nakayama's Lemma on each component, one can show that $R[It]$ is integral over $R[Jt]$, from which it follows that I is integral over J.

Proof that Rees's symbolic power algebra is not finitely generated

Here is a sketch of Rees's argument. Assume that the symbolic power algebra is finitely generated. We now replace the graded ring R by its localization at the homogeneous maximal ideal. By the local and homogeneous versions of Nakayama's Lemma, the least number of generators of an ideal generated by homogeneous elements of positive degree does not change. It follows that P continues to have the property that no symbolic power is principal. We shall prove that the symbolic power algebra cannot be finitely generated even in this localized situation, which implies the result over the original ring R.

Henceforth, (R, m, K) is a normal local domain of dimension 2 and P is a height one prime such that no symbolic power of P is prinicpal. We shall show that the symbolic power algebra of P cannot be finitely generated over R. Assume that it is finitely generated.

This implies that for some integer k, $P^{(nk)} = (P^{(k)})^n$ for all positive integers n. Let $I = P^{(k)}$. The ring $S = R[It]$ has dimension 3, since the transcendence degree over R is one. The elements x, y are a system of parameters for R. We claim that there is a regular sequence of length two in m on each symbolic power $J = P^{(h)}$. To see this, we take x to be the first term. Consider J/xJ. If there is no choice for the second term, then the maximal ideal m of R must be an associated prime of J/xJ, and we can choose $v \in J - xJ$ such that $mv \subseteq xJ$. But then $yv \in xR$, and x, y is a regular sequence in R. It follows that $v = xu$ with $u \in R - J$. Then $mxu \subseteq xJ$ shows $mu \subseteq J$. But elements of $m - P$ are not zerodivisors on J, so that $u \in J$, a contradiction. It follows that every system of parameters in R is a regular sequence on J: J is a Cohen-Macaulay module.

Thus, if the symbolic power algebra is finitely generated, x, y is a regular sequence on every $P^{(n)}$, and therefore x, y is a regular sequence in S. It follows that killing (x, y) decreases the dimension of the ring S by two. Since the radical of (x, y) is the homogeneous maximal ideal of R, we see that $(R/m) \otimes_R S$ has dimension one. This shows that the analytic spread of I is one. But then I is integral over a principal ideal. In a normal ring, principal ideals are integrally closed. Thus, I is principal. But this contradicts the fact that no symbolic power of P is principal. $\square$

The notion of tight closure for ideals

We next want to introduce tight closure for ideals in prime characteristic $p > 0$. We need some notations. If R is a Noetherian ring, we use R° to denote the set of elements in R that are not in any minimal prime of R. If R is a domain, $R^\circ = R - \{0\}$. Of course, R° is a multiplicative system.

We shall use e to denote an element of $\mathbb{N}$, the nonnegative integers. For typographical convenience, shall use q as a symbol interchangeable with p^e, so that whenever one writes

q it is understood that there is a corresponding value of e such that $q = p^e$, even though it may be that e is not shown explicitly.

When R is an arbitrary ring of characteristic $p > 0$, we write F_R or simply F for the Frobenius endomorphism of the ring R. Thus, $F(r) = r^p$ for all $r \in R$. F_R^e or F^e indicates the e th iteration of F_R, so that $F^e(r) = r^q$ for all $r \in R$.

If R has characteristic p, $I^{[q]}$ denotes the ideal generated by all q th powers of elements of I. If one has generators for I, their q th powers generate $I^{[q]}$. (More generally, if $f : R \to S$ is any ring homomorphism and $I \subseteq R$ is an ideal with generators $\{r_\lambda\}_{\lambda \in \Lambda}$, the elements $\{f(r_\lambda)\}_{\lambda \in \Lambda}$ generate IS.)

Definition. Let R be a Noetherian ring of prime characteristic $p > 0$. Let $I \subseteq R$ be an ideal and let $u \in R$ be an element. Then u is in the *tight closure* of I in R, denoted I^*, if there exists $c \in R^\circ$ such that for all sufficiently large q, $cu^q \in I^{[q]}$.

This may seem like a very strange definition at first, but it turns out to be astonishingly useful. Of course, in presenting the definition, we might have written "for all sufficiently large e, $cu^{p^e} \in I^{[p^e]}$" instead.

The choice of c is allowed to depend on I and u, but *not* on q.

It is quite easy to see that I^* is an ideal containing I. Of great importance is the following fact, to be proved later:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. If R is regular, then every ideal of R is tightly closed.*

If one were to use tight closure only to study regular rings, then one might think of this Theorem as asserting that the condition in the Definition above gives a criterion for when an element is in an ideal that, on the face of it, is somewhat weaker than being in the ideal. Even if the whole theory were limited in this fashion, it provides easy proofs of many results that cannot be readily obtained in any other way. We want to give a somewhat different way of thinking of the definition above. First note that it turns out that tight closure over a Noetherian ring can be tested modulo every minimal prime. Therefore, for many purposes, it suffices to consider the case of a domain.

Let R be any domain of prime characteristic $p > 0$. Within an algebraic closure L of the fraction field of R, we can form the ring $\{r^{1/q} : r \in R\}$. The Frobenius map F is an automorphism of L: this is the image of R under the inverse of F^e, and so is a subring of L isomorphic to R. We denote this ring $R^{1/q}$. This ring extension of R is unique up to canonical isomorphism: it is independent of the choice of L, and its only R-automorphism is the identity: r has a unique q th root in $R^{1/q}$, since the difference of two distinct q th roots would be nilpotent, and so every automorphism that fixes r fixes $r^{1/q}$ as well. Moreover, there is a commutative diagram:

$$(*)\qquad \begin{array}{ccc} R & \hookrightarrow & R^{1/q} \\ \Big\| & & \Big\uparrow{\scriptstyle F^{-e}} \\ R & \xrightarrow{F^e} & R \end{array}$$

where both vertical arrows are isomorphisms and $F^{-e}(r) = r^{1/q}$.

The reduced case

When R is reduced rather than a domain there is also a unique (up to unique isomorphism) reduced R-algebra extension ring $R^{1/q}$ whose elements are precisely all q th roots of elements of R. One can construct such an extension ring by taking the map $R \xrightarrow{F^e} R$ to give the algebra map, so that one has the same commutative diagram $(*)$ as in the domain case. The proof of uniqueness is straightforward: if S_1 and S_2 are two such extensions, the only possible isomorphism must let the unique q th root of $r \in R$ in S_1 correspond to the unique q th root of R in S_2 for all $r \in R$. It is easy to check that this gives a well-defined map that is the identity on R, and that it is a bijection and a homomorphism.

In both the domain and the reduced case, we have canonical embeddings $R^{1/q} \hookrightarrow R^{1/q'}$ when $q \le q'$, and we define

$$R^\infty = \bigcup_q R^{1/q}.$$

When one has that

$$cu^q = r_1 f_1^q + \cdots + r_h f_h^q$$

one can take q th roots to obtain

$$c^{1/q} u = r_1^{1/q} f_1 + \cdots + r_h^{1/q} f_h.$$

Keep in mind that in a reduced ring, taking q th roots preserves the ring operations. We can therefore rephrase the definition of tight closure of an ideal I in a Noetherian domain R of characteristic $p > 0$ as follows:

(#) An element $u \in R$ is in I^* iff there is an element $c \in R^\circ$ such that for all sufficiently large q, $c^{1/q} u \in IR^{1/q}$.

Heuristically, one should think of an element of R that is in IS, where S is a domain that is an integral extension of R, as "almost" in I. Note that in this situation one will have $u = f_1 s_1 + \cdots + f_h s_h$ for $f_1, \ldots, f_h \in I$ and $s_1, \ldots, s_h \in S$, and so one also has $u \in IS_0$, where $S_0 = R[s_1, \ldots, s_h]$ is module-finite over R.

The condition (#) is weaker in a way: $R^{1/q} \subseteq R^\infty$ is an integral extension of R, but, u is not necessarily in IR^∞: instead, it is multiplied into IR^∞ by infinitely many elements $c^{1/q}$. These elements may be thought of as approaching 1 in some vague sense: this is not literally true for a topology, but the exponents $1/q \to 0$ as $q \to \infty$.

Some useful properties of tight closure

We state some properties of tight closure for ideals: proofs will be given later. Here, R is a Noetherian ring of prime characteristic $p > 0$, and I, J are ideals of R. We shall write R_{red} for the homomorphic image of R obtained by killing the ideal of nilpotent elements. (R, m, K) is called *equidimensional* if for every minimal prime P of R, $\dim(R/P) = \dim(R)$. An algebra over R is called *essentially of finite type* over R if it is a localization at some multiplicative system of a finitely generated R-algebra. If I, J are ideals of R, we define $I :_R J = \{r \in R : rJ \subseteq I\}$, which is an ideal of R. If $J = uR$, we may write $I :_R u$ for $I :_R uR$.

Excellent rings

In some of the statements below, we have used the term "excellent ring." The excellent rings form a subclass of Noetherian rings with many of the good properties of finitely generated algebras over fields and their localizations. We shall not give a full treatment in these notes, but we do discuss certain basic facts that we need. For the moment, the reader should know that the excellent rings include any ring that is a localization of a finitely generated algebra over a complete local (or semilocal) ring. The class is closed under localization at any multiplicative system, under taking homomorphic images, and under formation of finitely generated algebras. We give more detail later. Typically, Noetherian rings arising in algebraic geometry, number theory, and several complex variables are excellent.

Here are nine properties of tight closure. Property (2) was already stated as a Theorem earlier.

(1) $I \subseteq I^* = (I^*)^*$. If $I \subseteq J$, then $I^* \subseteq J^*$.

(2) If R is regular, every ideal of R is tightly closed.

(3) If $R \subseteq S$ is a module-finite extension, $IS \cap R \subseteq I^*$.

(4) If $P_1, \ldots, P_h$ are the minimal primes of R, then $u \in R$ is in I^* if and only if the image of u in $D_j = R/P_j$ is in the tight closure of ID_j in D_j, working over D_j, for $1 \leq j \leq h$.

(5) If $u \in R$ then $u \in I^*$ if and only if its image in R_{red} is in the tight closure of IR_{red}, working over R_{red}.

The statements in (4) and (5) show that the study of tight closure can often be reduced to the case where R is reduced or even a domain.

The following is one of the most important properties of tight closure. It is what enables one to use tight closure as a substitute for the Cohen-Macaulay property in many instances. It is the key to proving that direct summands of regular rings are Cohen-Macaulay in characteristic $p > 0$.

(6) **(Colon-capturing)** If (R, m, K) is a complete local domain (more generally, if (R, m, K) is a reduced, excellent, and equidimensional), the elements $x_1, \dots, x_k, x_{k+1}$ are part of a system of parameters for R, and $I_k = (x_1, \dots, x_k)R$, then $I_k :_R x_{k+1} \subseteq I_k^*$.

Of course, if R were Cohen-Macaulay then we would have $I_k :_R x_{k+1} = I_k$.

(7) Under mild conditions on R, $u \in R$ is in the tight closure of $I \subseteq R$ if and only if the image of u in R_P is in the tight closure of IR_P, working over R_P, for all prime (respectively, maximal) ideals P of R. (The result holds, in particular, for algebras essentially of finite type over an excellent semilocal ring.)

Tight closure is not known to commute with localization, and this is now believed likely to be false. But property (7) shows that it has an important form of compatibility with localization.

(8) If (R, m, K) is excellent, $I^* = \bigcap_n (I + m^n)^*$.

Property (8) shows that tight closure is determined by its behavior on m-primary ideals in the excellent case.

(9) If (R, m, K) is reduced and excellent, $u \in I^*$ if and only if u is in the tight closure of $I\widehat{R}$ in $\widehat{R}$ working over $\widehat{R}$.

These properties together show that for a large class of rings, tight closure is determined by its behavior in complete local rings and, in fact, in complete local domains. Moreover, in a complete local domain it is determined by its behavior on m-primary ideals.

We next want to give several further characterizations of tight closure, although these require some additional condition on the ring. For the first of these, we need to discuss the notion of R^+ for a domain R first.

The absolute integral closure R^+ of a domain R

Let R be any integral domain (there are no finiteness restrictions, and no restriction on the characteristic). By an *absolute integral closure* of R, we mean the integral closure of R in an algebraic closure of its fraction field. It is immediate that R^+ is unique up to non-unique isomorphism, just as the algebraic closure of a field is.

Consider any domain extension S of R that is integral over R. Then the fraction field $\mathrm{frac}\,(R)$ is contained in the algebraic closure L of $\mathrm{frac}\,(S)$, and L is also an algebraic closure for R, since the elements of S are integral over R and, hence, algebraic over $\mathrm{frac}\,(R)$.

The algebraic closure of R in L is R^+. Thus, we have an embedding $S \hookrightarrow R^+$ as R-algebras. Therefore, R^+ is a maximal domain extension of R that is integral over R: this characterizes R^+. It is also clear that $(R^+)^+ = R^+$. When $R = R^+$ we say that R is *absolutely integrally closed*. The reader can easily verify that a domain S is absolutely integrally closed if and only if every monic polynomial in one variable $f \in S[x]$ factors into monic linear factors over S. It is easy to check that a localization at any multiplicative system of an absolutely integrally closed domain is absolutely integrally closed, and that a domain that is a homomorphic image of an absolutely integrally closed domain is absolutely integrally closed. (A monic polynomial over S/P lifts to a monic polynomial over S, whose factorization into monic linear factors gives such a factorizaton of the original polynomial over S/P.)

If $S \hookrightarrow T$ is an extension of domains, the algebraic closure of the fraction field of S contains an algebraic closure of the fraction field of R. Thus, we have a commutative diagram

$$\begin{array}{ccc} S^+ & \hookrightarrow & T^+ \\ \uparrow & & \uparrow \\ S & \hookrightarrow & T \end{array}$$

where the vertical maps are inclusions.

If $R \twoheadrightarrow S$ is a surjection of domains, so that $S \cong R/P$, by the lying-over theorem there is a prime ideal Q of R^+ lying over P, since $R \hookrightarrow R^+$ is an integral extension. Then $R \to R^+/Q$ has kernel $Q \cap R = P$, and so we have $S \cong R/P \hookrightarrow R^+/Q$. Since R^+ is integral over R, R^+/Q is integral over $R/P \cong S$. But since R^+ is absolutely integrally closed, so is R^+/Q. Thus, R^+/Q is an integral extenson of S, and is an absolutely integrally closed domain. It follows that we may identify this extension with S^+, and so we have a commutative diagram

$$\begin{array}{ccc} R^+ & \twoheadrightarrow & S^+ \\ \uparrow & & \uparrow \\ R & \twoheadrightarrow & S \end{array}$$

where both vertical maps are inclusions.

Any homomorphism of domains $R \to T$ factors $R \twoheadrightarrow S \hookrightarrow T$ where S is the image of R in T. The two facts that we have proved yield a commutative diagram

$$\begin{array}{ccccc} R^+ & \twoheadrightarrow & S^+ & \hookrightarrow & T^+ \\ \uparrow & & \uparrow & & \uparrow \\ R & \twoheadrightarrow & S & \hookrightarrow & T \end{array}$$

where all of the vertical maps are inclusions. Hence:

Proposition. *For any homomorphism $R \to T$ of integral domains there is a commutative diagram*

$$\begin{array}{ccc} R^+ & \longrightarrow & T^+ \\ \uparrow & & \uparrow \\ R & \longrightarrow & T \end{array}$$

where both vertical maps are inclusions. $\square$

Other characterizations of tight closure

For many purposes it suffices to characterize tight closure in the case of a complete local domain. Let $(R,\, m,\, K)$ be a complete local domain of prime characteristic $p > 0$. One can always choose a DVR $(V,\, t_V V,\, L)$ containing R such that $R \subseteq V$ is local. This gives a $\mathbb{Z}$-valued valuation nonnegative on R and positive on m. This valuation extends to a $\mathbb{Q}$-valued valuation on R^+. To see this, note that $R^+ \subseteq V^+$. V^+ is a directed union of module-finite normal local extensions W of V, each of which is a DVR. Let t_W be the generator of the maximal ideal of W. Then $t_V = t_W^{h_W}\alpha$ for some positive integer h_W and unit α of W, and we can extend the valuation to W by letting the order of t_W be $1/h_W$. (To construct V in the first place, we may write R as a module-finite extension of a complete regular local ring $(A,\, m_A,\, K)$. By the remarks above, it suffices to construct the required DVR for A. There are many possibilities. One is to define the order of a nonzero element $a \in A$ to be the largest integer k such that $u \in m_A^k$. This gives a valuation because $\mathrm{gr}_{m_A} A$ is a polynomial ring over K, and, in particular, a domain.)

Theorem. *Let $(R,\, m,\, K)$ be a complete local domain of prime characteristic $p > 0$, $u \in R$, and $I \subseteq R$. Choose a complete DVR $(V,\, m_V, L)$ containing $(R,\, m,\, K)$ such that $R \subseteq V$ is local. Extend the valuation on R given by V to a $\mathbb{Q}$-valued valuation on R^+: call this ord. Then $u \in I^*$ if and only if there exists a sequence of nonzero elements $c_n \in R^+$ such that for all n, $c_n u \in IR^+$ and $\mathrm{ord}(c_n) \to 0$ as $n \to \infty$.*

See Theorem (3.1) of [M. Hochster and C. Huneke, *Tight closure and elements of small order in integral extensions*, J. of Pure and Applied Alg. **71** (1991) 233–247].

This is clearly a necessary condition for u to be in the tight closure of I. We have $R^{1/q} \subseteq R^\infty \subseteq R^+$, and in so in the reformulation (#) of the definition of tight closure for the domain case, one has $c^{1/q}u \in IR^{1/q} \subseteq IR^+$ for all sufficiently large q. Since one has

$$\mathrm{ord}\,(c^{1/q}) = \frac{1}{q}\,\mathrm{ord}\,(c),$$

we may use the elements $c^{1/q}$ to form the required sequence. What is surprising in the theorem above is that one can use arbitrary, completely unrelated multipliers in testing for tight closure, and u is still forced to be in I^*.

Solid modules and algebras and solid closure

Ler R be any domain. An R-module M is called *solid* if it has a nonzero R-linear map $M \to R$. That is, $\mathrm{Hom}_R(M, R) \neq 0$.

An R-algebra S is called *solid* if it is solid as an R-module. In this case, we can actually find an R-linear map $\theta : S \to R$ such that $\theta(1) \neq 0$. For if θ_0 is any nonzero map $S \to M$, we can choose $s \in S$ such that $\theta_0(s) \neq 0$, and then define θ by $\theta(u) = \theta_0(su)$ for all $u \in S$.

When R is a Noetherian domain and M is a finitely generated R-module, the property of being solid is easy to understand. It simply means that M is not a torsion module over R. In this case, we can kill the torsion submodule N of M, and the torsion-free module M/N will embed a free module R^h. One of the coordinate projections π_j will be nonzero on M/N, and the composite

$$M \twoheadrightarrow M/N \hookrightarrow R^h \xrightarrow{\pi_j} R$$

will give the required nonzero map.

However, if S is a finitely generated R-algebra it is oftem very difficult to determine whether M is solid or not.

For those familiar with local cohomology, we note that if (R, m, K) is a complete local domain of Krull dimension d, then M is solid over R if and only $H^d_m(M) \neq 0$. Local cohomology theory will be developed in supplementary lectures, and we will eventually prove this criterion. This criterion can be used to show the following.

Theorem. *Let (R, m, K) be a complete local domain. Then a big Cohen-Macaulay algebra for R is solid.*

We will eventually prove the following characterization of tight closure for complete local domains. This result begins to show the close connection between tight closure and the existence of big Cohen-Macaulay algebras.

Theorem. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$. Let $u \in R$. Let $I \subseteq R$ be an ideal. The following conditions are equivalent:*

(1) $u \in I^*$.

(2) *There exists a solid R-algebra S such that $u \in IS$.*

(3) *There exists a big Cohen-Macaulay algebra S over R such that $u \in IS$.*

Of course, (3) $\Rightarrow$ (2) is immediate from the preceding theorem. Conditions (2) and (3) are of considerable interest because they characterize tight closure without referrring to the Frobenius endomorphism, and thereby suggest closure operations not necessarily in characteristic $p > 0$ that may be useful. The characterization (2) leads to a notion of "solid closure" which has many properties of tight closure in dimension at most 2. In equal characteristic 0 in dimension 3 and higher it appears to be the wrong notion, in that ideals of regular rings need not be closed. However, whether solid closure gives a really useful theory in mixed characteristic in dimension 3 and higher remains mysterious.

The characterization in (3) suggests defining a "big Cohen-Macaulay algebra" closure. This is promising idea in all characteristics and all dimensions, but the existence of big Cohen-Macaulay algebras in mixed characteristic and dimension 4 and higher remains unsettled. One of our goals is to explore what is understood about this problem.

Math 711: Lecture of September 10, 2007

In order to give our next characterization of tight closure, we need to discuss a theory of multiplicities suggested by work of Kunz and developed much further by P. Monsky. We use $\ell(M)$ for the length of a finite length module M.

Hilbert-Kunz multiplicities

Let (R, m, K) be a local ring, $\mathfrak{A}$ an m-primary ideal and M a finitely generated nonzero R-module. The standard theory of multiplicities studies $\ell(M/\mathfrak{A}^n M)$ as a function of n, especially for large n. This function, the *Hilbert function of M with respect to* $\mathfrak{A}$, is known to coincide, for all sufficiently large n, with a polynomial in n whose degree d is the Krull dimension of M. This polynomial is called the *Hilbert polynomial* of M with respect to $\mathfrak{A}$. The leading term of this polynomial has the form $\dfrac{e}{d!}\, n^d$, where e is a positive integer.

In prime characteristic $p > 0$ one can define another sort of multiplicity by using Frobenius powers instead of ordinary powers.

Theorem (P. Monsky). *Let (R, m, K) be a local ring of prime characteristic $p > 0$ and let $M \neq 0$ be a finitely generated R-module of Krull dimension d. Let $\mathfrak{A}$ be an m-primary ideal of R. Then there exist a positive real number γ and a positive real constant C such that*

$$|\ell(M/\mathfrak{A}^{[q]}M) - \gamma q^d| \leq C q^{d-1}$$

for all $q = p^e$.

One may also paraphrase the conclusion by writing

$$\ell(M/\mathfrak{A}^{[q]}M) = \gamma q^d + O(q^{d-1})$$

where the vague notation $O(q^{d-1})$ is used for a function of q bounded in absolute value by some fixed positive real number times q^{d-1}. The function $e \mapsto \ell(M/\mathfrak{A}^{[q]}M)$ is called the *Hilbert-Kunz* function of M with respect to $\mathfrak{A}$. The real number γ is called the *Hilbert-Kunz multiplicity* of M with respect to $\mathfrak{A}$. In particular, one can conclude that

$$\gamma = \lim_{q \to \infty} \frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}.$$

Note that this is the behavior one would have if $\ell(M/\mathfrak{A}^{[q]}M)$ were eventually a polynomial of degree d in q with leading term γq^d: *but this is not true.* One often gets functions that are not polynomial.

When $M = R$, we shall write $\gamma_{\mathfrak{A}}$ for the Hilbert-Kunz multiplicity of R with respect to $\mathfrak{A}$.

Monsky's proof (cf. [P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983) 43–49]) of the existence of the limit γ is, in a sense, not constructive. He achieves this by proving that $\{\frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}\}_q$ is a Cauchy sequence. The limit is only known to be a real number, not a rational number.

Example. Here is one instance of the non-polynomial behavior of Hilbert-Kunz functions. Let

$$R = (\mathbb{Z}/5\mathbb{Z})[[W,\, X,\, Y,\, Z]]/(W^4 + X^4 + Y^4 + Z^4),$$

with maximal ideal m. Then

$$\ell(R/m^{[5^e]}) = \frac{168}{61}(5^e)^3 - \frac{107}{61}(3^e).$$

See [C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, Math Z. **214** (1983) 119–135.]

Hilbert-Kunz multiplicities give a characterization of tight closure in certain complete local rings:

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring of prime characteristic $p > 0$ that is reduced and equidimensional. Let $\mathfrak{A}$ and $\mathfrak{B}$ be m-primary ideals such that $\mathfrak{A} \subseteq \mathfrak{B}$. Then $\mathfrak{B} \subseteq \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}} = \gamma_{\mathfrak{B}}$.*

This has two immediate corollaries. Suppose that $(R,\, m,\, K)$ and $\mathfrak{A}$ are as in the statement of the Theorem. Then, first, $\mathfrak{A}^*$ is the largest ideal $\mathfrak{B}$ between $\mathfrak{A}$ and m such that $\gamma_{\mathfrak{B}} = \gamma_{\mathfrak{A}}$. Second, if $u \in m$, then $u \in \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}+Ru} = \gamma_{\mathfrak{A}}$. Therefore, the behavior of Hilbert-Kunz multiplicities determines what tight closure is in the case of a complete local ring, since one can first reduce to the case of a complete local domain, and then to the case of an m-primary ideal. This in turn determines the behavior of tight closure in all algebras essentially of finite type over an excellent local (or semilocal) ring.

We shall spend some effort in these lectures on understanding the behavior of the rings R^+. One of the early motivations for doing so is the following result from [M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. bf 135 (1992) 53–89].

Theorem. *Let $(R,\, m,\, K)$ be a complete (excellent also suffices) local domain of prime characteristic $p > 0$. Then R^+ is a big Cohen-Macaulay algebra over R.*

Although this result has been stated in terms of the very large ring R^+, it can also be thought of as a theorem entirely about Noetherian rings. Here is another statement, which is readily seen to be equivalent.

Theorem. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$. Let $x_1, \ldots, x_{k+1}$ be part of a system of parameters for R. Suppose that we have a relation $r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$. Then there is a module-finite extension domain S of R such that $r_{k+1} \in (x_1, \ldots, x_k)S$.*

The point here is that R^+ is the directed union of all module-finite extension domains S of R.

We should note that this Theorem is not at all true in equal characteristic 0. In fact, if one has a relation

$$(*) \quad r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$$

on part of a system of parameters in a normal local ring (R, m, K) that contains the rational numbers $\mathbb{Q}$ and $r_{k+1} \notin (x_1, \ldots, x_k)R$, then there does not exist any module-finite extension S of R such that $r_{k+1} \in (x_1, \ldots, x_k)S$. In dimension 3 or more there are always complete normal local domains that are not Cohen-Macaulay. One such example is given at the bottom of p. 12 and top of p. 13 of the Lecture Notes of September 5. In such a ring one has relations such as $(*)$ on a system of parameters with $r_{k+1} \notin (x_1, \ldots, x_k)R$, and one can never "get rid of" these relations in a module-finite extension domain. Thus, these relations persist even in R^+.

One key point is the following:

Theorem. *Let R be a normal domain. Let S be a module-finite extension domain of R such that the fraction field $\mathcal{L}$ of S has degree d over the fraction field $\mathcal{K}$ of R. Suppose that $\frac{1}{d} \in R$, which is automatic if $\mathbb{Q} \subseteq R$. Then*

$$\frac{1}{d}\,\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$$

gives an R-module retraction of S to R. In particular, for every ideal I of R, $IS \cap R = I$.

The last statement follows from part (a) of the Proposition on p. 11 of the Lecture Notes of September 5.

Here is an explanation of why trace gives such a retraction. First off, recall that $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$ is defined as follows: if $\lambda \in \mathcal{L}$, multiplication by λ defines a $\mathcal{K}$-linear map $\mathcal{L} \to \mathcal{L}$. The value of $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(\lambda)$ is simply the trace of this $\mathcal{K}$-linear endomorphism of $\mathcal{L}$ to itself. It may be computed by choosing any basis $v_1, \ldots, v_d$ for $\mathcal{L}$ as a vector space over $\mathcal{K}$. If M is the matrix of the $\mathcal{K}$-linear map given by multiplication by λ, this trace is simply the sum of the entries on the main diagonal of this matrix. Its value is independent of the choice of basis, since a different basis will yield a similar matrix, and the similar matrix will have the same trace. It is then easy to verify that this gives a $\mathcal{K}$-linear map from $\mathcal{L} \to \mathcal{K}$.

Now suppose that $s \in S$. We want to verify that its trace is in R. There are several ways to argue. We shall give an argument in which we descend to the case where R is the integral closure of Noetherian domain, and we shall then be able to reduce to the case where R is a DVR, i.e., a Noetherian valuation domain, which is very easy.

Note that $\mathcal{K} \otimes_R S$ is a localization of S, hence, a domain, and that it is module-finite over $\mathcal{K}$, so that it is zero-dimensional. Hence, it is a field, and it follows that $\mathcal{K} \otimes_R S = \mathcal{L}$. Hence, every element of $\mathcal{L}$ has a multiple by a nonzero element of R that is in S. In particular, we can choose a basis $s_1, \ldots, s_d$ for $\mathcal{L}$ over $\mathcal{K}$ consisting of elements of S. Extend it to a set of generators $s_1, \ldots, s_n$ for S as an R-module. Without loss of generality we may assume that $s = s_n$ is among them. We shall now construct a new counter-example in which R is replaced by the integral closure R_0 of a Noetherian subdomain and S by

$$R_0 s_1 + \cdots + R_0 s_n.$$

To construct R_0, note that every $s_i s_j$ is an R-linear combination of $s_1, \ldots, s_n$. Hence, for all $1 \leq i,\, j \leq n$ we have equations

$$(*) \quad s_i s_j = \sum_{k=1}^{n} r_{ijk} s_k$$

with all of the r_{ijk} in R. For $j > d$, each s_j is a $\mathcal{K}$-linear combination of $s_1, \ldots, s_d$. By clearing denominators we obtain equations

$$(**) \quad r_j s_j = \sum_{k=1}^{d} r_{jk} s_j$$

for $d < j \leq n$ such that every $r_j \in R - \{0\}$ and every $r_{jk} \in R$.

Let R_1 denote the ring generated over the prime ring (either $\mathbb{Z}$ or some finite field $\mathbb{Z}/p\mathbb{Z}$) by all the r_{ijk}, rjk, and r_j. Of course, R_1 is a Noetherian ring. Let R_0 be the integral closure of R_1 in its fraction field. (It is possible to show that R_0 is Noetherian, but we don't need this fact.) Now let $S_0 = R_0 s_1 + \cdots + R_0 s_n$, which is evidently generated as an R_0-module by $s_1, \ldots, s_n$. The equations $(*)$ hold over R_0, and so S_0 is a subring of S. It is module-finite over R_0. The equations $(**)$ hold over R_0, and $s_{d+1}, \ldots,\, s_n$ are linearly dependent on $s_1, \ldots, s_d$ over the fraction field $\mathcal{K}_0$ of R_0. Finally, $s_1, \ldots, s_d$ are linearly independent over $\mathcal{K}_0$, since this is true even over $\mathcal{K}$. Hence, $s_1, \ldots, s_d$ is a vector space basis for $\mathcal{L}_0$ over $\mathcal{K}_0$.

The matrix of multiplication by $s = s_n$ with respect to the basis $s_1, \ldots, s_d$ is the same as in the calculation of the trace of s from $\mathcal{L}$ to $\mathcal{K}$. This trace is not in R_0, since it is not in R. We therefore have a new counterexample in which R_0 is the integral closure of the Noetherian ring R_1. By the Theorem near the bottom of the first page of the Lecture Notes of September 13 from Math 711, Fall 2006, R_0 is an intersection of Noetherian valuation domains that lie between R_0 and $\mathcal{K}_0$. Hence, we can choose such a valuation domain V that does not contain the trace of s. We replace R_0 by V and S_0 by

$$T = Vs_1 + \cdots + Vs_n,$$

which gives a new counter-example in which the smaller ring is a DVR. The proof that T is a ring module-finite over V with module generators $s_1, \ldots, s_n$ such that a basis for the field extension is $s_1, \ldots, s_d$ is the same as in the earlier argument when we replaced R by R_0. Likewise, the trace of s with respect to the two new fraction fields is not affected. In fact, we can use any integrally closed ring in between R_0 and R.

Consequently, we may assume without loss of generality that $R = V$ is a DVR. Since S is a finitely generated torsion-free R-module and R is a principal ideal domain, S is free as R-module. Therefore, we may choose $s_1, \ldots, s_d \in S$ to be a free basis for S over R, and it will also be a basis for $\mathcal{L}$ over $\mathcal{K}$. The matrix for multiplication by s then has entries in R. It follows that its trace is in R, as required. □

Corollary. *Let R be a normal domain containing the rational numbers $\mathbb{Q}$. Let S be an extension ring of R, not necessarily a domain.*

(a) *If S is module-finite over R, then R is a direct summand of S.*

(b) *If S is integral over R, then for every ideal I of R, $IS \cap R = I$.*

Proof. For part (a), we may choose a minimal prime P of S disjoint from the multiplicative system $R - \{0\} \subseteq S$. Then $R \to S \to S/P$ is module-finite over R, and since $P \cap R = \{0\}$, $\iota : R \hookrightarrow S/P$ is injective. By the result just proved, R is a direct summand of S/P: let $\theta : S/P \to R$ be a splitting, so that $\theta \circ \iota$ is the identity on R. Then the composite $S \to S/P \xrightarrow{\theta} R$ splits the map $R \to S$.

For the second part, suppose that $r \in R$ and $r \in IS$. Then there exist $f_1, \ldots, f_h \in I$ and $s_1, \ldots, s_h \in S$ such that

$$r = f_1 s_1 + \cdots + f_h s_h.$$

Let $S_1 = R[s_1, \ldots, s_h]$. Then S_1 is module-finite over R, and so by part (a), R is a direct summand of S_1. But we still have that $r \in IS_1 \cap R$, and so by part (a) of the Proposition on p. 11 of the Lecture Notes of September 5, we have that $r \in I$. □

The fact that ideals of normal rings containing $\mathbb{Q}$ are contracted from integral extensions may seem to be an advantage. But the failure of this property in characteristic $p > 0$, which, in fact, enables one to use module-finite extensions to get rid of relations on systems of parameters, is perhaps an even bigger advantage of working in positive characteristic.

Note that the result on homomorphisms of plus closures of rings given in the Proposition at the top of p. 10 of the Lecture Notes of September 7 then yields:

Theorem. *Let $R \to S$ be a local homomorphism of complete local domains of prime characteristic $p > 0$. Then there is a commutative diagram:*

$$\begin{array}{ccc} B & \longrightarrow & C \\ \uparrow & & \uparrow \\ R & \longrightarrow & S \end{array}$$

such that B is a big Cohen-Macaulay algebra over R and C is a big Cohen-Macaulay algebra over S.

The point is that one can take $B = R^+$ and $C = S^+$, and then one has the required map $B \to C$ by the Proposition cited just before the statement of the Theorem. The same result can be proved in equal characteristic 0, but the proof depends on reduction to characteristic $p > 0$. When we discussed the existence of "sufficiently many big Cohen-Macaulay algebras" in mixed characteristic, it is this sort of result that we had in mind.

The following result of Karen Smith [K. E. Smith, *Tight Closure of Parameter Ideals,* Inventiones Math. **115** (1994) 41–60] (which also contains a form of the result when the ring is not necessarily local) may be viewed as providing another connection between big Cohen-Macaulay algebras and tight closure.

Theorem. *Let R be a complete (or excellent) local domain and let I be an ideal generated by part of a system of parameters for R. Then $I^* = IR^+ \cap R$.*

Property (3) stated on p. 7 of the Lecture Notes of September 7 implies that $IR^+ \cap R \subseteq I^*$, since R^+ is a directed union of module-finite extension domains S. The converse for parameter ideals is a difficult theorem.

This result suggests defining a closure operation on ideals of any domain R as follows: the *plus closure* of I is $IR^+ \cap R$. This plus closure is denoted I^+. Thus, plus closure coincides with tight closure for parameters ideals in excellent local domains of characteristic $p > 0$. Note that plus closure is not very interesting in equal characteristic 0, for if I is an ideal of a normal ring R that contains the rationals, $I^+ = I$.

It is very easy to show that plus closure commutes with localization. Thus, if it were true in general that plus closure agrees with tight closure, it would follow that tight closure commutes with localization. However, recent work of H. Brenner and others suggests that tight closure does not commute with localization in general, and that tight closure is not the same as plus closure in general. This is not yet proved, however.

Recently, the Theorem that R^+ is a big Cohen-Macaulay algebra when (R, m, K) is an excellent local domain of prime characteristic $p > 0$ has been strengthened by C. Huneke and G. Lyubeznik. See [C. Huneke and G. Lyubeznik, *Absolute integral closure in positive characteristic,* Advances in Math. **210** (2007) 498–504]. Roughly speaking, the original version provides a module-finite extension domain S of R that trivializes *one* given relation on parameters. The Huneke-Lyubeznik result provides a module-finite extension S that simultaneously trivializes *all* relations on all systems of parameters in the original ring. Their hypothesis is somewhat different. R need not be excellent: instead, it is assumed that R is a homomorphic image of a Gorenstein ring. Note, however, that the new ring S need not be Cohen-Macaulay: new relations on parameters may have been introduced.

The arguments of Huneke and Lyubeznik give a global result. The ring need not be assumed local. Under mild hypotheses, in characteristic p, the Noetherian domain R has a module finite extension S such that for every local ring R_P of R, all of the relations on all systems of parameters in R_P become trivial in S_P. In order to prove this result, we need to develop some local cohomology theory.

Finally, we want to mention the following result of Ray Heitmann, referred to earlier.

Theorem (R. Heitmann). *Let R be a complete local domain of mixed characteristic p. Let x, y, z be a system of parameters for R. Suppose that $rz \in (x, y)R$. Then for every $N \in \mathbb{N}$, $p^{1/N}r \in (x, y)R^+$.*

See [R. C. Heitmann, *The direct summand conjecture in dimension three,* Annals of Math. **156** (2002) 695–712].

The condition satisfied by r in this Theorem bears a striking resemblance to one of our characterizations of tight closure: see condition (#) near the bottom of p. 6 of the Lecture Notes of September 6. In a way, it is very different: in tight closure theory, the element c is anything but p, which is 0. Heitmann later proved (cf. [R. C. Heitmann, *Extended plus closure and colon-capturing,* J. Algebra **293** (2005) 407–426]) that in the Theorem above, one can use any element of R^+, not just p. The entire maximal ideal of R^+ multiplies r into $(x, y)R^+$.

Heitmann's result stated in the Theorem above already suffices to prove the existence of big Cohen-Macaulay algebras in dimension 3 in mixed characteristic: see [M. Hochster, *Big Cohen-Macaulay algebras in dimension three via Heitmann's theorem,* J. Algebra **254** (2002) 395–408].

It is possible that, for a complete local domain R of dimension 3 and mixed characteristic, R^+ is a big Cohen-Macaulay algebra. This is an open question.

It is also an open question whether an analogue of Heitmann's theorem holds in complete local domains of mixed characteristic in higher dimension. We shall further discuss these issues later.

Math 711: Lecture of September 10, 2007

In order to give our next characterization of tight closure, we need to discuss a theory of multiplicities suggested by work of Kunz and developed much further by P. Monsky. We use $\ell(M)$ for the length of a finite length module M.

Hilbert-Kunz multiplicities

Let (R, m, K) be a local ring, $\mathfrak{A}$ an m-primary ideal and M a finitely generated nonzero R-module. The standard theory of multiplicities studies $\ell(M/\mathfrak{A}^n M)$ as a function of n, especially for large n. This function, the *Hilbert function of M with respect to* $\mathfrak{A}$, is known to coincide, for all sufficiently large n, with a polynomial in n whose degree d is the Krull dimension of M. This polynomial is called the *Hilbert polynomial* of M with respect to $\mathfrak{A}$. The leading term of this polynomial has the form $\dfrac{e}{d!}\,n^d$, where e is a positive integer.

In prime characteristic $p > 0$ one can define another sort of multiplicity by using Frobenius powers instead of ordinary powers.

Theorem (P. Monsky). *Let (R, m, K) be a local ring of prime characteristic $p > 0$ and let $M \neq 0$ be a finitely generated R-module of Krull dimension d. Let $\mathfrak{A}$ be an m-primary ideal of R. Then there exist a positive real number γ and a positive real constant C such that*

$$|\ell(M/\mathfrak{A}^{[q]}M) - \gamma q^d| \leq C q^{d-1}$$

for all $q = p^e$.

One may also paraphrase the conclusion by writing

$$\ell(M/\mathfrak{A}^{[q]}M) = \gamma q^d + O(q^{d-1})$$

where the vague notation $O(q^{d-1})$ is used for a function of q bounded in absolute value by some fixed positive real number times q^{d-1}. The function $e \mapsto \ell(M/\mathfrak{A}^{[q]}M)$ is called the *Hilbert-Kunz* function of M with respect to $\mathfrak{A}$. The real number γ is called the *Hilbert-Kunz multiplicity* of M with respect to $\mathfrak{A}$. In particular, one can conclude that

$$\gamma = \lim_{q \to \infty} \frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}.$$

Note that this is the behavior one would have if $\ell(M/\mathfrak{A}^{[q]}M)$ were eventually a polynomial of degree d in q with leading term γq^d: *but this is not true.* One often gets functions that are not polynomial.

When $M = R$, we shall write $\gamma_{\mathfrak{A}}$ for the Hilbert-Kunz multiplicity of R with respect to $\mathfrak{A}$.

Monsky's proof (cf. [P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983) 43–49]) of the existence of the limit γ is, in a sense, not constructive. He achieves this by proving that $\{\frac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}\}_q$ is a Cauchy sequence. The limit is only known to be a real number, not a rational number.

Example. Here is one instance of the non-polynomial behavior of Hilbert-Kunz functions. Let

$$R = (\mathbb{Z}/5\mathbb{Z})[[W,\, X,\, Y,\, Z]]/(W^4 + X^4 + Y^4 + Z^4),$$

with maximal ideal m. Then

$$\ell(R/m^{[5^e]}) = \frac{168}{61}(5^e)^3 - \frac{107}{61}(3^e).$$

See [C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, Math Z. **214** (1983) 119–135.]

Hilbert-Kunz multiplicities give a characterization of tight closure in certain complete local rings:

Theorem. *Let $(R,\, m,\, K)$ be a complete local ring of prime characteristic $p > 0$ that is reduced and equidimensional. Let $\mathfrak{A}$ and $\mathfrak{B}$ be m-primary ideals such that $\mathfrak{A} \subseteq \mathfrak{B}$. Then $\mathfrak{B} \subseteq \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}} = \gamma_{\mathfrak{B}}$.*

This has two immediate corollaries. Suppose that $(R,\, m,\, K)$ and $\mathfrak{A}$ are as in the statement of the Theorem. Then, first, $\mathfrak{A}^*$ is the largest ideal $\mathfrak{B}$ between $\mathfrak{A}$ and m such that $\gamma_{\mathfrak{B}} = \gamma_{\mathfrak{A}}$. Second, if $u \in m$, then $u \in \mathfrak{A}^*$ if and only if $\gamma_{\mathfrak{A}+Ru} = \gamma_{\mathfrak{A}}$. Therefore, the behavior of Hilbert-Kunz multiplicities determines what tight closure is in the case of a complete local ring, since one can first reduce to the case of a complete local domain, and then to the case of an m-primary ideal. This in turn determines the behavior of tight closure in all algebras essentially of finite type over an excellent local (or semilocal) ring.

We shall spend some effort in these lectures on understanding the behavior of the rings R^+. One of the early motivations for doing so is the following result from [M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. bf 135 (1992) 53–89].

Theorem. *Let $(R,\, m,\, K)$ be a complete (excellent also suffices) local domain of prime characteristic $p > 0$. Then R^+ is a big Cohen-Macaulay algebra over R.*

Although this result has been stated in terms of the very large ring R^+, it can also be thought of as a theorem entirely about Noetherian rings. Here is another statement, which is readily seen to be equivalent.

Theorem. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$. Let $x_1, \dots, x_{k+1}$ be part of a system of parameters for R. Suppose that we have a relation $r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$. Then there is a module-finite extension domain S of R such that $r_{k+1} \in (x_1, \dots, x_k)S$.*

The point here is that R^+ is the directed union of all module-finite extension domains S of R.

We should note that this Theorem is not at all true in equal characteristic 0. In fact, if one has a relation

$$(*) \quad r_{k+1}x_{k+1} = r_1x_1 + \cdots + r_kx_k$$

on part of a system of parameters in a normal local ring (R, m, K) that contains the rational numbers $\mathbb{Q}$ and $r_{k+1} \notin (x_1, \dots, x_k)R$, then there does not exist any module-finite extension S of R such that $r_{k+1} \in (x_1, \dots, x_k)S$. In dimension 3 or more there are always complete normal local domains that are not Cohen-Macaulay. One such example is given at the bottom of p. 12 and top of p. 13 of the Lecture Notes of September 5. In such a ring one has relations such as $(*)$ on a system of parameters with $r_{k+1} \notin (x_1, \dots, x_k)R$, and one can never "get rid of" these relations in a module-finite extension domain. Thus, these relations persist even in R^+.

One key point is the following:

Theorem. *Let R be a normal domain. Let S be a module-finite extension domain of R such that the fraction field $\mathcal{L}$ of S has degree d over the fraction field $\mathcal{K}$ of R. Suppose that $\frac{1}{d} \in R$, which is automatic if $\mathbb{Q} \subseteq R$. Then*

$$\frac{1}{d}\,\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$$

gives an R-module retraction of S to R. In particular, for every ideal I of R, $IS \cap R = I$.

The last statement follows from part (a) of the Proposition on p. 11 of the Lecture Notes of September 5.

Here is an explanation of why trace gives such a retraction. First off, recall that $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}$ is defined as follows: if $\lambda \in \mathcal{L}$, multiplication by λ defines a $\mathcal{K}$-linear map $\mathcal{L} \to \mathcal{L}$. The value of $\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(\lambda)$ is simply the trace of this $\mathcal{K}$-linear endomorphism of $\mathcal{L}$ to itself. It may be computed by choosing any basis $v_1, \dots, v_d$ for $\mathcal{L}$ as a vector space over $\mathcal{K}$. If M is the matrix of the $\mathcal{K}$-linear map given by multiplication by λ, this trace is simply the sum of the entries on the main diagonal of this matrix. Its value is independent of the choice of basis, since a different basis will yield a similar matrix, and the similar matrix will have the same trace. It is then easy to verify that this gives a $\mathcal{K}$-linear map from $\mathcal{L} \to \mathcal{K}$.

Now suppose that $s \in S$. We want to verify that its trace is in R. There are several ways to argue. We shall give an argument in which we descend to the case where R is the integral closure of Noetherian domain, and we shall then be able to reduce to the case where R is a DVR, i.e., a Noetherian valuation domain, which is very easy.

Note that $\mathcal{K} \otimes_R S$ is a localization of S, hence, a domain, and that it is module-finite over $\mathcal{K}$, so that it is zero-dimensional. Hence, it is a field, and it follows that $\mathcal{K} \otimes_R S = \mathcal{L}$. Hence, every element of $\mathcal{L}$ has a multiple by a nonzero element of R that is in S. In particular, we can choose a basis $s_1, \ldots, s_d$ for $\mathcal{L}$ over $\mathcal{K}$ consisting of elements of S. Extend it to a set of generators $s_1, \ldots, s_n$ for S as an R-module. Without loss of generality we may assume that $s = s_n$ is among them. We shall now construct a new counter-example in which R is replaced by the integral closure R_0 of a Noetherian subdomain and S by

$$R_0 s_1 + \cdots + R_0 s_n.$$

To construct R_0, note that every $s_i s_j$ is an R-linear combination of $s_1, \ldots, s_n$. Hence, for all $1 \leq i, j \leq n$ we have equations

$$(*) \quad s_i s_j = \sum_{k=1}^{n} r_{ijk} s_k$$

with all of the r_{ijk} in R. For $j > d$, each s_j is a $\mathcal{K}$-linear combination of $s_1, \ldots, s_d$. By clearing denominators we obtain equations

$$(**) \quad r_j s_j = \sum_{k=1}^{d} r_{jk} s_j$$

for $d < j \leq n$ such that every $r_j \in R - \{0\}$ and every $r_{jk} \in R$.

Let R_1 denote the ring generated over the prime ring (either $\mathbb{Z}$ or some finite field $\mathbb{Z}/p\mathbb{Z}$) by all the r_{ijk}, rjk, and r_j. Of course, R_1 is a Noetherian ring. Let R_0 be the integral closure of R_1 in its fraction field. (It is possible to show that R_0 is Noetherian, but we don't need this fact.) Now let $S_0 = R_0 s_1 + \cdots + R_0 s_n$, which is evidently generated as an R_0-module by $s_1, \ldots, s_n$. The equations $(*)$ hold over R_0, and so S_0 is a subring of S. It is module-finite over R_0. The equations $(**)$ hold over R_0, and $s_{d+1}, \ldots, s_n$ are linearly dependent on $s_1, \ldots, s_d$ over the fraction field $\mathcal{K}_0$ of R_0. Finally, $s_1, \ldots, s_d$ are linearly independent over $\mathcal{K}_0$, since this is true even over $\mathcal{K}$. Hence, $s_1, \ldots, s_d$ is a vector space basis for $\mathcal{L}_0$ over $\mathcal{K}_0$.

The matrix of multiplication by $s = s_n$ with respect to the basis $s_1, \ldots, s_d$ is the same as in the calculation of the trace of s from $\mathcal{L}$ to $\mathcal{K}$. This trace is not in R_0, since it is not in R. We therefore have a new counterexample in which R_0 is the integral closure of the Noetherian ring R_1. By the Theorem near the bottom of the first page of the Lecture Notes of September 13 from Math 711, Fall 2006, R_0 is an intersection of Noetherian valuation domains that lie between R_0 and $\mathcal{K}_0$. Hence, we can choose such a valuation domain V that does not contain the trace of s. We replace R_0 by V and S_0 by

$$T = Vs_1 + \cdots + Vs_n,$$

which gives a new counter-example in which the smaller ring is a DVR. The proof that T is a ring module-finite over V with module generators $s_1, \ldots, s_n$ such that a basis for the field extension is $s_1, \ldots, s_d$ is the same as in the earlier argument when we replaced R by R_0. Likewise, the trace of s with respect to the two new fraction fields is not affected. In fact, we can use any integrally closed ring in between R_0 and R.

Consequently, we may assume without loss of generality that $R = V$ is a DVR. Since S is a finitely generated torsion-free R-module and R is a principal ideal domain, S is free as R-module. Therefore, we may choose $s_1, \ldots, s_d \in S$ to be a free basis for S over R, and it will also be a basis for $\mathcal{L}$ over $\mathcal{K}$. The matrix for multiplication by s then has entries in R. It follows that its trace is in R, as required. $\square$

Corollary. *Let R be a normal domain containing the rational numbers $\mathbb{Q}$. Let S be an extension ring of R, not necessarily a domain.*

(a) *If S is module-finite over R, then R is a direct summand of S.*

(b) *If S is integral over R, then for every ideal I of R, $IS \cap R = I$.*

Proof. For part (a), we may choose a minimal prime P of S disjoint from the multiplicative system $R - \{0\} \subseteq S$. Then $R \to S \to S/P$ is module-finite over R, and since $P \cap R = \{0\}$, $\iota : R \hookrightarrow S/P$ is injective. By the result just proved, R is a direct summand of S/P: let $\theta : S/P \to R$ be a splitting, so that $\theta \circ \iota$ is the identity on R. Then the composite $S \to S/P \xrightarrow{\theta} R$ splits the map $R \to S$.

For the second part, suppose that $r \in R$ and $r \in IS$. Then there exist $f_1, \ldots, f_h \in I$ and $s_1, \ldots, s_h \in S$ such that

$$r = f_1 s_1 + \cdots + f_h s_h.$$

Let $S_1 = R[s_1, \ldots, s_h]$. Then S_1 is module-finite over R, and so by part (a), R is a direct summand of S_1. But we still have that $r \in IS_1 \cap R$, and so by part (a) of the Proposition on p. 11 of the Lecture Notes of September 5, we have that $r \in I$. $\square$

The fact that ideals of normal rings containing $\mathbb{Q}$ are contracted from integral extensions may seem to be an advantage. But the failure of this property in characteristic $p > 0$, which, in fact, enables one to use module-finite extensions to get rid of relations on systems of parameters, is perhaps an even bigger advantage of working in positive characteristic.

Note that the result on homomorphisms of plus closures of rings given in the Proposition at the top of p. 10 of the Lecture Notes of September 7 then yields:

Theorem. *Let $R \to S$ be a local homomorphism of complete local domains of prime characteristic $p > 0$. Then there is a commutative diagram:*

$$\begin{array}{ccc} B & \longrightarrow & C \\ \uparrow & & \uparrow \\ R & \longrightarrow & S \end{array}$$

such that B is a big Cohen-Macaulay algebra over R and C is a big Cohen-Macaulay algebra over S.

The point is that one can take $B = R^+$ and $C = S^+$, and then one has the required map $B \to C$ by the Proposition cited just before the statement of the Theorem. The same result can be proved in equal characteristic 0, but the proof depends on reduction to characteristic $p > 0$. When we discussed the existence of "sufficiently many big Cohen-Macaulay algebras" in mixed characteristic, it is this sort of result that we had in mind.

The following result of Karen Smith [K. E. Smith, *Tight Closure of Parameter Ideals,* Inventiones Math. **115** (1994) 41–60] (which also contains a form of the result when the ring is not necessarily local) may be viewed as providing another connection between big Cohen-Macaulay algebras and tight closure.

Theorem. *Let R be a complete (or excellent) local domain and let I be an ideal generated by part of a system of parameters for R. Then $I^* = IR^+ \cap R$.*

Property (3) stated on p. 7 of the Lecture Notes of September 7 implies that $IR^+ \cap R \subseteq I^*$, since R^+ is a directed union of module-finite extension domains S. The converse for parameter ideals is a difficult theorem.

This result suggests defining a closure operation on ideals of any domain R as follows: the *plus closure* of I is $IR^+ \cap R$. This plus closure is denoted I^+. Thus, plus closure coincides with tight closure for parameters ideals in excellent local domains of characteristic $p > 0$. Note that plus closure is not very interesting in equal characteristic 0, for if I is an ideal of a normal ring R that contains the rationals, $I^+ = I$.

It is very easy to show that plus closure commutes with localization. Thus, if it were true in general that plus closure agrees with tight closure, it would follow that tight closure commutes with localization. However, recent work of H. Brenner and others suggests that tight closure does not commute with localization in general, and that tight closure is not the same as plus closure in general. This is not yet proved, however.

Recently, the Theorem that R^+ is a big Cohen-Macaulay algebra when (R, m, K) is an excellent local domain of prime characteristic $p > 0$ has been strengthened by C. Huneke and G. Lyubeznik. See [C. Huneke and G. Lyubeznik, *Absolute integral closure in positive characteristic,* Advances in Math. **210** (2007) 498–504]. Roughly speaking, the original version provides a module-finite extension domain S of R that trivializes *one* given relation on parameters. The Huneke-Lyubeznik result provides a module-finite extension S that simultaneously trivializes *all* relations on all systems of parameters in the original ring. Their hypothesis is somewhat different. R need not be excellent: instead, it is assumed that R is a homomorphic image of a Gorenstein ring. Note, however, that the new ring S need not be Cohen-Macaulay: new relations on parameters may have been introduced.

The arguments of Huneke and Lyubeznik give a global result. The ring need not be assumed local. Under mild hypotheses, in characteristic p, the Noetherian domain R has a module finite extension S such that for every local ring R_P of R, all of the relations on all systems of parameters in R_P become trivial in S_P. In order to prove this result, we need to develop some local cohomology theory.

Finally, we want to mention the following result of Ray Heitmann, referred to earlier.

Theorem (R. Heitmann). *Let R be a complete local domain of mixed characteristic p. Let x, y, z be a system of parameters for R. Suppose that $rz \in (x, y)R$. Then for every $N \in \mathbb{N}$, $p^{1/N}r \in (x, y)R^+$.*

See [R. C. Heitmann, *The direct summand conjecture in dimension three,* Annals of Math. **156** (2002) 695–712].

The condition satisfied by r in this Theorem bears a striking resemblance to one of our characterizations of tight closure: see condition (#) near the bottom of p. 6 of the Lecture Notes of September 6. In a way, it is very different: in tight closure theory, the element c is anything but p, which is 0. Heitmann later proved (cf. [R. C. Heitmann, *Extended plus closure and colon-capturing,* J. Algebra **293** (2005) 407–426]) that in the Theorem above, one can use any element of R^+, not just p. The entire maximal ideal of R^+ multiplies r into $(x, y)R^+$.

Heitmann's result stated in the Theorem above already suffices to prove the existence of big Cohen-Macaulay algebras in dimension 3 in mixed characteristic: see [M. Hochster, *Big Cohen-Macaulay algebras in dimension three via Heitmann's theorem,* J. Algebra **254** (2002) 395–408].

It is possible that, for a complete local domain R of dimension 3 and mixed characteristic, R^+ is a big Cohen-Macaulay algebra. This is an open question.

It is also an open question whether an analogue of Heitmann's theorem holds in complete local domains of mixed characteristic in higher dimension. We shall further discuss these issues later.

Math 711: Lecture of September 12, 2007

In our treatment of tight closure for modules it will be convenient to use the Frobenius functors, which we view as special cases of base change. We first review some basic facts about base change.

Base change

If $f : R \to S$ is an ring homomorphism, there is a base change functor $S \otimes_R \_$ from R-modules to S-modules. It takes the R-module M to the R-module $S \otimes_R M$ and the map $h : M \to N$ to the unique S-linear map $S \otimes_R M \to S \otimes_R N$ that sends $s \otimes u \mapsto s \otimes h(u)$ for all $s \in S$ and $u \in M$. This map may be denoted $\mathbf{1}_S \otimes_R h$ or $S \otimes_R h$. Evidently, base change from R to S is a covariant functor. We shall temporarily denote this functor as $\mathcal{B}_{R \to S}$. It also has the following properties.

(1) Base change takes R to S.

(2) Base change commutes with arbitrary direct sums and with arbitrary direct limits.

(3) Base change takes R^n to S^n and free modules to free modules.

(4) Base change takes projective R-modules to projective S-modules.

(5) Base change takes flat R-modules to flat S-modules.

(6) Base change is right exact: if

$$M' \to M \to M'' \to 0$$

is exact, then so is

$$S \otimes_R M' \to S \otimes_R M \to S \otimes_R M'' \to 0.$$

(7) Base change takes finitely generated modules to finitely generated modules: the number of generators does not increase.

(8) Base change takes the cokernel of the matrix $\bigl(r_{ij}\bigr)$ to the cokernel of the matrix $\bigl(f(r_{ij})\bigr)$.

(9) Base change takes R/I to S/IS.

(10) For every R-module M there is a natural R-lineaar map $M \to S \otimes M$ that sends $u \mapsto 1 \otimes u$. More precisely, R-linearity means that $ru \mapsto g(r)(1 \otimes u) = g(r) \otimes u$ for all $r \in R$ and $u \in M$.

(11) Given homomorphisms $R \to S$ and $S \to T$, the base change functor $\mathcal{B}_{R \to T}$ for the composite homomorphism $R \to T$ is the composition $\mathcal{B}_{S \to T} \circ \mathcal{B}_{R \to S}$.

Part (1) is immediate from the definition. Part (2) holds because tensor product commutes with arbitrary direct sums and arbitrary direct limits. Part (3) is immediate from parts (1) and (2). If P is a projective R-module, one can choose Q such that $P \oplus Q$ is free. Then $(S \otimes_R P) \oplus (S \otimes_R Q)$ is free over S, and it follows that both direct summands are projective over S. Part (5) follows because if M is an R-module, the functor $(S \otimes_R M) \otimes_S \_$ on S-modules may be identified with the functor $M \otimes_R \_$ on S-modules. We have

$$(S \otimes_R M) \otimes_S U \cong (M \otimes_R S) \otimes_S U \cong M \otimes_R M,$$

by the associativity of tensor. Part (6) follows from the corresponding general fact for tensor products. Part (7) is immediate, for if M is finitely generated by n elements, we have a surjection $R^n \twoheadrightarrow M$, and this yields $S^n \twoheadrightarrow S \otimes_R M$. Part (8) is immediate from part (6), and part (9) is a consequence of (6) as well. (10) is completely straightforward, and (11) follows at once from the associativity of tensor products.

The Frobenius functors

Let R be a ring of prime characteristic $p > 0$. The *Frobenius* or *Peskine-Szpiro* functor $\mathcal{F}_R$ from R-modules to R-modules is simply the base change functor for $f : R \to S$ when $S = R$ and the homomorphism $f : R \to S$ is the Frobenius endomorphism $F : R \to R$, i.e, $F(r) = r^p$ for all $r \in R$. We may take the e-fold iterated composition of this functor with itself, which we denote $\mathcal{F}^e_R$. This is the same as the base change functor for the homomorphism $F^e : R \to R$, where $F^e(r) = r^{p^e}$ for all $r \in R$, by the iterated application of (11) above. When the ring is clear from context, the subscript $_R$ is omitted, and we simply write $\mathcal{F}$ or $\mathcal{F}^e$.

We then have, from the corresponding facts above:

(1) $\mathcal{F}^e(R) = R$.

(2) $\mathcal{F}^e$ commutes with arbitrary direct sums and with arbitrary direct limits.

(3) $\mathcal{F}^e(R^n) = R^n$ and $\mathcal{F}^e$ takes free modules to free modules.

(4) $\mathcal{F}^e$ takes projective R-modules to projective R-modules.

(5) $\mathcal{F}^e$ takes flat R-modules to flat R-modules.

(6) $\mathcal{F}^e$ is right exact: if

$$M' \to M \to M'' \to 0$$

is exact, then so is

$$\mathcal{F}^e(M') \to \mathcal{F}^e(M) \to \mathcal{F}^e(M'') \to 0.$$

(7) $\mathcal{F}^e$ takes finitely generated modules to finitely generated modules: the number of generators does not increase.

(8) $\mathcal{F}^e$ takes the cokernel of the matrix $\big(r_{ij}\big)$ to the cokernel of the matrix $\big(r_{ij}^{p^e}\big)$.

(9) $\mathcal{F}^e$ takes R/I to $R/I^{[q]}R$.

By part (10) in the list of properties of base change, for every R-module M there is a natural map $M \to \mathcal{F}^e(M)$. We shall use u^q to denote the image of u under this map, which agrees with usual the usual notation when $M = R$. R-linearity then takes the following form:

(10) For every R-module M the natural map $M \to \mathcal{F}^e(M)$ is such that for all $r \in R$ and all $u \in M$, $(ru)^q = r^q u^q$.

We also note the following: given a homomorphism $g : R \to S$ of rings of prime characteristic $p > 0$, we always have that $g \circ F_R^e = F_S^e \circ g$. In fact, all this says is that $g(r^q) = g(r)^q$ for all $r \in R$. This yields a corresponding isomorphism of compositions of base change functors:

(11) Let $R \to S$ be a homomorphism of rings of prime characteristic $p > 0$. Then for every R-module M, there is an identification $S \otimes_R \mathcal{F}_R^e(M) \cong \mathcal{F}_S^e(S \otimes_R M)$ that is natural in the R-module M.

When $N \subseteq M$ the map $\mathcal{F}^e(N) \to \mathcal{F}^e(M)$ need not be injective. We denote that image of this map by $N^{[q]}$ or, more precisely, by $N_M^{[q]}$. *However, one should keep in mind that* $N^{[q]}$ *is a submodule of* $\mathcal{F}^e(M)$, **not** *of* M *itself.* It is very easy to see that $N^{[q]}$ is the R-span of the elements of $\mathcal{F}^e(M)$ of the form u^q for $u \in N$. The module $N^{[q]}$ is also the R-span of the elements u_λ^q as u_λ runs through any set of generators for N.

A very important special case is when $M = R$ and $N = I$, an ideal of R. In this situation, $I_R^{[q]}$ is the same as $I^{[q]}$ as defined earlier. What happens here is atypical, because $F^e(R) = R$ for all e.

Tight closure for modules

Let R be a Noetherian ring of prime characteristic $p > 0$. If $N \subseteq M$, we define the *tight closure* N_M^* of N in M to consist of all elements $u \in M$ such that for some $c \in R^\circ$,

$$cu^q \in N_M^{[q]} \subseteq \mathcal{F}^e(M)$$

for all $q \gg 0$. Evidently, this agrees with our definition of tight closure for an ideal I, which is the case where $M = R$ and $N = I$. If M is clear from context, the subscript $_M$ is omitted, and we write N^* for N_M^*. Notice that we have not assumed that M or N is finitely generated. The theory of tight closure in Artinian modules is of very great interest. Note that c may depend on M, N, and even u. However, c is *not* permitted to depend on q. Here are some properties of tight closure:

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let N, M, and Q be R-modules.*

(a) N_M^* *is an R-module.*

(b) *If* $N \subseteq M \subseteq Q$ *are* R*-modules, then* $N^*_Q \subseteq M^*_Q$ *and* $N^*_M \subseteq N^*_Q$.

(c) *If* $N_\lambda \subseteq M_\lambda$ *is any family of inclusions, and* $N = \bigoplus_\lambda N_\lambda \subseteq \bigoplus_\lambda M_\lambda = M$*, then* $N^*_M = \bigoplus_\lambda (N^*_\lambda)_{M_\lambda}$.

(d) *If* R *is a finite product of rings* $R_1 \times \cdots \times R_n$*,* $N_i \subseteq M_i$ *are* R_i*-modules,* $1 \leq i \leq n$*,* M *is the* R*-module* $M_1 \times \cdots \times M_n$*, and* $N \subseteq M$ *is* $N_1 \times \cdots \times N_n$*, then* N^*_M *may be identify with* $(N_1)^*_{M_1} \times \cdots \times (N_n)^*_{M_n}$.

(e) *If* I *is an ideal of* R*,* $I^* N^*_M \subseteq (IN)^*_M$.

(f) *If* $N \subseteq M$ *and* $V \subseteq W$ *are* R*-modules and* $h : M \to W$ *is an* R*-linear map such that* $h(N) \subseteq V$*, then* $h(N^*_M) \subseteq V^*_W$.

Proof. (a) Let $c, c' \in R^\circ$. If $cu^q \in N^{[q]}$ for $q \geq q_0$, then $c(ru)^q \in N^{[q]}$ for $q \geq q_0$. If $c'v^q \in N^q$ for $q \geq q_1$ then $(cc')(u+v)^q \in N^{[q]}$ for $q \geq \max\{q_0, q_1\}$.

(b) The first statment holds because we have that $N^{[q]}_Q \subseteq M^{[q]}_Q$ for all q, and the second because the map $F^e(M) \to F^e(Q)$ carries $N^{[q]}_M$ into $N^{[q]}_Q$.

(c) is a straightforward application of the fact that tensor product commutes with direct sum and the definition of tight closure. Keep in mind that every element of the direct sum has nonzero components from only finitely many of the modules.

(d) is clear: note that $(R_1 \times \cdots \times R_n)^\circ = R_1^\circ \times \cdots \times R_n^\circ$.

(e) If $c, c' \in R^\circ$, $cf^q \in I^{[q]}$ for $q \gg 0$, and $c'u^{[q]} \in N^{[q]}$ for $q \gg 0$, then $(cc')(fu)^q = (cf^q)(c'u^q) \in I^{[q]}N^{[q]}$ for $q \gg 0$, and $I^{[q]}N^{[q]} = (IN)^{[q]}$ for every q.

(f) This argument is left as an exercise. □

Let R and S be Noetherian rings of prime characteristic $p > 0$. We will frequently be in the situation where we want to study the effect of base change on tight closure. For this purpose, when $N \subseteq M$ are R-modules, it will be convenient to use the notation $\langle S \otimes_R N \rangle$ for the image of $S \otimes_R N$ in $S \otimes_R M$. Of course, one must know what the map $N \hookrightarrow M$ is, not just what N is, to be able to interpret this notation. Therefore, we may also use the more informative notation $\langle S \otimes_R N \rangle_M$ in cases where it is not clear what M is. Note that in the case where $M = R$ and $N = I \subseteq R$, $\langle S \otimes_R I \rangle = IS$, the expansion of I to S. More generally, if $N \subseteq G$, where G is free, we may write NS for $\langle S \otimes_R N \rangle_G \subseteq S \otimes G$, and refer to NS as the *expansion* of N, by analogy with the ideal case.

Proposition. *Let* $R \to S$ *be a homomorphism of Noetherian rings of prime characteristic* $p > 0$ *such that* R° *maps into* S°*. In particular, this hypothesis holds (1) if* $R \subseteq S$ *are domains, (2) if* $R \to S$ *is flat, or if (3)* $S = R/P$ *where* P *is a minimal prime of* S*. Then for all modules* $N \subseteq M$*,* $\langle S \otimes_R N^*_M \rangle_M \subseteq (\langle S \otimes_R N \rangle_M)^*_{S \otimes_R M}$.

Proof. It suffices to show that if $u \in N^*$ then $1 \otimes u \in \langle S \otimes_R N \rangle^*$. Since the image of c is in S°, this follows because $c(1 \otimes u^q) = 1 \otimes cu^q \in \langle S \otimes_R N^{[q]} \rangle = \langle S \otimes_R N \rangle^{[q]}$.

The statement about when the hypothesis holds is easily checked: the only case that is not immediate from the definition is when $R \to S$ is flat. This can be checked by proving that every minimal prime Q of S lies over a minimal prime P of R. But the induced map of localizations $R_P \to S_Q$ is faithfully flat, and so injective, and QS_Q is nilpotent, which shows that PR_P is nilpotent. □

Tight closure, like integral closure, can be checked modulo every minimal prime of R.

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Let $P_1, \ldots, P_n$ be the minimal primes of R. Let $D_i = R/P_i$. Let $N \subseteq M$ be R-modules, and let $u \in M$. Let $M_i = D_i \otimes_R M = M/P_iM$, and let $N_i = \langle D_i \otimes_R N \rangle$. Let u_i be the image of u in M_i. Then $u \in N^*_M$ over R if and only if for all i, $1 \le i \le n$, $u_i \in (N_i)^*_{M_i}$ over D_i.*

If $M = R$ and $N = I$, we have that $u \in I^*$ if and only if the image of u in D_i is in $(ID_i)^*$ in D_i, working over D_i, for all i, $1 \le i \le n$.

Proof. The final statement is just a special case of the Theorem. The "only if" part follows from the preceding Proposition. It remains to prove that if u is in the tight closure modulo every P_i, then it is in the tight closure. This means that for every i there exists $c_i \in R - P_i$ such that for all $q \gg 0$, $c_i u^q \in N^{[q]} + P_i F^e(M)$, since $\mathcal{F}^e(M/P_iM)$ working over D_i may be identified with $\mathcal{F}^e(M)/P_i\mathcal{F}^e(M)$. Choose d_i so that it is in all the P_j except P_i. Let J be the intersection of the P_i, which is the ideal of all nilpotents. Then for all i and all $q \gg 0$,

$$(*_i) \quad d_i c_i u^q \in N^{[q]} + JF^e(M),$$

since every $d_iP_i \subseteq J$.

Then $c = \sum_{i=1}^n d_i c_i$ cannot be contained in the union of P_i, since for all i the i th term in the sum is contained in all of the P_j except P_i. Adding the equations $(*_i)$ yields

$$cu^q \in N^{[q]} + JF^e(M)$$

for all $q \gg 0$, say for all $q \ge q_0$. Choose q_1 such that $J^{[q_1]} = 0$. Then $c^{q_1} u^{qq_1} \in N^{[qq_1]}$ for all $q \ge q_0$, which implies that $c^q u^q \in N^{[q]}$ for all $q \ge q_1 q_0$. □

Let R have minimal primes $P_1, \ldots, P_n$, and let $J = P_! \cap \cdots \cap P_n$, the ideal of nilpotent elements of R, so that $R_{\mathrm{red}} = R/J$. The minimal primes of R/J are the ideals P_i/J, and for every i, $R_{\mathrm{red}}/(P_i/J) \cong R/P_i$. Hence:

Corollary. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let J be the ideal of all nilpotent elements of R. Let $N \subseteq M$ be R-modules, and let $u \in M$. Then $u \in N^*_M$ if and only if the image of u in M/JM is in $\langle N/J \rangle^*_{M/JM}$ working over $R_{\mathrm{red}} = R/J$.*

We should point out that it is easy to prove the result of the Corollary directly without using the preceding Theorem.

We also note the following easy fact:

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$. Let $N \subseteq M$ be R-modules. If $u \in N^*_M$, then for all $q_0 = p^{e_0}$, $u^{q_0} \in (N^{[q_0]})^*_{\mathcal{F}^{e_0}(M)}$.*

Proof. This is immediate from the fact that $(N^{[q_0]})^{[q]} \subseteq \mathcal{F}^e\big(\mathcal{F}^{e_0}(M)\big)$, if we identify the latter with $\mathcal{F}^{e_0+e}(M)$, is the same as $N^{[q_0q]}$. □

We next want to consider what happens when we iterate the tight closure operation. When M is finitely generated, and quite a bit more generally, we do not get anything new. Later we shall develop a theory of *test elements* for tight closure that will enable us to prove corresponding results for a large class of rings without any finiteness conditions on the modules.

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let $N \subseteq M$ be R-modules. Consider the condtion :*

(#) *there exist an element $c \in R^\circ$ and $q_0 = p^{e_0}$ such that for all $u \in N^*$, $cu^q \in N^{[q]}$ for all $q \geq q_0$,*

which holds whenever N^*/N is a finitely generated R-module. If (#) holds, then $(N^*_M)^*_M = N^*_M$.

Proof. We first check that (#) holds when N^*/N is finitely generated. Let $u_1, \ldots, u_n$ be elements of N^* whose images generate N^*/N. Then for every i we can choose $c_i \in R^\circ$ and q_i such that for all $q \geq q_i$, we have that $c_iu^q \in N^{[q]}$ for all $q \geq q_i$. Let $c = c_1 \cdots c_n$ and let $q_0 = \max\{q_1, \ldots, q_n\}$. Then for all $q \geq q_0$, $cu_i^q \in N^{[q]}$, and if $u \in N$, the same condition obviously holds. Since every element of N^* has the form $r_1u_1 + \cdots + r_nu_n + u$ where the $r_i \in R$ and $u \in N$, it follows that (#) holds.

Now assume # and let $v \in (N^*)^*$. Then there exists $d \in R^\circ$ and q' such that for all $q \geq q'$, $dv^q \in (N^*)^{[q]}$, and so dv^q is in the span of elements w^q for $w \in N^*$. If $q \geq q_0$, we know that every $cw^q \in N^{[q]}$. Hence, for all $q \geq \max\{q', q_0\}$, we have that $(cd)v^q \in N^{[q]}$, and it follows that $v \in N^*$. □

Of course, if M is Noetherian, then so is N^*, and condition (#) holds. Thus:

Corollary. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let $N \subseteq M$ be finitely generated R-modules. Then $(N^*_M)^*_M = N^*_M$.* □

Math 711: Lecture of September 14, 2007

The following result is very useful in thinking about tight closure.

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$, let $N \subseteq M$ be R-modules, and let $u \in M$. Then $u \in N^*_M$ if and only if the image $\overline{u}$ of u in the quotient M/N is in $0^*_{M/N}$.*

Hence, if we map a free module G onto M, say $h : G \twoheadrightarrow M$, let $H = h^{-1}(N) \subseteq G$, and let $v \in G$ be such that $h(v) = u$, then $u \in N^*_M$ if and only if $v \in H^*_G$.

Proof. For the first part, let $c \in R^0$. Note that, by the right exactness of tensor products, $\mathcal{F}^e(M/N) \cong \mathcal{F}^e(M)/N^{[q]}$. Consequently, $cu^q \in N^{[q]}$ for all $q \geq q_0$ if and only if $c\overline{u}^q = 0$ in $\mathcal{F}^e(M/N)$ for $q \geq q_0$.

For the second part, simply note that the image of v in $G/H \cong M/N$ corresponds to $\overline{u}$ in M/N. □

It follows many questions about tight closure can be formulated in terms of the behavior of tight closures of submodules of free modules. Of course, when M is finitely generated, the free module G can be taken to be finitely generated with the same number of generators.

Given a free module G of rank n, we can choose an ordered free basis for G. This is equivalent to choosng an isomorphism $G \cong R^n = R \oplus \cdots \oplus R$. In the case of R^n, one may understand the action of Frobenius in a very down-to-earth way. We may identify $\mathcal{F}^e(R^n) \cong R^n$, since we have this identification when $n = 1$. Keep in mind, however, that the identification of $\mathcal{F}^e(G)$ with G depends on the choice of an ordered free basis for G. If $u = r_1 \oplus \cdots \oplus r_n \in R^n$, then $u^q = r_1^q \oplus \cdots \oplus r_n^q$. With $H \in R^n$, $H^{[q]}$ is the R-span of the elements u^q for $u \in H$ (or for u running through generators of H). Very similar remarks apply to the case of an infinitely generated free module G with a specified basis b_λ. The elements b_λ^q give a free basis for $\mathcal{F}^e(G)$, and if $u = r_1 b_{\lambda_1} + \cdots + r_s b_{\lambda_s}$, then $u^q = r_1^q b_{\lambda_1}^q + \cdots + r_s^q b_{\lambda_s}^q$ gives the representation of u^q as a linear combination of elements of the free basis $\{b_\lambda^q\}_\lambda$.

We could have defined tight closure for submodules of free modules using this very concrete description of u^q and $H^{[q]}$. The similarity to the case of ideals in the ring is visibly very great. But we are then saddled with the problem of proving that the notion is independent of the choice of free basis. Moreover, if we take this approach, we need to define N^*_M by mapping a free module G onto M and replacing N by its inverse image in G. We then have the problem of proving that the notion we get is independent of the choices we make.

Our next objective is to prove that in a regular ring, every ideal is tightly closed. This depends on knowing that $F : R \to R$ is flat for regular rings of prime characteristic $p > 0$.

Eventually we sketch below a proof of the flatness of F that depends on the structure theory for complete local rings of prime characteristic $p > 0$. Later, we shall give a different proof, based on the following result, which is valid without restriction on the characteristic:

Theorem. *Let (R, m, K) be a regular local ring and M and R-module. Then M is a big Cohen-Macaulay module for R if and only if M is faithfully flat over R.*

We postpone the proof of this result for a while: it makes considerable use of the properties of the functor Tor. However, we do want to make several comments.

First note that it immediately implies that when R is regular, $F : R \to R$ is flat. In general, $R \to S$ is flat if and only if for every prime ideal Q of S with contraction P to R, the map $R_P \to S_Q$ is flat.

To see this, note that for R_P-modules M, the natural map $S_Q \otimes_R M \to S_Q \otimes_{R_P} M$ is an isomorphism, because $M \to R_P \otimes_{R_P} M$ is an isomorphism, and we have

$$S_Q \otimes_{R_P} M \cong S_Q \otimes_{R_P} (R_P \otimes_R M) \cong S_Q \otimes_R M.$$

The latter is also $S_Q \otimes_S (S \otimes_R M)$. If S is flat over R, since S_P is flat over S we have that S_P is flat over R. On the other hand, if $N \hookrightarrow M$ is an injection of R-modules and $S \otimes_R N \to S \otimes_R M$ is not injective, we can localize at a prime Q of S in the support of the kernel. This yields a map $S_Q \otimes_R N \to S_Q \otimes_R M$ that is not injective. But if Q contracts to P, we do have that $N_P \to M_P$ is injective. This shows that S_Q is not flat over R_P. $\square$

Note that when $S = R$ and the map is F, the contraction of $P \in \operatorname{Spec}(R)$ is P. Thus, it suffices to show that F is flat on R_P for all primes P. This is now obvious given the Theorem above: any regular sequence (equivalently, system of parameters) in R, say $x_1, \ldots, x_n$, maps to $x_1^p, \ldots, x_n^p$ in R, which is again a regular sequence. Hence, R is a big Cohen-Macaulay algebra for R under the map $F : R \to R$, and this proves that R is faithfully flat over R.

We have the following additional comments on the Theorem. Suppose that M is a module over a local ring (R, m, K) and suppose that we know that $x_1, \ldots, x_n$ is a system of parameters that is a regular sequence on M. Let $\mathfrak{A} = (x_1, \ldots, x_n)R$. By the definition of a regular sequence, we have that $\mathfrak{A}M \neq M$. We want to point out that this condition implies the *a priori* stronger condition that $mM \neq M$. The reason is that m is nilpotent modulo $\mathfrak{A}$. Thus, we can choose s such that $m^s \subseteq \mathfrak{A}$. If $M = mM$, we can multiply by m^t to conclude that $m^t M = m^t(mM) = m^{t+1}M$. Thus

$$M = mM = m^2M = \cdots = m^tM = \cdots.$$

Then

$$M = m^sM \subseteq \mathfrak{A}M \subseteq M,$$

and we find that $\mathfrak{A}M = M$, a contradiction.

If M is faithfully flat over R, we have that $(R/m) \otimes M = M/mM \neq 0$, so that $mM \neq M$. Moreover, whenever $x_1, \ldots, x_n$ is a system of parameters for R, it is a regular sequence on R, and the fact that M is faithfully flat over R implies that $x_1, \ldots, x_n$ is a regular sequence on M. This shows that a faithfully flat R-module is a big Cohen-Macaulay module over R. The converse remains to be proved.

We next sketch a completely different proof that F is flat for a regular ring R. As noted above, this comes down to the local case. We use the fact that a local map $R \to S$ of local rings is flat if and only if the induced map $\widehat{R} \to \widehat{S}$ is flat. Hence, by the structure theory of complete local rings, we may assume that $R = K[[x_1, \ldots, x_n]]$ is a formal power series ring over a field. Since this ring is the completion of $K[x_1, \ldots, x_n]_P$ where $P = (x_1, \ldots, x_n)$, it suffices to prove the result for the localized polynomial ring $R = K[x_1, \ldots, x_n]$ itself. But $F(R) = K^p[x_1^p, \ldots, x_n^p]$. Thus, all we need to show is that $K^p[x_1, \ldots, x_n] \subseteq K[x_1, \ldots, x_n]$ is flat. We prove a stronger result: R is free over $F(R)$ in this case. Since K is free over K^p, $K[x_1^p, \ldots, x_n^p]$ is free on the same basis over $K^p[x_1^p, \ldots, x_n^p]$. Thus, we need only see that $K[x_1, \ldots, x_n]$ is free over $K[x_1^p, \ldots, x_n^p]$. It is easy to check that the monomials $x_1^{a_1} \cdots x_n^{a_n}$ such that $0 \leq a_i \leq p-1$ are free basis. $\square$

We now fill in the missing details of the argument sketched above.

Proposition. *Let $\theta : (R, m, K) \to (S, \mathfrak{n}, L)$ be a homomorphism of local rings that is* local, *i.e., $\theta(m) \subseteq \mathfrak{n}$. Let Q be a finitely generated S-module. Then Q is flat over R if and only if for every injective map $N \hookrightarrow M$ of finite length R-modules, $Q \otimes_R N \to Q \otimes_R M$ is injective.*

Proof. The condition is obviously necessary. We shall show that it is sufficient. Since tensor commutes with direct limits and every injection $N \hookrightarrow M$ is a direct limit of injections of finitely generated R-modules, it suffices to consider the case where $N \subseteq M$ are finitely generated. Suppose that some $u \in S \otimes_R N$ is such that $u \mapsto 0$ in $S \otimes_R M$. It will suffice to show that there is also such an example in which M and N have finite length. Fix any integer $t > 0$. Then we have an injection

$$N/(m^t M \cap N) \hookrightarrow M/m^t M$$

and there is a commutative diagram

$$\begin{array}{ccc} Q \otimes_R N & \xrightarrow{\iota} & Q \otimes_R M \\ f\big\downarrow & & g\big\downarrow \\ Q \otimes_R \big(N/(m^t M \cap N)\big) & \xrightarrow{\iota'} & Q \otimes_R \big(M/m^t M\big) \end{array}.$$

The image $f(u)$ of u in $Q \otimes_R \bigl(N/(m^t M \cap N)\bigr)$ maps to 0 under ι', by the commutativity of the diagram. Therefore, we have the required example provided that $f(u) \neq 0$. However, for all $h > 0$, we have from the Artin-Rees Lemma that for every sufficiently large integer t, $m^t M \cap N \subseteq m^h N$. Hence, the proof will be complete provided that we can show that the image of u is nonzero in

$$Q \otimes_R (N/m^h N) \cong Q \otimes_R \bigl((R/m^h) \otimes_R N\bigr) \cong (R/m^h) \otimes_R (Q \otimes_R N) \cong (Q \otimes_R N)/m^h (Q \otimes_R N)$$

for $h \gg 0$. But

$$m^h (Q \otimes_R N) \subseteq \mathfrak{n}^h (Q \otimes_R N),$$

and the result follows from the fact that the finitely generated S-module $Q \otimes_R N$ is $\mathfrak{n}$-adically separated. □

We can now prove the following result, which is the only missing ingredient needed to fill in the details of our proof that F is flat.

Lemma. *Let $(R,\, m,\, K) \to (S,\, \mathfrak{n}, L)$ be a local homomorphism of local rings. Then S is flat over R if and only if $\widehat{S}$ is flat over $\widehat{R}$, and this holds iff $\widehat{S}$ is flat over R.*

Proof. If S is flat over R then, since $\widehat{S}$ is flat over S, we have that $\widehat{S}$ is flat over R. Conversely, if $\widehat{S}$ is flat over R, then S is flat over R because $\widehat{S}$ is faithfully flat over S: if $N \hookrightarrow M$ is injective but $S \otimes_R N \to S \otimes_R M$ has a nonzero kernel, the kernel remains nonzero when we apply $\widehat{S} \otimes_S \_$, and this has the same effect as applying $\widehat{S} \otimes_R \_$ to $N \hookrightarrow M$, a contradiction.

We have shown that $R \to S$ is flat if and only $R \to \widehat{S}$ is flat. If $\widehat{R} \to \widehat{S}$ is flat then since $R \to \widehat{R}$ is flat, we have that $R \to \widehat{S}$ is flat, and we are done. It remains only to show that if $R \to S$ is flat, then $\widehat{R} \to \widehat{S}$ is flat. By the Proposition, it suffices to show that if $N \subseteq M$ have finite length, then $\widehat{S} \otimes N \to \widehat{S} \otimes M$ is injective. Suppose that both modules are killed by m^t. Since $S/m^t S$ is flat over R/m^t, if Q is either M or N we have that

$$\widehat{S} \otimes_{\widehat{R}} Q \cong \widehat{S}/m^t \widehat{S} \otimes_{\widehat{R}/m^t \widehat{R}} Q \cong \widehat{S}/m^t \widehat{S} \otimes_{R/m^t} Q \cong \widehat{S} \otimes_R Q,$$

and the result now follow because $\widehat{S}$ is flat over R. □

The following result on behavior of the colon operation on ideals under flat base change, while quite easy and elementary, plays a very important role in tight closure theory. Recall that when $I \subseteq R$ and $R \to S$ is a flat homomorphism, the map $I \otimes_R S \to R \otimes_R S = S$ is injective. Its image is clearly IS, the expansion of I to S. Thus, $I \otimes_R S$ may be naturally identified with IS when S is flat over R. Recall that if I and J are ideals of R, then

$$I :_R J = \{r \in R : rJ \subseteq I\},$$

which is an ideal of R. If $J = fR$ is principal, we may write $I :_R f$ for $I_R : fR$.

Proposition. *Let $R \to S$ be flat and let I and J be ideals of R such that J is finitely generated. Then $IS :_R JS = (I :_R J)S$.*

Proof. Let $J = (f_1, \dots, f_n)R$. We have an exact sequence

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

where the rightmost map sends $r \mapsto (\overline{rf_1}, \dots, \overline{rf_n})$; here, $\overline{g}$ denotes the image of g modulo I. The exactness is preserved when we apply $S \otimes_R \_$, which yields an exact sequence

$$(*) \quad 0 \to (I :_R J)S \hookrightarrow S \to (S/IS)^{\oplus n}$$

where the rightmost map sends $s \mapsto (\widetilde{sf_1}, \dots, \widetilde{sf_n})$ and $\widetilde{g}$ denotes the image of g modulo IS. From the definition of this map, the kernel is $IS :_S JS$, while from the exact sequence $(*)$ just above, the kernel is $(I :_R J)S$. $\square$

The result is false without the hypothesis that J be finitely generated. Let K be a field, and let $R = K[y, x_1, x_2, x_3, \dots]$ be a polynomial ring in infinitely many variables over K. Let $I = (x_1 y, x_2 y^2, \dots, x_n y^n, \dots)$ and let $J = (x_1, x_2, \dots, x_n, \dots)$. Then $I :_R J = I$, but if $S = R_y$, $IS = JS$ and $IS :_S JS = S$.

The proposition above has the following very important consequence:

Corollary. *Let R be a regular Noetherian ring of prime characteristic $p > 0$. Let I and J be any two ideals of R. Then for every $q = p^e$, we have that $I^{[q]} :_R J^{[q]} = (I :_R J)^{[q]}$.*

Proof. Take $R \to S$ to be the map $F^e : R \to R$, which is flat. Then

$$I^{[q]} :_R J^{[q]} = IS :_S JS = (I :_R J)S = (I :_R J)^{[q]}. \qquad \square$$

We can now prove that every ideal of a regular ring is tightly closed.

Theorem. *Let R be a regular Noetherian ring of prime characteristic $p > 0$. Let $I \subseteq R$ be any ideal. Then $I = I^*$.*

Proof. Suppose that we have a counterexample with $u \in I^* - I$. Choose a prime P in the support of $(I + Ru)/I$. In R_P, the image of u is still in $(IR_P)^*$ working over R_P, while it is not in IR_P by our choice of P. Therefore, it suffices to prove the result for a regular local ring (R, m, K). Since $u \in I^* - I$, we have that $I :_R u$ is a proper ideal of R. Hence, $I :_R u \subseteq m$. We know that there exists $c \in R^\circ$ such that for all $q \gg 0$, $cu^q \in I^{[q]}$. Hence, for all $q \geq q_0$ we have

$$c \in I^{[q]} :_R u^q = (I :_R u)^{[q]} \subseteq m^{[q]} \subseteq m^q,$$

i.e., $c \in \bigcap_{q \geq q_0} m^q = (0)$, contradicting that $c \in R^\circ$. $\square$

Math 711: Lecture of September 17, 2007

Definition. Let R be a Noetherian ring of prime characteristic $p > 0$. R is called *weakly F-regular* if every ideal is tightly closed. R is called *F-regular* if all of its localizations are weakly F-regular.

It is an open question whether, under mild conditions, e.g., excellence, weakly F-regular implies F-regular.

We shall show eventually that over a weakly F-regular ring, every submodule of every finitely generated module is tightly closed.

Since we have already proved that every regular ring of prime characteristic $p > 0$ is weakly F-regular and since the class of regular rings is closed under localization, it follows that every regular ring is F-regular.

We note the following fact.

Lemma. *Let R be any Noetherian ring, let M be a finitely generated module, and let $u \in M$. Suppose that $N \subseteq M$ is maximal with respect to the condition that $u \notin N$. Then M/N has finite length, and it has a unique associated prime, which is a maximal ideal m with a power that kills M. In this case u spans the socle $\mathrm{Ann}_{MN} m$ of M/N.*

Proof. The maximality of N implies that the image of u is in every nonzero submodule of M/N. We change notation: we may replace M by M/N, u by its image in M/N, and N by 0. Thus, we may assume that u is in every nonzero submodule of M, and we want to show that M has a unique associated prime. We also want to show that this prime is maximal. If $v \in M$ and $w \in M$ have distinct prime annihilators P and Q, we have that $Rv \cong R/P$ and $Rw \cong R/Q$. Any nonzero element of $Rv \cap Rw$ has annihilator P (thinking in R/P) and also has annihilator Q. It follows that $P = Q$ after all.

Thus, $\mathrm{Ass}\,(M)$ consists of a single prime ideal P. If P is not maximal, we have an embedding $R/P \hookrightarrow M$. Then u is in the image of R/P, and is in every nonzero ideal of R/P. If $R/P = D$ has dimension one or more, then it has a prime ideal P' other than 0. Then u must be in every power of P', and so u is in every power of the maximal ideal of the local ring $D_{P'}$, a contradiction. It follows that $\mathrm{Ass}\,(M)$ consists of a single maximal ideal m. This implies that M has a finite filtration by copies of R/m, and is therefore killed by a power of m. Then u must be in the socle $\mathrm{Ann}_M m$, which must be a one-dimensional vector space over $K = R/m$, or else it will have a subspace that does not contain u. $\square$

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

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 $Sx + I \subseteq P_k$ 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. □

Proposition. *Let R be a Noetherian ring and let W be a multiplicative system. Then every element of $(W^{-1}R)^\circ$ has the form c/w where $c \in R^\circ$ and $w \in W$.*

Proof. Suppose that $c/w \in (W^{-1}R)^\circ$ where $c \in R$ and $w \in W$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the minimal primes of R that do not meet W, so that the ideals $\mathfrak{p}_j W^{-1}R$ for $1 \leq j \leq k$ are *all* of the minimal primes of $W^{-1}R$. It follows that the image of $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$ is nilpotent in $W^{-1}R$, and so we can choose an integer $N > 0$ such that $I = (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k)^N$ has image 0 in $W^{-1}R$. If $c + I$ is contained in the union of the minimal primes of R, then by the coset form of prime avoidance above, it follows that $cR + I \subseteq \mathfrak{p}$ for some minimal prime $\mathfrak{p}$ of R. Since $I \subseteq \mathfrak{p}$, we have that $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k \subseteq \mathfrak{p}$, and it follows that $\mathfrak{p}_j = \mathfrak{p}$ for some j, where $1 \leq j \leq k$. But then $c \in \mathfrak{p}_j$, a contradiction, since c/w and, hence, $c/1$, is not in any minimal prime of R°. Thus, we can choose $g \in I$ such that $c + g$ is in R°, and we have that $c/w = (c + g)/w$ since $g \in I$. □

Lemma. *Let R be a Noetherian ring of prime characteristic $p > 0$. Let $\mathfrak{A}$ be an ideal of R primary to a maximal ideal m of R. Then $\mathfrak{A}$ is tightly closed in R if and only if $\mathfrak{A}R_m$ is tightly closed in R_m.*

Proof. Note that $R/\mathfrak{A}$ is already a local ring whose only maximal ideal is $m/\mathfrak{A}$. It follows that $(*)\quad R/\mathfrak{A} \cong (R/\mathfrak{A})_m = R_m/\mathfrak{A}R_m$. If $u \in R - \mathfrak{A}$ but $u \in \mathfrak{A}^*$, this is evidently preserved when we localize at m. Hence, if $\mathfrak{A}R_m$ is tightly closed in R_m, then $\mathfrak{A}$ is tightly closed in R. Now suppose $(\mathfrak{A}R_m)^*$ in R_m contains an element not in $\mathfrak{A}R_m$. Without loss of generality, we may assume that this element has the form $f/1$ where $f \in R$. Suppose that $c_1 \in R_m^\circ$ has the property that $c_1 f^q \in \mathfrak{A}^{[q]}R_m = (\mathfrak{A}R_m)^{[q]}$ for all $q \gg 0$. By the preceding Proposition, c_1 has the form c/w where $c \in R^\circ$ and $w \in R - m$. We may replace c_1 by wc_1, since w is a unit, and therefore assume that $c_1 = c/1$ is the image of $c \in R^\circ$. Then $cf^q/1 \in \mathfrak{A}^{[q]}R_m$ for all $q \gg 0$. It follows from $(*)$ above that $cf^q \in \mathfrak{A}^{[q]}$ for all $q \gg 0$, and so $f \in \mathfrak{A}_R^*$, as required. □

We have the following consequence:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Then the following conditions are equivalent:*

(a) *R is weakly F-regular.*

(b) *R_m is weakly F-regular for every maximal ideal m of R.*

(c) *Every ideal of R primary to a maximal ideal of R is tightly closed.*

Proof. It is clear that (a) $\Rightarrow$ (c). To see that (c) $\Rightarrow$ (a), assume (c) and suppose, to the contrary, that $u \in I^* - I$ in R. Let $\mathfrak{A}$ be maximal in R with respect to the property of containing I but not u. By the Lemma on p. 1, $R/\mathfrak{A}$ is killed by a power of a maximal ideal m, so that $\mathfrak{A}$ is m-primary. We still have $u \in \mathfrak{A}^* - \mathfrak{A}$, a contradiction. Then (b) holds if and only if all ideals primary to the maximal ideal of some R_m are tightly closed, and the equivalence with (c) follows from the preceding Lemma. □

We next make the following elementary observations about tight closure.

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$.*

(a) *The tight closure of 0 in R is the ideal J of all nilpotent elements of R.*

(b) *For every ideal $I \subseteq R$, $I^* \subseteq \overline{I} \subseteq \mathrm{Rad}\,(I)$.*

(c) *Prime ideals, radical ideals, and integrally closed ideals are tightly closed in R.*

Proof. (a) If $cu^q = 0$ and c is not in any minimal prime, then u^q is in every minimal prime, and, hence, so is u. This shows that $0^* \subseteq J$. On the other hand, if u is nilpotent, $u^{q_0} = 0$ for sufficiently large q_0, and then $1 \cdot u^q = 0$ for all $q \geq q_0$.

(b) Suppose $u \in I^*$. To show that $u \in \overline{I}$, it suffices to verify this modulo every minimal prime P of R. When we pass to R/P, we still have that the image of u is in the tight closure of $I(R/P)$. Hence, we may assume that R is a domain. We then have $c \neq 0$ such that $cu^q \in I^{[q]} \subseteq I^q$ for all sufficiently large q, and, in particular, for infinitely many q. This is sufficient for $u \in \overline{I}$. If $u \in \overline{I}$, u satisfies a monic polynomial

$$u^n + f_1 u^{n-1} + \cdots + f_n = 0$$

with $f_j \in I^J$ for $j \geq 1$. Thus, all terms but the first are in I, and so $u^n \in I$, which implies that $u \in \mathrm{Rad}\,(I)$.

(c) It is immediate from part (b) that integrally closed ideals are tightly closed in R, and that radical ideals are integrally closed. Of course, prime ideals are radical. □

We next give a tight closure version of the Briançon-Skoda theorem. This result was proved by Briançon and Skoda [J. Briançon and H. Skoda, *Sur la clôture intégrale d'un idéal de germes de fonctions holomorphes en un point de C^n*, C.R. Acad. Sci. Paris Sér. A **278** (1974) 949–951] for finitely generated $\mathbb{C}$-algebras and analytic regular local rings using a criterion of Skoda [H. Skoda, *Applications des techniques L^2 a la théorie des idéaux d'une algébre de fonctions holomorphes avec poids,* Ann. Scient. Ec. Norm. Sup. 4éme série, t. **5** (1972) 545–579] for when an analytic function is in an ideal in terms of the finiteness of a certain integral. Lipman and Teissier [J. Lipman and B. Teissier, *Pseudo-rational local rings and a theorem of Briançon-Skoda about integral closures of ideals,* Michigan Math. J. **28** (1981) 97–116] gave an algebraic proof for certain cases, and Lipman and

Sathaye [J. Lipman and A. Sathaye, *Jacobian ideals and a theorem of Briançon-Skoda*, Michigan Math. J. **28** (1981) 199–222] proved the result in general for regular rings. A detailed treatment of the Lipman-Sathaye argument is given in the Lecture Notes from Math 711, Fall 2006: see particularly the Lectures of September 25, 27, and 29, as well as the Lectures of October 2, 4, 6, 9, 11, and 13.

Tight closure gives an unbelievably simple proof of the theorem that is more general than these results in the equicharacteristic case, but the Lipman-Sathaye argument is the only one that is valid in mixed characteristic. Notice that in the tight closure version of the Theorem just below, the first statement is valid for *any* Noetherian ring of prime characteristic $p > 0$.

Theorem (Briançon-Skoda). *Let R be a Noetherian ring of prime characteristic $p > 0$. Let I be an ideal of R that is generated by n elements. Then $\overline{I^n} \subseteq I^*$. Hence, if R is regular (or weakly F-regular) then $\overline{I^n} \subseteq I$.*

Proof. We may work modulo each minimal prime in turn, and so assume that R is a domain. If $u \in \overline{I^n}$ there exists $c \neq 0$ such that for all $k \gg 0$, $cu^k \in (I^n)^k = I^{nk}$. In particular, this is true when $k = q = p^e$. The ideal $I^{nq} = (f_1, \ldots, f_n)^{nq}$ is generated by the monomials $f_1^{a_1} \cdots f_n^{a_n}$ of degree nq in the f_j. But when $a_1 + \cdots + a_q = nq$, at least one of the a_i is $\geq q$: if all are $\leq q-1$, their sum is $\leq n(q-1) < nq$. Thus, $I^{nq} \subseteq I^{[q]}$, and we have that $cu^q \in I^{[q]}$ for all $q \gg 0$. This shows that $u \in I^*$. The final statement holds because all ideals of a regular ring are tightly closed, $\square$

The Briançon-Skoda Theorem is often stated in a stronger but more technical form. The hypothesis is the same: I is an ideal generated by n elements. The conclusion is that $\overline{I^{n+m-1}} \subseteq (I^m)^*$ for all integers $m \geq 1$. The version we stated first is the case where $m = 1$. The argument for the strengthened version is very similar, but slightly more technical. Again, we may assume that R is a domain and that $cu^q \subseteq (I^{n+m-1})^q$ for all $q \gg 0$. Consider a monomial $f_1^{a_1} \cdots f_n^{a_n}$ where the sum of the a_i is $(n+m-1)q$. We can write each $a_i = b_i q + r_i$, where $0 \leq r_i \leq q-1$. It will suffice to show that the sum of the b_i is at least m, for then the monomial is in $(I^m)^{[q]}$, and we have that $u \in (I^m)^*$. But if the sum of the b_i is at most $m-1$, then the sum of the a_i is bounded by $(m-1)q + n(q-1) = (n+m-1)q - n < (n+m-1)q$, a contradiction. $\square$

The equal characteristic 0 form of the Theorem can be deduced from the characteristic p form by standard methods of reduction to characteristic p.

The basic tight closure form of the Briançon-Skoda theorem is of interest even in the case where $n = 1$, which has the following consequence.

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$. The tight closure of the principal ideal $I = fR$ is the same as its integral closure.*

Proof. By the Briançon-Skoda theorem when $n = 1$, we have that $\overline{I} \subseteq I^*$, while the other inclusion always holds. $\square$

We next observe:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. If the ideal (0) and the principal ideals generated by nonzerodivisors are tightly closed, then R is normal. Thus, if every principal ideal of R is tightly closed, then R is normal. Consequently, weakly F-regular rings are normal.*

Proof. The hypothesis that (0) is tightly closed is equivalent to the assumption that R is reduced. Henceforth, we assume that R is reduced.

If R is a product $S \times T$ then the hypothesis on R holds in both factors. E.g., if s is a nonzerodivisor in s, then $(s,\, 1)$ is a nonzerodivisor in T: it generates the ideal $sS \times T$, and its tight closure in $S \times T$ is $(sS)^*_S \times T$. But this is the same as $sS \times T$ if and only if sS is tightly closed in S.

Therefore, we may assume that R is not a product, i.e., that $\mathrm{Spec}\,(R)$ is connected. We first want to show that R is a domain in this case. If not, there are minimal primes $P_1,\, \dots\, , P_n$, $n \geq 2$, and we can choose an element u_i in $P_i - \bigcup_{j \neq i} P_j$ for every i. Let $u = u_1$, which is in P_1 and no other minimal prime, and $v = u_2 \cdots u_n$, which is in $P_2 \cap \cdots \cap P_n$ and not in P_1. Then uv is in every minimal prime, and so is 0, while $f = u + v$ is a not in any minimal prime, and so is not a zerodivisor. We claim that $u \in (fR)^*$. It suffices to check this modulo every P_i. But mod P_1, $u \equiv 0 = 0 \cdot f$, and mod P_j for $j > 1$, $u \equiv f = 1 \cdot f$. Since $(fR)^* = fR$, we can write $u = e(u + v)$ for some element $e \in R$. This means that $(1 - e)u = ev$. Mod P_1, $u \equiv 0$ while $v \not\equiv 0$, and so $e \equiv 0$ mod P_1. Mod P_j for $j > 1$, $u \not\equiv 0$ while $v \equiv 0$, and so $e \equiv 1$ mod P_j. It follows that $e^2 - e$ is in every minimal prime, and so is 0. Since whether its value mod P_i is 0 or 1 depends on i, e is a non-trivial idempotent in R, a contradiction.

Thus, we may assume that R is a domain. Now suppose that $f,\, g \in R$ with $g \neq 0$ and that f/g is integral over R. Then we have an equation of integral dependence

$$(f/g)^s + r_1(f/g)^{s-1} + \cdots + r_j(f/g)^{s-j} + \cdots + r_s = 0$$

with the $r_j \in R$. Multiplying by g^s we obtain

$$f^s + (r_1g)f^{s-1} + \cdots (r_jg^j)f^{s-j} + \cdots + r_sg^s = 0,$$

which shows that f is in the integral closure of gR. Thus, $f \in (gR)^*$, and this is gR by hypothesis. Consequently, $f = gr$ with $r \in R$, which shows that $f/g = r \in R$, as required. $\square$

We next want to discuss the use of tight closure to prove Theorems about the behavior of symbolic powers in regular rings of prime characteristic $p > 0$. The characteristic p

results imply corresponding results in equal characteristic 0. The following result was first proved in equal characteristic 0 by Ein, Lazarsfeld, and Smith [L. Ein, R. Lazarsfeld, and K. E. Smith, *Uniform bounds and symbolic powers on smooth varieties*, Inventiones Math. **144** (2001) 241–252], using the theory of multiplier ideals. The proof we give here may be found in [M. Hochster and C. Huneke, *Comparison of symbolic and ordinary powers of ideals*, Inventiones Math. **147** (2002) 349–369].

Theorem. *Let P be a prime ideal of height h in a regular ring R of prime characteristic $p > 0$. Then for every integer $n \geq 1$, $P^{(hn)} \subseteq P^n$.*

There are sharper results if one places additional hypotheses on R/P. An extreme example is to assume that R/P is regular so that, locally, P is generated by a regular sequence. In this case, the symbolic and ordinary powers of P are equal. Doubtless the best results of this sort remain to be discovered. It is not known whether the conclusion of the Theorem above holds in regular rings of mixed characteristic. The version stated above remains true with the hypotheses weakened in various ways. There are further comments about what can be proved in the sequel: see the last paragraph on p. 7. We have attempted to give a result that is of substantial interest but that has relatively few technicalities in its proof. The methods used here also yield the result that, without any regularity hypothesis on R, if R/P has finite projective dimension over R then

$$P^{(hn)} \subseteq (P^n)^*.$$

Of course, if R is regular the hypothesis of finite projective dimension is automatic, while one does not need to take the tight closure on the right because, in a regular ring, every ideal is tightly closed.

We postpone the proof of the Theorem to give a preliminary result that we will need.

Lemma. *Let P be a prime ideal of height h in a regular ring R of prime characteristic $p > 0$.*

(a) *$P^{[q]}$ is primary to P.*

(b) *$P^{(qh)} \subseteq P^{[q]}$.*

Proof. For part (a), we have that $\mathrm{Rad}\,(P^{[q]}) = P$, clearly. Let $f \in R - P$. It suffices to show that f is not a zerodivisor on $R/P^{[q]}$. Since

$$0 \to R/P \xrightarrow{f\cdot} R/P$$

is exact, it remains exact when we tensor with R viewed as an R-algebra via F^e, since this is a flat base change. Thus,

$$0 \to \mathcal{F}^e(R/P) \xrightarrow{f^q\cdot} \mathcal{F}^e(R/P)$$

is exact, and this is

$$0 \to R/P^{[q]} \xrightarrow{f^q \cdot} R/P^{[q]}.$$

Since f^q is not a zerodivisor on $R/P^{[q]}$, neither is f.

Suppose $u \in P^{(qh)} - P^{[q]}$. Make a base change to R_P. Then the image of u is in $P^{qh}R_P$, but not in $P^{[q]}R_P = (PR_P)^{[q]}$: if u were in the expansion of $P^{[q]}R_P$, it would be multiplied into $P^{[q]}$ by some element of $R - P$. Since such an element is not in $P^{[q]}$ by part (a), we have $u \notin (PR_P)^{[q]}$. But PR_P is generated by h elements, and so

$$(PR_P)^{qh} \subseteq (PR_P)^{[q]}$$

exactly as in the proof of the Briançon-Skoda Theorem: if a monomial in h elements has degree qh, at least one of the exponents occurring on one of the elements must be at least q. □

Proof of the symbolic power theorem. If $u \in P^{(hn)} - P^n$, then this continues to be the case after localizing at a maximal ideal in the support of $(P^n + Ru)/P^n$. Hence, we may assume that R is regular local. We may also assume that $P \neq 0$. Given $q = p^e$ we can write $q = an + r$ where $a \geq 0$ and $0 \leq r \leq n - 1$ are integers. Then $u^a \in P^{(han)}$ and

$$P^{hn}u^a \subseteq P^{hr}u^a \subseteq P^{(han+hr)} = P^{(hq)} \subseteq P^{[q]}.$$

Taking n th powers gives that

$$P^{hn^2}u^{an} \subseteq (P^{[q]})^n = (P^n)^{[q]},$$

and since $q \geq an$, we have that

$$P^{hn^2}u^q \subseteq (P^n)^{[q]}$$

for fixed h and n and for all q. Let d be any nonzero element of P^{hn^2}. The condition that $du^q \in (P^n)^{[q]}$ for all q says precisely that u is in the tight closure of P^n in R. But in a regular ring, every ideal is tightly closed, and so $u \in P^n$, as required. □

One can prove a similar result for ideals I without assuming that I is prime and without assuming that the ring is regular. We can define symbolic powers of ideals that are not necessarily prime as follows. If W is the multiplicative system of nonzerodivisors on I, define $I^{(t)}$ as the contraction of $I^tW^{-1}R$ to R. Suppose that R/I has finite projective dimension over R and that the localization of I at any associated prime of I can be generated by at most h elements (or even that its analytic spread is at most h). Then one can show $I^{(nh)} \subseteq (I^n)^*$ for all $n \geq 1$. See Theorem (1.1) of [M. Hochster and C. Huneke, *Comparison of symbolic and ordinary powers of ideals*, Inventiones Math. **147** (2002) 349–369].

Test elements

The definition of tight closure allows the element $c \in R^\circ$ to vary with N, M, and the element $u \in M$ being "tested" for membership in N^*_M. But under mild conditions on a reduced ring R, there exist elements, called *test elements*, that can be used in every tight closure test. It is somewhat difficult to prove their existence, but they play a very important role in the theory of tight closure.

Definition. Let R be a Noetherian ring of prime characteristic $p > 0$. An element $c \in R^\circ$ is called a *test element* (respectively, *big test element*) for R if for every inclusion of finitely generated modules $N \subseteq M$ (respectively, arbitrary modules $N \subseteq M$) and every $u \in M$, $u \in N^*_M$ if and only if $cu^q \in N^{[q]}_M$ for every $q = p^e \geq 1$. A (big) test element is called *locally stable* if it is a (big) test element in every localization of R. A (big) test element is called *completely stable* if it is a (big) test element in the completion of every local ring of R.

It will be a while before we can prove that test elements exist. But we shall eventually prove the following:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$ that is reduced and essentially of finite type over an excellent semilocal ring R. Let $c \in R^\circ$ be such that R_c is regular (such elements always exist). Then c has a power that is a completely stable big test element for R.*

We want to record some easy facts related to test elements. We first note:

Lemma. *If $N \subseteq M$ are R-modules, S is faithfully flat over R, and $v \in M - N$, then $1 \otimes v$ is not in $\langle S \otimes_R N \rangle$ in $S \otimes_R M$.*

Proof. We may replace M by M/N, N by 0, and v by its image in M/N. The result then asserts that the map $M \to S \otimes_R M$ is injective. Let $v \in M$ be in the kernel. Then $S \otimes_R Rv \hookrightarrow S \otimes_R M$, and it suffices to see that $(*)$ $Rv \to S \otimes_R Rv$ is injective. Let $I = \mathrm{Ann}_R v$. Then $(*)$ is equivalent to the assertion that $R/I \to S/IS$ is injective. Since S/IS is faithfully flat over R/I, we need only show that if $R \to S$ is faithfully flat, it is injective. Let $J \subseteq R$ be the kernel. Then $J \otimes S \cong JS = 0$, which implies that $J = 0$. $\square$

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let $c \in R$.*

(a) *If for every pair of modules (respectively, finitely generated modules) $N \subseteq M$ one has $cN^*_M \subseteq N$, then one also has that whenever $u \in N^*_M$, then $cu^q \in N^{[q]}_M$ for all q. Thus, c is a big test element (respectively, test element) for R if and only if $c \in R^\circ$ and $cN^*_M \subseteq N$ for all inclusions of modules (respectively, finitely generated modules) $N \subseteq M$.*

(b) *If $c \in R^0$, S is faithfully flat over R, and c is (big) test element for S, then it is a (big) test element for R. If c is a completely stable (big) test element for S, then c is a completely stable (big) test element for S.*

(c) *If the image of $c \in R^\circ$ is a (big) test element in R_m for every maximal ideal m of R, then c is a test element for R.*

(d) *If $c \in R^\circ$ and c is a (big) test element for R_P for every prime ideal P of R, then c is a (big) test element for $W^{-1}R$ for every multiplicative system W of R, i.e., c is a locally stable (big) test element for R.*

(e) *If c is a completely stable (big) test element for R then it is a locally stable (big) test element for R.*

Proof. In each part, if we are proving a statement about test elements we assume that $N \subseteq M$ are finitely generated, while if we are proving a statement about big test elements, we allow them to be arbitrary.

(a) If $u \in N^*_M$ we also have that $u^q \in (N^{[q]})^*_{\mathcal{F}^e(M)}$ for all q, and hence that $cu^q \in N^{[q]}$, as required.

(b) Suppose that $u \in N^*_M$. Then $1 \otimes u$ is in $\langle S \otimes_R N\rangle^*$ in $S \otimes_R M$, and it follows that $c(1 \otimes u) = 1 \otimes cu$ is in $\langle S \otimes_R N\rangle$ in $S \otimes_R M$. Because S is faithfully flat over R, it follows from the preceding Lemma that $cu \in N$. The second statement follows from the first, because of P is prime in R and Q is a minimal prime of PS, then $R_P \to S_Q$ is faithfully flat, and hence so is the induced map of completions $\widehat{R_P} \to \widehat{S_Q}$. Since c is a (big) test element for $\widehat{S_Q}$, it is a (big) test element for $\widehat{R_P}$.

(c) Suppose that $u \in N^*_M$ in R. If $cu \notin N$, then there exists a maximal ideal m in the support of $(N + Rcu)/N$. When we pass to R_m, $N_m \subseteq M_m$, and $u/1$, the image of u in M, we still have that $u/1$ is in $(N^m)^*_{M_m}$ working over R_m. If follows that $cu/1 \in N_m$, a contradiction.

(d) follows from (c), because every localization of $W^{-1}R$ at a maximal ideal is a localization of R at some prime ideal P.

(e) follows from (d) and (b), because for every prime ideal P of R, the completion of R_P is faithfully flat over R_P. $\square$

Definition: test ideals. Let R be a Noetherian ring of prime characteristic $p > 0$, and assume that R is reduced. We define $\tau(R)$ to be the set of elements $c \in R$ such that $cN^*_M \subseteq N$ for all inclusion maps $N \subseteq M$ of finitely generated R-modules. Alternatively, we may write:

$$\tau(R) = \bigcap_{N\subseteq M \text{ finitely generated}} N :_R N^*_M,$$

and we also have that

$$N :_R N^*_M = \mathrm{Ann}_R(N^*_M/N).$$

We refer $\tau(R)$ as the *test ideal* of R.

We define $\tau_{\mathrm{b}}(R)$ to be the set of elements $c \in R$ such that $cN^*_M \subseteq N$ for all inclusion maps $N \subseteq M$ of arbitrary R-modules. Alternatively, we may write:

$$\tau_{\mathrm{b}}(R) = \bigcap_{N \subseteq M} N :_R N^*_M,$$

and refer to $\tau_{\mathrm{b}}(R)$ as the *big test ideal* of R, although it is obviously contained in $\tau(R)$. We shall see below that if R has a (big) test element, then $\tau(R)$ (respectively, $\tau_{\mathrm{b}}(R)$) is generated by all the (big) test elements of R. We first note:

Lemma. *Let R be any ring and $P_1, \ldots, P_k$ any finite set of primes of R. Let*

$$W = R - \bigcup_{i=1}^{k} P_i.$$

If an ideal I of R is not contained in any of the P_j, then I is generated by its intersection with W. In particular, if R is Noetherian and I is not contained in any minimal prime of R, then I is generated by its intersection with R°.

Proof. Let J be the ideal generated by all elements of $I \cap W$. Then

$$I \subseteq J \cup P_1 \cup \cdots \cup P_k,$$

since every element of I not in any of the P_i is in J. Since all but one of the ideals on the right is prime, we have that $I \subseteq J$ or $I \subseteq P_i$ for some i. Since I contains at least one element of W, it is not contained in any of the P_i. Thus, $J \subseteq I \subseteq J$, and so $J = I$, as required. The final statement now follows because a Noetherian ring has only finitely many minimal primes. □

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$, and assume that R is reduced.*

(a) $\tau_{\mathrm{b}}(R) \subseteq \tau(R)$.

(b) *$\tau(R) \cap R^\circ$ (respectively, $\tau_{\mathrm{b}}(R) \cap R^\circ$) is the set of test elements (respectively, big test elements) of R.*

(c) *If R has at least one test element (respectively, one big test element), then $\tau(R)$ (respectively, $\tau_{\mathrm{b}}(R)$) is the ideal of R generated by all test elements (respectively, all big test elements) of R.*

Proof. (a) is clear from the definition, and so is (b). Part (c) then follows from the preceding Lemma. □

Math 711: Lecture of September 19, 2007

Earlier (see the Lecture of September 7, p. 7) we discussed very briefly the class of excellent Noetherian rings. The condition that a ring be excellent or, at least, locally excellent, is the right hypothesis for many theorems on tight closure. The theory of excellent rings is substantial enough to occupy an entire course, and we do not want to spend an inordinate amount of time on it here. We shall summarize what we need to know about excellent rings in this lecture. In the sequel, the reader who prefers may restrict attention to rings essentially of finite type over a field or over a complete local ring, which is the most important family of rings for applications. The definition of an excellent Noetherian ring was given by Grothendieck. A readable treatment of the subject, which is a reference for all of the facts about excellent rings stated without proof in this lecture, is [H. Matsumura, *Commutative Algebra,* W.A. Benjamin, New York, 1970], Chapter 13.

Before discussing excellence, we want to review the notion of fibers of ring homomorphisms.

Fibers

Let $f : R \to S$ be a ring homomorphism and let P be a prime ideal of R. We write κ_P for the canonically isomorphic R-algrebras

$$\mathrm{frac}\,(R/P) \cong R_P/PR_P.$$

By the *fiber* of f over P we mean the κ_P-algebra

$$\kappa_P \otimes_R S \cong (R-P)^{-1}S/PS$$

which is also an R-algebra (since we have $R \to \kappa_P$) and an S-algebra. One of the key points about this terminology is that the map

$$\mathrm{Spec}\,(\kappa_P \otimes_R S) \to \mathrm{Spec}\,(S)$$

gives a bijection between the prime ideals of $\kappa_P \otimes_R S$ and the prime ideals of S that lie over $P \subseteq R$. In fact, it is straightforward to check that $\mathrm{Spec}\,(\kappa_P \otimes_R S)$ is homeomorphic with its image in $\mathrm{Spec}\,(S)$.

It is also said that $\mathrm{Spec}\,(\kappa_P \otimes_R S)$ is the *scheme-theoretic* fiber of the map

$$\mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R).$$

This is entirely consistent with thinking of the fiber of a map of sets $g : Y \to X$ over a point $P \in X$ as

$$g^{-1}(P) = \{Q \in Y : g(Q) = P\}.$$

In our case, we may take $g = \mathrm{Spec}\,(f)$, $Y = \mathrm{Spec}\,(S)$, and $X = \mathrm{Spec}\,(R)$, and then $\mathrm{Spec}\,(\kappa_P \otimes_R S)$ may be naturally identified with the set-theoretic fiber of

$$\mathrm{Spec}\,(S) \to \mathrm{Spec}\,(R).$$

If R is a domain, the fiber over the prime ideal (0) of R, namely $\mathrm{frac}\,(R) \otimes_R S$, is called the *generic fiber* of $R \to S$.

If (R, m, K) is quasilocal, the fiber $K \otimes_R S = S/mS$ over the unique closed point m of $\mathrm{Spec}\,(R)$ is called the *closed fiber* of $R \to S$.

Geometric regularity

Let κ be a field. A Noetherian κ-algebra R, is called *geometrically regular* over κ if the following two equivalent conditions hold:

(1) For every finite algebraic field extension κ' of κ, $\kappa' \otimes_\kappa R$ is regular.

(2) For every finite purely inseparable field extension κ' of κ, $\kappa' \otimes_\kappa R$ is regular.

Of course, since we may take $\kappa' = \kappa$, if R is geometrically regular over κ then it is regular. In equal characteristic 0, geometric regularity is equivalent to regularity, using characterization (2).

When R is essentially of finite type over κ, these conditions are also equivalent to

(3) $K \otimes_\kappa R$ is regular for every field K

(4) $K \otimes_\kappa R$ is regular for one perfect field extension K of κ.

(5) $K \otimes_\kappa R$ is regular when $K = \overline{\kappa}$ is the algebraic closure of κ.

These conditions are not equivalent to (1) and (2) in general, because $K \otimes_\kappa R$ need not be Noetherian.

We indicate how the equivalences are proved. This will require a very considerable effort.

Theorem. *Let $R \to S$ be a faithfully flat homomorphism of Noetherian rings. If S is regular, then R is regular.*

Proof. We use the fact that a local ring A is regular if and only its residue class field has finite projective dimension over A, in which case every finitely generated module has finite projective dimension over A. Given a prime P of R, there is a prime Q of S lying over it. It suffices to show that R_P is regular, and we have a faithfully flat map $R_P \to S_Q$. Therefore we may assume that $(R, P, K) \to (S, Q, L)$ is a flat, local homomorphism and that S is regular. Consider a minimal free resolution of R/P over R, which, *a priori*, may be infinite:

$$\cdots \to R^{b_n} \xrightarrow{\alpha_n} R^{b_{n-1}} \to \cdots \xrightarrow{\alpha_1} R^{b_0} \to R/P \to 0.$$

By the minimality of the resolution, the matrices α_j all have entries in P. Now apply $S \otimes_R \_$. We obtain a free resolution

$$\cdots \to S^{b_n} \xrightarrow{\alpha_n} S^{b_{n-1}} \to \cdots \xrightarrow{\alpha_1} S^{b_0} \to S \otimes_R S/PS \to 0,$$

where we have identified R with its image in S under the injection $R \hookrightarrow S$. This resolution of S/PS is minimal: the matrices have entries in Q because $R \hookrightarrow S$ is local. Since S is regular, S/PS has finite projective dimension over S, and so the matrices α_j must be 0 for all $j \gg 0$. But this implies that the projective dimension of R/P over R is finite. □

Corollary. *If R is a Noetherian K-algebra and L is an extension field of K such that $L \otimes_K R$ is regular (in general, this ring may not be Noetherian, although it is if R is essentially of finite type over K, because in that case $L \otimes_K R$ is essentially of finite type over L, and therefore Noetherian), then R is regular.*

Proof. Since L is free over K, it is faithfully flat over K, and so $L \otimes_K R$ is faithfully flat over R and we may apply the preceding result. □

Proposition. *Let $(R, m, K) \to (S, Q, L)$ be a flat local homomorphism of local rings. Then*

(a) $\dim(S) = \dim(R) + \dim(S/mS)$*, the sum of the dimensions of the base and of the closed fiber.*

(b) *If R is regular and S/mS is regular, then S is regular.*

Proof. (a) We use induction on $\dim(R)$. If $\dim(R) = 0$, m and mS are nilpotent. Then $\dim(S) = \dim(S/mS) = \dim(R) + \dim(S/mS)$, as required. If $\dim(R) > 0$, let J be the ideal of nilpotent elements in R. Then $\dim(R/J) = \dim(R)$, $\dim(S/JS) = \dim(S)$, and the closed fiber of $R/J \to S/JS$, which is still a flat and local homomorphism, is S/mS. Therefore, we may consider the map $R/J \to S/JS$ instead, and so we may assume that R is reduced. Since $\dim(R) > 0$, there is an element $f \in m$ not in any minimal prime of R, and, since R is reduced, f is not in any associated prime of R, i.e., f is a nonzerodivisor in R. Then the fact that S is flat over R implies that f is not a zerodivisor in S. We may apply the induction hypothesis to $R/fR \to S/fS$, and so

$$\dim(S) - 1 = \dim(S/fS) = \dim(R/f) + \dim(S/mS) = \dim(R) - 1 + \dim(S/mS),$$

and the result follows.

(b) The least number of generators of Q is at most the sum of the number of generators of m and the number of generators of Q/mS, i.e., it is bounded by $\dim(R)+\dim(S/mS) = \dim(S)$ by part (a). The other inequality always holds, and so S is regular. □

Corollary. *Let $R \to S$ be a flat homomorphism of Noetherian rings. If R is regular and the fibers of $R \to S$ are regular, then S is regular.*

Proof. If Q is any prime of S we may apply part (b) of the preceding Theorem, since S_Q/PS_Q is a localization of the fiber $\kappa_P \otimes_R S$, and therefore regular. $\square$

Corollary. *Let R be a regular Noetherian K-algebra, where K is a field, and let L be a separable extension field of K such that $L \otimes_K R$ is Noetherian. Then $L \otimes_K R$ is regular.*

Proof. The extension is flat, and so it suffices to show that every $\kappa_P \otimes_R (L \otimes_K R) \cong \kappa_P \otimes_K L$ is regular. Since L is algebraic over K, this ring is integral over κ_P and so zero-dimensional. Since $L \otimes_K R$ is Noetherian by hypothesis, $\kappa_P \otimes_K L$ is Noetherian, and so has finitely many minimal primes. Hence, it is Artinian, and if it is reduced, it is a product of fields and, therefore, regular as required. Thus, it suffices to show that $\kappa_P \otimes_K L$ is reduced. Since L is a direct limit of finite separable algebraic extension, it suffices to prove the result when L is a finite separable extension of K. In this case, L has a primitive element θ, and $L \cong K[x]/g$ where $g \in K[x]$ is a monic irreducible separable polynomial over $K \subseteq \kappa_P$. Let Ω denote the algebraic closure of κ_P. Then $\kappa_P \otimes_K L \subseteq \Omega \otimes_K L$, and so it suffices to show that

$$\Omega \otimes_K L \cong \Omega \otimes_K (K[x]/gK[x]) \cong \Omega[x]/g\Omega[x]$$

is reduced. This follows because g is separable, and so has distinct roots in Ω. $\square$

Theorem. *Let K be an algebraically closed field and let L be any finitely generated field extension of K. Then L has a separating transcendence basis $\mathcal{B}$, i.e., a transcendence basis $\mathcal{B}$ such that L is separable over the pure transcendental extension $K(\mathcal{B})$.*

Proof. If F is a subfield of L, let F^{sep} denote the separable closure of F in L. Choose a transcendence basis $x_1, \ldots, x_n$ so as to minimize $[L : L']$ where $L' = K(x_1, \ldots, x_n)^{\mathrm{sep}}$. Suppose that $y \in L$ is not separable over $K(x_1, \ldots, x_n)$. Choose a minimal polynomial $F(z)$ for y over $K(x_1, \ldots, x_n)$. Then every exponent on z is divisible by p. Put each coefficient in lowest terms, and multiply $F(z)$ by a least common multiple of the denominators of the coefficients. This yields a polynomial $H(x_1, \ldots, x_n, z) \in K[x_1, \ldots, x_n][z]$ such that the coefficients in $K[x_1, \ldots, x_n]$ are relatively prime, and such that the polynomial is irreducible over $K(x_1, \ldots, x_n)[z]$. By Gauss's Lemma, this polynomial is irreducible in $K[x_1, \ldots, x_n, z]$. It cannot be the case that every exponent on every x_j is divisible by p, for if that were true, since the field is perfect, H would be a pth power, and not irreducible. By renumbering the x_i we may assume that x_n occurs with an exponent not divisible by p. Then the element x_n is separable algebraic over the field $K(x_1, \ldots, x_{n-1}, y)$, and we may use the transcendence basis $x_1, \ldots, x_{n-1}, y$ for L. Note that $x_n, y \in K(x_1, \ldots, x_{n-1}, y)^{\mathrm{sep}} = L''$, which is therefore strictly larger than $L' = K(x_1, \ldots, x_n)^{\mathrm{sep}}$. Hence, $[L : L''] < [L : L']$, a contradiction. $\square$

We can now prove:

Theorem. *Let R be a Noetherian κ-algebra, where κ is a field. Then the following two conditions are equivalent:*

(1) *For every finite algebraic field extension κ' of κ, $\kappa' \otimes_\kappa R$ is regular.*

(2) *For every finite purely inseparable field extension κ' of κ, $\kappa' \otimes_\kappa R$ is regular.*

Moreover, if R is essentially of finite type over κ then the following three conditions are equivalent to (1) and (2) as well:

(3) *$K \otimes_\kappa R$ is regular for every field K*

(4) *$K \otimes_\kappa R$ is regular for one perfect field extension K of κ.*

(5) *$K \otimes_\kappa R$ is regular when $K = \overline{\kappa}$ is the algebraic closure of κ.*

Proof. We shall repeatedly use that if we have regularity for a larger field extension, then we also have it for a smaller one: this follows from the Corollary on p. 3.

Evidently, (1) $\Rightarrow$ (2). But (2) $\Rightarrow$ (1) as well, because given any finite algebraic extension κ' of κ, there is a larger finite field extension obtained by first making a finite purely inseparable extension and then a finite separable extension. The purely inseparable extension yields a regular ring by hypothesis, and the separable field extension yields a regular ring by the second Corollary on p. 4.

Now consider the case where R is essentially of finite type over κ. Evidently, (3) $\Rightarrow$ (5) $\Rightarrow$ (4) $\Rightarrow$ (2) (the last holds because any perfect field extension contains the perfect closure, and this contains every finite purely inseparable algebraic extension), and it will suffice to prove that (2) $\Rightarrow$ (3).

Let κ^∞ denote the perfect closure $\bigcup_q \kappa^{1/q}$ of κ. We first show that $\kappa^\infty \otimes_\kappa R$ is regular. Replace R by R_m. Then $B = \kappa^\infty \otimes_R R_m$ is purely inseparable over R_m: consequently, it is a local ring of the same dimension as R_m, and it is the directed union of the local rings $\kappa' \otimes_\kappa R_m$ as κ' runs through finite purely inseparable extensions of κ contained in κ^∞. All of these local rings have the same dimension: call it d. Let $u_1, \ldots, u_n$ be a minimal set of generators of the maximal ideal of $B = \kappa^\infty \otimes_\kappa R_m$, and choose κ' sufficiently large that $u_1, \ldots, u_n$ are elements of $A = \kappa' \otimes_R R_m$. Let $J = (u_1, \ldots, u_n)A$. Since B is faithfully flat over A, we have that $JB \cap A = J$. But JB is the maximal ideal of B, which lies over the maximal ideal of A, and so J generates the maximal ideal of A. None of the generators is an A-linear combination of the others, or else this would also be true in B. Hence, $u_1, \ldots, u_n$ is a minimal set of generators of the maximal ideal of A. Since A is regular, $n = d$, and so B is regular.

Since the algebraic closure of κ is separable over κ^∞, it follows from the second Corollary on p. 4 that (2) $\Rightarrow$ (5). To complete the proof, it suffices to show that if κ is algebraically closed, R is regular, and L is any field extension of κ, then $L \otimes_\kappa R$ is regular. Since $R \to L \otimes_\kappa R$ is flat, it suffices to show the fibers $L \otimes_\kappa \kappa_P$ are regular, and κ_P is finitely generated as a field over κ. Hence, κ_P has a separating transcendence basis $x_1, \ldots, x_n$

over κ. Let $K = \kappa(x_1, \ldots, x_n)$. Then

$$L \otimes_\kappa \kappa_P = (L \otimes_\kappa \kappa(x_1, \ldots, x_n)) \otimes_K \kappa_P.$$

Since κ_P is a finite separable algebraic extension of K, it suffices prove that $L \otimes_\kappa K$ is regular. But this ring is a localization of $L[x_1, \ldots, x_n]$, and so the proof is complete. □

We say that a homomorphism $R \to S$ of Noetherian rings is *geometrically regular* if it is flat and all the fibers $\kappa_P \to \kappa_P \otimes_R S$ are geometrically regular. (Some authors use the term "regular" for this property.)

For those readers familiar with *smooth homomorphisms*, we mention that if S is essentially of finite type over R, then S is geometrically regular if and only if it is smooth.

By a very deep result of Popescu (cf. [D. Popescu, *General Néron desingularization,* Nagoya Math. J. **100** (1985) 97–126], every geometrically regular map is a direct limit of smooth maps. Whether Popescu's argument was correct was controversial for a while. Richard Swan showed that Popescu's argument was essentially correct in [R. G Swan, *Néron-Popescu desingularization,* Algebra and geometry (Taipei, 1995), 135–192, Lect. Algebra Geom. **2** Int. Press, Cambridge, MA, 1998].

Catenary and universally catenary rings

A Noetherian ring is called *catenary* if for any two prime ideals $P \subseteq Q$, any two saturated chains of primes joining P to Q have the same length. In this case, the common length will be the same as the dimension of the local domain R_Q/PR_Q.

Nagata was the first to give examples of Notherian rings that are not catenary. E.g., in [M. Nagata, *Local Rings*, Interscience, New York, 1962] Appendix, pp. 204–5, Nagata gives an example of a local domain (D, m) of dimension 3 containing a height one prime P such that $\dim(D/P) = 1$, so that $(0) \subset Q \subset m$ is a saturated chain, while the longest saturated chains joining (0) to m have the form $(0) \subset P_1 \subset P_2 \subset m$. One has to work hard to construct Noetherian rings that are not catenary. Nagata also gives an example of a ring R that is catenary, but such that $R[x]$ is not catenary.

Notice that a localization or homomorphic image of a catenary ring is automatically catenary.

R is called *universally catenary* if every polynomial ring over R is catenary. This implies that every ring essentially of finite type over R is catenary.

A very important fact about Cohen-Macaulay rings is that they are catenary. Moreover, a polynomial ring over a Cohen-Macaulay ring is again a Cohen-Macaulay ring, which then implies that every Cohen-Macaulay ring is universally catenary. In particular, regular rings are universally catenary. Cohen-Macaulay local rings have a stronger property: they are equidimensional, and all saturated chains from a minimal prime to the maximal ideal have length equal to the dimension of the local ring.

We shall prove the statements in the paragraph above. We first note:

Theorem. *If R is Cohen-Macaulay, so is the polynomial ring in n variables over R.*

Proof. By induction, we may assume that $n = 1$. Let $\mathcal{M}$ be a maximal ideal of $R[X]$ lying over m in R. We may replace R by R_m and so we may assume that (R, m, K) is local. Then $\mathcal{M}$, which is a maximal ideal of $R[x]$ lying over m, corresponds to a maximal ideal of $K[x]$: each of these is generated by a monic irreducible polynomial f, which lifts to a monic polynomial F in $R[x]$. Thus, we may assume that $\mathcal{M} = mR[x] + FR[X]$. Let $x_1, \ldots, x_d$ be a system of parameters in R, which is also a regular sequence. We may kill the ideal generated by these elements, which also form a regular sequence in $R[X]_{\mathcal{M}}$. We are now in the case where R is an Artin local ring. It is clear that the height of $\mathcal{M}$ is one. Because F is monic, it is not a zerodivisor: a monic polynomial over any ring is not a zerodivisor. This shows that the depth of $\mathcal{M}$ is one, as needed. $\square$

Theorem. *Let (R, m, K) be a local ring and $M \neq 0$ a finitely generated Cohen-Macaulay R-module of Krull dimension d. Then every nonzero submodule N of M has Krull dimension d.*

Proof. We replace R by $R/\mathrm{Ann}_R M$. Then every system of parameters for R is a regular sequence on M. We use induction on d. If $d = 0$ there is nothing to prove. Assume $d > 0$ and that the result holds for smaller d. If M has a submodule $N \neq 0$ of dimension $\leq d - 1$, we may choose N maximal with respect to this property. If N' is any nonzero submodule of M of dimension $< d$, then $N' \subseteq N$. To see this, note that $N \oplus N'$ has dimension $< d$, and maps onto $N + N' \subseteq M$, which therefore also has dimension $< d$. By the maximality of N, we must have $N + N' = N$. Since M is Cohen-Macaulay and $d \geq 1$, we can choose $x \in m$ not a zerodivisor on M, and, hence, also not a zerodivisor on N. We claim that x is not a zerodivisor on $\overline{M} = M/N$, for if $u \in M - N$ and $xu \in N$, then $Rxu \subseteq N$ has dimension $< d$. But this module is isomorphic with $Ru \subseteq M$, since x is not a zerodivisor, and so $\dim(Ru) < d$. But then $Ru \subseteq N$. Consequently, multiplication by x induces an isomorphism of the exact sequence $0 \to N \to M \to \overline{M} \to 0$ with the sequence $0 \to xN \to xM \to x\overline{M} \to 0$, and so this sequence is also exact. But we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & \overline{M} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & xN & \longrightarrow & xM & \longrightarrow & x\overline{M} & \longrightarrow & 0 \end{array}$$

where the vertical arrows are inclusions. By the nine lemma, or by an elementary diagram chase, the sequence of cokernels $0 \to N/xN \to M/xM \to \overline{M}/x\overline{M} \to 0$ is exact. Because x

is not a zerodivisor on M, it is part of a system of parameters for R, and can be extended to a system of parameters of length d, which is a regular sequence on M. Since x is a nonzerodivisor on N and M, $\dim(N/xN) = \dim(N) - 1 < d - 1$, while M/xM is Cohen-Macaulay of dimension $d - 1$. This contradicts the induction hypothesis. □

Corollary. *If (R, m, K) is Cohen-Macaulay, R is equidimensional: every minimal prime $\mathfrak{p}$ is such that $\dim(R/\mathfrak{p}) = \dim(R)$.*

Proof. If $\mathfrak{p}$ is minimal, it is an associated prime of R, and we have $R/\mathfrak{p} \hookrightarrow R$. Since all nonzero submodules of R have dimension $\dim(R)$, the result follows. □

Thus, a Cohen-Macaulay local ring cannot exhibit the kind of behavior one observes in $R = K[[x, y, z]]/\big((x, y) \cap (z)\big)$: this ring has two minimal primes. One of them, $\mathfrak{p}_1$, generated by the images of x and y, is such that $R/\mathfrak{p}_1$ has dimension 1. The other, $\mathfrak{p}_2$, generated by the image of z, is such that $R/\mathfrak{p}_2$ has dimension 2. Note that while R is not equidimensional, it is still catenary.

We next observe:

Theorem. *In a Cohen-Macaulay ring R, if $P \subseteq Q$ are prime ideals of R then every saturated chain of prime ideals from P to Q has length* $\mathrm{height}(Q) - \mathrm{height}(P)$. *Thus, R is catenary.*

It follows that every ring essentially of finite type over a Cohen-Macaulay ring is universally catenary.

Proof. The issues are unaffected by localizing at Q. Thus, we may assume that R is local and that Q is the maximal ideal. There is part of a system of parameters of length $h = \mathrm{height}(P)$ contained in P, call it $x_1, \ldots, x_h$, by the Corollary near the bottom of p. 7 of the Lecture Notes of Septermber 5. This sequence is a regular sequence on R and so on R_P, which implies that its image in R_P is system of parameters. We now replace R by $R/(x_1, \ldots, x_h)$: when we kill part of a system of parameters in a Cohen-Macaulay ring, the image of the rest of that system of parameters is both a system of parameters and a regular sequence in the quotient. Thus, R remains Cohen-Macaulay. Q and P are replaced by their images, which have heights $\dim(R) - h$ and 0, and $\dim(R) - h = \dim\big(R/(x_1, \ldots, x_h)\big)$. We have therefore reduced to the case where (R, Q) is local and P is a minimal prime.

We know that $\dim(R) = \dim(R/P)$, and so at least one saturated chain from P to Q has length $\mathrm{height}(Q) - \mathrm{height}(P) = \mathrm{height}(Q) - 0 = \dim(R)$. To complete the proof, it will suffice to show that all saturated chains from P to Q have the same length, and we may use induction on $\dim(R)$. Consider two such chains, and let their smallest elements other than P be P_1 and P_1'. We claim that both of these are height one primes: if, say, P_1 is not height one we can localize at it and obtain a Cohen-Macaulay local ring (S, m) of dimension at least two and a saturated chain $\mathfrak{p} \subseteq m$ with $\mathfrak{p} = PS$ minimal in S. Choose an element $y \in m$ that is not in any minimal primes of S: its image will be a system of parameters for $S/\mathfrak{p}$, so that $Ry + \mathfrak{p}$ is m-primary. Extend y to a regular sequence of length two in S: the second element has a power of the form $ry+u$, so that y, $ry+u$ is a regular sequence, and, hence, so is y, u. But then u, y is a regular sequence, a contradiction, since $u \in \mathfrak{p}$. Thus, P_1 (and, similarly, P_1'), have height one.

Choose an element f in P_1 not in any minimal prime of R, and an element g of P_1' not in any minimal prime of R. Then fg is a nonzerodivisor in R, and P_1, P_1' are both minimal primes of xy. The ring $R/(xy)$ is Cohen-Macaulay of dimension $\dim(R) - 1$. The result now follows from the induction hypothesis applied to $R/(xy)$: the images of the two saturated chains (omitting P from each) give saturated chains joining $P_1/(xy)$ (respectively, $P_1'/(xy)$) to $Q/(xy)$ in $R/(xy)$. These have the same length, and, hence, so did the original two chains.

The final statement now follows because a polynomial ring over a Cohen-Macaulay ring is again Cohen-Macaulay. □

Excellent rings

A Noetherian ring R is called a *G-ring* ("G" as in "Grothendieck") if for every local ring A of R, the map $A \to \widehat{A}$ is geometrically regular.

An *excellent* ring is a universally catenary Noetherian G-ring R such that in every finitely generated R-algebra S, the regular locus $\{P \in \mathrm{Spec}\,(S) : S_P \text{ is regular}\}$ is Zariski open.

Excellent rings include the integers, fields, and complete local rings, as well as convergent power series rings over $\mathbb{C}$ and $\mathbb{R}$. Every discrete valuation ring of equal characteristic 0 or of mixed characteristic is excellent. The following two results contain most of what we need to know about excellent rings.

Theorem. *Let R be an excellent ring. Then every localization of R, every homomorphic image of R, and every finitely generated R-algebra is excellent. Hence, every algebra essentially of finite type over R is excellent.*

Theorem. *Let R be an excellent ring.*

(a) *If R is reduced, the normalization of R is module-finite over R.*

(b) *If R is local and reduced, then $\widehat{R}$ is reduced.*

(c) *If R is local and equidimensional, then $\widehat{R}$ is equidimensional.*

(d) *If R is local and normal, then $\widehat{R}$ is normal.*

For proofs of these results, we refer the reader to [H. Matsumura, *Commutative Algebra,* W.A. Benjamin, New York, 1970], as mentioned earlier.

Note that one does not expect the completion of an excellent local doman to be a domain. For example, consider the one-dimensional domain S $= \mathbb{C}[x, y]/(y^2 - x^2 - x^3)$. This is a domain because $x^2 + x^3$ is not a perfect square in $\mathbb{C}[x, y]$ (and, hence, not in its fraction field either, since $\mathbb{C}[x, y]$ is normal). If $m = (x, y)S$, then S_m is a local domain of dimension one. The completion of this ring is $\cong \mathbb{C}[[x, y]]/(y^2 - x^2 - x^3)$. This ring is not a domain: the point is that $x^2 + x^3 = x^2(1 + x)$ is a perfect square in the formal power series ring. Its square root may be written down explicitly using Newton's binomial theorem. Alternatively, one may see this using Hensel's Lemma: see p. 2 of the lecture notes of March 21 from Math 615, Winter 2007.

One does have from parts (b) and (c) of the Theorem above that the completion of an excellent local domain is reduced and equidimensional.

Example: a DVR that is not excellent. Let K be a perfect field of prime characteristic $p > 0$, and let

$$t_1, t_2, t_3, \ldots, t_n, \ldots$$

be countably many indeterminates over K. Let

$$L = K(t_1, \ldots, t_n, \ldots),$$

and let $L_n = L^p(t_1, \ldots, t_n)$, which contains the p th power of every t_j and the first powers of $t_1, \ldots, t_n$. Let x be a formal indeterminate, and let $V_n = L_n[[x]]$, a DVR in which every nonzero element is a unit times a power of x. Let

$$V = \bigcup_{n=1}^{\infty} V_n,$$

which is also a DVR in which every element is unit times a power of x. V has residue field L, and $\widehat{V} \cong L[[x]]$, but V only contains those power series such that all coefficients lie in a fixed choice of L_n. For example,

$$f = t_1 x + t_2 x^2 + \cdots + t_n x^n + \cdots \in \widehat{V} - V.$$

Note that the p th power of every element of $\widehat{V}$ is in V. Thus, the generic fiber

$$\mathcal{K} = \mathrm{frac}\,(V) \to \mathrm{frac}\,(\widehat{V}) = \mathcal{L}$$

is a purely inseparable field extension, and is *not* geometrically regular. The ring

$$\mathcal{K}[f] \otimes_{\mathcal{K}} \mathcal{L}$$

is not even reduced: $f \otimes 1 - 1 \otimes f$ is a nonzero nilpotent. Thus, V is not a G-ring.

Math 711: Lecture of September 21, 2007

F-finite rings

Let R be a Noetherian ring of prime characteristic $p > 0$. R is called *F-finite* if the Frobenius endomorphism $F : R \to R$ makes R into a module-finite R-algebra. This is equivalent to the assertion that R is module-finite over the subring $F(R) = \{r^p : r \in R\}$, which may also be denoted R^p. When R is reduced, this is equivalent to the condition that $R^{1/p}$ is module-finite over R, since in the reduced case the inclusion $R \subseteq R^{1/p}$ is isomorphic to the homomorphism $F : R \to R$.

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$.*

(a) *R is F-finite if and only if R_{red} is F-finite.*

(b) *R is F-finite if and only and only if $F^e : R \to R$ is module-finite for all e if and only if $F^e : R \to R$ is module-finite for some $e \geq 1$.*

(c) *If R is F-finite, so is every homomorphic image of R.*

(d) *If R is F-finite so is every localization of R.*

(e) *If R is F-finite, so is every algebra finitely generated over R.*

(f) *If R is F-finite, so is the formal power series ring $R[[x_1, \ldots, x_n]]$.*

(g) *If (R, m, K) is a complete local ring, R is F-finite if and only if the field K is F-finite.*

(h) *If R is F-finite, so is every ring essentially of finite type over R.*

(i) *If K is a field that is finitely generated as a field over a perfect field, then every ring essentially of finite type over K is F-finite.*

Proof. Parts (c) and (d) both follow from the fact that if B is a finite set of generators for R as $F(R)$-module, the image of B in S will generate S over $F(S)$ if $S = R/J$ and also if $S = W^{-1}R$. In the second case, it should be noted that $F(W^{-1}R)$ may be identified with $W^{-1}F(R)$ because localizing at w and a w^p have the same effect.

For part (a), note that if R is F-finite, so is R_{red} by part (c), since $R_{\mathrm{red}} = R/J$, where J is the ideal of all nilpotent elements. Now suppose that I is any ideal of R such that R/I is F-finite. Let the images of $u_1, \ldots, u_n$ span R/I over the image of $(R/I)^p$, and let $v_1, \ldots, v_h$ generate I over R. Let $A = R^p u_1 + \cdots + R^p u_n$. Then $R = A + Rv_1 + \cdots + Rv_h$. If we substitute the same formula for each copy of R occuring in an Rv_j term on the right, we find thtat

$$R = A + \sum_{i,j} R^p u_i v_j + \sum_{j,j'} R v'_j v_j.$$

It follows that the $n + nh$ elements u_i and $u_i v_j$ span R/I^2 over the image of $(R/I^2)^p$. Thus, (R/I^2) is F-finite. By a straightforward induction, R/I^{2^k} is F-finite for all k. Hence if $I = J$ is the ideal of nilpotents, we see that R itself is F-finite.

For part (b), note that if $F : R \to R$ is F-finite, so is the e-fold composition. On the other hand, if $F^e : R \to R$ is finite, so is $F^e : S \to S$, where $S = R_{\text{red}}$. Then we have $S \subseteq S^{1/p} \subseteq S^{1/q}$, and since $S^{1/q}$ is a Noetherian S-module, so is $S^{1/p}$. Thus, S is F-finite, and so is R by part (a).

To prove (e), it suffices to consider the case of a polynomial ring in a finite number of variables over R, and, by induction it suffices to consider the case where $S = R[x]$. Likewise, for part (f) we need only show that $R[[x]]$ is F-finite. Let $u_1, \ldots, u_n$ span R over R^p. Then, in both cases, the elements $u_i x^j$, $1 \le i \le n$, $1 \le j \le p-1$, span S over $S^p = R^p[x^p]$ (respectively, $R^p[[x^p]]$).

For (g), note that $K = R/m$, so that if (R, m, K) is F-finite, so is K. If R is complete it is a homomorphic image of a formal power series ring $K[[x_1, \ldots, x_n]]$, where K is the residue class field of R. By part (f), if K is F-finite, so is R.

Part (h) is immediate from parts (e) and (d). For part (i) first note that K itself is essentially of finite type over a perfect field, and a perfect field is obviously F-finite. The final statement is then immediate from part (h). □

A proof of the following result of Ernst Kunz would take us far afield. We refer the reader to [E. Kunz, *On Noetherian rings of characteristic p*, Amer. J. Math. **98** (1976) 999–1013].

Theorem (Kunz). *Every F-finite ring is excellent.*

We are aiming to prove the following result about F-finite rings:

Theorem (existence of test elements). *Let R be a reduced F-finite ring, and let $c \in R^\circ$ be such that R_c is regular. Then c has a power c^N that is a completely stable big test element.*

This is terrifically useful. Elements $c \in R^\circ$ such that R_c is regular always exist. In any excellent ring,
$$\{P \in \operatorname{Spec}(R) : R_P \text{ is regular}\}$$
is open. Since the complement is closed, there is an ideal I such that
$$\mathcal{V}(I) = \{P \in \operatorname{Spec}(R) : R_P \text{ is not regular}\}.$$
We refer to this set of primes as the *singular locus* of $\operatorname{Spec}(R)$ or of R. Note that if R is reduced, we cannot have $I \subseteq \mathfrak{p}$ for any minimal prime $\mathfrak{p}$ of R, because that would mean the $R_{\mathfrak{p}}$ is not regular, and $R_{\mathfrak{p}}$ is a field. Hence, I is not contained in the union of the minimal primes of R, which means that I meets R°. If $c \in I \cap R^\circ$, then R_c is regular: primes that do not contain c cannot contain I. Hence, in a reduced F-finite (or any reduced excellent) ring, there is always an element $r \in R^\circ$ such that R_c is regular, and this means that Theorem above can be applied. Hence:

Corollary. *Every reduced F-finite ring has a completely stable big test element.*

It will take some time before we can prove the Theorem on existence of test elements. Our approach requires studying the notion of a *strongly F-regular* ring. We give the definition below. However, we first want to comment on the notion of an *F-split* ring.

Definition: F-split rings. Let R be a ring of prime characteristic $p > 0$. We shall say that R is *F-split* if, under the map $F : R \to R$, the left hand copy of R is a direct summand of the right hand copy of R.

If R is F-split, $F : R \to R$ must be injective. This is equivalent to the condition that R be reduced. An equivalent condition is therefore that R be reduced and that R be a direct summand of $R^{1/p}$ as an R-module, i.e., there exists an R-linear map $\theta : R^{1/p} \to 1$ such that $\theta(1) = 1$.

Proposition. *Let R be a reduced ring of prime characteristic $p > 0$. The following conditions are equivalent:*

(1) *R is F-split.*

(2) *$R \to R^{1/q}$ splits as a map of R-modules for all q.*

(3) *$R \to R^{1/q}$ splits as a map of R-modules for at least one value of $q > 1$.*

Proof. (1) $\Rightarrow$ (2). Let $\theta : R^{1/p} \to R$ be a splitting. Then for all $q = p^e > 1$, if $q' = p^{e-1}$, we may define a splitting $\theta_e : R^{1/q} \to R^{1/q'}$ by

$$\theta_e(r^{1/q}) = \big(\theta(r^{1/p})\big)^{1/q'}.$$

Thus, the diagram:

$$\begin{array}{ccc} R^{1/q} & \xrightarrow{\theta_e} & R^{1/q'} \\ \cong\big\uparrow & & \cong\big\uparrow \\ R^{1/p} & \xrightarrow{\theta} & R \end{array}$$

commutes, where the vertical arrows are the isomorphisms $r^{1/p} \mapsto r^{1/q}$ and $r \mapsto r^{1/q'}$, respectively. Of course, $\theta_1 = \theta$. Then θ_e is $R^{1/q'}$-linear and, in particular, R-linear. Hence, the composite map

$$\theta_1 \circ \theta_2 \circ \cdots \circ \theta_e : R^{1/q} \to R$$

gives the required splitting.

(2) $\Rightarrow$ (3) is clear. Finally, assume (3). Then $R \subseteq R^{1/p} \subseteq R^{1/q}$, so that a splitting $R^{1/q} \to R$ may simply be restricted to $R^{1/p}$, and (1) follows. $\square$

Strongly F-regular rings

We have defined a ring to be weakly F-regular if every ideal is tightly closed, and to be F-regular if all of its localizations have this property as well. We next want to introduce the notion of a *strongly F-regular ring* R: for the moment, we make this definition only when R is F-finite.

The definition is rather technical, but this condition turns out to be easier to work with than the other notions. It implies that every submodule of every module is tightly closed, it passes to localizations automatically, and it leads to a proof of the Theorem on existence of test elements stated on p. 2.

Of course, the value of this notion rests on whether there are examples of strongly F-regular rings. We shall soon see that every regular F-finite ring is strongly F-regular. Let $1 \leq t \leq r \leq s$ be integers. If K is an algebraically closed field (or an F-finite field), and X is an $r \times s$ matrix of indeterminates over K, then the ring obtained from the polynomial ring $K[X]$ in the entries of X by killing the ideal $I_t(X)$ generated by the $t \times t$ minors of X is strongly F-regular, and so is the ring generated over K by the $r \times r$ minors of X (this is the homogeneous coordinate ring of a Grassman variety). The normal rings generated by finitely many monomials in indeterminates are also strongly F-regular. Thus, there are many important examples.

In fact, in the F-finite case, every ring that is known to be weakly F-regular is known to be strongly F-regular.

Conjecture. *Every weakly F-regular F-finite ring is strongly F-regular.*

This is a very important open question. It is known to be true in many cases: we shall discuss what is known at a later point.

Definition: strong F-regularity. Let R be a Noetherian ring of prime characteristic $p > 0$, and suppose that R is reduced and F-finite. We define R to be *strongly F-regular* if for every $c \in R^\circ$ there exists q_c such that the map $R \to R^{1/q_c}$ that sends $1 \mapsto c^{1/q_c}$ splits over R. That is, for all $c \in R^\circ$ there exist q_c and an R-linear map $\theta : R^{1/q_c} \to R$ such that $\theta(c^{1/q_c}) = 1$.

The element q_c will usually depend on c. For example, one will typically need to make a larger choice for c^p than for c.

Remark. The following elementary fact is very useful. Let $h : R \to S$ be a ring homomorphism and let M be any S-module. Let u be any element of M. Suppose that the unique R-linear map $R \to M$ such that $1 \mapsto u$ (and $r \mapsto ru$) splits over R. Then R is a direct summand of S, i.e., there is an R-module splitting for $h : R \to S$. In fact, if $\theta : M \to R$ is R-linear and $\theta(u) = 1$, we get the required splitting by defining $\phi(s) = \theta(su)$ for all $s \in S$. Note also that the fact that $R \to M$ splits is equivalent to the assertion that $R \to Ru$

such that $1 \mapsto u$ is an isomorphism of R-modules, together with the assertion that Ru is a direct summand of M as an R-module.

We may apply this remark to the case where $S = R^{1/q_c}$ in the above definition. Thus:

Proposition. *A strongly F-regular ring R is F-split.*

We also note:

Proposition. *Suppose that R is a reduced Noetherian ring of prime characteristic $p > 0$, that $c \in R^\circ$, and that $R \to R^{1/q_c}$ sending $1 \mapsto c^{1/q_c}$ splits over R. Then for all $q \geq q_c$, the map $R \to R^{1/q}$ sending $1 \mapsto c^{1/q}$ splits over R.*

Proof. It suffices to show that if we have a splitting for a certain q, we also get a splitting for the next higher value of q, which is qp. Suppose that $\theta : R^{1/q} \to R$ is R-linear and $\theta(c^{1/q}) = 1$. We define $\theta' : R^{1/pq} \to R^{1/p}$ by the rule

$$\theta'(r^{1/pq}) = \big(\theta(r^{1/q})\big)^{1/p}.$$

That is, the diagram

$$\begin{array}{ccc} R^{1/pq} & \xrightarrow{\theta'} & R^{1/p} \\ \cong\big\uparrow & & \cong\big\uparrow \\ R^{1/q} & \xrightarrow{\theta} & R \end{array}$$

commutes. Then θ' is $R^{1/p}$-linear and $\theta'(c^{1/pq}) = 1 \in R^{1/p}$. By the Remark beginning on the bottom of p. 4, $R \to R^{1/q}$ splits, and so R is F-split, i.e., we have an R-linear map $\beta : R^{1/p} \to R$ such that $\beta(1) = 1$. Then $\beta \circ \theta'$ is the required splitting. $\square$

The following fact is now remarkably easy to prove.

Theorem. *Let R be a strongly F-regular ring. Then for every inclusion of $N \subseteq M$ of modules (these are not required to be finitely generated), N is tightly closed in M.*

Proof. We may map a free module G onto M and replace N by its inverse image $H \subseteq G$. Thus, it suffices to show that $H = H^*_G$ when G is free. Suppose that $u \in H^*_G$. We want to prove that $u \in H$. Since $u \in H^*_G$, for all $q \gg 0$, $cu^q \in H^{[q]}$. Choose q_c such that $R \to R^{1/q_c}$ with $1 \mapsto c^{1/q_c}$ splits. Then fix $q \geq q_c$ such that $cu^q \in H^{[q]}$. Then the map $R \to R^{1/q}$ sending $1 \to c^{1/q}$ also splits, and we can choose $\theta : R^{1/q} \to R$ such that $\theta(c^{1/q}) = 1$.

The fact that $cu^q \in H^{[q]}$ gives an equation

$$cu^q = \sum_{i=1}^{n} r_i h_i^q$$

with the $r_i \in R$ and the $h_i \in H$. We work in $R^{1/q} \otimes_R G$ and take q th roots to obtain

$$(*) \quad c^{1/q}u = \sum_{i=1}^{n} r_i^{1/q} h_i.$$

We have adopted the notation $r^{1/q}g$ for $r^{1/q} \otimes g$. By tensoring with G, from the R-linear map $\theta : R^{1/q} \to R$ we get an R-linear map $\theta' : R^{1/q} \otimes G \to G$ such that $\theta'(r^{1/q}g) = \theta(r^{1/q})g$ for all $g \in G$. We may now apply θ' to $(*)$ to obtain

$$u = 1 \cdot u = \theta(c^{1/q})u = \sum_{i=1}^{n} \theta(r_i^{1/q})h_i.$$

Since every $\theta(r_i^{1/q}) \in R$, the right hand side is in H, i.e., $u \in H$. □

Corollary. *A strongly F-regular ring is weakly F-regular and, in particular, normal.* □

Math 711: Lecture of September 24, 2007

Flat base change and Hom

We want to discuss in some detail when a short exact sequence splits. The following result is very useful.

Theorem (Hom commutes with flat base change). *If S is a flat R-algebra and M, N are R-modules such that M is finitely presented over R, then the canonical homomorphism*

$$\theta_M : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N)$$

sending $s \otimes f$ to $s(\mathbf{1}_S \otimes f)$ is an isomorphism.

Proof. It is easy to see that θ_R is an isomorphism and that $\theta_{M_1 \oplus M_2}$ may be identified with $\theta_{M_1} \oplus \theta_{M_2}$, so that θ_G is an isomorphism whenever G is a finitely generated free R-module.

Since M is finitely presented, we have an exact sequence $H \to G \twoheadrightarrow M \to 0$ where G, H are finitely generated free R-modules. In the diagram below the right column is obtained by first applying $S \otimes_R \_$ (exactness is preserved since $\otimes$ is right exact), and then applying $\mathrm{Hom}_S(\_, S \otimes_R N)$, so that the right column is exact. The left column is obtained by first applying $\mathrm{Hom}_R(\_, N)$, and then $S \otimes_R \_$ (exactness is preserved because of the hypothesis that S is R-flat). The squares are easily seen to commute.

$$\begin{array}{ccc}
S \otimes_R \mathrm{Hom}_R(H, N) & \xrightarrow{\theta_H} & \mathrm{Hom}_S(S \otimes_R H, S \otimes_R N) \\
\uparrow & & \uparrow \\
S \otimes_R \mathrm{Hom}_R(G, N) & \xrightarrow{\theta_G} & \mathrm{Hom}_S(S \otimes_R G, S \otimes_R N) \\
\uparrow & & \uparrow \\
S \otimes_R \mathrm{Hom}_R(M, N) & \xrightarrow{\theta_M} & \mathrm{Hom}_S(S \otimes_R M, S \otimes_R N) \\
\uparrow & & \uparrow \\
0 & \longrightarrow & 0
\end{array}$$

From the fact, established in the first paragraph, that θ_G and θ_H are isomorphisms and the exactness of the two columns, it follows that θ_M is an isomorphism as well (kernels of isomorphic maps are isomorphic). $\square$

Corollary. *If W is a multiplicative system in R and M is finitely presented, we have that* $W^{-1}\mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{W^{-1}R}(W^{-1}M, W^{-1}N)$.

Moreover, if (R, m) is a local ring and both M, N are finitely generated, we may identify $\mathrm{Hom}_{\widehat{R}}(\widehat{M}, \widehat{N})$ *with the m-adic completion of* $\mathrm{Hom}_R(M, N)$ *(since m-adic completion is the same as tensoring over R with $\widehat{R}$ (as covariant functors) on finitely generated R-modules).* $\square$

When does a short exact sequence split?

Throughout this section, $0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} Q \longrightarrow 0$ is a short exact sequence of modules over a ring R. There is no restriction on the characteristic of R. We want to discuss the problem of when this sequence splits. One condition is that there exist a map $\eta : M \to N$ such that $\eta\alpha = \mathbf{1}_N$. Let $Q' = \mathrm{Ker}\,(\eta)$. Then Q' is disjoint from the image $\alpha(N) = N'$ of N in M, and $N' + Q' = M$. It follows that M is the internal direct sum of N' and Q' and that β maps Q' isomorphically onto Q.

Similarly, the sequence splits if there is a map $\theta : Q \to M$ such that $\beta\theta = \mathbf{1}_Q$. In this case let $N' = \alpha(N)$ and $Q' = \theta(Q)$. Again, N' and Q' are disjoint, and $N' + Q' = M$, so that M is again the internal direct sum of N' and Q'.

Proposition. *Let R be an arbitrary ring and let*

$$(\#) \quad 0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} Q \longrightarrow 0$$

be a short exact sequence of R-modules. Consider the sequence

$$(*) \quad 0 \longrightarrow \mathrm{Hom}_R(Q,\, N) \xrightarrow{\alpha_*} \mathrm{Hom}_R(Q,\, M) \xrightarrow{\beta_*} \mathrm{Hom}_R(Q,\, Q) \longrightarrow 0$$

which is exact except possibly at $\mathrm{Hom}_R(Q,\, Q)$*, and let* $C = \mathrm{Coker}\,(\beta_*)$*. The following conditions are equivalent:*

(1) *The sequence $(\#)$ is split.*

(2) *The sequence $(*)$ is exact.*

(3) *The map β_* is surjective.*

(4) $C = 0$.

(5) *The element $\mathbf{1}_Q$ is in the image of β_*.*

Proof. Because Hom commutes with finite direct sum, we have that (1) $\Rightarrow$ (2), while (2) $\Rightarrow$ (3) $\Leftrightarrow$ (4) $\Rightarrow$ (5) is clear. It remains to show that (5) $\Rightarrow$ (1). Suppose $\theta : Q \to M$ is such that $\beta_*(\theta) = \mathbf{1}_Q$. Since β_* is induced by composition with β, we have that $\beta\theta = \mathbf{1}_Q$. $\square$

A split exact sequence remains split after any base change. In particular, it remains split after localization. There are partial converses. Recall that if $I \subseteq R$,

$$\mathcal{V}(I) = \{P \in \mathrm{Spec}\,(R) : I \subseteq P\},$$

and that

$$\mathcal{D}(I) = \text{Spec}\,(R) - \mathcal{V}(I).$$

In particular,

$$\mathcal{D}(fR) = \{P \in \text{Spec}\,(R) : f \notin P\},$$

and we also write $\mathcal{D}(f)$ or $\mathcal{D}_f$ for $\mathcal{D}(fR)$.

Theorem. *Let R be an arbitrary ring and let*

$$(\#) \quad 0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} Q \to 0$$

be a short exact sequence of R-modules such that Q is finitely presented.

(a) *(#) is split if and only if for every maximal ideal m of R, the sequence*

$$0 \to N_m \to M_m \to Q_m \to 0$$

is split.

(b) *Let S be a faithfully flat R-algebra. The sequence (#) is split if and only if the sequence*

$$0 \to S \otimes_R N \to S \otimes_R M \to S \otimes_R Q \to 0$$

is split.

(c) *Let W be a multiplicative system in R. If the sequence*

$$0 \to W^{-1}N \to W^{-1}M \to W^{-1}Q \to 0$$

is split over $W^{-1}R$, then there exists a single element $c \in W$ such that

$$0 \to N_c \to M_c \to Q_c \to 0$$

is split over R_c.

(d) *If P is a prime ideal of R such that*

$$0 \to N_P \to M_P \to Q_P \to 0$$

is split, there exists an element $c \in R - P$ such that

$$0 \to N_c \to M_c \to Q_c \to 0$$

is split over R_c. Hence, (#) becomes split after localization at any prime P' that does not contain c, i.e., any prime P' such that $c \notin P'$.

(e) *The split locus for (#), by which we mean the set of primes $P \in \text{Spec}\,(R)$ such that*

$$0 \to N_P \to M_P \to Q_P \to 0$$

is split over R_P, is a Zariski open set in Spec (R).

Proof. Let $C = \mathrm{Coker}\big(\mathrm{Hom}(Q,\, M) \to \mathrm{Hom}_R(Q,\, Q)\big)$, as in the preceding Proposition, and let γ denote the image of $\mathbf{1}_Q$ in C. By part (4) of the preceding Propostion, (#) is split if and only if $\gamma = 0$.

(a) The "only if" part is clear, since splitting is preserved by any base change. For the "if" part, suppose that $\gamma \neq 0$. The we can choose a maximal ideal m in the support of $R\gamma \subseteq C$, i.e., such that $\mathrm{Ann}_R\gamma \subseteq m$. The fact that Q is finitely presented implies that localization commutes with Hom. Thus, localizing at m yields

$$0 \to \mathrm{Hom}_{R_m}(Q_m,\, N_m) \to \mathrm{Hom}_{R_m}(Q_m,\, M_m) \to \mathrm{Hom}_{R_m}(Q_m,\, Q_m) \to C_m \to 0,$$

and since the image of γ is not 0, the sequence $0 \to N_m \to M_m \to Q_m \to 0$ does not split.

(b) Again, the "only if" part is clear, and since Q is finitely presented and S is flat, Hom commutes with base change to S. After base change, the new cokernel is $S \otimes_R C$. But $C = 0$ if and only if $S \otimes_R C = 0$, since S is faithfully flat, and the result follows.

(c) Similarly, the sequence is split after localization at W if and only if the image of γ is 0 after localization at W, and this happens if and only if $c\gamma = 0$ for some $c \in W$. But then localiziing at the element c kills γ.

(d) This is simply part (c) applied with $W = R - P$

(e) If P is in the split locus and $c \notin P$ is chosen as in part (d), $\mathcal{D}(c)$ is a Zariski open neighborhood of P in the split locus. □

Behavior of strongly F-regular rings

Theorem. *Let R be an F-finite reduced ring. Then the following conditions are equivalent:*

(1) *R is strongly F-regular.*

(2) *R_m is strongly F-regular for every maximal ideal m of R.*

(3) *$W^{-1}R$ is strongly F-regular for every multiplicative system W in R.*

Proof. We shall show that (1) ⇒ (3) ⇒ (2) ⇒ (1).

To show that (1) ⇒ (3), suppose that R is strongly F-regular and let W be a multiplicative system. By the Proposition on p. 2 of the Lecture Notes of September 17, every element of $(W^{-1}R)^\circ$ has the form c/w where $w \in W$ and $c \in R^\circ$. Given such an element c/w, we can choose q_c and an R-linear map $\theta : R^{1/q_c} \to R$ such that $\theta(c^{1/q}) = 1$. After localization at c, θ induces a map $\theta_c : (R_c)^{1/q_c} \to R_c$ sending $(c/1)^{1/q_c}$ to $1/1$. Define $\eta : (R_c)^{1/q_c} \to R_c$ by $\eta(u) = \theta_c(w^{1/q_c}u)$. Then $\eta : (R_c)^{1/q_c} \to R_c$ is an R_c-linear map such that $\eta\big((c/w)^{1/q_c}\big) = 1$, as required. (3) ⇒ (2) is obvious.

It remains to show that (2) ⇒ (1). Fix $c \in R^\circ$. Then for every maximal ideal m of R, the image of c is in $(R_m)^\circ$, and so there exist q_m and a splitting of the map $R_m \to$

$(R^{1/q_m})m \cong (R_m)^{1/q_m}$ that sends $1 \mapsto c^{1/q_m}$. Then there is also such a splitting of the map $R \to R^{1/q_m}$ after localizing at any prime in a Zariski neighborhood U_m of m. Since the U_m cover MaxSpec$\,(R)$, they cover Spec$\,(R)$, and by the quasicompactness of Spec$\,(R)$ there are finitely many maximal ideals $m_1, \ldots, m_n$ such that the open sets $U_{m_1}, \ldots, U_{m_n}$ cover Spec$\,(R)$. Let $q_c = \max\{q_{m_1}, \ldots, q_{m_n}\}$. Then the map $R \to R^{1/q_c}$ that sends $1 \mapsto c^{1/q_c}$ splits after localizing at any maximal ideal in any of the U_{m_i}, i.e., after localizing at any maximal ideal. By part (a) of the preceding Proposition, the map $R \to R^{1/q_c}$ sending $1 \mapsto c^{1/q_c}$ splits, as required. □

Corollary. *A strongly F-regular ring is F-regular.*

Proof. This is immediate from the fact that strongly F-regular rings are weakly F-regular and the fact that a localization of a strongly F-regular ring is strongly F-regular. □

Corollary. *R is strongly F-regular if and only if it is a finite product of strongly F-regular domains.*

Proof. If R is strongly F-regular it is normal, and, therefore, a product of domains. Since the issue of whether R is strongly F-regular is local on the maximal ideals of R, when R is a product of domains it is strongly F-regular if and only if each of the factor domains is strongly F-regular. □

Proposition. *If S is strongly F-regular and R is a direct summand of S, then R is strongly F-regular.*

Proof. If R and S are domains, we may proceed as follows. Let $c \in R^\circ = R - \{0\}$ be given. Since S is strongly F-regular we may choose q and an S-linear map $\theta : S^{1/q} \to S$ such that $\theta(c^{1/q}) = 1$. Let $\alpha : S \to R$ be R-linear such that $\alpha(1) = 1$. Then $\alpha \circ \theta : S^{1/q} \to R$ is R-linear and sends $c^{1/q} \mapsto 1$. We may restrict this map to $R^{1/q}$.

In the general case, we may first localize at a prime of R: it suffices to see that every such localization is strongly F-regular. S is a product of F-regular domains $S_1 \times \cdots \times S_n$ each of which is an R-algebra. Let $\alpha : S \to R$ be such that $\alpha(1) = 1$. The element $1 \in S$ is the sum of n idempotents e_i, where e_i has component 0 in S_j for $j \neq i$ while the component in S_i is 1. Then $1 = \alpha(1) = \sum_{i=1}^n \alpha(e_i)$, and since R is local, at least one $\alpha(e_i)$ is not in the maximal ideal m of the local ring R, i.e., we can fix i such that $\alpha(e_i)$ is a unit a of R. We have an R-linear injection $\iota : S_i \to S$ by identifying S_i with $0 \times 0 \times S_i \times 0 \times 0$, i.e., with the set of elements of S all of whose coordinates except the i th are 0. Then $a^{-1}\alpha \circ \iota$ is a splitting of $R \to S_i$ over R, and so we have reduced to the domain case, which was handled in the first paragraph. □

We also have:

Proposition. *If $R \to S$ is faithfully flat and S is strongly F-regular then R is strongly F-regular.*

Proof. Let $c \in R^\circ$. Then $c \in S^\circ$, and so there exists q and an S-linear map $S^{1/q} \to S$ such that $c^{1/q} \mapsto 1$. There is an obvious map $S \otimes_R R^{1/q} \to S^{1/q}$, since both factors in the tensor product have maps to $S^{1/q}$ as R-algebras. This yields a map $S \otimes_R R^{1/q} \to S = S \otimes_R R$ that sends $1 \otimes c^{1/q} \mapsto 1 \otimes 1$ that is S-linear. This implies that the map $R \to R^{1/q}$ sending $1 \mapsto c^{1/q}$ splits after a faithfully flat base change to S. By part (b) of the Theorem at the top of p. 3, the map $R \to R^{1/q}$ such that $1 \mapsto c^{1/q}$ spits over R, as required. □

Theorem. *An F-finite regular ring is strongly F-regular.*

Proof. We may assume that (R, m, K) is local: it is therefore a domain. Let $c \neq 0$ be given. Choose q so large that $c \notin m^{[q]}$: this is possible because $\bigcap_q m^{[q]} \subseteq \bigcap_q m^q = (0)$. The flatness of Frobenius implies that $R^{1/q}$ is flat and, therefore, free over R since $R^{1/q}$ is module-finite over R. (Alternatively, $R^{1/q}$ is free because a regular system of parameters $x_1, \ldots, x_n$ in R is a regular sequence on $R^{1/q}$: one may apply the Lemma in the middle of p. 8 of the Lecture Notes of September 5. Or one may further reduce to the case where R is complete, using the preceding Proposition, and even pass from the complete regular ring $K[[x_1, \ldots, x_n]$ to $\overline{K}[[x_1, \ldots, x_n]]$, where $\overline{K}$ is an algebraic closure of K. This is simply a further faithfully flat extension. Now the fact that $R^{1/q}$ is R-free is easy.) Since $c \notin m^{[q]}$, we have that $c^{1/q} \notin mR^{1/q}$. By Nakayama's Lemma, $c^{1/q}$ is part of a minimal basis for the R-free module $R^{1/q}$, and a minimal basis is a free basis. It follows that there is an R-linear map $R^{1/q} \to R$ such that $c^{1/q} \mapsto 1$: the values can be specified arbitrarily on a free basis containing $c^{1/q}$. □

Remark: qth roots of maps. The following situation arises frequently in studying strongly F-regular rings. One has q, q_0, q_1, q_2, where these are all powers of p, the prime characteristic, such that $q_0 \leq q_1$ and $q_0 \leq q_2$, and we have an R^{1/q_0}-linear map $\alpha : R^{1/q_1} \to R^{1/q_2}$. This map might have certain specified values, e.g., $\alpha(u) = v$. Here, one or more of the integers q, q_i may be 1. Then one has a map which we denote $\alpha^{1/q} : R^{1/q_1 q} \to R^{1/q_2 q}$ which is $R^{1/q_0 q}$-linear, that is simply defined by the rule $\alpha^{1/q}(s^{1/q}) = \alpha(s)^{1/q}$. Then $\alpha^{1/q}(u^{1/q}) = v^{1/q}$.

The following result makes the property of being a strongly F-regular ring much easier to test: instead of needing to worry about constructing a splitting for every element of R°, one only needs to construct a splitting for *one* element of R°.

Theorem. *Let R be a reduced F-finite ring of prime characteristic $p > 0$, and let $c \in R^\circ$ be such that R_c is strongly F-regular. Then R is strongly F-regular if and only if*

(∗) *there exists q_c such that the map $R \to R^{1/q_c}$ sending $1 \mapsto c^{1/q_c}$ splits.*

Proof. The condition (∗) is obviously necessary for R to be strongly F-regular: we need to show that it is sufficient. Therefore, assume that we have an R-linear splitting

$$\theta : R^{1/q_c} \to R,$$

with $\theta(c^{1/q_c}) = 1$. By the Remark beginning near the bottom of p. 4 of the Lecture Notes of September 21, we know that R is F-split. Suppose that $d \in R^\circ$ is given.

Since R_c is strongly F-regular we can choose q_d and an R_c-linear map $\beta : R_c^{1/q_d} \to R_c$ such that $\beta(d^{1/q_d}) = 1$. Since $\mathrm{Hom}_{R_c}(R_c^{1/q_d}, R_c)$ is the localization of $\mathrm{Hom}_R(R^{1/q_d}, R)$ at c, we have that $\beta = \dfrac{1}{c^q}\alpha$ for some sufficiently large choice of q: since we are free to make the power of c in the denominator larger if we choose, there is no loss of generality in assuming that the exponent is a power of p. Then $\alpha : R^{1/q_d} \to R$ is an R-linear map such that

$$\alpha(d^{1/q_d}) = c^q \beta(d^{1/q_d}) = c^q.$$

By taking qq_c roots we obtain a map

$$\alpha^{1/qq_c} : R^{1/qq_cq_d} \to R^{1/qq_c}$$

that is R^{1/qq_c}-linear and sends $d^{1/qq_cq_d} \mapsto c^{1/q_c}$. Because R is F-split, the inclusion $R \hookrightarrow R^{1/q}$ splits: let $\gamma : R^{1/q} \to R$ be R linear such that $\gamma(1) = 1$. Then $\gamma^{1/q_c} : R^{1/qq_c} \to R^{1/q_c}$ is an R^{1/q_c}-linear retraction and sends $c^{1/q_c} \mapsto c^{1/q_c}$. Then $\theta \circ \gamma^{1/q_c} \circ \alpha^{1/qq_c} : R^{1/qq_cq_d} \to R$ and sends $d^{1/qq_cq_d} \mapsto 1$, as required. $\square$

Math 711, Fall 2007 **Problem Set #1**
Due: Monday, October 8

1. Let R be a Noetherian domain of characteristic p. Let S be a solid R-algebra: this means that there is an R-linear map $\theta : S \to R$ such that $\theta(1) \neq 0$. Show that $IS \cap R \subseteq I^*$. Note that there is no finiteness condition on S.

2. Let S be weakly F-regular, and let $R \subseteq S$ be such that for every ideal of R, $IS \cap R = I$. Show that R is weakly F-regular.

3. Let M be a finitely generated module over a regular ring R of prime characteristic $p > 0$. Show that that for all $e \geq 1$, the set of associated primes of $\mathcal{F}^e(M)$ is equal to the set of associated primes of M.

4. Let (R, m, K) be a local ring of prime characteristic $p > 0$ with $\dim(R) = d > 0$. Let $I \subseteq J$ be two m-primary ideals of R such that $J \subseteq I^*$. Prove that there is a positive constant C such that $\ell(R/J^{[q]}) - \ell(R/I^{[q]})| \leq Cq^{d-1}$. (This implies that the Hilbert-Kunz multiplicities of I and J are the same.) [Here is one approach. Let h, k be the numbers of generators of I, J, respectively. Show that there exists $c \in R^\circ$ such that $cJ^{[q]} \subseteq I^{[q]}$ for $q \gg 0$, so that $J^{[q]}/I^{[q]}$ is a module with at most k generators over $R/(I^{[q]} + cR) = \overline{R}/\mathfrak{A}^{[q]}$ where $\overline{R} = R/cR$ and $\mathfrak{A} = I\overline{R}$. Moreover, $\dim(\overline{R}) = d - 1$ and $\mathfrak{A}^{qh} \subseteq \mathfrak{A}^{[q]}$.]

5. Let R be a reduced Noetherian ring of prime characteristic $p > 0$. Show that if $R/\mathfrak{p}_i$ has a test element for every minimal prime $\mathfrak{p}_i$ of R, then R has a test element.

6. Let (R, m, K) be a Cohen-Macaulay local ring, and let $x_1, \ldots, x_n$ be a system of parameters. Let $I_t = (x_1^t, \ldots, x_n^t)R$ for $t \geq n$ and let $I = I_1$.

(a) Prove that there is an isomorphism between the socle (annihilator of the maximal ideal) in R/I and the socle in R/I_t induced by multiplication by $x_1^{t-1} \cdots x_n^{t-1}$.

(b) Prove that an m-primary ideal J is tightly closed iff no element of $(J :_R m) - J$ is in J^*. Note that $(J :_R m)/J$ is the socle in R/J. (That R is Cohen-Macaulay is not needed here.)

(c) Prove that I is tightly closed in R if and only if I_t is tightly closed in R for every $t \geq 1$.

Math 711: Lecture of September 26, 2007

We want to use the theory of strongly F-regular F-finite rings to prove the existence of test elements.

We first prove two preliminary results:

Lemma. *Let R be an F-finite reduced ring and $c \in R^\circ$ be such that R_c is F-split (which is automatic if R_c is strongly F-regular). Then there exists an R-linear map $\theta : R^{1/p} \to R$ such that the value on 1 is a power of c.*

Proof. We can choose an R_c-linear map $(R_c)^{1/p} \to R_c$ such that $1 \mapsto 1$, and

$$(R_c)^{1/p} \cong (R^{1/p})_c.$$

Then $\mathrm{Hom}_{R_c}(R_c^{1/p},\, R_c)$ is the localization of $\mathrm{Hom}_R(R^{1/p},\, R)$ at c, and so we can write $\theta = \dfrac{1}{c^N}\alpha$, where $N \in \mathbb{N}$ and $\alpha : R^{1/p} \to R$ is R-linear. But then $\alpha = c^N\beta$ and so $\alpha(1) = c^N\beta(1) = c^N$, as required. $\square$

Lemma. *Let R be a reduced F-finite ring and suppose that there exists an R-linear map $\theta : R^{1/p} \to R$ such that $\theta(1) = c \in R^\circ$. Then for every $q = p^e$, there exists an R-linear map $\eta_q : R^{1/q} \to R$ such that $\eta_q(1) = c^2$.*

Proof. We use induction on q. If $q = 1$ we may take $\eta_1 = c^2\mathbf{1}_R$, and if $q = p$ we may take $\eta_p = c\,\theta$. Now suppose that η_q has been constructed for $q \geq p$. Then $\eta_q^{1/p} : R^{1/pq} \to R^{1/p}$, it is $R^{1/p}$-linear, hence, R-linear, and its value on 1 is $c^{2/p}$. Define

$$\eta_{pq}(u) = \theta\bigl(c^{(p-2)/p}\eta_q(u)\bigr).$$

Consequently, we have, as required, that

$$\eta_{pq}(1) = \theta\bigl(c^{(p-2)/p}\eta_q(1)\bigr) = \theta(c^{(p-2)/p}c^{2/p}) = \theta(c) = c\theta(1) = c^2. \qquad \square$$

We can now prove the following:

Theorem (existence of big test elements). *Let R be F-finite and reduced. If $c \in R^\circ$ and R_c is strongly F-regular, then c has a power that is a big test element. If R_c is strongly F-regular and there exists an R-linear map $\theta : R^{1/p} \to R$ such that $\theta(1) = c$, then c^3 is a big test element.*

Proof. Since R_c is strongly F-regular it is F-split. By the first Lemma on p. 1 there exist an integer N and an R-linear map $\theta : R^{1/p} \to R$ such that $\theta(1) = c^N$. By the second statement of the Theorem, c^{3N} is then a big test element, and so it suffices to prove the second statement.

Suppose that c satsifies the hypothesis of the second statement. By part (a) of the Proposition at the bottom of p. 8 of the Lecture Notes of September 17, it suffices to show that if $N \subseteq M$ are arbitrary modules and $u \in N^*_M$, then $c^3 u \in N$. We may map a free module G onto M, let H be the inverse image of N in G, and let $v \in G$ be an element that maps to $u \in N$. Then we have $v \in H^*_G$, and it suffices to prove that $c^3 v \in H$. Since $v \in H^*_G$ there exists $d \in R^\circ$ such that $dv^q \in H^{[q]}$ for all $q \geq q_1$. Since R_c is strongly F-regular, there exist q_d and an R_c-linear map $\beta : (R_c)^{1/q_d} \to R_c$ that sends $d^{1/q_d} \to 1$: we may take q_d larger, if necessary, and so we may assume that $q_d \geq q_1$. As usual, we may assume that $\beta = \dfrac{1}{c^q}\alpha$ where $\alpha : R^{1/q_d} \to R$ is R-linear. Hence, $\alpha = c^q\beta$, and $\alpha(d^{1/q_d}) = c^q$. It follows that $\alpha^{1/q} : R^{1/q_d q} \to R^{1/q}$ is $R^{1/q}$-linear, hence, R-linear, and its value on 1 is c. By the preceding Lemma we have an R-linear map $\eta_q : R^{1/q} \to R$ whose value on 1 is c^2, so that $\eta_q(c) = c\eta^q(1) = c^3$. Let $\gamma = \eta_q \circ \alpha^{1/q}$, which is an R-linear map $R^{1/q_d q} \to R$ sending $d^{1/q_d q}$ to $\eta_q(c) = c^3$. Since $q_d q \geq q_1$, we have $dv^{q_d q} \in H^{[q_d q]}$, i.e.,

$$(\#) \quad dv^{q_d q} = \sum_{i=1}^{n} r_i h_i^q$$

for some integer $n > 0$ and elements $r_1, \ldots, r_n \in R$ and $h_1, \ldots, h_n \in H$.

Consider $G' = R^{1/qq_d} \otimes G$. We identify G with its image under the map $G \to G'$ that sends $g \mapsto 1 \otimes g$. Thus, if $s \in R^{1/q_d q}$, we may write sg instead of $s \otimes g$. Note that G' is free over $R^{1/qqd}$, and the R-linear map $\gamma : R^{1/qq_d} \to R$ induces an R-linear map

$$\gamma' : G' = R^{qq_d} \otimes_R G \to R \otimes_R G \cong G$$

that sends $sg \mapsto \gamma(s)g$ for all $s \in R^{1/qq_d}$ and all $g \in G$. Note that by taking $q_d q$ th roots in the displayed equation (#) above, we obtain

$$(\dagger) \quad d^{1/q_d q} v = \sum_{i=1}^{n} r_i^{1/q_d q} h_i.$$

We may now apply γ' to both sides of (†): we have

$$c^3 v = \sum_{i=1}^{n} \gamma(r_i^{1/q_d q}) h_i \in H,$$

exactly as required. □

Disccussion. As noted on the bottom of p. 2 and top of p. 3 of the Lecture Notes of September 21, it follows that every F-finite reduced ring has a big test element: one can choose $c \in R^\circ$ such that R_c is regular. This is a consequence of the fact that F-finite rings are excellent. But one can give a proof of the existence of such elements c in F-finite rings of characteristic p very easily if one assumes that a Noetherian ring is regular if and only if the Frobenius endomorphism is flat (we proved the "only if" direction earlier). See [E. Kunz, *Characterizations of regular local rings of characteristic* p, Amer. J. Math. **91** (1969) 772–784]. Assuming the "if" direction, we may argue as follows. First note that one can localize at one such element c so that the idempotent elements of the total quotient ring of R are in the localization. Therefore, there is no loss of generality in assuming that R is a domain. Then $R^{1/p}$ is a finitely generated torsion-free R-module. Choose a maximal set $s_1, \ldots, s_n$ of R-linearly independent elements in $R^{1/p}$. This gives an inclusion

$$R^n \cong Rs_1 + \cdots + Rs_n \subseteq R^{1/p}.$$

Call the cokernel C. Then C is finitely generated, and C must be a torsion module over R: if $s_{n+1} \in R^{1/p}$ represents an element of C that is not a torsion element, then $s_1, \ldots, s_{n+1}$ are linearly independent over R, a contradiction. Hence, there exists $c \in R^\circ$ that kills C, and so $cR^{1/p} \subseteq R^n$. It follows that $(R^{1/p})_c \cong R_c^n$, and so $(R_c)^{1p}$ is free over R_c. But this implies that F_{R_c} is flat, and so R_c is regular, as required. □

In any case, we have proved:

Corollary. *If R is reduced and F-finite, then R has a big test element. Hence, $\tau_{\mathrm{b}}(R)$ is generated by the big test elements of R, and $\tau(R)$ is generated by the test elements of R.* □

Our next objective is to show that the big test elements produced by the Theorem on p. 1 are actually completely stable. In fact, we shall prove something more: they remain test elements after any geometrically regular base change, i.e., their images under a flat map $R \to S$ with geometrically regular fibers are again test elements.

Math 711: Lecture of September 28, 2007

We next want to note some elementary connections between properties of regular sequences and the vanishing of Tor.

Proposition. *Let $x_1, \ldots, x_n \in R$ and let M be an R-module. Suppose that $x_1, \ldots, x_n$ is a possibly improper regular sequence in R, and is also a possibly improper regular sequence on M. Let $I_k = (x_1, \ldots, x_k)R$, $0 \leq k \leq n$, so that $I_0 = 0$. Then*

$$\mathrm{Tor}_i^R(R/I_k, M) = 0$$

for $i \geq 1$ and $0 \leq k \leq n$.

Proof. If $k = 0$ this is clear, since R is free and has a projective resolution in which the terms with a positive index all vanish. We use induction on k. We assume the result for some $k < n$, and we prove it for $k+1$. From the short exact sequence

$$0 \to R/I_k \xrightarrow{x_{k+1}\cdot} R/I_k \to R/I_{k+1} \to 0$$

we have a long exact sequence for Tor, part of which is

$$\mathrm{Tor}_i^R(R/I_k,\, M) \to \mathrm{Tor}_i^R(R/I_{k+1},\, M) \to \mathrm{Tor}_{i-1}^R(R/I_k,\, M) \xrightarrow{x_{k+1}\cdot} \mathrm{Tor}_{i-1}^R(R/I_k,\, M)$$

If $i \geq 2$, the result is immediate from the induction hypothesis, because the terms surrounding $\mathrm{Tor}_i^R(R/I_{k+1},\, M)$ are 0. If $i = 1$, this becomes:

$$0 \to \mathrm{Tor}_1^R(I_{k+1},\, M) \to M/I_kM \xrightarrow{x_{k+1}\cdot} M/I_kM$$

which shows that $\mathrm{Tor}_1^R(I_{k+1},\, M)$ is isomorphic with the kernel of the map given by multiplication by x_{k+1} on M/I_kM, and this is 0 because $x_1, \ldots, x_n$ is a possibly improper regular sequence on M. □

The following result was stated earlier, in the Lecture Notes of September 14, p. 2. where it was used to give one of the proofs of the flatness of the Frobenius endomorphism for a regular ring R. We now give a proof, but in the course of the proof, we assume the theorem that $(*)$ over a regular local ring, every module has a finite free resolution of length at most the dimension of the ring. The condition $(*)$ actually characterizes regularity. Later, we shall develop results on Koszul complexes that permit a very easy proof that the condition $(*)$ holds over every regular local ring.

Theorem. *Let (R, m, K) be a regular local ring and let M be an R-module. Them M is a big Cohen-Macaulay module over R if and only if M is faithfully flat over R.*

Proof. By the comments at the bottom of p. 2 and top of p. 3 of the Lecture Notes of September 14, we already know that both conditions in the Theorem imply that $mM \neq M$, and that a faithfully flat module is a big Cohen-Macaulay module. It remains only to prove that if M is a big Cohen-Macaulay module over R, then M is flat.

It suffices to show that for every R-module N and every $i \geq 1$, $\mathrm{Tor}_i^R(N, M) = 0$. In fact, it suffices to show this when $i = 1$, for then if $0 \to N_0 \to N_1 \to N \to 0$ is exact, we have

$$0 = \mathrm{Tor}_1^R(M, N) \to M \otimes_R N_0 \to M \otimes_R N_1$$

is exact, which yields the needed injectivity. However, we carry through the proof by reverse induction on i, so that we need to consider all $i \geq 1$.

Because Tor commutes with direct limits, we may reduce to the case where N is finitely generated. We then know that $\mathrm{Tor}_i^R(N, M) = 0$ for $i > n$, because N has a free resolution of length at most n by the condition $(*)$ satisfied by regular local rings that was discussed in the paragraph just before the statement of the Theorem. Hence, it suffices to prove that if $i \geq 1$ and for all finitely generated R-modules N we have that $\mathrm{Tor}_j^R(N, M) = 0$ for $j \geq i + 1$, then $\mathrm{Tor}_i(N, M) = 0$ for all finitely generated R-modules N as well.

We first consider the case where $N = R/P$ is prime cyclic. By the Corollary near the bottom of p. 7 of the Lecture Notes of September 5, there is a regular sequence whose length is the height of P contained in P, say $x_1, \ldots, x_h$, and then P is a minimal prime of $R/(x_1, \ldots, x_h)$. This implies that P is also an assoicated prime of $R/(x_1, \ldots, x_h)R$, so that we have a short exact sequence

$$0 \to R/P \to R/(x_1, \ldots, x_h)R \to C \to 0$$

for some R-module C. The long exact sequence for Tor then yields, in part:

$$\mathrm{Tor}_{i+1}^R(C, M) \to \mathrm{Tor}_i^R(R/P, M) \to \mathrm{Tor}_i^R(R/(x_1, \ldots, x_h)R, M)$$

The leftmost term is 0 by the induction hypothesis, and the rightmost term is 0 by the first Proposition on p. 1. Hence, $\mathrm{Tor}_i^R(R/P, M) = 0$.

We can now proceed by induction on the least number of factors in a finite filtration of N by prime cyclic modules. The case where there is just one factor was handled in the preceding paragraph. Suppose that $R/P = N_1 \subseteq N$ begins such a filtration. Then N/N_1 has a shorter filtration. The long exact sequence for Tor yields

$$\mathrm{Tor}_i^R(R/P, M) \to \mathrm{Tor}_i^R(N, M) \to \mathrm{Tor}_i^R(N/N_1, M).$$

The first term vanishes by the result of the preceding paragraph, and the third term by the induction hypothesis. □

We are aiming to prove that if $R \to S$ is geometrically regular (i.e., flat, with geometrically regular fibers) and R is strongly F-regular, then S is strongly F-regular. In order to prove this, we will make use of the following result:

Theorem (Radu-André). *Let $R \to S$ be a geometrically regular map of F-finite rings of prime characteristic $p > 0$. Then for all q, the map $R^{1/q} \otimes_R S \to S^{1/q}$ is faithfully flat.*

The Radu-André theorem asserts the same conclusion even when R and S are not assumed to be F-finite. In fact, $R \to S$ is geometrically regular if and only if the homomorphisms $R^{1/q} \otimes_R S \to S^{1/q}$ are flat. However, we do not need the converse, and we only need the theorem in the F-finite case, where the argument is easier.

The proof of this Theorem will require some effort. We first want to note that it has the following consequence:

Corollary. *Let $R \to S$ be a geometrically regular map of F-finite rings of prime characteristic $p > 0$. Then for all q, the map $R^{1/q} \otimes_R S \to S^{1/q}$ makes $R^{1/q} \otimes_R S$ a direct summand of $S^{1/q}$.*

Note that since $S \to S^{1/q}$ is module-finite, we have that $R^{1/q} \otimes_R S \to S^{1/q}$ is module-finite as well. The Corollary above then follows from the Radu-André Theorem and the following fact.

Proposition. *Let $A \to B$ be a faithfully flat map of Noetherian rings such that B is module-finite over A. Then A is a direct summand of B as an A-module.*

Proof. The issue is local on A. But when (A, m, K) is local, a finitely generated module is flat if and only if it is free, and so B is a nonzero free A-algebra. The element $1 \in B$ is not in mB, and so is part of a minimal basis, which will be a free basis, for B over A. Hence, there is an A-linear map $B \to A$ whose value on $1 \in B$ is $1 \in A$. $\square$

Math 711: Lecture of October 1, 2007

In the proof of the Radu-André Theorem we will need the result just below. A more general theorem may be found in [H. Matsumura, *Commutative Algebra*, W. A. Benjamin, New York, 1 970], Ch. 8 (20.C) Theorem 49, p. 146, but the version we give here will suffice for our purposes.

First note the following fact: if $I \subseteq A$ is an ideal and M is an A-module, then $\mathrm{Tor}_1^A(A/I,\, M) = 0$ if and only if the map $I \otimes_A M \to IM$, which is alway surjective, is an isomorphism. This map sends $i \otimes u \mapsto iu$. The reason is that we may start with the short exact sequence $0 \to I \to A \to A/I \to 0$ and apply $\_ \otimes_A M$. The long exact sequence then gives, in part:

$$0 = \mathrm{Tor}_1^A(A,\, M) \to \mathrm{Tor}_1^A(A/I,\, M) \to I \otimes_A M \to M$$

The image of the rightmost map is IM, and so we have

$$0 \to \mathrm{Tor}_1^A(A/I,\, M) \to I \otimes_A M \to IM \to 0$$

is exact, from which the statement we want is clear.

Theorem (local criterion for flatness). *Let $A \to B$ be a local homomorphism of local rings, let M be a finitely generated B-module and let I be a proper ideal of A. Then the following three conditions are equivalent:*

(1) *M is flat over A.*

(2) *M/IM is flat over A/I and $I \otimes_A M \to IM$ is an isomorphism.*

(3) *M/IM is flat over A/I and $\mathrm{Tor}_1^A(A/I,\, M) = 0$.*

Proof. The discussion of the preceding paragraph shows that (2) $\Leftrightarrow$ (3), and (1) $\Rightarrow$ (3) is clear. It remains to prove (3) $\Rightarrow$ (1), and so we assume (3). To show that M is flat, it suffices to show that if $N_0 \subseteq N$ is an injection of finitely generated R-modules then $N_0 \otimes_A M \to N \otimes_A M$ is injective. Moreover, by the Proposition at the bottom of p. 3 of the Lecture Notes of September 14, we need only prove this when N has finite length. Consequently, we may assume that N is killed by a power of I, and so we have that $I^k N \subseteq N_0$ for some k. Let $N_i = N_0 + I^{k-i}N$ for $0 \leq i \leq k$. The $N_0 \subseteq N_1 \subseteq \cdots \subseteq N_k = N$, and it suffices to show that $N_j \otimes_A M \to N_{j+1} \otimes_A M$ is injective for each j. We have now reduced to the case where $Q = N_{j+1}/N_j$ is killed by I. From the long exact sequence for Tor arising from applying $\_ \otimes_A M$ to the short exact sequence

$$0 \to N_j \to N_{j+1} \to Q \to 0,$$

we have

$$\mathrm{Tor}_1^A(Q,\, M) \to N_j \otimes_A M \to N_{j+1} \otimes_A M$$

is exact, and so it suffices to show that if Q is a finitely generated A-module killed by I, then $\mathrm{Tor}_1^A(Q,\, M) = 0$.

Since Q is killed by I, we may think of it as a finitely generated module over A/I. Hence, there is a short exact sequence

$$0 \to Z \to (A/I)^{\oplus h} \to Q \to 0.$$

Applying $\_ \otimes_A M$, from the long exact sequence for Tor we have that

$$\mathrm{Tor}_1^A\big((A/I)^{\oplus h},\, M\big) \to \mathrm{Tor}_1^A(Q,\, M) \to Z \otimes_A M \xrightarrow{\alpha} (A/I)^{\oplus h} \otimes_A M$$

is exact. By hypothesis, $\mathrm{Tor}_1^A(A/I,\, M) = 0$, and so the leftmost term is 0. It follows that $\mathrm{Tor}_1^A(Q,\, M) \cong \mathrm{Ker}\,(\alpha)$. To conclude the proof, it will suffice to show that α is injective.

Hence, it is enough to show that $\_ \otimes_A M$ is an exact functor on A-modules Y that are killed by I. For such an A-module Y we have that

$$Y \otimes_A M \cong (Y \otimes_{A/I} A/I) \otimes_A M \cong Y \otimes_{A/I} \big((A/I) \otimes_A M\big) \cong Y \otimes_{A/I} M/IM,$$

and this is an isomorphism as functors of Y. Since M/IM is flat over A/I, the injectivity of α follows. $\square$

We want to record the following observation.

Proposition. *Let $f : A \to B$ be a homorphism of Noetherian rings of prime characteristic $p > 0$ such that the kernel of f consists of nilpotent elements of A and for every element $b \in B$ there exists q such that $b^q \in f(A)$. Then $\mathrm{Spec}\,(f) : \mathrm{Spec}\,(B) \to \mathrm{Spec}\,(A)$ is a homeomorphism (recall that this map sends the prime ideal $Q \in \mathrm{Spec}\,(B)$ to the contraction $f^{-1}(Q)$ of Q to A). The inverse maps $P \in \mathrm{Spec}\,(A)$ to the radical of PB, which is the unique prime ideal of B lying over P.*

Proof. Since the induced map $\mathrm{Spec}\,(A) \to \mathrm{Spec}\,(A/J)$ is a homeomorphism whenever J is an ideal whose elements are nilpotent, and the unique prime of A/J lying over $P \in \mathrm{Spec}\,(A)$ is P/J, the image of P in A/J, there is no loss of generality in considering instead the induced map $A_{\mathrm{red}} \to B_{\mathrm{red}}$, which is injective. We therefore assume that A and B are reduced, and, by replacing A by its image, we may also assume that $A \subseteq B$. Then $A \hookrightarrow B$ is an integral extension, since every $b \in B$ has a power in A, and it follows that there is a prime ideal Q of S lying over a given prime P of A. If $u \in Q$, then $u^q \in A$ for some q, and so $u^q \in Q \cap A = P$. It follows that $Q \subseteq \mathrm{Rad}\,(PB)$, and since Q is a radical ideal containing PB, we have that $Q = \mathrm{Rad}\,(PB)$. Therefore, as claimed in the statement of the Proposition, we have that $\mathrm{Rad}\,(PB)$ is the unique prime ideal of S lying over P. This shows that $\mathrm{Spec}\,(f)$ is bijective. To show that $g = \mathrm{Spec}\,(f)$ is a homeomorphism, it suffices to show that its inverse is continuous, i.e., that g maps closed sets to closed sets. But for any $b \in B$, we may choose q so that $b^q \in A$, and then

$$g\big(\mathcal{V}(bB)\big) = \mathcal{V}(b^q A) \subseteq \mathrm{Spec}\,(A). \qquad \square$$

The Radu-André Theorem is valid even when R is not reduced. In this case, we do not want to use the notation $R^{1/q}$. Instead, we let $R^{(e)}$ denote R viewed as an R algebra via the structural homomorphism $F^e : R \to R$. We restate the result using this notation.

Theorem (Radu-André). *Let R and S be F-finite rings of prime characteristic $p > 0$ such that $R \to S$ is flat with geometrically regular fibers. Then for all e, $R^{(e)} \otimes_R S \to S^{(e)}$ is faithfully flat.*

Proof. Let $T_e = R^{(e)} \otimes_R S$. Consider the maps $S \to T_e \to S^{(e)}$. Any element in the kernel of $S \to S^{(e)}$ is nilpotent. It follows that this is also true of any element in the kernel of $S \to T_e$. Note that every element of T_e has q th power in the image of S, since $(r \otimes s)^q = r^q \otimes s^q = 1 \otimes r^q s^q$. It follows that $\mathrm{Spec}\,(S^{(e)}) \to \mathrm{Spec}\,(T_e) \to \mathrm{Spec}\,(S)$ are homeomorphisms. Hence, if $S^{(e)}$ is flat over T_e, then it is faithfully flat over T_e.

It is easy to see that geometric regularity is preserved by localization of either ring, and the issue of flatness is local on the primes of $S^{(e)}$ and their contractions to T_e. Localizing $S^{(e)}$ at a prime gives the same result as localizing at the contraction of that prime to S. It follows that we may replace S by a typical localization S_Q and R by R_P where P is the contraction of S ot R. Thus, we may assume that (R, m, K) is local, and that $R \to S$ is a local homomorphism of local rings. Evidently, $S^{(e)}$ and $R^{(e)}$ are local as well, and it follows from the remarks in the first paragraph that the maps $S \to T_e \to S^{(e)}$ are also local.

Let $m^{(e)}$ be the maximal ideal of $R^{(e)}$: of course, if we identify $R^{(e)}$ with the ring R, then $m^{(e)}$ is identified with the maximal ideal m of R.

We shall now prove that $A = T_e \to S^{(e)} = B$ is flat using the local criterion for flatness, taking $I = m^{(e)}T_e$. Note that since $R \to S$ is flat, so is $R^{(e)} \to R^{(e)} \otimes_R S = T_e$. Therefore, $m^{(e)}T_e \cong m^{(e)} \otimes_R S$. The expansion of I to $B = S^{(e)}$ may be identified with $m^{(e)}S^{(e)}$, and since $R^{(e)} \to S^{(e)}$ as a map of rings is the same as $R \to S$, we have that $S^{(e)}$ is flat over $R^{(e)}$, and we may identify $m^{(e)}S^{(e)}$ with $m^{(e)} \otimes_{R^{(e)}} S^{(e)}$.

There are two things to check. One is that B/I is flat over A/I, which says that $S^{(e)}/(m^{(e)} \otimes_{R^{(e)}} S^{(e)})$ is flat over $(R^{(e)} \otimes_R S)/(m^{(e)} \otimes_R S)$. The former may be identified with $(S/mS)^{(e)}$, and the latter with $K^{(e)} \otimes_K (S/mS)$, since $R^{(e)}/m^{(e)}$ may be identified with $K^{(e)}$. Since R is F-finite, so is K, and it follows that $K^{(e)} \cong K^{1/q}$ is a finite purely inseparable extension of K. Since the fiber $K \to K \otimes_R S = S/mS$ is geometrically regular, we have that $K^{(e)} \otimes_R (S/mS) \cong K^{(e)} \otimes_K (S/mS)$ is regular and, in particular, reduced. Since it is purely inseparable over the regular local ring S/mS we have from the Proposition on p. 2 that

$$K^{(e)} \otimes_K (S/mS) \cong (S/mS)[K^{1/q}].$$

is a local ring. Hence, it is a regular local ring.

We have as well that $(S/mS)^{(e)} \cong (S/mS)^{1/q}$ is regular, since S/mS is, and is a module-finite extension of $(S/mS)[K^{1/q}]$. Thus, $B/IB = (S/mS)^{1/q}$ is module-finite local and Cohen-Macaulay over $A/IA = (S/mS)[K^{1/q}]$, which is regular local. By the Lemma on p. 8 of the Lecture Notes of September 8, B/IB is free over A/I, and therefore flat.

Finally, we need to check that $I \otimes_A B \twoheadrightarrow IB$ is an isomorphism, and this the map

$$\phi : (m^{(e)} \otimes_R S) \otimes_{R^{(e)} \otimes_R S} S^{(e)} \twoheadrightarrow m^{(e)} \otimes_{R^{(e)}} S^{(e)}.$$

The map takes $(u \otimes s) \otimes v$ to $u \otimes (sv)$. We prove that ϕ is injective by showing that it has an inverse. There is an $R^{(e)}$-bilinear map

$$m^{(e)} \times S^{(e)} \to (m^{(e)} \otimes_R S) \otimes_{R^{(e)} \otimes_R S} S^{(e)}$$

that sends $(u,\, v) \mapsto (u \otimes 1) \otimes v$. This induces a map

$$\psi : m^{(e)} \otimes_{R^{(e)}} S^{(e)} \to (m^{(e)} \otimes_R S) \otimes_{R^{(e)} \otimes_R S} S^{(e)}$$

and it is straightforward to see that $\psi \circ \phi$ sends

$$(u \otimes s) \otimes v \mapsto (u \otimes 1) \otimes (sv) = (u \otimes s) \otimes v,$$

and that $\phi \circ \psi$ sends $u \otimes v$ to itself. $\square$

Note that if a Noetherian ring R is reduced and $R \to S$ is flat with reduced fibers over the minimal primes of R, then S is reduced. (Because nonzerodivisors in R are nonzerodivisors on S, we can replace R by its total quotient ring, which is a product of fields, and S becomes the product of the fibers over the minimal primes of R.) Hence, if $R \to S$ is flat with geometrically regular (or even reduced) fibers and R is reduced, so is S. This is used several times in the sequel.

Theorem. *If $R \to S$ is a flat map of F-finite rings of prime characteristic $p > 0$ with geometrically regular fibers and R is strongly F-regular then so is S.*

Proof. We can choose $c \in R^\circ$ such that R_c is regular, and then we know that there is an R-linear map $\theta : R^{1/q} \to R$ sending $c^{1/q} \mapsto 1$. Now $R_c \to S_c$ is flat with regular fibers and R_c is regular, so that S_c is regular as well. By Theorem at the bottom of p. 6 of the Lecture Notes of September 24, it suffices to show that there is an S-linear map $S^{1/q} \to S$ such that $c^{1/q} \mapsto 1$. Let $\theta' = \theta \otimes_R \mathbf{1}_S : R^{1/q} \otimes_R S \to S$, so that θ' is an S-linear map such that $\theta'(c^{1/q} \otimes 1) = 1$. By the Corollary on p. 3 of the Lecture Notes of September 28, the inclusion $R^{1/q} \otimes_R S \to S^{1/q}$, which takes $c^{1/q} \otimes 1$ to $c^{1/q}$, has a splitting $\alpha : S^{1/q} \to R^{1/q} \otimes_R S$ that is linear over $R^{1/q} \otimes_R S$. Hence, α is also S-linear, and $\theta' \circ \alpha$ is the required S-linear map from $S^{1/q}$ to S. $\square$

We also can improve our result on the existence of big test elements now.

Theorem. *Let R be a reduced F-finite ring of prime characteristic $p > 0$ and let $c \in R^\circ$ be such that R_c is strongly F-regular. Also assume that there is an R-linear map $R^{1/p} \to R$ that sends 1 to c. If S is F-finite and flat over R with geometrically regular fibers, then the image of c^3 in S is a big test element for S.*

In particular, for every element c as above, c^3 is a completely stable big test element.

Hence, every element c of R° such that R_c is strongly F-regular has a power that is a completely stable big test element, and remains a completely stable big test element after every geometrically regular base change to an F-finite ring.

Proof. By the Theorem at the bottom of p. 1 of the Lecture Notes of September 26, to prove the result asserted in the first paragraph it suffices to show that the image of c in S has the same properties: because the map is flat, the image is in S°, and so it suffices to show that S_c is strongly F-regular and that there is an S-linear map $S^{1/p} \to S$ such that the value on 1 is the image of c in S. But the map $R_c \to S_c$ is flat, R_c is strongly F-regular, and the fibers are a subset of the fibers of the map $R \to S$ corresponding to primes of R not containing c. Hence, the fibers are geometrically regular, and so we can conclude that S_c is strongly F-regular. We have an R-linear map $R^{1/p} \to R$ that sends $1 \mapsto c$. We may apply $\_ \otimes_R \mathbf{1}_S$ to get a map $R^{1/p} \otimes_R S \to S$ sending 1 to the image of c, and then compose with a splitting of the inclusion $R^{1/p} \otimes_R S \to S^{1/p}$ to get the required map.

The statement of the second paragraph now follows because a localization map is geometrically regular, and F-finite rings are excellent, so that the map from a local ring to its completion is geometrically regular as well.

To prove the third statement note that whenever R_c is strongly F-regular, there is a map $R^{1/p} \to R$ whose value on 1 is a power of c: this is a consequence of the first Lemma on p. 1 of the Lecture Notes of September 26. $\square$

Mapping cones

Let $B_\bullet$ and $A_\bullet$ be complexes of R-modules with differentials $\delta_\bullet$ and $d_\bullet$, respectively. We assume that they are indexed by $\mathbb{Z}$, although in the current application that we have in mind they will be left complexes, i.e., all of the negative terms will be zero. Let $\phi_\bullet$ be a map of complexes, so that for every n we have $\phi_n : B_n \to A_n$, and all the squares

$$\begin{array}{ccc} A_n & \xrightarrow{d_n} & A_{n-1} \\ {\scriptstyle\phi_n}\uparrow & & \uparrow{\scriptstyle\phi_{n-1}} \\ B_n & \xrightarrow{\delta_n} & B_{n-1} \end{array}$$

commute. The *mapping cone* $\mathcal{C}_\bullet^{\phi_\bullet}$ of $\phi_\bullet$ is defined so that $\mathcal{C}_n^{\phi_\bullet} := A_n \oplus B_{n-1}$ with the differential that is simply d_n on A_n and is $(-1)^{n-1}\phi_{n-1} \oplus \delta_{n-1}$ on B_{n-1}. Thus, under the differential in the mapping cone,

$$a_n \oplus b_{n-1} \mapsto \big(d_n(a_n) + (-1)^{n-1}\phi(b_{n-1})\big) \oplus \delta_{n-1}(b_{n-1}).$$

If we apply the differential a second time, we obtain

$$\Big(d_{n-1}\big(d_n(a_n) + (-1)^{n-1}\phi_{n-1}(b_{n-1})\big) + (-1)^{n-2}\phi_{n-2}\delta_{n-1}(b_{n-1})\Big) \oplus \delta_{n-2}\delta_{n-1}(b_{n-1}),$$

which is 0, and so we really do get a complex. We frequently omit the superscript $^{\phi_\bullet}$, and simply write $\mathcal{C}_\bullet$ for $\mathcal{C}_\bullet^{\phi_\bullet}$.

Note that $A_\bullet \subseteq \mathcal{C}_\bullet$ is a subcomplex. The quotient complex is isomorphic with $B_\bullet$, except that degrees are shifted so that the degree n term in the quotient is B_{n-1}. This leads to a long exact sequence of homology:

$$\cdots \to H_n(A_\bullet) \to H_n(\mathcal{C}_\bullet) \to H_{n-1}(B_\bullet) \to H_{n-1}(A_\bullet) \to \cdots .$$

One immediate consequence of this long exact sequence is the following fact.

Proposition. *Let $\phi_\bullet : B_\bullet \to A_\bullet$ be a map of left complexes. Suppose that $A_\bullet$ and $B_\bullet$ are acyclic, and that the induced map of augmentations $H_0(B_\bullet) \to H_0(A_\bullet)$ (which may also be described as the induced map $B_0/\delta_0(B_1) \to A_0/d_0(A_1)$) is injective. Then the mapping cone is an acyclic left complex, and its augmentation is $A_0/\big(d(A_1) + \phi_0(B_0)\big)$.* $\square$

The Koszul complex

The Koszul complex $\mathcal{K}_\bullet(x_1, \ldots, x_n; R)$ of a sequence of elements $x_1, \ldots, x_n \in R$ on R may be defined as an iterated mapping cone as follows. Let $\mathcal{K}_\bullet(x_1; R)$ denote the left complex in which $\mathcal{K}_1(x_1; R) = Ru_1$, a free R-module, $\mathcal{K}_0(x_1, R) = R$, and the map is such that $u_1 \mapsto x_1$. I.e., we have $0 \to Ru_1 \xrightarrow{u_1 \mapsto x_1} R \to 0$.

Then we may define $\mathcal{K}_\bullet(x_1, \ldots, x_n; R)$ recursively as follows. If $n > 1$, multiplication by x_n (in every degree) gives a map of complexes

$$\mathcal{K}_\bullet(x_1, \ldots, x_{n-1}; R) \xrightarrow{x_n \cdot} \mathcal{K}_\bullet(x_1, \ldots, x_{n-1}),$$

and we let $\mathcal{K}_\bullet(x_1, \ldots, x_n; R)$ be the mapping cone of this map.

We may prove by induction that $\mathcal{K}_n(x_1, \ldots, x_n; R)$ is a free complex of length n in which the degree j term is isomorphic with the free R-module on $\binom{n}{j}$ generators, $0 \le j \le n$. Even more specifically, we show that we may identify $\mathcal{K}_j(x_1, \ldots, x_n; R)$ with the free module on generators u_σ indexed by the j element subsets σ of $\{1, 2, \ldots, n\}$ in such a way that if $\sigma = \{i_1, \ldots, i_j\}$ with $1 \le i_1 < \cdots < i_j \le n$, then

$$du_\sigma = \sum_{t=1}^{j} (-1)^{t-1} x_{i_t} u_{\sigma - \{i_t\}}.$$

We shall use the alternative notation $u_{i_1 i_2 \cdots i_j}$ for u_σ in this situation. We also identify $u_\emptyset$, the generator of $\mathcal{K}_0(x_1, \ldots, x_n; R)$, with $1 \in R$.

To carry out the inductive step, we assume that $A_\bullet = \mathcal{K}_\bullet(x_1, \ldots, x_{n-1}; R)$ has the specified form. We think of this complex as the target of the map multiplication by x_n, and index its generators by the subsets of $\{1, 2, \ldots, n-1\}$. This complex will be a subcomplex of $\mathcal{K}_\bullet(x_1, \ldots, x_n; R)$. We index the generators of the complex $B_\bullet$, which will be the domain for the map given by multiplication by x_n, and which is also isomorphic to

$\mathcal{K}_\bullet(x_1, \dots, x_{n-1}; R)$, by using the free generator $u_{\sigma\cup\{n\}}$ to correspond to u_σ. In this way, it is clear that $\mathcal{K}_\bullet(x_1, \dots, x_n; R)$ is free, and we have indexed its generators in degree j precisely by the j element subsets of $\{1, 2, \dots, n\}$. It is straightforward to check that the differential is as described above.

We can define the *Koszul complex* of $x_1, \dots, x_n \in R$ on an R-module M, which we denote $\mathcal{K}_\bullet(x_1, \dots, x_n; M)$, in two ways. One is simply as $\mathcal{K}_\bullet(x_1, \dots, x_n; R) \otimes_R M$. The second is to let $\mathcal{K}_\bullet(x_1; M)$ be the complex $0 \to M \otimes_R Ru_1 \to M \to 0$, and then to let $\mathcal{K}_\bullet(x_1, \dots, x_n; M)$ be the mapping cone of multiplication by x_n mapping the complex $\mathcal{K}_\bullet(x_1, \dots, x_{n-1}; M)$ to itself, just as we did in the case $M = R$. It is quite easy to verify that these two constructions give isomorphic results: in fact, quite generally, $\_ \otimes_R M$ commutes with the mapping cone construction on maps of complexes of R-modules.

Math 711: Lecture of October 3, 2007

Koszul homology

We define the i th *Koszul homology module* $H_i(x_1, \dots, x_n; M)$ of M with respect to $x_1, \dots, x_n$ as the i th homology module $H_i\bigl(\mathcal{K}_\bullet(x_1, \dots, x_n; M)\bigr)$ of the Koszul complex.

We note the following properties of Koszul homology.

Proposition. *Let R be a ring and $\underline{x} = x_1, \dots, x_n \in R$. Let $I = (\underline{x})R$. Let M be an R-module.*

(a) $H_i(\underline{x};\, M) = 0$ *if* $i < 0$ *or if* $i > n$.

(b) $H_0(\underline{x};\, M) \cong M/IM$.

(c) $H_n(\underline{x};\, M) = \mathrm{Ann}_M I$.

(d) $\mathrm{Ann}_R M$ *kills every* $H_i(x_1, \dots, x_n;\, M)$.

(e) *If M is Noetherian, so is its Koszul homology $H_i(\underline{x};\, M)$.*

(f) *For every i, $H_i(\underline{x};\, \_)$ is a covariant functor from R-modules to R-modules.*

(g) *If*

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of R-modules, there is a long exact sequence of Koszul homology

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

(h) *If $x_1, \dots, x_n$ is a possibly improper regular sequence on M, then $H_i(\underline{x};\, M) = 0$, $i \geq 1$.*

Proof. Part (a) is immediate from the definition. Part (b) follows from the fact that last map in the Koszul complex from $\mathcal{K}_1(\underline{x};\, M) \to \mathcal{K}_0(\underline{x};\, M)$ may be identified with the map $M^n \to M$ such that $(v_1, \dots, v_n) \mapsto x_1 v + \cdots + x_n v_n$. Part (c) follows from the fact that the map $\mathcal{K}_n(\underline{x};\, M) \to \mathcal{K}_{n-1}(\underline{x};\, M)$ may be identified with the map $M \to M^n$ such that $v \mapsto (x_1 v, -x_2 v, \cdots, (-1)^{n-1} x_n v)$.

Parts (d) and (e) are clear, since every term in the Koszul complex is itself a direct sum of copies of M.

To prove (f), note that if we are given a map $M \to M'$, there is an induced map of complexes

$$\mathcal{K}_\bullet(\underline{x};\, R) \otimes M \to \mathcal{K}_\bullet(\underline{x};\, R) \otimes M'.$$

This map induces a map $H_i(\underline{x};\, M) \to H_i\underline{x};\, M')$. Checking that this construction gives a functor is straightforward.

For part (g), we note that

$$(*) \quad 0 \to \mathcal{K}_\bullet(\underline{x};\, R) \otimes_R M' \to \mathcal{K}_\bullet(\underline{x};\, R) \otimes_R M \to \mathcal{K}_\bullet(\underline{x};\, R) \otimes_R M'' \to 0$$

is a short exact sequence of complexes, because each $\mathcal{K}_j(\underline{x};\, R)$ is R-free, so that the functor $\mathcal{K}_j(\underline{x};\, R) \otimes_R \_$ is exact. The long exact sequence is simply the result of applying the snake lemma to $(*)$. (This sequence can also be constructed by interpreting Koszul homology as a special case of Tor: we return to this point later.)

Finally, part (h) is immediate by induction from the iterative construction of the Koszul complex as a mapping cone and the Proposition at the top of p. 6 of the Lecture Notes of October 1. The map of augmentations is the map given by multiplication by x_n from $M/(x_1,\, \ldots,\, x_{n-1})M$ to itself, which is injective because $x_1,\, \ldots,\, x_n$ is a possibly improper regular sequence. $\square$

Corollary. *Let $\underline{x} = x_1,\, \ldots,\, x_n$ be a regular sequence on R and let $I = (\underline{x})R$. Then R/I has a finite free resolution of length n over R, and does not have any projective resolution of length shorter than n. Moreover, for every R-module M,*

$$\mathrm{Tor}_i^R(R/I,\, M) \cong H_i(\underline{x};\, M).$$

Proof. By part (f) of the preceding Proposition, $\mathcal{K}_\bullet(\underline{x};\, R)$ is acyclic. Since this is a free complex of finitely generated free modules whose augmentation is R/I, we see that R/I has the required resolution. Then, by definition of Tor, we may calculate $\mathrm{Tor}_i^R(R/I,\, M)$ as $H_i\big(\mathcal{K}_\bullet(\underline{x};\, R) \otimes_R M\big)$, which is precisely $H_i(\underline{x};\, M)$. To see that there is no shorter projective resolution of R/I, take $M = R/I$. Then

$$\mathrm{Tor}_n(R/I,\, R/I) = H_n(\underline{x};\, R/I) = \mathrm{Ann}_{R/I} I = R/I,$$

by part (c) of the preceding Proposition. If there were a shorter projective resolution, we would have $\mathrm{Tor}_n(R/I,\, R/I) = 0$. $\square$

Independence of Koszul homology of the base ring

The following observation is immensely useful. Suppose that we have a ring homomorphism $R \to S$ and an S-module M. By restriction of scalars, M is an R-module. Let $\underline{x} = x_1,\, \ldots,\, x_n \in R$ and let $\underline{y} = y_1,\, \ldots,\, y_n$ be the images of the x_i in S. Note that the actions of x_i and y_i on M are the same for every i. This means that the complexes $\mathcal{K}_\bullet(\underline{x};\, M)$ and $\mathcal{K}_\bullet(\underline{y};\, M)$ are the same. In consequence, $H_j(\underline{x};\, M) \cong H_j(\underline{y};\, M)$ for all j, as S-modules. Note that even if we treat M as an R-module initially in caclulating $H_j(\underline{x};\, M)$, we can recover the S-module structure on the Koszul homoolgy from the S-module structure of M. For every $s \in S$, multiplication by s is an R-linear map from M to M, and since $H_i(\underline{x};\ \_)$ is a covariant functor, we recover the action of s on $H_i(\underline{x};\, M)$.

Koszul homology and Tor

Let R be a ring and let $\underline{x} = x_1, \ldots, x_n \in R$. Let M be an R-module. We have already seen that if $x_1, \ldots, x_n$ is a regular sequence in R, then we may interpret $H_i(x_1, \ldots, x_n;\, M)$ as a Tor over R.

In general, we may interpret $H_i(\underline{x};\, M)$ as a Tor over an auxiliary ring. Let A be any ring such that R is an A-algebra. We may always take $A = \mathbb{Z}$ or $A = R$. If R contains a field K, we may choose $A = K$. Let $\underline{X} = X_1, \ldots, X_n$ be indeterminates over A, and map $B = A[X_1, \ldots, X_n] \to R$ by sending $X_j \mapsto x_j$ for all j. Then M is also a B-module, as in the section above, and $X_1, \ldots, X_n$ is a regular sequence in B.

Hence:

Proposition. *With notation as in the preceding paragraph,*

$$H_i(\underline{x}_1, \ldots, \underline{x}_; M) \cong \mathrm{Tor}_j^B\big(B/(\underline{X})B,\, M\big).$$

Corollary. *Let $\underline{x} = x_1, \ldots, x_n \in R$, let $I = (\underline{x})R$, and let M be an R-module. Then I kills $H_i(\underline{x};\, M)$ for all i.*

Proof. We use the idea of the discussion preceding the Proposition above, taking $A = R$, so that with $\underline{X} = X_1, \ldots, X_n$ we have an R-algebra map $B = R[\underline{X}] \to R$ such that $X_i \mapsto x_i$, $1 \le i \le n$. Then

$$(*) \quad H_i(\underline{x};\, M) \cong \mathrm{Tor}_i^B(B/(\underline{X})B,\, M).$$

When M is viewed as a B-module, every $X_i - x_i$ kiils M. But $\underline{X}$ kills $B/(\underline{X})B$, and so for every i, both $X_i - x_i$ and X_i kill $\mathrm{Tor}_i^B(B/(\underline{X})B,\, M)$. It follows that every $x_i = X_i - (X_i - x_i)$ kills it as well, and the result now follows from $(*)$. $\square$

An application to the study of regular local rings

Let M be a finitely generated R-module over a local ring $(R,\, m,\, K)$. A *minimal* free resolution of M may be constructed as follows. Let b_0 be the least number of generators of M, and begin by mapping R^{b_0} onto M using these generators. If

$$R^{b_i} \xrightarrow{\alpha_i} \cdots \xrightarrow{\alpha_1} R^{b_0} \xrightarrow{\alpha_0} M \longrightarrow 0$$

has already been constructed, let b_{i+1} be the least number of generators of $Z_i = \mathrm{Ker}\,(\alpha_i)$, and construct $\alpha_{i+1} : R^{b_{i+1}} \to R^{b_i}$ by mapping the free generators of $R^{b_{i+1}}$ to a minimal set of generators of $Z_i \subseteq R^{b_i}$. Think of the linear maps α_i , $i \ge 1$, as given by matrices. Then it is easy to see that a free resolution for M is minimal if and only if all of the matrices α_i for $i \ge 1$ have entries in m. We have the following consequence:

Proposition. *Let* (R, m, K) *be local, let* M *be a finitely generated* R*-modules, and let*

$$\cdots \to R^{b_i} \xrightarrow{\alpha_i} \cdots \to R^{b_0} \to M \to 0$$

be a minimal resolution of M*. Then for all* i*,* $\mathrm{Tor}_i^R(M, K) \cong K^{b_i}$*.*

Proof. We may use the minimal resolution displayed to calculate the values of Tor. We drop the augmentation M and apply $K \otimes_R \_$. Since all of the matrices have entries in m, the maps are alll 0, and we have the complex

$$\cdots \xrightarrow{0} K^{b_i} \xrightarrow{0} \cdots \xrightarrow{0} K^{b_0} \xrightarrow{0} 0.$$

Since all the maps are zero, the result stated is immediate. □

Theorem (Auslander-Buchsbaum). *Let* (R, m, K) *be a regular local ring. Then every finitely generated* R*-module has a finite projective resolution of length at most* $n = \dim(R)$*.*

Proof. Let $\underline{x} = x_1, \ldots, x_n$ be a regular system of parameters for R. These elements form a regular sequence. It follows that $K = R/(\underline{x})$ has a free resolution of length at most n. Hence, $\mathrm{Tor}_i(M, K) = 0$ for all $i > n$ and for every R-module M.

Now let M be a finitely generated R-module, and let

$$\cdots \to R^{b_i} \to \cdots \to R^{b_1} \to R^{b_0} \to R \to M \to 0$$

be a minimal free resolution of M. For $i > n$, $b_i = 0$ because $\mathrm{Tor}_i(M, K) = 0$, and so $R^{b_i} = 0$ for $i > n$, as required. □

It is true that a local ring is regular if and only if its residue class field has finite projective dimension: the converse part was proved by J.-P. Serre. The argument may be found in the Lecture Notes of February 13 and 16, Math 615, Winter 2004.

It is an open question whether, if M is a module of finite length over a regular local ring (R, m, K) of Krull dimension n, one has that

$$\dim_K \mathrm{Tor}_i(M, K) \geq \binom{n}{i}.$$

The numbers $\beta_i = \dim_K \mathrm{Tor}_i^R(M, K)$ are called the *Betti numbers* of M. If $\underline{x} = x_1, \ldots, x_n$ is a minimal set of generators of m, these may also be characterized as the dimensions of the Koszul homology modules $H_i(\underline{x}; M)$. A third point of view is that they give the ranks of the free modules in a minimal free resolution of M.

The binomial coefficients are the Betti numbers of $K = R/m$: they are the ranks of the free modules in the Koszul complex resolution of K. The question as to whether these are the smallest possible Betti numbers for an R-module was raised by David Buchsbaum and David Eisenbud in the first reference listed below, and was reported by Harthshorne in a

1979 paper (again, see the list below) as a question raised by Horrocks. The question is open in dimension 5 and greater. An affirmative answer would imply that the sum of the Betti numbers is at least 2^n: this weaker form is also open. We refer the reader interested in learning more about this problem to the following selected references:

D. Buchsbaum and D Eisenbud, *Algebra structures for finite free resolutions and some structure theorems for ideals of codimension 3*, Amer. J. of Math. **99** (1977) 447–485.

S.-T. Chang, *Betti numbers of modules of exponent two over regular local rings*, J. of Alg. **193** (1997) 640–659.

H. Charalambous, *Lower Bounds for Betti Numbers of Multigraded Modules*, J. of Alg. **137** (1991) 491–500.

D. Dugger, *Betti Numbers of Almost Complete Intersections*, Illinois J. Math. **44** (2000) 531–541.

D. Eisenbud and C. Huneke, editors, *Free resolutions in commutative algebra and algebraic geometry,* Research Notes in Mathematics: Sundance **90**, A. K. Peters, Ltd., 1992.

E.G. Evans and P. Griffith, *Syzygies*, London Math. Soc. Lecture Note Series **106** Cambridge Univ. Press, Cambridge, 1985.

R. Hartshorne, *Algebraic Vector Bundles on Projective Spaces: a Problem List*, Topology, **18** (1979) 117–128.

M. Hochster and B. Richert, *Lower bounds for Betti numbers of special extensions*, J. Pure and Appl. Alg **201** (2005) 328–339.

C. Huneke and B. Ulrich, *The Structure of Linkage*, Ann. of Math. **126** (1987) 277–334.

L. Santoni, *Horrocks' question for monomially graded modules*, Pacific J. Math. **141** (1990) 105–124.

Math 711: Lecture of October 5, 2007

More on mapping cones and Koszul complexes

Let $\phi_\bullet : B_\bullet \to A_\bullet$ be a map of complexes that is injective. We shall write $d_\bullet$ for the differential on $A_\bullet$ and $\delta_\bullet$ for the differential on $B_\bullet$. Then we may form a quotient complex $Q_\bullet$ such that $Q_n = B_n/\phi_n(A_n)$ for all n, and the differential on $Q_\bullet$ is induced by the differential on $B_\bullet$. Let $\mathcal{C}_\bullet$ be the mapping cone of $\phi_\bullet$.

Proposition. *With notation as in the preceding paragraph, $H_n(\mathcal{C}_\bullet) \cong H_n(Q_\bullet)$ for all n.*

Proof. We may assume that every ϕ_n is an inclusion map. A cycle in Q_n is represented by an element $z \in A_n$ whose boundary $d_n z$ is 0 in $A_{n-1}/\phi_{n-1}(B_{n-1})$. This means that $d_n z = \phi_{n-1}(b)$ for some $b \in B_{n-1}$. (Once we have specified z there is at most one choice of b, by the injectivity of ϕ_{n-1}.) The boundaries in Q_n are represented by the elements $d_{n+1}(A_{n+1}) + \phi_n(B)$. Thus,

$$H_n(Q_\bullet) \cong \frac{d_n^{-1}\big(\phi_{n-1}(B_{n-1})\big)}{d_{n+1}(A_{n+1}) + \phi_n(B_n)}.$$

A cycle in $\mathcal{C}_n$ is represented by a sum $z \oplus b'$ such that

$$\big(d_n(z) + (-1)^{n-1}\phi_{n-1}(b')\big) \oplus \delta_{n-1}(b') = 0$$

Again, this element is uniquely determined by z, which must satisfy $d_n(z) \in \phi_{n-1}(B_{n-1})$. b' is then uniquely determined as $(-1)^n b$ where $b \in B_{n-1}$ is such that $\phi_{n-1}(b) = d_n(z)$. Such an element b is automatically killed by δ_{n-1}, since

$$\phi_{n-2}\delta_{n-1}(b) = d_{n-1}\phi_{n-1}(b) = d_{n-1}d_n(z) = 0,$$

and ϕ_{n-2} is injective. A boundary in $\mathcal{C}_n$ has the form

$$\big(d_{n+1}(a) + (-1)^n\phi_n(b_n)\big) \oplus \delta_n b_n.$$

This shows that

$$H_n(\mathcal{C}_\bullet) \cong \frac{d_n^{-1}\big(\phi_{n-1}(B_{n-1})\big)}{d_{n+1}(A_{n+1}) + \phi_n(B_n)},$$

as required. $\square$

Corollary. *Let $\underline{x} = x_1, \ldots, x_n \in R$ be elements such that x_n is not a zerodivisor on the R-module M. Let $\underline{x}^- = x_1, \ldots, x_{n-1}$, i..e., the result of omitting x_n from the sequence. Then $H_i(\underline{x};\, M) \cong H_i(\underline{x}^-;\, M/x_nM)$ for all i.*

Proof. We apply that preceding Proposition with $A_\bullet = B_\bullet = \mathcal{K}_\bullet(\underline{x}^-;\, M)$, and ϕ_i given by multiplication by x_n in every degree i. Since every term of $\mathcal{K}_\bullet(\underline{x}^-;\, M)$ is a finite direct sum of copies of M, the maps ϕ_i are injective. The mapping cone, which is $\mathcal{K}_\bullet(\underline{x};\, M)$, therefore has the same homology as the quotient complex, which may be identified with

$$\mathcal{K}_\bullet(\underline{x}^-,\, M) \otimes (R/x_nR) \cong \mathcal{K}_\bullet(\underline{x}^-;\, R) \otimes_R M \otimes_R R/x_nR \cong \mathcal{K}_\bullet(\underline{x}^-;\, R) \otimes_R (M/x_nM)$$

which is $\mathcal{K}_\bullet(\underline{x}^-;\, M/x_nM)$, and the result follows. □

We also observe:

Proposition. *Let $\phi_\bullet : B_\bullet \to A_\bullet$ be any map of complexes and let $\mathcal{C}_\bullet$ be the mapping cone. In the long exact sequence*

$$\cdots \to H_n(A_\bullet) \to H_n(\mathcal{C}_\bullet) \to H_{n-1}(B_\bullet) \xrightarrow{\partial_{n-1}} H_{n-1}(A_\bullet) \to \cdots$$

the connecting homomorphism ∂_{n-1} is induced by $(-1)^{n-1}\phi_{n-1}$.

Proof. We follow the prescription for constructing the connecting homomorphism. Let $b \in B_{n-1}$ be a cycle in B_{n-1}. We lift this cycle to an element of $\mathcal{C}_n$ that maps to it: one such lifting is $0 \oplus b$ (the choice of lifting does not affect the result). We now apply the differential in the mapping cone $\mathcal{C}_\bullet$ to the lifting: this gives

$$(-1)^{n-1}\phi_{n-1}(b) \oplus \delta_{n-1}(b) = (-1)^{n-1}\phi_{n-1}(b) \oplus 0,$$

since b was a cycle in B_{n-1}. Call the element on the right α. Finally, we choose an element of A_{n-1} that maps to α: this gives $(-1)^{n-1}\phi_{n-1}(b)$, which represents the value of $\partial_{n-1}([b])$, as required. □

Corollary. *Let $\underline{x} = x_1, \ldots, x_n \in R$ be arbitrary elements. Let $\underline{x}^- = x_1, \ldots, x_{n-1}$, i..e., the result of omitting x_n from the sequence. Let M be any R-module. Then there are short exact sequences*

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

for every integer i.

Proof. By the preceding Proposition, the long exact sequence for the homology of the mapping cone of the map of complexes

$$\mathcal{K}_\bullet(\underline{x}^-;\, M) \xrightarrow{x_n \cdot} \mathcal{K}_\bullet(\underline{x}^-;\, M)$$

has the form

$$\cdots \to H_i(\underline{x}^-;\, M) \xrightarrow{(-1)^i x_n\cdot} H_i(\underline{x}^-;\, M) \to H_i(\underline{x};\, M)$$

$$\to H_{i-1}(\underline{x}^-;\, M) \xrightarrow{(-1)^{i-1} x_n\cdot} H_{i-1}(\underline{x}^-;\, M) \to \cdots$$

Since the maps given by multiplication by x_n and by $-x_n$ have the same kernel and cokernel, this sequence implies the existence of the short exact sequences specified in the statement of the Theorem. □

The cohomological Koszul complex

Notice that if P is a finitely generated projective module over a ring R, $\_^*$ denotes the functor that sends $N \mapsto \mathrm{Hom}_R(N,\, R)$, and M is any module, then there is a natural isomorphism

$$\mathrm{Hom}_R(P,\, M) \cong P^* \otimes_R M$$

such that the inverse map η_P is defined as follows: η_P is the linear map induced by the R-bilinear map B_P given by $B_P(g,\, u)(v) = g(v)u$ for $g \in P^*$, $u \in M$, and $v \in P$. It is easy to check that

(1) $\eta_{P\oplus Q} = \eta_P \oplus \eta_Q$ and

(2) that η_R is an isomorphism.

It follows at once that

(3) η_{R^n} is an isomorphism for all $n \in \mathbb{N}$.

For any finitely generated projective module P we can choose Q such that $P \oplus Q \cong R^n$, and then, since $\eta_P \oplus \eta_Q$ is an isomorphism, it follows that

(4) η_P is an isomorphism for every finitely generated projective module P.

If R is a ring, M an R-module, and $\underline{x} = x_1,\, \ldots\, , x_n \in R$, the *cohomological Koszul complex* $\mathcal{K}^\bullet(\underline{x};\, M)$, is defined as

$$\mathrm{Hom}_R\big(\mathcal{K}_\bullet(\underline{x};\, R),\, M\big),$$

and its cohomology, called *Koszul cohomology*, is denoted $H^\bullet(\underline{x};\, M)$. The cohomological Koszul complex of R (and, it easily follows, of M) is isomorphic with the homological Koszul complex numbered "backward," but this is not quite obvious: one needs to make sign changes on the obvious choices of bases to get the isomorphism.

To see this, take the elements $u_{j_1,\dots,j_i}$ with $1 \le j_1 < \cdots < j_i \le n$ as a basis for $\mathcal{K}_i = \mathcal{K}_i(\underline{x};\, R)$. We continue to use the notation $\_^*$ to indicate the functor $\mathrm{Hom}_R(\_,\, R)$. We want to set up isomorphisms $\mathcal{K}_{n-i}^* \cong \mathcal{K}_i$ that commute with the differentials.

Note that there is a bijection between the two free bases for $\mathcal{K}_i$ and $\mathcal{K}_{n-i}$ as follows: given $1 \le j_1 < \cdots < j_i \le n$, let $k_1, \dots, k_{n-i}$ be the elements of the set

$$\{1,\, 2,\, \dots,\, n\} - \{j_1, \dots, j_i\}$$

arranged in increasing order, and let $u_{j_1,\dots,j_i}$ correspond to $u_{k_1,\dots,k_{n-i}}$ which we shall also denote as $v_{j_1,\dots,j_i}$.

When a free R-module G has free basis $b_1, \dots, b_t$, this determines what is called a *dual basis* $b'_1, \dots, b'_t$ for G^*, where b'_j is the map $G \to R$ that sends b_j to 1 and kills the other elements in the free basis. Thus, $\mathcal{K}_{n-i}^*$ has basis $v'_{j_1,\dots,j_i}$. However, when we compute the value of the differential d_{n-i+1}^* on $v'_{j_1,\dots,j_i}$, while the coefficient of $v'_{h_1,\dots,h_{i-1}}$ does turn out to be zero unless the elements $h_1 < \cdots < h_{i-1}$ are included among the j_i, if the omitted element is j_t then the coefficient of $v'_{h_1,\dots,h_{i-1}}$ is

$$d_{n-i+1}^*(v'_{j_1,\dots,j_i})(v_{h_1,\dots,h_{i-1}}) = v'_{j_1,\dots,j_i}\big(d_{n-i+1}(v_{h_1,\dots,h_{i-1}})\big),$$

which is the coefficient of $v_{j_1,\dots,j_i}$ in $d_{n-i+1}(v_{h_1,\dots,h_{i-1}})$.

Note that the complement of $\{j_1, \dots, j_i\}$ in $\{1,\, 2,\, \dots,\, n\}$ is the same as the complement of $\{h_1, \dots, h_{i-1}\}$ in $\{1,\, 2,\, \dots,\, n\}$, except that one additional element, j_t, is included in the latter. Thus, the coefficient needed is $(-1)^{s-1}x_{j_t}$, where $s-1$ is the number of elements in the complement of $\{h_1, \dots, h_{i-1}\}$ that precede j_t. The signs don't match what we get from the differential in $\mathcal{K}_\bullet(\underline{x};\, R)$: we need a factor of $(-1)^{(s-1)-(t-1)}$ to correct (note that $t-1$ is the number of elements in $j_1, \dots, j_i$ that precede j_t). This sign correction may be written as $(-1)^{(s-1)+(t-1)}$, and the exponent is $j_t - 1$, the total number of elements preceding j_t in $\{1, 2, \dots, n\}$. This sign implies that the signs will match the ones in the homological Koszul complex if we replace every v'_{j_i} by $(-1)^{\Sigma}v'_{j_i}$, where $\Sigma = \sum_{t=1}^{i}(j_t - 1)$. This completes the proof. $\square$

This duality enables us to compute Ext using Koszul homology, and, hence, Tor in certain instances:

Theorem. *Let $\underline{x} = x_1, \dots, x_n$ be a possibly improper regular sequence in a ring R and let M be any R-module. Then*

$$\mathrm{Ext}_R^i(R/(\underline{x})R;\, M) \cong H^i(\underline{x};\, M) \cong H_{n-i}(\underline{x};\, M) \cong \mathrm{Tor}_{n-i}^R(R/(\underline{x})R,\, M).$$

Proof. Because the Koszul complex on the x_i is a free resolution of $R/(\underline{x})R$, we may use it to calculate $\mathrm{Ext}^j(R/(\underline{x})R,\, M)$: this yields the leftmost isomorphism. The middle isomorphism now follows from the self-duality of the Koszul complex proved above, and we have already proved that the Koszul homology yields Tor when $\underline{x}$ is a regular sequence in R: this is simply because we may use again that $\mathcal{K}_\bullet(\underline{x};\, R)$ is a free resolution of $R/(\underline{x})R$. □

Depth and Ext

When $R \to S$ is a homomorphism of Noetherian rings, N is a finitely generated R-module, and M is a finitely generated S-module, the modules $\mathrm{Ext}^j_R(N,\, M)$ are finitely generated S-modules. One can see this by taking a left resolution $G_\bullet$ of N by finitely generated free R-modules, so that

$$\mathrm{Ext}^j_R(N,\, M) = H^j\big(\mathrm{Hom}_R(G_\bullet,\, M)\big).$$

Since each term of $\mathrm{Hom}_R(G_\bullet,\, M)$ is a finite direct sum of copies of M, the statement follows.

If I is an ideal of R such that $IM \neq M$, then any regular sequence in I on M can be extended to a maximal such sequence that is necessarily finite. To see that we cannot have an infinite sequence $x_1, \, \ldots \, , x_n, \, \ldots \in I$ that is a regular sequence on M we may reason as follows. Because R is Noetherian, the ideals $J_n = (x_1, \, \ldots \, , x_n)R$ must be eventually constant. Alternatively, we may argue that because M is Noetherian over S, the submodules J_nM must be eventually constant. In either case, once $J_nM = J_{n+1}M$ we have that $x_{n+1}M \subseteq J_nM$, and so the action of x_{n+1} on M/J_nM is 0. Since $J_n \subseteq I$ and $IM \neq M$, we have that $M/J_nM \neq 0$, and this is a contradiction, since x_{n+1} is supposed to be a nonzerodivisor on M/J_nM. We shall show that maximal regular sequences on M in I all have the same length, which we will then define to be the *depth* of M on I.

The following result will be the basis for our treatment of depth.

Theorem. *Let $R \to S$ be a homomorphism of Noetherian rings, let $I \subseteq R$ be an ideal and let N be a finitely generated R-module with annihilator I. Let M be a finitely generated S-module with annihilator $J \subseteq S$.*

(a) *The support of $N \otimes_R M$ is $\mathcal{V}(IS + J)$. Hence, $N \otimes_R M = 0$ if and only if $IS + J = S$. In particular, $M = IM$ if and only if $IS + J = S$.*

(b) *If $IM \neq M$, then there are finite maximal regular sequences $x_1, \, \ldots \, , x_d$ on M in I. For any such maximal regular sequence, $\mathrm{Ext}^i_R(N,\, M) = 0$ if $i < d$ and $\mathrm{Ext}^d_R(N,\, M) \neq 0$. In particular, these statements hold when $N = R/I$. Hence, any two maximal regular sequences in I on M have the same length.*

(c) *$IM = M$ if and only if $\mathrm{Ext}^i_R(N,\, M) = 0$ for all i. In particular, this statement holds when $N = R/I$.*

Proof. (a) $N \otimes_R M$ is clealy killed by J and by I. Since it is an S-module, it is also killed by IS and so it is killed by $IS + J$. It follows that any prime in the support must contain

$IS+J$. Now suppose that $Q \in \mathrm{Spec}\,(S)$ is in $\mathcal{V}(IS+J)$, and let P be the contraction of Q to R. It suffices to show that $(N \otimes_R M)_Q \neq 0$, and so it suffices to show that $N_P \otimes_{R_P} M_Q \neq 0$. Since $I \subseteq P$, $N_P \neq 0$ and N_P/PN_P is a nonzero vector space over $\kappa = R_P/PR_P$: call it κ^s, where $s \geq 1$. M_Q maps onto $M_Q/QM_Q = \lambda^t$, where $\lambda = S_Q/QS_Q$, is a field, $t \geq 1$, and we have $\kappa \hookrightarrow \lambda$. But then we have

$$(N \otimes_R M)_Q \cong N_P \otimes_{R_P} M_Q \twoheadrightarrow \kappa^s \otimes_{R_P} \lambda^t \cong \kappa^s \otimes_\kappa \lambda^t \cong (\kappa \otimes_\kappa \lambda)^{st} \cong \lambda^{st} \neq 0,$$

as required. The second statement in part (a) is now clear, and the third is the special case where $N = R/I$.

Now assume that $M \neq IM$, and choose any maximal regular sequence $x_1, \ldots, x_d \in I$ on M. We shall prove by induction on d that $\mathrm{Ext}^i_R(N, M) = 0$ for $i < d$ and that $\mathrm{Ext}^d_R(N, M) \neq 0$.

First suppose that $d = 0$. Let $Q_1, \ldots, Q_h$ be the associated primes of M in S. Let P_j be the contraction of Q_j to R for $1 \leq j \leq h$. The fact that $\mathrm{depth}_I M = 0$ means that I consists entirely of zerodivisors on M, and so I maps into the union of the Q_j. This means that I is contained in the union of the P_j, and so I is contained in one of the P_j: called it $P_{j_0} = P$. Choose $u \in M$ whose annihilator in S is Q_{j_0}, and whose annihilator in R is therefore P. It will suffice to show that $\mathrm{Hom}_R(N, M) \neq 0$, and therefore to show that its localization at P is not 0, i.e., that $\mathrm{Hom}_{R_P}(N_P, M_P) \neq 0$. Since P contains $I = \mathrm{Ann}_R N$, we have that $N_P \neq 0$. Therefore, by Nakayama's lemma, we can conclude that $N_P/PN_P \neq 0$. This module is then a nonzero finite dimensional vector space over $\kappa_P = R_P/PR_P$, and we have a surjection $N_P/PN_P \twoheadrightarrow \kappa_P$ and therefore a composite surjection $N_P \twoheadrightarrow \kappa_P$. Consider the image of $u \in M$ in M_P. Since $\mathrm{Ann}_R u = P$, the image v of $u \in M_P$ is nonzero, and it is killed by P. Thus, $\mathrm{Ann}_{R_P} v = PR_P$, and it follows that v generates a copy of κ_P in M_P, i.e., we have an injection $\kappa_P \hookrightarrow M_P$. The composite map $N_P \twoheadrightarrow \kappa_P \hookrightarrow M_P$ gives a nonzero map $N_P \to M_P$, as required.

Finally, suppose that $d > 0$. Let $x = x_1$, which is a nonzerodivisor on M. Note that $x_2, \ldots, x_d \in I$ is a maximal regular sequence on M/xM. Since $x \in I$, we have that x kills N. The short exact sequence $0 \to M \to M \to M/xM \to 0$ gives a long exact sequence for Ext when we apply $\mathrm{Hom}_R(N, \_\,)$. Because x kills N, it kills all of the Ext modules in this sequence, and thus the maps induced by multiplication by x are all 0. This implies that the long exact sequence breaks up into short exact sequences

$$(*_j) \quad 0 \to \mathrm{Ext}^j_R(N, M) \to \mathrm{Ext}^j_R(N, M/xM) \to \mathrm{Ext}^{j+1}_R(N, M) \to 0$$

We have from the induction hypothesis that the modules $\mathrm{Ext}^j_R(N, M/xM) = 0$ for $j < d-1$, and the exact sequence above shows that $\mathrm{Ext}^j_R(N, M) = 0$ for $j < d$. Moreover, $\mathrm{Ext}^{d-1}_R(N, M/xM) \neq 0$, and $(*_{d-1})$ shows that $\mathrm{Ext}^{d-1}_R(N, M/xM)$ is isomorphic with $\mathrm{Ext}^d_R(N, M)$.

The final statement in part (b) follows because the least exponent j for which, say, $\mathrm{Ext}^j_R(R/I, M) \neq 0$ is independent of the choice of maximal regular sequence.

It remains to prove part (c). If $IM \neq M$, we can choose a maximal regular sequence $x_1, \ldots, x_d$ on M in I, and then we know from part (b) that $\mathrm{Ext}^d_R(N, M) \neq 0$. On the other hand, if $IM = M$, we know that $IS + \mathrm{Ann}_R M = S$ from part (a), and this ideal kills every $\mathrm{Ext}^j_R(N, M)$, so that all of the Ext modules vanish. □

If $R \to S$ is a map of Noetherian rings, M is a finitely generated S-module, and $IM \neq M$, we define $\mathrm{depth}_I M$, the *depth* of M on I, to be, equivalently, the length of *any* maximal regular sequence in I on M, or $\inf\{j \in \mathbb{Z} : \mathrm{Ext}^j_R(R/I, M) \neq 0\}$. If $IM = M$, we define the depth of M on I as $+\infty$, which is consistent with the Ext characterization.

Note the following:

Corollary. *With hypothesis as in the preceding Theorem,* $\mathrm{depth}_I M = \mathrm{depth}_{IS} M$. *Moreover, if R' is flat over R, e.g., a localization of R, then* $\mathrm{depth}_{IR'} R' \otimes_R M \geq \mathrm{depth}_I M$.

Proof. Choose a maximal regular sequence in I, say $x_1, \ldots, x_d$. These elements map to a regular sequence in IS. We may replace M by $M/(x_1, \ldots, x_d)M$. We therefore reduce to showing that when $\mathrm{depth}_I M = 0$, it is also true that $\mathrm{depth}_{IS} M = 0$. But it was shown in the proof of the Theorem above that that under the condition $\mathrm{depth}_I M = 0$ there is an element $u \in M$ whose annihilator is an associated prime $Q \in \mathrm{Spec}\,(S)$ of M that contains IS. The second statement follows from the fact that calculation of Ext_R commutes with flat base change when the first module is finitely generated over R. (One may also use the characterization in terms of regular sequences.) □

We also note:

Proposition. *With hypothesis as in the preceding Theorem, let $\underline{x} = x_1, \ldots, x_n$ be generators of $I \subseteq R$. If $IM = M$, then all of the Koszul homology $H_i(\underline{x};\, M) = 0$. If $IM \neq M$, then $H_{n-i}(\underline{x};\, M) = 0$ if $i < d$, and $H_{n-d}(\underline{x};\, M) \neq 0$.*

Proof. We may map a Noetherian ring B containing elements $X_1, \ldots, X_n$ that form a regular sequence in B to R so that $X_i \mapsto x_i$, $1 \leq i \leq n$. For example, we may take $B = R[X_1, \ldots, X_n]$ and map to R using the R-algebra map that sends $X_i \mapsto x_i$, $1 \leq i \leq n$. Let $J = (X_1, \ldots, X_n)B$. Then $\mathrm{depth}_I M = \mathrm{depth}_J M$, and the latter is determined by the least integer j such that $\mathrm{Ext}^j_B(B/(\underline{X})B, M) \neq 0$. The result is now immediate from the Theorem at the bottom of p. 4. □

Cohen-Macaulay rings and lifting while preserving height

Proposition. *A Noetherian ring R is Cohen-Macaulay if and only if for every proper ideal I of R,* $\mathrm{depth}_I R = \mathrm{height}\,(I)$.

Proof. Suppose that R is Cohen-Macaulay, and let I be any ideal of R. We use induction on $\mathrm{height}\,(I)$. If $\mathrm{height}\,(I) = 0$, then I is contained in a minimal prime of R, and so

$\operatorname{depth}_I R = 0$. Now suppose that height $(I) > 0$. Each prime in Ass (R) must be minimal: otherwise, we may localize at such a prime, which yields a Cohen-Macaulay ring of positive dimension such that every element of its maximal ideal is a zerodivisor, a contradiction. Since I is not contained in the union of the minimal primes, I is not contained in the union of the primes in Ass (R). Choose an element $x_1 \in I$ not in any minimal prime of R and, hence, not a zerodivisor on R. It follows that R/x_1R is Cohen-Macaulay, and the height of I drops exactly by one. The result now follows from the induction hypothesis applied to $I/x_1R \in R/x_1R$.

For the converse, we may apply the hypothesis with I a given maximal ideal m of height d. Then m contains a regular sequence of length d, say $x_1, \ldots, x_d$. This is preserved when we pass to R_m. The regular sequence remains regular in R_m, and so must be a system of parameters for R_m: killing a nonzerodivisor drops the dimension of a local ring by exactly 1. Hence, R_m is Cohen-Macaulay. $\square$

We also note:

Proposition. *Let R be a Noetherian ring and let $x_1, \ldots, x_d$ generate a proper ideal I of height d. Then there exist elements $y_1, \ldots, y_d \in R$ such that for every i, $1 \leq i \leq d$, $y_i \in x_i + (x_{i+1}, \ldots, x_d)R$, and for all i, $1 \leq i \leq d$, $y_1, \ldots, y_i$ generate an ideal of height i in R. Moreover, $(y_1, \ldots, y_d) = I$, and $y_d = x_d$.*

If R is Cohen-Macaulay, then $y_1, \ldots, y_d$ is a regular sequence.

Proof. We use induction on d. Note that by the coset form of the Lemma on prime avoidance, we cannot have that $x_1+(x_2, \ldots, x_d)R$ is contained in the union of the minimal primes of R, or else $(x_1, \ldots, x_d)R$ has height 0. This enables us to pick $y_1 = x_1 + \Delta_1$ with $\Delta_1 \in (x_2, \ldots, x_d)R$ such that y_1 is not in any minimal prime of R. In case R is Cohen-Macaulay, this implies that y_1 is not a zerodivisor. It is clear that $(y_1, x_2, \ldots, x_d)R = I$. The result now follows from the induction hypothesis applied to the images of $x_2, \ldots, x_d$ in R/y_1R. $\square$

Note that even in the polynomial ring $K[x, y, z]$ the fact that three elements generate an ideal of height three does not imply that these elements form a regular sequence: $(1-x)y$, $(1-x)z$, x gives a counterexample.

Proposition. *Let R be a Noetherian ring, let $\mathfrak{p}$ be a minimal prime of R, and let $x_1, \ldots, x_d$ be elements of R such that $(x_1, \ldots, x_i)(R/\mathfrak{p})$ has height i, $1 \leq i \leq d$. Then there are elements $\delta_1, \ldots, \delta_d \in \mathfrak{p}$ such that if $y_i = x_i + \delta_i$, $1 \leq i \leq d$, then $(y_1, \ldots, y_i)R$ has height i, $1 \leq i \leq d$.*

Proof. We construct the δ_i recursively. Suppose that $\delta_1, \ldots, \delta_t$ have already been chosen: t may be 0. If $t < d$, we cannot have that $x_{t+1} + \mathfrak{p}$ is contained in the union of the minimal primes of $(y_1, \ldots, y_t)$. If that were the case, by the coset form of prime avoidance we would have that $x_{t+1}R + \mathfrak{p} \subseteq Q$ for one such minimal prime Q. Then Q has height at most t, but modulo $\mathfrak{p}$ all of $x_1, \ldots, x_{t+1}$ are in Q, so that height $(Q/\mathfrak{p}) \geq t+1$, a contradiction. $\square$

The following result will be useful in proving the colon-capturing property for tight closure.

Lemma. *Let P be a prime ideal of height h in a Cohen-Macaulay ring S. Let $x_1, \ldots, x_{k+1}$ be elements of $R = S/P$ such that $(x_1, \ldots, x_k)R$ has height k in R while $(x_1, \ldots, x_{k+1})R$ has height $k+1$. Then we can choose elements $y_1, \ldots, y_h \in P$ and $z_1, \ldots, z_{k+1} \in S$ such that:*

(1) *$y_1, \ldots, y_h, z_1, \ldots, z_{k+1}$ is a regular sequence in S.*

(2) *The images of $z_1, \ldots, z_k$ in R generate the ideal $(x_1, \ldots, x_k)R$.*

(3) *The image of z_{k+1} in R is x_{k+1}.*

Proof. By the first Proposition on p. 8, we may assume without loss of generality that $x_1, \ldots, x_i$ generate an ideal of height i in R, $1 \leq i \leq k$. We also know this for $i = k+1$. Choose z_i arbitrarily such that z_i maps to x_i, $1 \leq i \leq k+1$. Choose a regular sequence $y_1, \ldots, y_h$ of length h in P. Then P is a minimal prime of $(y_1, \ldots, y_h)S$. By the second Proposition on p. 8 applied to the images of the of the z_i in $S/(y_1, \ldots, y_h)S$ with $\mathfrak{p} = P/(y_1, \ldots, y_h)S$, we may alter the z_i by adding elements of P so that the height of the image of the ideal generated by the images of $z_1, \ldots, z_i$ in $S/(y_1, \ldots, y_h)$ is i, $1 \leq i \leq k+1$. Since $S/(y_1, \ldots, y_h)S$ is again Cohen-Macaulay, it follows from the first Proposition on p. 8 that the images of the $z_1, \ldots, z_{k+1}$ modulo $(y_1, \ldots, y_h)S$ form a regular sequence. But this means that $y_1, \ldots, y_h, z_1, \ldots, z_{k+1}$ is a regular sequence. $\square$

Colon-capturing

We can now prove a result on the colon-capturing property of tight closure.

Theorem (colon-capturing). *Let R be a reduced Noetherian ring of prime characteristic $p > 0$ that is a homomorphic image of a Cohen-Macaulay ring. Let $x_1, \ldots, x_{k+1}$ be elements of R. Let I_t denote the ideal $(x_1, \ldots, x_t)R$, $0 \leq t \leq k+1$. Suppose that the image of the ideal I_k has height k modulo every minimal prime of R, and that the image of the ideal $I_{k+1}R$ has height $k+1$ modulo every minimal prime of R. Then:*

(a) $I_k :_R x_{k+1} \subseteq I_k^*$.

(b) *If R has a test element, $I_k^* :_R x_{k+1} \subseteq I_k^*$, i.e., x_{k+1} is not a zerodivisor on R/I_k^*.*

Proof. To prove part (a), note that it suffices to prove the result working in turn modulo each of the finitely many minimal primes of R. We may therefore assume that R is a domain. We can consequently write $R = S/P$, where S is Cohen-Macaulay. Let h be the height of P. Then we can choose $y_1, \ldots, y_h \in P$ and $z_1, \ldots, z_{k+1}$ in S as in the conclusion of the Lemma just above, i.e., so $y_1, \ldots, y_h, z_1, \ldots, z_{k+1}$ is a regular sequence in S, and so that we may replace $x_1, \ldots, x_{k+1}$ by the images of the z_i in R. Since P has height h, it is a minimal prime of $J = (y_1, \ldots, y_h)S$, and so if we localize at $S - P$, we have that

P is nilpotent modulo J. Hence, for each generator g_i of P we can choose $c_i \in S - P$ and an expoment of the form $q_i = p^{e_i}$ such that $c_i g_i^{q_i} \in J$. It follows that if $c \in S - P$ is the product of the c_i and q_0 is the maximum of the q_i, then $cP^{[q_0]} \subseteq J$.

Now suppose that we have a relation

$$rx_{k+1} = r_1 x_1 + \cdots + r_k x_k$$

in R. Then we can lift $r, r_1, \ldots, r_k$ to elements $s, s_1, \ldots, s_k \in S$ such that

$$sz_{k+1} = s_1 z_1 + \cdots + s_k z_k + v,$$

where $v \in P$. Then for all $q \geq q_0$ we may raise both sides to the qth power and multiply by c to obtain

$$cs^q z_{k+1}^q = cs_1^q z_1^q + \cdots + cs_k^q z_k^q + cv^q;$$

moreover, $cv^q \in (y_1, \ldots, y_h)$. Therefore

$$cs^q z_{k+1}^q \in (z_1^q, \ldots, z_k^q, y_1, \ldots, y_h)S.$$

Since $y_1, \ldots, y_h, z_1^q, \ldots, z_{k+1}^q$ is a regular sequence in S, we have that

$$cs^q \in (z_1^q, \ldots, z_k^q)S + (y_1, \ldots, y_h)S.$$

Let $\overline{c} \in R^\circ$ be the image of c. Then, working modulo $P \supseteq (y_1, \ldots, y_h)R$, we have

$$\overline{c}r^q \in (x_1, \ldots, x_k)^{[q]}$$

for all $q \geq q_0$, and so $r \in (x_1, \ldots, x_k)^*$ in R, as required. This completes the argument for part (a).

It remains to prove part (b). Suppose that R has a test element $d \in R^\circ$, that $r \in R$, and that $rx_{k+1} \in I_k^*$. Then there exists $c \in R^\circ$ such that $c(rx_{k+1})^q \in (I_k^*)^{[q]}$ for all $q \gg 0$. Note that $(I_k^*)^{[q]} \subseteq (I_k^{[q]})^*$, so that $cr^q x_{k+1}^q \in (I_k^{[q]})^*$, and $dcr^q x_{k+1}^q \in I_k^{[q]}$. From part (a), it follows that $dcr^q \in (I_k^{[q]})^*$ for all $q \gg 0$, and so $d^2 cr^q \in I_k^{[q]}$ for all $q \gg 0$. But then $r \in I_k^*$, as required. $\square$

Corollary. *Let R be a Noetherian ring of prime characteristic $p > 0$ that is a homomorphic image of a Cohen-Macaulay ring, and suppose that R is weakly F-regular. Then R is Cohen-Macaulay.*

Proof. Consider a local ring of R at a maximal ideal. Then this local ring remains weakly F-regular, and is normal. Therefore, we may assume that R is a local domain. Let $x_1, \ldots, x_n$ be a system of parameters. Then for every $k < n$, $(x_1, \ldots, x_k) :_R x_{k+1} \subseteq (x_1, \ldots, x_k)^* = (x_1, \ldots, x_k)$, since $(x_1, \ldots, x_k)$ is tightly closed. $\square$

Math 711: Lecture of October 8, 2007

Properties of regular sequences

In the sequel we shall need to make use of certain standard facts about regular sequences on a module: for convenience, we collect these facts here. Many of the proofs can be made simpler in the case of a regular sequence that is *permutable*, i.e., whose terms form a regular sequence in every order. This hypothesis holds automatically for regular sequences on a finitely generated module over a local ring. However, we shall give complete proofs here for the general case, without assuming permutability. The following fact will be needed repeatedly.

Lemma. *Let R be a ring, M an R-module, and let $x_1, \ldots, x_n$ be a possibly improper regular sequence on M. If $u_1, \ldots, u_n \in M$ are such that*

$$\sum_{j=1}^{n} x_j u_j = 0,$$

then every $u_j \in (x_1, \ldots, x_n)M$.

Proof. We use induction on n. The case where $n = 1$ is obvious. We have from the definition of possibly improper regular sequence that $u_n = \sum_{j=1}^{n-1} x_j v_j$, with $v_1, \ldots, v_{n-1} \in M$, and so $\sum_{j=1}^{n-1} x_j(u_j + x_n v_j) = 0$. By the induction hypothesis, every $u_j + x_n v_j \in (x_1, \ldots, x_{n-1})M$, from which the desired conclusion follows at once $\square$

Proposition. *Let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_h = M$ be a finite filtration of M. If $x_1, \ldots, x_n$ is a possibly improper regular sequence on every factor M_{k+1}/M_k, $0 \le k \le h-1$, then it is a possibly improper regular sequence on M. If, moreover, it is a regular sequence on M/M_{h-1}, then it is a regular sequence on M.*

Proof. If we know the result in the possibly improper case, the final statement follows, for if $I = (x_1, \ldots, x_n)R$ and $IM = M$, then the same hold for every homomorphic image of M, contradicting the hypothesis on M/M_{h-1}.

It remains to prove the result when $x_1, \ldots, x_n$ is a possibly improper regular sequence on every factor. The case where $h = 1$ is obvious. We use induction on h. Suppose that $h = 2$, so that we have a short exact sequence

$$0 \to M_1 \to M \to N \to 0$$

and $x_1, \dots, x_n$ is a possibly regular sequence on M_1 and N. Then x_1 is a nonzerodivisor on M, for if $x_1u = 0$, then x_1 kills the image of u in N. But this shows that the image of u in N must be 0, which means that $u \in M_1$. But x_1 is not a zerodivisor on M_1. It follows that

$$0 \to xM_1 \to xM \to xN \to 0$$

is also exact, since it is isomorphic with the original short exact sequence. Therefore, we have a short exact sequence of quotients

$$0 \to M_1/x_1M_1 \to M/x_1N \to M/x_1N \to 0.$$

We may now apply the induction hypothesis to conclude that $x_2, \dots, x_n$ is a possibly improper regular sequence on M/x_1M, and hence that $x_1, \dots, x_n$ is a possibly improper regular sequence on M.

We now carry through the induction on h. Suppose we know the result for filtrations of length $h-1$. We can conclude that $x_1, \dots, x_n$ is a possibly improper regular sequence on M_{h-1}, and we also have this for M/M_{h-1}. The result for M now follows from the case where $h = 2$. $\square$

Theorem. *Let $x_1, \dots, x_n \in R$ and let M be an R-module. Let $t_1, \dots, t_n$ be integers ≥ 1. Then $x_1, \dots, x_n$ is a regular sequence (respectively, a possibly improper regular sequence) on M iff $x_1^{t_1}, \dots, x_n^{t_n}$ is a regular sequence on M (respectively, a possibly improper regular sequence on M).*

Proof. If $IM = M$ then $I^kM = M$ for all k. If each of I and J has a power in the other, it follows that $IM = M$ iff $JM = M$. Thus, we will have a proper regular sequence in one case iff we do in the other, once we have established that we have a possibly improper regular sequence. In the sequel we deal with possibly improper regular sequences, but for the rest of this proof we omit the words "possibly improper."

Suppose that $x_1, \dots, x_n$ is a regular sequence on M. By induction on n, it will suffice to show that $x_1^{t_1}, x_2, \dots, x_n$ is a regular sequence on M: we may pass to $x_2, \dots, x_n$ and $M/x_n^{t_1}M$ and then apply the induction hypothesis. It is clear that $x_1^{t_1}$ is a nonzerodivisor when x_1 is. Moreover, $M/x_1^{t_1}M$ has a finite filtration by submodules $x_1^jM/x_1^{t_1}M$ with factors $x_1^jM/x_1^{j+1}M \cong M/x_1M$, $1 \leq j \leq t_1 - 1$. Since $x_2, \dots, x_n$ is a regular sequence on each factor, it is a regular sequence on $M/x_1^{t_1}M$ by the preceding Proposition.

For the other implication, it will suffice to show that if $x_1, \dots, x_{j-1}, x_j^t, x_{j+1}, \dots, x_n$ is a regular sequence on M, then $x_1, \dots, x_n$ is: we may change the exponents to 1 one at a time. The issue may be considered mod $(x_1, \dots, x_{j-1})M$. Therefore, it suffices to consider the case $j = 1$, and we need only show that if $x_1^t, x_2, \dots, x_n$ is a regular sequence on M then so is $x_1, \dots, x_n$. It is clear that if x_1^t is a nonzerodivisor then so is x_1.

By induction on n we may assume that $x_1, \dots, x_{n-1}$ is a regular sequence on M. We need to show that if $x_nu \in (x_1, \dots, x_{n-1})M$, then $u \in (x_1, x_2, \dots, x_{n-1})M$. If we multiply by x_1^{t-1}, we find that

$$x_n(x_1^{t-1}u) \in (x_1^t, x_2, \dots, x_{n-1})M,$$

and so

$$x_1^{t-1}u = x_1^t v_1 + x_2 v_2 + \cdots + x_{n-1}v_{n-1},$$

i.e.,

$$x_1^{t-1}(u - x_1 v_1) - x_2 v_2 - \cdots - x_{n-1}v_{n-1} = 0.$$

By the induction hypothesis, $x_1, \ldots, x_{n-1}$ is a regular sequence on M, and by the first part, $x_1^{t-1}, x_2, ..., x_{n-1}$ is a regular sequence on M. By the Lemma on p. 1, we have that

$$u - x_1 v_1 \in (x_1^{t-1}, x_2, \ldots, x_{n-1})M,$$

and so $u \in (x_1, \ldots, x_{n-1})M$, as required. □

Theorem. *Let $x_1, \ldots, x_n$ be a regular sequence on the R-module M, and let I denote the ideal $(x_1, \ldots, x_n)R$. Let $a_1, \ldots, a_n$ be nonnegative integers, and suppose that $u, u_1, \ldots, u_n$ are elements of M such that*

$$(\#) \quad x_1^{a_1} \cdots x_n^{a_n} u = \sum_{j=1}^{n} x_j^{a_j+1} u_j.$$

Then $u \in IM$.

Proof. We use induction on the number of nonzero a_j: we are done if all are 0. If $a_i > 0$, let y be $\Pi_{j \neq i} x_j^{a_j}$. Rewrite (#) as $\sum_{j \neq i} x_j^{a_j+1} u_j - x_i^{a_i}(yu - x_i u_i) = 0$. Since powers of the x_j are again regular, the Lemma on p. 1 yields that $yu - x_i u_i \in x_i^{a_i} M + (x_j^{a_j+1} : j \neq i)M$ and so $yu \in x_i M + (x_j^{a_j+1} : j \neq i)M$. Now $a_i = 0$ in the monomial y, and there is one fewer nonzero a_j. The desired result now follows from the induction hypothesis. □

If I is an ideal of a ring R, we can form the *associated graded ring*

$$\mathrm{gr}_I(R) = R/I \oplus I/I^2 \oplus \cdots \oplus I^k/I^{k+1} \oplus \cdots,$$

an $\mathbb{N}$-graded ring whose kth graded piece is I^k/I^{k+1}. If $f \in I^h$ represents an element $a \in I^h/I^{h+1} = [\mathrm{gr}_I R]_h$ and $g \in I^k$ represents an element $b \in I^k/I^{k+1} = [\mathrm{gr}_I(R)]_k$, then ab is the class of fg in I^{h+k}/I^{h+k+1}. Likewise, if M is an R-module, we can form

$$\mathrm{gr}_I M = M/IM \oplus IM/I^2 M \oplus \cdots \oplus I^k M/I^{k+1} M \oplus \cdots.$$

This is an $\mathbb{N}$-graded module over $\mathrm{gr}_I(R)$ in an obvious way: with f and a as above, if $u \in I^k M$ represents an element $z \in I^k M/I^{k+1} M$, then the class of fu in $I^{h+k} M/I^{h+k+1} M$ represents az.

If $x_1, \ldots, x_n \in R$ generate I, the classes $[x_i] \in I/I^2$ generate $\mathrm{gr}_I(R)$ as an (R/I)-algebra. Let $\theta : (R/I)[X_1, \ldots, X_n] \twoheadrightarrow \mathrm{gr}_I(R)$ be the (R/I)-algebra map such that $X_i \mapsto [x_i]$. This is a surjection of graded (R/I)-algebras. By restriction of scalars, $\mathrm{gr}_I(M)$ is also a module over $(R/I)[X_1, \ldots, X_n]$. The (R/I)-linear map $M/IM \hookrightarrow \mathrm{gr}_I M$ then gives a map

$$\theta_M : (R/I)[X_1, \ldots, X_n] \otimes_{R/I} M/IM \to \mathrm{gr}_I(M).$$

Note that $\theta_R = \theta$. If $u \in M$ represents $[u]$ in M/IM and $t_1, \ldots, t_n$ are nonnegative integers whose sum is k, then

$$X_1^{t_1} \cdots X_n^{t_n} \otimes [u] \mapsto [x_1^{t_1} \cdots x_n^{t_n} u],$$

where the right hand side is to be interpreted in $I^k M/I^{k+1}M$. Note that θ_M is surjective.

Theorem. *Let $x_1, \ldots, x_n$ be a regular sequence on the R-module M, and suppose that $I = (x_1, \ldots, x_n)R$. Let $X_1, \ldots, X_n$ be indeterminates over the ring R/I. Then*

$$\mathrm{gr}_I(M) \cong (R/I)[X_1, \ldots, X_n] \otimes_{R/I} (M/IM)$$

in such a way that the action of $[x_i] \in I/I^2 = [\mathrm{gr}_I(R)]_1$ on $\mathrm{gr}_I(M)$ is the same as multiplication by the variable X_i.

In particular, if $x_1, \ldots, x_n$ is a regular sequence in R, then $\mathrm{gr}_I(R) \cong (R/I)[X_1, \ldots, X_n]$ in such a way that $[x_i]$ corresponds to X_i.

In other words, if $x_1, \ldots, x_n$ is a regular sequence on M (respectively, R), then the map θ_M (respectively, θ) discussed in the paragraph above is an isomorphism.

Proof. The issue is whether θ_M is injective. If not, there is a nontrivial relation on the monomials in the elements $[x_i]$ with coefficients in M/IM, and then there must be such a relation that is homogeneous of, say, degree k. Lifting to M, we see that this means that there is an $(M - IM)$-linear combination of mutually distinct monomials of degree k in $x_1, \ldots, x_n$ which is in $I^{k+1}M$. Choose one monomial term in this relation: it will have the form $x_1^{a_1} \cdots x_n^{a_n} u$, where the sum of the a_j is k and $u \in M - IM$. The other monomials of degree k in the elements $x_1, \ldots, x_n$ and the monomial generators of I^{k+1} all have as a factor at least one of the terms $x_1^{a_1+1}, \ldots, x_n^{a_n+1}$. This yields that

$$(\#) \quad (\Pi_j x_j^{a_j})u = \sum_{j=1}^{n} x_j^{a_j+1} u_j.$$

By the preceding Theorem, $u \in IM$, contradictioning that $u \in M - IM$. $\square$

Another description of the Koszul complex

Let R be a ring and let $\underline{x} = x_1, \ldots, x_n \in R$. In our development of the Koszul complex, we showed that $\mathcal{K}_i(\underline{x};\, R)$ has $\binom{n}{i}$ generators $u_{j_1 \cdots j_i}$ where $1 \le j_1 < \cdots < j_i \le n$, so that the generators may the thought of as indexed by strictly increasing sequences of integers between 1 and n inclusive of length i. We may also think of the generators as indexed by the i element subsets of $\{1, \ldots, n\}$.

This means that with

$$G = \mathcal{K}_1(\underline{x};\, R) = Ku_1 \oplus \cdots \oplus Ku_n,$$

we have that

$$\mathcal{K}_i(\underline{x};\, R) \cong \bigwedge^i G,$$

for all $i \in \mathbb{Z}$ in such a way that $u_{j_1 \cdots j_i}$ corresponds to $u_{j_1} \wedge \cdots \wedge u_{j_i}$. Thus, the Koszul complex coincides with the *skew-commutative* $\mathbb{N}$-*graded* algebra $\bigwedge^\bullet(G)$. (A *skew-commutative* $\mathbb{N}$-*graded* algebra is an associative $\mathbb{N}$-graded ring with identity such that if u and v are forms of degree d, e respectively, then $vu = (-1)^{de}uv$. The elements of even degree span a subalgebra that is in the center.) A *graded derivation* of such an algebra of degree -1 is a $\mathbb{Z}$-linear map δ that lowers degrees by 1 and satisfies

$$\delta(uv) = \big(\delta(u)\big)v + (-1)^d u\delta(v)$$

when u and v or forms as above.

It is easy to check that the differential of the Koszul complex is a derivation of degree -1 in the sense specified. Moreover, given any R-linear map $G \to R$, it extends uniqely to an R-linear derivation of $\bigwedge^\bullet(G)$ of degree -1. If we choose a basis for G, call it $u_1, \ldots, u_n$, and let x_i be the value of the map on u_i, we recover $\mathcal{K}_\bullet(\underline{x};\ R)$ in this way.

Maps of quotients by regular sequences

Let $\underline{x} = x_1, \ldots, x_n$ and $\underline{y} = y_1, \ldots, y_n$ be two regular sequences in R such that $J = (y_1, \ldots, y_n)R \subseteq (x_1, \ldots, x_n)R = I$. It is obvious that there is a surjection $R/J \twoheadrightarrow R/I$. It is far less obvious, but very useful, that there is an injection $R/I \to R/J$.

Theorem. *Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two regular sequences on a Noetherian module M over a Noetherian ring R. Suppose that*

$$J = (y_1, \ldots, y_n)R \subseteq (x_1, \ldots, x_n)R = I.$$

Choose elements $a_{ij} \in R$ such that for all j, $y_j = \sum_{i=1}^n a_{ij}x_i$. Let A be the matrix $\big(a_{ij}\big)$, so that we have a matrix equation

$$(y_1 \ \ldots \ y_n) = (x_1 \ \ldots \ x_n)A.$$

Let $D = \det(A)$. Then $DI \subseteq J$, and the map $M/IM \to M/JM$ induced by multiplication by D on the numerators in injective.

Proof. Let B be the classical adjoint of A, so that $BA = AB = DI_n$, where I_n is the $n \times n$ identity matrix. Then

$$(y_1 \ \dots \ y_n)B = (x_1 \ \dots \ x_n)AB = (x_1 \ \dots \ x_n)D$$

shows that $DI \subseteq J$.

The surjection $R/J \twoheadrightarrow R/I$ lifts to a map of projective resolutions of these modules: we can use any projective resolutions, but in this case we use the two Koszul complexes $\mathcal{K}_\bullet(\underline{x};\, R)$ and $\mathcal{K}_\bullet(\underline{y};\, R)$. With these specific resolutions, we can use the matrix A to give the lifting as far as degree 1:

$$\begin{array}{ccccccc}
\mathcal{K}_1(\underline{x};\, R) & \xrightarrow{(x_1 \,\dots\, x_n)} & R & \longrightarrow & R/(x_1,\, \dots\, , x_n) & \longrightarrow & 0 \\
{\scriptstyle A}\uparrow & & {\scriptstyle \mathbf{1}_R}\uparrow & & \uparrow & & \\
\mathcal{K}_1(\underline{y};\, R) & \xrightarrow{(y_1 \,\dots\, y_n)} & R & \longrightarrow & R/(y_1,\, \dots\, , y_n) & \longrightarrow & 0
\end{array}$$

Here, we are using the usual bases for $\mathcal{K}_1(\underline{x};\, R)$ and $\mathcal{K}_1(\underline{y};\, R)$. It is easy to check that if we use the maps

$$\bigwedge^i A : \mathcal{K}_i(\underline{y};\, R) \to \mathcal{K}_i(\underline{x};\, R)$$

for all i, we get a map of complexes. This means that the map

$$R \cong \mathcal{K}_n(\underline{y};\, R) \to \mathcal{K}_n(\underline{x};\, R) \cong R$$

is given by multiplication by D. It follows that the map induced by multiplication by D gives the induced map

$$\mathrm{Ext}^n_R(R/(x_1,\, \dots\, , x_d),\, M) \to \mathrm{Ext}^n(R/(y_1,\, \dots\, , y_n),\, M).$$

We have already seen that these top Ext modules may be identified with $M/(x_1,\, \dots\, , x_)M$ and $M/(y_1,\, \dots\, , y_n)M$, respectively: this is the special case of the Theorem at the bottom of p. 4 of the Lecture Notes of October 5 in the case where $i = n$.

Consider the short exact sequence

$$0 \to I/J \to R/J \to R/I \to 0.$$

The long exact sequence for Ext yields, in part,

$$\mathrm{Ext}^{n-1}_R(I/J; M) \to \mathrm{Ext}^n_R(R/I;\, M) \to \mathrm{Ext}^n_R(R/J; M).$$

Since the depth of M on $\mathrm{Ann}_R(I/J) \supseteq J$ is at least n, the leftmost term vanishes, which proves the injectivity of the map on the right. $\square$

Remark. We focus on the case where $M = R$: a similar comment may be made in general. We simply want to emphasize that the identification of $\mathrm{Ext}^n_R(R/I,\, R)$ with R/I is *not* canonical: it depends on the choice of generators for I. But a different identification can only arise from multiplication by a unit of R/I. A similar remark applies to the identification of $\mathrm{Ext}^n_R(R/J,\, R)$ with R/J.

Remark. The hypothesis that R and M be Noetherian is not really needed. Even if the ring is not Noetherian, if the annihilator of a module N contains a regular sequence $x_1, \ldots, x_d$ of length d on M, it is true that $\mathrm{Ext}^i_R(N,\, M) = 0$ for $i < d$. If $d \geq 1$, it is easy to see that any map $N \to M$ must be 0: any element in the image of the map must be killed by x_1, and $\mathrm{Ann}_M x_1 = 0$. The inductive step in the argument is then the same as in the Noetherian case: consider the long exact sequence for Ext arising when $\mathrm{Hom}_R(N,\, \_\,)$ is applied to

$$0 \to M \xrightarrow{x_1 \cdot} M \to M/x_1M \to 0.$$

The type of a Cohen-Macaulay module over a local ring

Let $(R,\, m,\, K)$ be local and let M be a finitely generated nonzero R-module that is Cohen-Macaulay, i.e., every system of parameters for R/I, where $I = \mathrm{Ann}_R M$, is a regular sequence on M. (It is equivalent to assume that $\mathrm{depth}_m M = \dim(M)$.) Recall that the *socle* of an R-module M is $\mathrm{Ann}_M m \cong \mathrm{Hom}_R(K,\, M)$. It turns out that for any maximal regular sequence $x_1, \ldots, x_d$ on M, the dimension as a K-vector space of the socle in $M/(x_1, \ldots, x_d)M$ is independent of the choice of the system of parameters. One way to see this is as follows:

Propostion. *Let $(R,\, m,\, K)$ and M be as above with M Cohen-Macaulay of dimension d over R. Then for every maximal regular sequence $x_1, \ldots, x_d$ on M and for every i, $1 \leq i \leq d$,*

$$\mathrm{Ext}^d_R(K,\, M) \cong \mathrm{Ext}^{d-i}_R\big(K,\, M/(x_1, \ldots, x_i)M\big).$$

In particular, for every maximal regular sequence on M, the socle in $M/(x_1, \ldots, x_d)M$ is isomorphic to $\mathrm{Ext}^d_R(K,\, M)$, and so its K-vector space dimension is independent of the choice maximal regular sequence.

Proof. The statement in the second paragraph follows from the result of the first paragraph in the case where $i = d$. By induction, the proof that

$$\mathrm{Ext}^d_R(K,\, M) \cong \mathrm{Ext}^{d-i}_R\big(K,\, M/(x_1, \ldots, x_i)M\big)$$

reduces at once to the case where $i = 1$. To see this, apply the long exact sequence for Ext arising from the application of $\mathrm{Hom}_R(K,\, \_\,)$ to the short exact sequence

$$0 \to M \to M \to M/x_1M \to 0.$$

Note that $\text{Ext}^j(K,\, M) = 0$ for $j < d$, since the depth of M on $\text{Ann}_R K = m$ is d, and that $\text{Ext}^j(K,\, M/x_1M) = 0$ for $j < d-1$, similarly. Hence, we obtain, in part,

$$0 \to \text{Ext}^{d-1}_R(K,\, M/x_1M) \to \text{Ext}^d_R(K,\, M) \xrightarrow{x_1\cdot} \text{Ext}^d_R(K,\, M).$$

Since $x_1 \in m$ kills K, the map on the right is 0, which gives the required isomorphism. $\square$

Proposition. *Let $M \neq 0$ be a Cohen-Macaulay module over a local ring R. Let $x_1, \, \dots \, , x_n$ and $y_1, \, \dots \, , y_n$ be two systems of parameters on M with $(y_1, \, \dots \, , y_n)R \subseteq (x_1, \, \dots \, , x_n)R$ and let $A = \big(a_{ij}\big)$ be a matrix of elements of R such that $(y_1 \, \dots \, y_n) = (x_1 \, \dots \, x_n)A$. Let $D = \det(A)$. Then the map $M/(x_1, \, \dots \, , x_n)M \to M/(y_1, \, \dots \, , y_n)M$ induced by multiplication by D on the numerators carries the socle of $M/(x_1, \, \dots \, , x_n)M$ isomorphically onto the socle of $M/(y_1, \, \dots \, , y_n)M$.*

In particular, if $y_i = x_i^t$, $1 \leq i \leq n$, then the map induced by multiplication by $x_1^{t-1} \cdots x_n^{t-1}$ carries the socle of the quotient module $M/(x_1, \, \dots \, , x_n)M$ isomorphically onto the socle of $M/(x_1^t, \, \dots \, , x_n^t)M$.

Proof. By the Theorem on p. 5, multiplication by D gives an injection

$$M/(x_1, \, \dots \, , x_n)M \hookrightarrow M/(y_1, \, \dots \, , y_n)M$$

which must map the socle in the left hand module injectively into the socle in the right hand module. Since, by the preceding Proposition, the two socles have the same finite dimension as vector spaces over K, the map yields an isomorphism of the two socles. The final statement follows because in the case of this specific pair of systems of parameters, we may take A to be the diagonal matrix with diagonal entries $x_1^{t-1}, \, \dots \, , x_n^{t-1}$. $\square$

F-rational rings

Definition: F-rational rings. We shall say that a local ring $(R,\, m,\, K)$ is *F-rational* if it is a homomorphic image of a Cohen-Macaulay ring and every ideal generated by a system of parameters is tightly closed.

We first note:

Theorem. *An F-rational local ring is Cohen-Macaulay, and every ideal generated by part of a system parameters is tightly closed. Hence, an F-rational local ring is a normal domain.*

Proof. Let $x_1, \, \dots \, , x_k$ be part of a system of parameters (it may be the empty sequence) and let $I = (x_1, \, \dots \, , x_k)$. Let $x_1, \, \dots \, , x_n$ be a system of parameters for R, and for every $t \geq 1$ let $J_t = (x_1, \, \dots \, , x_k, \, x_{k+1}^t, \, \dots \, , x_n^t)R$. Then for all t, $I \subseteq J_t$ and J_t is tightly closed, so that $I^* \subseteq J_t$ and $I^* \subseteq \bigcap_t J_t = I$, as required. In particular, (0) and principal ideals generated by nonzerodivisors are tightly closed, so that R is a normal domain, by the

Theorem on the top of p. 5 of the Lecture Notes from September 17. In particular, R is equidimensional, and by part (a) of the Theorem on colon-capturing from p. 9 of the Lecture Notes from October 5, we have that for every k, $0 \leq k \leq n-1$,

$$(x_1, \ldots, x_k) :_R x_{k+1} \subseteq (x_1, \ldots, x_k)^* = (x_1, \ldots, x_k),$$

so that R is Cohen-Macaulay. $\square$

Theorem. *Let (R, m, K) be a reduced local ring of prime characteristic $p > 0$. If R is Cohen-Macaulay and the ideal $I = (x_1, \ldots, x_n)$ generated by one system of parameters is tightly closed, then R is F-rational, i.e., every ideal generated by part of a system of parameters is tightly closed.*

Proof. Let $I_t = (x_1^t, \ldots, x_n^t)R$. We first show that all of the ideals I_t are tightly closed. If not, suppose that $u \in (I_t)^* - I_t$. Since $(I_t)^*/I_t$ has finite length, u has a nonzero multiple v that represents an element of the socle of I_t^*/I_t, which is contained in the socle of R/I_t. Thus, we might as well assume that $u = v$ represents an element of the socle in R/I_t. By the last statement of the Proposition on p. 8, , we can choose z representing an element of the socle in R/I such that the class of v mod I has the form $[x_1^{t-1} \cdots x_n^{t-1} z]$. Then $x_1^{t-1} \cdots x_n^{t-1} z$ also represents an element of $I^* - I$. Hence, we can choose $c \in R^\circ$ such that for all $q \gg 0$,

$$c(x_1^{t-1} \cdots x_n^{t-1} z)^q \in I_t^{[q]} = I_{tq},$$

i.e., $cx_1^{tq-q} \cdots x_n^{tq-q} z^q \in I_{tq}$, which implies that

$$cz^q \in \bigl((x_1^q)^t, \ldots, (x_n^q)^t\bigr) :_R (x_1^q)^{t-1} \cdots (x_n^q)^{t-1}.$$

By the Theorem on p. 3 applied to the regular sequence $x_1^q, \ldots, x_n^q$, the right hand side is $(x_1^q, \ldots, x_n^q) = I^{[q]}$, and so

$$cz^q \in I^{[q]}$$

for all $q \gg 0$. This shows that $z \in I^* = I$, contradicting the fact that z represents a nonzero socle element in R/I.

Now consider any system of parameters $y_1, \ldots, y_n$. For $t \gg 0$, $(x_1^t, \ldots, x_n^t)R \subseteq (y_1, \ldots, y_n)R$. Then there is an injectiion $R/y_1, \ldots, y_n)R \hookrightarrow R/(x_1^t, \ldots, x_n^t)R$ by the Theorem at the bottom of p. 5. Since 0 is tightly closed in the latter, it is tightly closed in $R/(y_1, \ldots, y_n)R$, and so $(y_1, \ldots, y_n)R$ is tightly closed in R. $\square$

We shall see soon that under mild conditions, if (R, m, K) is a local ring of prime characteristic $p > 0$ and a single ideal generated by a system of parameters is tightly closed, then R is F-rational: we can prove that R is Cohen-Macaulay even though we are not assuming it.

Math 711, Fall 2007 **Problem Set #2**
Due: Wednesday, October 24

In all problems, R, S are Noetherian rings of prime characteristic $p > 0$.

1. Suppose that (R, m, K) has a test element. Show that for every proper ideal $I \subseteq R$,

$$I^* = \bigcap_n (I + m^n)^*.$$

2. Suppose that c is a completely stable test element in $(R,\ m,\ K)$. Let I be an m-primary ideal. Show that $u \in I^*$ if and only if $u \in (I\widehat{R})^*$ in $\widehat{R}$.

3. Let R be a Noetherian domain of characteristic $p > 0$, and suppose that the integral closure S of R in its fraction field is weakly F-regular. Prove that for every ideal I of R, $I^* = IS \cap R$. (This is the case in subrings of polynomial rings over a field K generated over K by finitely many monomials.)

4. If R is a ring of prime characteristic $p > 0$, define the *Frobenius closure* I^{F} of I to be the set of elements $r \in R$ such that for some $q = p^e$, $r^q \in I^{[q]}$. Suppose that $c \in R^\circ$ has the property that for every maximal ideal m of R, there exists an integer N_m such that c^{N_m} is a test element for R_m. Prove that for every ideal I of R, $cI^* \subseteq I^{\mathrm{F}}$.

5. Let $R \subseteq S$ be integral domains such that S is module-finite over R, and suppose that S has a test element. Prove that R has a test element.

6. Let $(R,\ m,\ K)$ be a local Gorenstein ring, and let $x_1,\ \ldots,x_d$ be a system of parameters for R. Let $y \in R$ generate the socle modulo $(x_1,\ \ldots,x_d)$. Suppose that for every integer $t \geq 1$, the ideal $\bigl(x_1^t,\ \ldots,x_d^t,\ (x_1 \cdots x_d)^{t-1}y\bigr)R$ is tightly closed. Prove that either R is weakly F-regular, or else that $\tau(R) = m$.

Math 711: Lecture of October 10, 2007

We now want to make precise the assertion at the end of the preceding lecture to the effect that, under mild conditions on the local ring R, if one system of parameters of R generates a tightly closed ideal then R is F-rational. We already know that this is true when R is Cohen-Macaulay. The new point is that we do not need to assume that R is Cohen-Macaulay — we can prove it. However, we need the strong form of colon-capturing, and so we assume the existence of a test element. The following Theorem will enable us to prove the result that we want.

Theorem. *Let (R, m, K) be a reduced local ring of prime characteristic $p > 0$, and let $x_1, \ldots, x_n$ be a sequence of elements of m such that $I_k = (x_1, \ldots, x_k)$ has height k modulo every minimal prime of R, $1 \le k \le n$. Suppose that R has a test element. If $(x_1, \ldots, x_n)R$ is tighly closed, then I_k is tightly closed, $0 \le k \le n$, and $x_1, \ldots, x_n$ is a regular sequence in R.*

Proof. We first prove that every I_k is tightly closed, $0 \le k \le n$, by reverse induction on k. We are given that I_n is tightly closed. Now suppose that we know that I_{k+1} is tightly closed, where $0 \le k \le n-1$. We prove that I_k is tightly closed. Let $u \in I_k^*$ be given. Since $I_k \subseteq I_{k+1}$, we have that $I_k^* \subseteq I_{k+1}^* = I_{k+1}$ by hypothesis,, and $I_{k+1} = I_k + x_{k+1}R$. Thus, $u = v + x_{k+1}w$, where $v \in I_k$ and $w \in R$. But then $x_{k+1}w = u - v \in I_k^*$, since $u \in I_k^*$ and $v \in I_k$. Consequently, $v \in I_k^* :_R x_{k+1}$. By part (b) of the Theorem on colon-capturing at the bottom of p. 9 of the Lecture Notes from October 5, we have that $I_k^* :_R x_{k+1} = I_k^*$. That is, $u \in I_k + x_{k+1}I_k^*$. Since $u \in I_k^*$ was arbitrary, we have shown that $I_k^* \subseteq I_k + x_{k+1}I_k^*$, and the opposite inclusion is obvious. Let $N = I_k^*/I_k$. Then we have that $x_{k+1}N = N$, and so $N = 0$ by Nakayama's Lemma. But this says that $I_k^* = I_k$, as required. The fact that the x_i form a regular sequence is then obvious from the Theorem at the bottom of p. 9 of the Lecture Notes from October 5 cited above. $\square$

We then have:

Theorem. *Let (R, m, K) be a reduced, equidimensional local ring that is a homomorphic image of a Cohen-Macaulay ring. Suppose that R has a test element. If the ideal generated by one system of parameters of R is tightly closed, then R is F-rational. That is, R is Cohen-Macaulay and every ideal generated by part of a system of parameters is tightly closed.*

Proof. By the preceding Theorem, R is Cohen-Macaulay, and the result now follows from the Theorem on p. 9 of the Lecture Notes from October 8. $\square$

A localization of an F-rational local ring at any prime is F-rational. The proof is left as an exercise in Problem Set #3. It is therefore natural to define a Noetherian ring R of prime characteristic $p > 0$ to be *F-rational* if its localization at every maximal ideal (equivalently, at every prime ideal) is F-rational.

Definition: Gorenstein local rings. A local ring (R, m, K) is called *Gorenstein* if it is Cohen-Macaulay of type 1. Thus, if $x_1, \ldots, x_n$ is any system of parameters in R, the Artin local ring $R/(x_1, \ldots, x_n)R$ has a one-dimensional socle, which is contained in every nonzero ideal of R. Notice that if (R, m, K) is Gorenstein of dimension n, we know that $\mathrm{Ext}^i_R(K, R) = 0$ if $i < n$, while $\mathrm{Ext}^n_R(K, R) \cong K$.

Note that killing part of a system of parameters in a Gorenstein local ring does not change its type: hence such a quotient is again Gorenstein. Regular local rings are Gorenstein, since the quotient of a regular local ring by a regular system of parameters is K. The quotient of a regular local ring by part of a system of parameters is therefore Gorenstein. In particular, the quotient R/f of a regular local ring R by a nonzero proper principal ideal fR is Gorenstein. Such a ring R/fR is called a *local hypersurface*.

We shall need the following very important result.

Theorem. *If an Artin local ring is Gorenstein, it is injective as a module over itself.*

This was proved in seminar. See also, for example, [W. Bruns and J. Herzog, *Cohen-Macaulay rings,* Cambridge Studies in Advanced Math. **39** Cambridge Univ. Press, Cambridge, 1993] Theorems (3.1.17) and (3.2.10).

In consequence, we are able to prove the following most useful result. Notice that it reduces checking whether a given Gorenstein local ring is weakly F-regular to determining whether one specific element is in the tight closure of the ideal generated by one system of parameters.

Theorem. *Let (R, m, K) be a reduced Gorenstein local ring of prime characteristic $p > 0$. Let $x_1, \ldots, x_n$ be a system of parameters for R, and let u in R represent a generator of the socle in $R/(x_1, \ldots, x_n)R$. Then the following conditions are equivalent.*

(1) *R is weakly F-regular.*

(2) *R is F-rational*

(3) *$(x_1, \ldots, x_n)R$ is tightly closed.*

(4) *The element u is not in the tight closure of $(x_1, \ldots, x_n)R$.*

Proof. Let $I = (x_1, \ldots, x_n)$. It is clear that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4). But (4) $\Rightarrow$ (3) because if I^* is strictly larger than I, then I^*/I is a nonzero ideal of R/I and must contain the socle element represented by u, from which it follows that $u \in I^*$. The fact the (3) $\Rightarrow$ (2) follows from the Theorem on p. 9 of the Lecture Notes from October 8. What remains to be proved is the most interesting implication, that (2) $\Rightarrow$ (1).

Assume that R is F-rational, and let $N \subseteq M$ be finitely generated R-modules. We must show that N is tightly closed. If not, choose $u \in N^* - M$. We may replace N by a submodule N' of M with $N \subseteq N' \subseteq M$ such that N' is maximal witth respect to the property of not containing u. We will still have that u is in the tight closure of N' in M, and $u \notin N'$. We may then replace M and N' by M/N' and 0, respectively, and u by its image in M/N'. The maximality of N' implies that u is in every submodules of M/N'. We change notation: we may assume that $u \in M$ is in every nonzero submodule of M, and that $u \in 0^*_M$.

By the Lemma on the first page of the Lecture Notes from September 17, we have that M has finite length and is killed by a power of the maximal ideal of R. Moreover, u is in every nonzero submodule of M. Let $x_1, \ldots, x_n$ be a system of parameters for R. For $t \gg 0$, we have that every x_i^t kills M. Thus, we may think of M as a module over the Artin local ring $A = R/(x_1^t, \ldots, x_n^t)R$, which is a Gorenstein Artin local ring. Let v be the socle element in A. Then

$$Ru \cong K \cong Rv \subseteq A$$

gives an injective map of $Ru \subseteq M$ to A. Since A is injective as an A-module and M is an A-module, this map extends to a map $\theta : M \to A$ that is A-linear and, hence, R-linear. We claim that θ is injective: if the kernel were nonzero, it would be a nonzero submodule of M, and so it would contain u, contradicting the fact that u has nonzero image in A. Since $M \hookrightarrow A$R, to show that 0 is tightly closed in M over R, it suffices to show that 0 is tightly closed in A over R. Since $A = R/(x_1^t, \ldots, x_n^t)R$, this is simply equivalent to the statement that $(x_1^t, \ldots, x_n^t)R$ is tightly closed in R. $\square$

Math 711: Lecture of October 12, 2007

Capturing the contracted expansion from an integral extension

Using the result of the first problem in Problem Set #1, we can now prove that tight closure has one of the good properties, namely property (3) on p. 15 of the Lecture Notes from September 5, described in the introduction to the subject in the first lecture.

Recall that if M is a module over a domain D, the *torsion-free rank* of M is

$$\dim_{\mathcal{K}}(\mathcal{K} \otimes_D M).$$

We first note a preliminary result that comes up frequently:

Lemma. *Let D be a domain with fraction field $\mathcal{K}$, and let M be a finitely generated torsion-free module over D. Then M can be embedded in a finitely generated free D-module D^h, where h is the torsion-free rank of M over D. In particular, given any nonzero element $u \in M$, there is a D-linear map $\theta : M \to D$ such that $\theta(u) \neq 0$.*

Proof. We can choose h elements $b_1, \dots, b_h$ of M that are linearly independent over $\mathcal{K}$ and, hence, over D. This gives an inclusion map

$$Db_1 + \cdots + Db_h = D^h \hookrightarrow M.$$

Let $u_1, \dots, u_n$ generate M. Then each u_n is a linear combination of $b_1, \dots, b_h$ over $\mathcal{K}$, and we may multiply by a common denominator $c_i \in D - \{0\}$ to see that $c_i u_i \in D^h \subseteq M$ for $1 \leq i \leq n$. Let $c = c_1 \cdots c_n$. Then $cu_i \in D^h$ for all i, and so $cM \subseteq D^h$. But $M \cong cM$ via the map $u \mapsto cu$, and so we have that $f : M \hookrightarrow D^h$, as required.

If $u \neq 0$, then $f(u) = (d_1, \dots, d_h)$ has some coordinate not 0, say d_j. Let π_j denote the j th coordinate projection $D^h \to D$. Then we may take $\theta = \pi \circ f$. $\square$

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Suppose that $R \subseteq S$ is an integral extension, and that I is an ideal of R. Then $IS \cap R \subseteq I^*$.*

Proof. Let $r \in IS \cap R$. It suffices to show that the image of r is in I^* working modulo every minimal prime $\mathfrak{p}$ of R in turn. Let $\mathfrak{q}$ be a prime ideal of S lying over $\mathfrak{p}$: we can choose such a prime $\mathfrak{q}$ by the Lying Over Theorem. Then we have $R/\mathfrak{p} \hookrightarrow S/\mathfrak{q}$, and the image of r in $R/\mathfrak{p}$ is in $I(S/\mathfrak{q})$. We have therefore reduced to the case where R and S are domains.

Since $r \in IS$, if $f_1, \dots, f_n$ generate I we can write

$$r = s_1 f_1 + \cdots + s_n f_n.$$

Hence, we may replace S by $R[f_1, \dots, f_n] \subseteq SW$, and so assume that S is module-finite over R. By the preceding Lemma, S is solid as an R-algebra, and the result now follows from Problem 1 of Problem Set #1. $\square$

Test elements for reduced algebras essentially of finite type over excellent semilocal rings

Although we have test elements for F-finite rings, we do not yet have a satisfactory theory for excellent local rings. In fact, as indicated in the title of this section, we can do much better. In this section, we want to sketch the method that will enable us to prove the following result:

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Suppose that R is reduced and essentially of finite type over an excellent semilocal ring B. Then there are elements $c \in R^\circ$ such that R_c is regular, and every such element c has a power that is a completely stable big test element.*

We shall, in fact, prove better results in which the hypotheses on R_c are weakened, but we want to use the Theorem stated to motivate the constructions we need.

The idea of the argument is as follows. We first replace the semilocal ring B by its completion $\widehat{B}$ with respect to its Jacobson radical. Then $R_1 = \widehat{B} \otimes_B R$ is essentially of finite type over $\widehat{B}$, is still reduced, and the map $R \to R_1$ is flat with geometrically regular fibers. It follows that $(R_1)_c$ is still regular. Thus, we have reduced to the case where B is a complete semilocal ring. Such a ring is a finite product of complete local rings, and so is the B-algebra R. The problem can be treated for each factor separately. Therefore, we can assume that B is a complete local ring. Then B is module-finite over a complete regular local ring A, and we henceforth want to think about the case where R is essentially of finite type over a regular local ring (A, m, K). We can choose a coefficient field $K \subseteq A$ such that the composite map $K \hookrightarrow A \twoheadrightarrow A/m$ is an isomorphism. We know from the structure theory of complete local rings that A has the form $K[[x_1, \dots, x_n]]$, where $x_1, \dots, x_n$ are formal power series indeterminates over K.

We know that R has the form $W^{-1}R_0$ where R_0 is finitely generated as an A-algebra. It is not hard to see that if $(W^{-1}R_0)_c$ is regular, then there exists $w \in W$ such that $\big((R_0)_w\big)_c$ is regular. If we show that c^N is a completely stable big test element for $(R_0)_w$, this is automatically true for every further localization as well, and so we have it for $W^{-1}R_0 = R$. This enables us to reduce to the case where R is finitely generated over $A = K[[x_1, \dots, x_n]]$. The key to proving the Theorem above is then the following result.

Theorem. *Let K be a field of characteristic $p > 0$, let (A, m, K) denote the regular local ring $K[[x_1, \dots, x_n]]$, and let R be a reduced finitely generated A-algebra. Suppose that R_c is regular. Then A has an extension A^Γ such that*

(1) $A \to A^\Gamma$ *is faithfully flat and local.*

(2) A^Γ *is purely inseparable over* A.

(3) *The maximal ideal of* A^Γ *is* mA^Γ.

(4) A^Γ *is F-finite.*

(5) $A^\Gamma \otimes_A R$ *is reduced.*

(6) $(A^\Gamma \otimes_A R)_c$ *is regular.*

It will take quite an effort to prove this. However, once we have this Theorem, the rest of the argument for the Theorem on p. 2 is easy. The point is that $R^\Gamma = A^\Gamma \otimes_A R$ is faithfully flat over R and is F-finite and reduced by (4) and (5) above, Moreover, we still have that $(R^\Gamma)_c$ is regular, by part (6). It follows that c^N is a completely stable big test element for R^Γ by the Theorem at the bottom of p. 4 of the Lecture Notes from October 1, and then we have the corresponding result for R.

This motivates the task of proving the existence of extensions $A \to A^\Gamma$ with properties stated above. The construction depends heavily on the behavior of p-bases for fields of prime characteristic $p > 0$.

Properties of p-bases

We begin by recalling the notion of a *p-base* for a field K of characteristic $p > 0$. As usual, if $q = p^e$ we write

$$K^q = \{c^q : c \in K\},$$

the subfield of K consisting of all elements that are qth powers. It will be convenient to call a polynomial in several variables *e-special*, where $e \geq 1$ is an integer, if every variable occurs with exponent at most $p^e - 1$ in every term. This terminology is *not* standard.

Let K be a field of characteristic $p > 0$. Finitely many elements $\lambda_1, \ldots, \lambda_n$ in K (they will turn out to be, necessarily, in $K - K^p$) are called *p-independent* if the following three equivalent conditions are satisfied:

(1) $[K^p[\lambda_1, \ldots, \lambda_n] : K^p] = p^n$.

(2) $K^p \subseteq K[\lambda_1] \subseteq K^p[\lambda_1, \lambda_2] \subseteq \cdots \subseteq K^p[\lambda_1, \lambda_2, \ldots, \lambda_n]$ is a strictly increasing tower of fields.

(3) The p^n monomials $\lambda_1^{a_1} \cdots \lambda_n^{a_n}$ such that $0 \leq a_j \leq p-1$ for all j with $1 \leq j \leq n$ are a K^p-vecctor space basis for K over K^p.

Note that since every λ_j satisfies $\lambda_j^p \in K^p$, in the tower considered in part (2) at each stage there are only two possibilities: the degree of λ_{j+1} over $K^p[\lambda_1, \ldots, \lambda_j]$ is either 1, which means that

$$\theta_{j+1} \in K^p[\lambda_1, \ldots, \lambda_j],$$

or p. Thus, $K[\lambda_1, \ldots, \lambda_n] = p^n$ occurs only when the degree is p at every stage, and this is equivalent to the statement that the tower of fields is strictly increasing. Condition (3) clearly implies condition (1). The fact that (2) $\Rightarrow$ (3) follows by mathematical induction from the observation that

$$1,\, \lambda_{j+1},\, \lambda_{j+1}^2,\, \dots\, ,\, \lambda_{j+1}^{p-1}$$

is a basis for $L_{j+1} = K^p[\lambda_1, \dots, \lambda_{j+1}]$ over $L_j = K[\lambda_1, \dots, \lambda_j]$ for every j, and the fact that if one has a basis $\mathcal{C}$ for L_{j+1} over L_j and a basis $\mathcal{B}$ for L_j over K^p then all products of an element from $\mathcal{C}$ with an element from $\mathcal{B}$ form a basis for L_{j+1} over K^p.

Every subset of a p-independent set is p-independent. An infinite subset of K is called *p-independent* if every finite subset is p-independent.

A maximal p-independent subset of K, which will necessarily be a subset of $K - K^p$, is called a *p-base* for K. Zorn's Lemma guarantees the existence of a p-base, since the union of a chain of p-independent sets is p-independent. If Λ is a x-base, then $K = K^p[\Lambda]$, for if there were an element θ' of $K - K^p[\Theta]$, it could be used to enlarge the p-base. The empty set is a p-base for K if and only if K is perfect. If K is not perfect, a p-base for K is *never* unique: one can change an element of it by adding an element of K^p.

From the condition above, it is easy to see that Λ is a p-base for K if and only if every element of K is uniquely expressible as a polynomial in the elements of Λ with coefficients in K^p such that the exponent on every $\lambda \in \Lambda$ is at most $p-1$: this is equivalent to the assertion that the monomials in the elements of Λ of degree at most $p-1$ in each element are a basis for K over K^p. Another equivalent statement is that every element of K is uniquely expressible as as 1-special polynomial in the elements of Λ with coefficients in K^p.

If $q = p^e$, then the elements of $\Lambda^q = \{\lambda^q : \lambda \in \Lambda\}$ are a p-base for K^q over K^{pq}: in fact we have a commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{F^q} & K^q \\ \uparrow & & \uparrow \\ K^p & \xrightarrow[F^{pq}]{} & K^{pq} \end{array}$$

where the vertical arrows are inclusions and the horizontal arrows are isomorphisms: here, $F^q(c) = c^q$. In particular, $\Lambda^p = \{\lambda^p : \lambda \in \Lambda\}$ is a p-base for K^p, and it follows by multiplying the two bases together that the monomials in the elements of Λ of degree at most $p^2 - 1$ are a basis for K over K^{p^2}. By a straightforward induction, the monomials in the elements of Λ of degree at most $p^e - 1$ in each element are a basis for K over K^{p^e} for every $e \geq 1$. An equivalent statement is that every element of K can be written uniquely as an e-special polynomial in the elements of Λ with coefficients in K^{p^e}.

By taking pth roots, we also have that $K^{1/p} = K[\lambda^{1/p} : \lambda \in \Lambda]$. It is also true that for any h distinct elements $\lambda_1, \dots, \lambda_h$ of the p-base and for all q, $[K^q[\lambda_1, \dots, \lambda_h] : K^q] = q^h$ and that $K^{1/q} = K[\lambda^{1/q} : \lambda \in \Lambda]$. It follows that the monomials of the form

$$(*) \quad \lambda_{i_1}^{\alpha_1} \cdots \lambda_{i_h}^{\alpha_h}$$

where every α is a rational number in $[0,\,1)$ that can be written with denominator dividing q is a basis for $K^{1/q}$ over K.

Hence, with $K^\infty = \bigcap_q K^{1/q}$, we have

Proposition. *With K a field of prime characteristic $p > 0$ and Λ a p-base as above, the monomials of the form displayed in $(*)$ with $\lambda_1, \, \ldots \, , \lambda_h \in \Lambda$ and with the denominators of the $\alpha_i \in [0,\,1)$ allowed to be arbitrary powers of p form a basis for K^∞ over K.* $\square$

The gamma construction for complete regular local rings

Let K be a fixed field of characteristic $p > 0$ and let Λ be a fixed p-base for K. Let $A = K[[x_1, \, \ldots \, , x_n]]$ be a formal power series ring over K. We shall always use Γ to indicate a subset of Λ that is *cofinite*, by which we mean that $\Lambda - \Gamma$ is a finite set. For every such Γ we define a ring A^Γ as follows.

Let K_e (or K_e^Γ if we need to be more precise) denote the field $K[\lambda^{1/q} : \lambda \in \Gamma]$, where $q = p^e$ as usual. Then $K \subseteq K_e \subseteq K^{1/q}$, and the qth power of every element of K_e is in K. We define

$$A^\Gamma = \bigcup_e K_e[[x_1, \, \ldots \, , x_n]].$$

We refer to A^Γ as being obtained from A by the *gamma construction*.

Our next objective is to prove the following:

Theorem. *Consider the local ring (A, m, K) obtained from a field K of characteristic $p > 0$ by adjoining n formal power series indeterminiates $x_1, \, \ldots \, , x_n$. That is, $A = K[[x_1, \, \ldots \, , x_n]]$ and $m = (x_1, \, \ldots \, , x_n)A$. Fix a p-base Λ for K, let Γ be a cofinite subset of Λ, and let A^Γ be defined as above. Then $A \hookrightarrow A^\Gamma$ is a flat local homomorphism, and the ring A^Γ is regular local ring of Krull dimension n. Its maximal ideal is mA^Γ and its residue class field is $K^\Gamma = \bigcup_e K_e^\Gamma$. Moreover, A^Γ is purely inseparable over A, and A^Γ is F-finite.*

It will take some work to prove all of this.

Math 711: Lecture of October 17, 2007

We next want to prove the Theorem stated at the end of the Lecture Notes from October 12. Recall that $A = K[[x_1, \ldots, x_n]]$ and that Γ is cofinite in a fixed p-base Λ for K.

First note that it is clear that $K[[x_1, \ldots, x_n]] \to K_e[[x_1, \ldots, x_n]]$ is faithfully flat: every system of parameters in the former maps to a system of parameters in the extension ring, and since the extension is regular it is Cohen-Macaulay. Faithful flatness follows from the Theorem at the top of p. 2 of the Lecture Notes of September 14. Since a direct limit of flat extensions is flat, it is clear that A^Γ is flat over A.

Since $(K_e)^q \subseteq K$, we have that

$$(A^\Gamma)^q \in (K_e)^q[[x_1^q, \ldots, x_n^q]] \in K[[x_1, \ldots, x_n]] = A.$$

Thus, every $A_e = K_e[[x_1, \ldots, x_n]]$ is purely inseparable over A, and it follows that the union A^Γ is as well. Hence, $A \to A^\Gamma$ is local. Note that the maximal ideal in each A_e is $mA_e = (x_1, \ldots, x_n)A_e$. Every element of the maximal ideal of A^Γ is in the maximal ideal of some A_e, and so in $mA_e \subseteq mA^\Gamma$. Thus, $mA^\Gamma = (x_1, \ldots, x_n)A^\Gamma$ is the maximal ideal of A^Γ. The residue class field of A^Γ is clearly the direct limit of the residue class fields K_e, which is the union $\bigcup_e K_e = K^\Gamma$: this is the gamma construction applied to $A = K$.

We next want to check that A^Γ is Noetherian. Note that A^Γ is contained in the regular ring $K^\Gamma[[x_1, \ldots, x_n]] = B$, and that each of the maps $A_e \to B$ is faithfully flat. Hence, for every ideal I of A_e, $IB \cap A_e = I$. The Noetherian property for A^Γ now follows from:

Lemma. *Let $\{A_i\}_i$ be a directed family of rings and injective homomorphisms whose direct limit A embeds in a ring B. Suppose that for all i and for every ideal J of any A_i, $JB \cap A_i = I$. Then for every ideal I of A, $IB \cap A = I$. Hence, if B is Noetherian, then A is Noetherian.*

Proof. Suppose that $u \in A$, $I \subseteq A$ and $u \in IB - IA$. Then $u = f_1b_1 + \cdots + f_nb_n$ where $f_1, \ldots, f_n \in I$ and $b_1, \ldots, b_n \in B$. We can choose i so large that $u, f_1, \ldots, f_n \in A_i$, and let $J = (f_1, \ldots, f_n)A_i$. Evidently, $u \in JB \cap A_i = J$, and, clearly, $J \subseteq IA$, a contradiction.

For the final statement, let I be any ideal of A. Then a finite subset $g_1, \ldots, g_n \in I$ generates IB. Let $I_0 = (g_1, \ldots, g_n)A$. Then $I \subseteq IB \cap A = I_0B \cap A = I_0 \subseteq I$, so that $I = I_0$. $\square$

Since A^Γ is Noetherian of Krull dimension n with maximal ideal $(x_1, \ldots, x_n)A^\Gamma$, we have that A^Γ is regular. To complete the proof of the final Theorem stated in the Lecture Notes from October 12, it remains only to prove:

Theorem. A^Γ *is F-finite.*

Proof. Throughout this argument, we write K_e for $K_e^\Gamma = K[\lambda^{1/q} : \lambda \in \Gamma]$, and A_e for $K_e[[x_1, \ldots, x_n]]$. Let $\theta_1, \ldots, \theta_h$ be the finitely many elements that are in the p-base Λ but not in Γ. Let $\mathcal{M}$ be the set of monomials in $\theta_1^{1/p}, \ldots, \theta_h^{1/p}$ of degree at most $p-1$ in each element, and let $\mathcal{N}$ be the set of monomials in $x_1^{1/p}, \ldots, x_d^{1/p}$ of degree at most $p-1$ in each element. Let

$$\mathcal{T} = \mathcal{M}\mathcal{N} = \{\mu\nu : \mu \in \mathcal{M},\, \nu \in \mathcal{N}\}.$$

We shall complete the proof by showing that $\mathcal{T}$ spans $(A^\Gamma)^{1/p}$ as an A^Γ-module. First note that

$$(A^\Gamma)^{1/p} = \bigcup_e (A_e)^{1/p},$$

and for every e,

$$(A_e)^{1/p} = K_e^{1/p}[[x_1^{1/p}, \ldots, x_d^{1/p}]].$$

This is spanned over $K_e^{1/p}[[x_1, \ldots, x_d]]$ by $\mathcal{N}$. Also observe that $K_e^{1/p}$ is spanned over K by products of monomials in $\mathcal{N}$ and monomials in the elements $\lambda^{1/qp}$ for $\lambda \in \Gamma$, and the latter are in K_{e+1}. Hence, $K_e^{1/p}$ is spanned by $\mathcal{N}$ over K_{e+1}, and it follows that $K_e^{1/p}[[x_1, \ldots, x_n]]$ is spanned by $\mathcal{N}$ over $K_{e+1}[[x_1, \ldots, x_n]] = A_{e+1}$. Hence, $A_e^{1/p}$ is spanned by $\mathcal{T} = \mathcal{M}\mathcal{N}$ over A_{e+1}, as claimed. $\square$

Note that $A^\Gamma \subseteq K^\Gamma[[x_1, \ldots, x_n]]$, but these are not, in general, the same. Any single power series in A^Γ has all coefficients in a single K_e. When the chain of fields K_e is infinite, we can choose $c_e \in K_{e+1} - K_e$ for every for every $e \geq 0$, and then

$$\sum_{e=0}^{\infty} c_e x^e \in K^\Gamma[[x]] - K[[x]]^\Gamma.$$

Complete tensor products, and an alternative view of the gamma construction

Let (R, m, K) be a complete local ring with coefficient field $K \subseteq R$. When $R = A = K[[x_1, \ldots, x_n]]$, we may enlarge the residue class field K of A to L by considering instead $L[[x_1, \ldots, x_n]]$. This construction can be done in a more functorial way, and one does not need the ring to be regular.

Consider first the ring $R_L = L \otimes_K R$. This ring need not be Noetherian, and will not be complete except in special cases, e.g., if L is finite algebraic over K. However, $R_L/mR_L \cong L$, so that mR_L is a maximal ideal of this ring, and we may form the (mR_L)-adic completion of R_L. This ring is denoted $L\widehat{\otimes}_K R$, and is called the *complete tensor product* of L with R over K. Of course, we have a map $R \to R_L \to L\widehat{\otimes}_K R$.

Note that

$$L\widehat{\otimes}_K R = \varprojlim_t \frac{L \otimes_K R}{m^t(L \otimes_K R)} \cong \varprojlim_t \big(L \otimes_K \frac{R}{m^t}\big).$$

In case $R = K[[\underline{x}]]$, where $\underline{x} = x_1, \dots, x_n$ are formal power series indeterminates, this yields

$$\varprojlim_t L \otimes_K \big(\frac{K[[\underline{x}]]}{(\underline{x})^t}\big) \cong \varprojlim_t L \otimes_K \big(\frac{K[\underline{x}]}{(\underline{x})^t}\big) \cong \varprojlim_t \frac{L[\underline{x}]}{(\underline{x})^t} \cong L[[\underline{x}]],$$

which gives the result we wanted.

Now suppose that we have a local map $(R, m, K) \to (S, \mathfrak{n}, K)$ of complete local rings such that S is module-finite over R, i.e., over the image of R: we are not assuming that the map is injective. For every t, we have a map $R/m^tR \to S/m^tS$ and hence a map $L \otimes_K R/m^tR \to L \otimes_K S/m^tS$. This yields a map

$$(*) \quad \varprojlim_t L \otimes_K R/m^tR \to \varprojlim_t L \otimes_K S/m^tS.$$

The map $R/mS \to S/mS$ is module-finite, which shows that S/mS has Krull dimension 0. It follows that mR is primary to $\mathfrak{n}$, so that the ideals m^tR are cofinal with the power of $\mathfrak{n}$. Therefore the inverse limit on the right in $(*)$ is the same as $\varprojlim_t L \otimes_K R/\mathfrak{n}^tR$, and we see that we have a map $L\widehat{\otimes}_K R \to L\widehat{\otimes}_K S$.

We next note that when $R \to S$ is surjective, so is the map $L\widehat{\otimes}_K R \to L\widehat{\otimes}_K S$. First note that $R_L \to S_L$ is surjective, and that mR_L maps onto $\mathfrak{n}S_L$. Second, each element σ of the completion of S_L with respect to $\mathfrak{n}$ can be thought of as arising from the classes modulo successive powers of $\mathfrak{n}$ of the partial sums of a series

$$s_0 + s_1 + \cdots + s_t + \cdots$$

such that $s_t \in \mathfrak{n}^tS_L = m^tS_L$ for all $t \in \mathbb{N}$. Since m^tR_L maps onto $\mathfrak{n}^tS_L$, we can left this series to

$$r_0 + r_1 + \cdots + r_t + \cdots$$

where for every $t \in \mathbb{N}$, $r_t \in m^tR_L$ and maps to s_t. The lifted series represents an element of the completion of R_L that maps to σ.

Since every complete local ring R with coefficient field K is a homomorphic image of a ring of the form $K[[x_1, \dots, x_n]$, it follows that $L\widehat{\otimes}_K R$ is a homomorphic image of a ring of the form $L[[x_1, \dots, x_n]]$, and so $L\widehat{\otimes}_K R$ is a complete local ring with coefficient field L.

Next note that when $R \to S$ is a module-finite (not necessarily injective) K-homomorphism of local rings with coefficient field K, we have a map

$$(L\widehat{\otimes}_K R) \otimes_R S \to L\widehat{\otimes}_K S,$$

since both factors in the (ordinary) tensor product on the left map to $L\widehat{\otimes}_K S$. We claim that this map is an isomorphism. Since, as noted above, mS is primary to $\mathfrak{n}$, and both sides are complete in the m-adic topology, it suffices to show that the map induces an isomorphism modulo the expansions of m^t for every $t \in \mathbb{N}$. But the left hand side becomes

$$\big(L \otimes_K (R/m^t)\big) \otimes_R S \cong L \otimes_K (S/m^t S),$$

which is exactly what we need.

It follows that $L\widehat{\otimes}_K R$ is ffaithfully flat over R: we can represent R as a module-finite extension of a complete regular local ring A with the same residue class field, and then $L\widehat{\otimes}_K R = (L\widehat{\otimes}_K A) \otimes_A R$, so that the result follows from the fact that $L\widehat{\otimes} A$ is faithfully flat over A.

With this machinery available, we can construct R^Γ, when R is complete local with coefficient field K and Γ is cofinite in a p-base Λ for K, as $\bigcup_e K_e\widehat{\otimes}_K R$. If R is regular this agrees with our previous construction.

If A, R are complete local both with coefficient field K, and $A \to R$ is a local K-algebra homomorphism that is module-finite (not necessarily injective), then we have

$$K_e\widehat{\otimes}_K R = (K_e\widehat{\otimes}_K A) \otimes_A R$$

for all e. Since tensor commutes with direct limit, it follows that

$$R^\Gamma \cong A^\Gamma \otimes_A R.$$

In particular, this holds when A is regular. It follows that R^Γ is faithfully flat over R.

Properties preserved for small choices of Γ

Suppose that Λ is a p-basse for a field K of characteristic $p > 0$. We shall say that a property holds *for all sufficiently small cofinite* $\Gamma \subseteq \Lambda$ or *for all* $\Gamma \ll \Lambda$ if there exists $\Gamma_0 \subseteq \Lambda$, cofinite in Λ, such that the property holds for all $\Gamma \subseteq \Gamma_0$ that are cofinite in Λ.

We are aiming to prove the following:

Theorem. *Let B be a complete local ring of prime characteristic $p > 0$ with cooefficient field K, let Λ be a p-base for K, and and let R an algebra essentially of finite type over B. For Γ cofinite in Λ, let R^Γ denote $B^\Gamma \otimes_B R$.*

(a) *If R is a domain, then R^Γ is a domain for all $\Gamma \ll \Lambda$.*

(b) *If R is reduced, then R^Γ is reduced for all $\Gamma \ll \Lambda$.*

(c) *If $P \subseteq R$ is prime, then PR^Γ is prime for all $\Gamma \ll \Lambda$.*

(d) *If $I \subseteq R$ is radical, then IR^Γ is radical for all $\Gamma \ll \Lambda$.*

We shall also prove similar results about the behavior of the singular locus. We first note:

Lemma. *Let M be an R-module, let $P_1, \dots, P_h$ be submodules of M, and let S be a flat R-module. Then the intersection of the submodules $S \otimes_R P_i$ for $1 \le i \le h$ is*

$$(P_1 \cap \cdots \cap P_h) \otimes_R M.$$

Here, for $P \subseteq M$, we are identifying $S \otimes_R P$ with its image in $S \otimes_R M$: of course, the map $S \otimes_R P \to S \otimes_R M$ is injective.

Proof. By a straightforward indcution on h, this comes down to the intersection of two submodules P and Q of the R-module M. We have an exact sequence

$$0 \longrightarrow P \cap Q \longrightarrow M \xrightarrow{f} (M/P \oplus M/Q)$$

where the rightmost map f sends $u \in M$ to $(u+P) \oplus (u+Q)$. Since S is R-flat, applying $S \otimes_R \_$ yields an exact sequence

$$0 \to S \otimes_R (P \cap Q) \to S \otimes_R M \xrightarrow{\mathbf{1}_S \otimes f} \bigl(S \otimes_R (M/P)\bigr) \oplus \bigl(S \otimes_R (M/Q)\bigr).$$

The rightmost term may be identified with

$$(S \otimes_R M)/(S \otimes_R P) \oplus (S \otimes_R M)/(S \otimes_R Q),$$

from which it follows that the kernel of $\mathbf{1}_S \otimes f$ is the intersection of $S \otimes_R P$ and $S \otimes_R Q$. Consequently, this intersection is given by $S \otimes_R (P \cap Q)$. $\square$

We next want to show that part (a) of the Theorem stated above implies the other parts.

Proof that part (a) implies the other parts of the Theorem. Part (c) follows from part (a) applied to (R/P), since

$$(R/P)^\Gamma = B^\Gamma \otimes_B (R/P) \cong R^\Gamma/PR^\Gamma.$$

To prove that $(a) \Rightarrow (d)$, let $I = P_1 \cap \cdots \cap P_n$ be the primary decomposition of the radical ideal I, where the P_i are prime. Since B^Γ is flat over B, R^Γ is flat over R. Hence, IR^Γ, which may be identified with $R^\Gamma \otimes_R I$, is the intersection of the ideals $R^\Gamma \otimes_R P_i$, $1 \le i \le h$, by the Lemma above. By part (a), we can choose Γ cofinite in Λ such that every $R^\Gamma \otimes_R P_i$ is prime, and for this Γ, IR^Γ is radical.

Finally, (c) is part (d) in the case where $I = (0)$. $\square$

It remains to prove part (a). Several preliminary results are needed. We begin by replacing B by its image in the domain R, taking the image of K as a coefficient ring. Thus, we may assume that $B \hookrightarrow R$ is injective. Then B is a module-finite extension of a subring of the form $K[[x_1, \dots, x_n]]$ with the same coefficient field, by the structure theory of complete local rings. We still have that R is essentially of finite type over A. Moreover, $B^\Gamma \cong A^\Gamma \otimes_A B$, from which it follows that $R^\Gamma \cong A^\Gamma \otimes_R A$. Therefore, in proving part (a) of the Theorem, it suffices to consider the case where $B = A = K[[x_1, \dots, x_n]]$ and $A \subseteq R$. For each Γ cofinite in $\Lambda \subseteq K$, let $\mathcal{L}_\Gamma$ denote the fraction field of A_Γ. Let $\mathcal{L}$ denote the fraction field of A. Let Ω be any field finitely generated over R that contains the fraction field of R. To prove part (a) of the Theorem stated on p. 4, it will suffice to prove the following:

Theorem. *Let K be a field of characteristic p with p-base Λ. Let $A = K[[x_1, \ldots, x_n]]$, and let $\mathcal{L}$, A^Γ and $\mathcal{L}_\Gamma$ be defined as above for every cofinite subset Γ of Λ. Let Ω be any field finitely generated over $\mathcal{L}$. Then for all $\Gamma \ll \Lambda$, $\mathcal{L}_\Gamma \otimes_{\mathcal{L}} \Omega$ is a field.*

We postpone the proof of this result. We first want to see (just below) that it implies part (a) of the Theorem stated on p. 4. Beyond that, we shall need to prove some auxiliary results first.

To see why the preceding Theorem implies part (a) of the Theorem on page 4, choose Ω containing the fraction field of R (we can choose $\Omega = \mathrm{frac}\,(R)$, for example). Since A^Γ is A-flat, we have an injection $A^\Gamma \otimes_A R \hookrightarrow A^\Gamma \otimes_A \Omega$. Thus, it suffices to show that this ring is a domain. Since the elements of $A - \{0\}$ are already invertible in Ω, we have that $\Omega \cong \mathrm{frac}\,(A) \otimes_A \Omega$. Since A^Γ is purely inseparable over A, inverting the nonzero elements of A inverts all nonzero elements of A^Γ. Moreover, the tensor product of two $\mathrm{frac}\,(A)$-modules over $\mathrm{frac}\,(A)$ is the same as their tensor product over A. Hence,

$$A^\Gamma \otimes_A \Omega \cong A^\Gamma \otimes_A \mathrm{frac}\,(A) \otimes_A \Omega \cong \mathrm{frac}\,(A^\Gamma) \otimes_{\mathrm{frac}(A)} \Omega = \mathcal{L}_\Gamma \otimes_{\mathcal{L}} \Omega.$$

It is now clear that Theorem above implies part (a) of the Theorem on p. 4.

In order to prove the Theorem above, we need several preliminary results. One of them is quite easy:

Lemma. *Let K be a field of characteristic $p > 0$ and let Λ be a p-base for K. The family of subfields K^Γ as Γ runs through the cofinite subsets of Λ is directed by $\supseteq$, and the intersection of these fields is K.*

Proof. K^∞ has as a basis 1 and all monomials

$$(\#) \quad \lambda_1^{\alpha_1} \cdots \lambda_t^{\alpha_t}$$

where t is some positive integer, $\lambda_1, \ldots, \lambda_t$ are mutually distinct elements of Λ, and the α_j are positive rational numbers in $(0, 1)$ whose denominators are powers of p. If u were in the intersection and not in K it would have a unique representation as a K-linear combination of these elements, including at least one monomial μ as above other than 1. Choose $\lambda \in \Lambda$ that occurs in the monomial μ with positive exponent. Choose Γ cofinite in Λ such that $\lambda \notin \Gamma$. Then the monomial μ is not in K^Γ, which has a basis consisting of 1 and all monomials as in (#) such that the λ_j occurring are in Γ. It follows that $u \notin K^\Gamma$. $\square$

We shall also need the following result, as well as part (b) of the Theorem stated after it.

Theorem. *Let $\mathcal{L}$ be a field of characteristic $p > 0$, and let $\mathcal{L}'$ be a finite purely inseparable extension of $\mathcal{L}$. Let $\{\mathcal{L}_i\}_i$ be a family of fields directed by $\supseteq$ whose intersection is $\mathcal{L}$. Then there exists j such that for all $i \leq j$, $\mathcal{L}_i \otimes \mathcal{L}'$ is a field.*

Theorem. *Let $\{\mathcal{K}_i\}_i$ be a nonempty family of subfields of an ambient field $\mathcal{K}_0$ such that the family is directed by $\supseteq$, and has intersection $\mathcal{K}$. Let $x_1, \ldots, x_n$ be formal power series indeterminates over these fields. Then*

(a) $\bigcap_i \operatorname{frac}(\mathcal{K}_i[x_1, \ldots, x_n]) = \operatorname{frac}(\mathcal{K}[x_1, \ldots, x_n])$.

(b) $\bigcap_i \operatorname{frac}(\mathcal{K}_i[[x_1, \ldots, x_n]]) = \operatorname{frac}(\mathcal{K}[[x_1, \ldots, x_n]])$.

We note that part (a) is easy. Choose an arbitrary total ordering of the monomials in the variables $x_1, \ldots, x_n$. Let f/g be an element of the intersection on the left hand side written as the ratio of polynomials $f,\, g \neq 0$ in $\mathcal{K}_0[x_1, \ldots, x_n]$, where f and g are chosen so that $\mathrm{GCD}(f,\, g) = 1$. Also choose g so that the greatest monomial occurring has coefficient 1. This representation is unique. If the same element is also in $\operatorname{frac}(\mathcal{K}_i[x_1, \ldots, x_n])$, it can be represented in the same way working over $\mathcal{K}_i$, and the two representations must be the same. Hence, all coefficients of f and of g must be in all of the $\mathcal{K}_i$, i.e., in $\mathcal{K}$ which shows that $f/g \in \operatorname{frac}(\mathcal{K}[x_1, \ldots, x_n])$, as required.

We shall have to work a great deal harder to prove part (b).

Math 711: Lecture of October 19, 2007

Our next goal is to prove the two results stated at the end of the Lecture Notes of October 17.

Proof of the theorem on preserving the field property for a finite purely inseparable extension. Recall that $\mathcal{L}'$ is a finite purely inseparable extension of $\mathcal{L}$, and $\{\mathcal{L}_i\}_i$ is a family of fields directed by $\supseteq$ whose intersection if $\mathcal{L}$. Fix $\mathcal{L}_0$ in the family: we need only consider fields in the family contained in $\mathcal{L}_0$. Let $\overline{\mathcal{L}_0}$ be an algebraic closure of $\mathcal{L}_0$. Since $\mathcal{L}'$ is purely inseparable over $\mathcal{L}$, $\mathcal{L}'$ may be viewed, in a unique way, as a subfield of $\overline{\mathcal{L}_0}$. Choose a basis $b_1, \ldots, b_h$ for $\mathcal{L}'$ over $\mathcal{L}$. For every i we have a map

$$\mathcal{L}_i \otimes_{\mathcal{L}} \mathcal{L}' \to \mathcal{L}_i[\mathcal{L}'],$$

where the right hand side is the smallest subfield of $\overline{\mathcal{L}_0}$ containing $\mathcal{L}_i$ and $\mathcal{L}'$. The image of this map is evidently a field. Therefore, to prove the Theorem, we need only prove that the map is an isomorphism whenever i is sufficiently small.

Note that the elements $1 \otimes b_j$ span the left hand side as a vector space over $\mathcal{L}_i$. Hence, for every i, the left hand side is a vector space of dimension h over $\mathcal{L}_i$. The image of the map is a ring containing $\mathcal{L}_i$ and the b_j. It therefore contains $\mathcal{L}b_1 + \cdots + \mathcal{L}b_n = \mathcal{L}'$. It follows that the image of the map is $\mathcal{L}_i[\mathcal{L}']$, i.e., the map is onto. The image of the map is spanned by $b_1, \ldots, b_h$ as an $\mathcal{L}_i$-vector space. Therefore, the map is an isomorphism whenever $b_1, \ldots, b_h$ are linearly indpendent over $\mathcal{L}_i$. Choose i so as to make the dimension of the vector space span of $b_1, \ldots, b_h$ over $\mathcal{L}_i$ as large as possible. Since this dimension must be an integer in $\{0, \ldots, h\}$, this is possible. Note that if a subset of the $b_1, \ldots, b_h$ has no nonzero linear relation over $\mathcal{L}_i$, this remains true for all smaller fields in the family.

Call the maximum possible dimension d. By renumbering, if necessary, we may assume that $b_1, \ldots, b_d$ are linearly independent over $\mathcal{L}_i$. We can conclude the proof of the Theorem by showing that $d = h$. If not, b_{d+1} is linearly dependent on $b_1, \ldots, b_d$, so that there is a unique linear relation

$$(*) \quad b_{d+1} = c_1 b_1 + \cdots + c_d b_d,$$

where every $c_j \in \mathcal{L}_i$. Since $b_1, \ldots, b_h$ are linearly independent over $\mathcal{L}$, at least one $c_{j_0} \notin \mathcal{L}$. Choose $\mathcal{L}_{i'} \subseteq \mathcal{L}_i$ such that $c_{j_0} \notin \mathcal{L}_{i'}$. Then $b_1, \ldots, b_{d+1}$ are linearly independent over $\mathcal{L}_{i'}$: if there were a relation different from $(*)$, it would imply the dependence of $b_1, \ldots, b_d$. This contradictis that d is maximum. $\square$

Our next objective is to prove part (b) of the Theorem stated at the top of p. 7 of the Lecture Notes from October 17. We first introduce some terminology. An module C over B (which in the applications here will be a B-algebra) is called *injectively free* over B if for every $u \neq 0$ in C there is an element $f \in \mathrm{Hom}_B(C, B)$ such that $f(u) \neq 0$. This is equivalent to the assumption that C can be embedded in a (possibly infinite) product of copies of B: if ${}_fB = B$ for every $f \in \mathrm{Hom}_B(C,\, B)$, then

$$C \to \prod_{f \in \mathrm{Hom}_B(C,\, B)} {}_fB$$

is an injection if and only if C is injectively free over B. It is also quite easy to see that C is injectively free over B if and only if the natural map

$$C \to \mathrm{Hom}_B\bigl(\mathrm{Hom}(C,\, B),\, B\bigr)$$

from C to its double dual over B is injective.

Note that if C is injectively free over B then $C[x_1,\, \ldots\, , x_n]$ is injectively free over $B[x_1,\, \ldots\, , x_n]$, and that $C[[x_1,\, \ldots\, , x_n]]$ in injectively free over $B[[x_1,\, \ldots\, , x_n]]$: choose a nonzero coefficient of u, choose a map $C \to B$ which is nonzero on that coefficient, and then extend it by letting it act on coefficients.

We shall use the notation $\mathcal{F}((x_1,\, \ldots\, , x_n))$ for $\mathrm{frac}\,(\mathcal{F}[[x_1,\, \ldots\, , x_n]])$ when $\mathcal{F}$ is a field. Note that in case there is just one indeterminates $\mathcal{F}((x)) = \mathcal{F}[[x]][x^{-1}]$ is the ring of Laurent power series in x with coefficients in the field $\mathcal{F}$: any given series contains at most finitely many terms in which the exponent on x is negative, but the largest negative exponent depends on the series under consideration.

We next observe the following fact:

Lemma. *If $B \subseteq C$ are domains, $\mathcal{F} = \mathrm{frac}\,(B)$, C is injectively free over B, and x is a formal indeterminate over C, then*

$$\bigl(\mathrm{frac}\,(C[[x]])\bigr) \cap \mathcal{F}((x)) = \mathrm{frac}\,(B[[x]]).$$

Proof. It suffices to show $\subseteq$: the other inclusion is obvious. Suppose that

$$u \in \mathrm{frac}\,(C[[x]]) \cap \mathcal{F}((x)) - \{0\}.$$

Then we can write

$$u = x^h(\sum_{j=0}^{\infty} \beta_j x^j)$$

where $h \in \mathbb{Z}$, the $\beta_j \in \mathcal{F}$, and $\beta_0 \neq 0$. All three fields contain the powers of x, and so we may multiply by x^{-h} without affecting the issue. Thus, we may assume that $h = 0$. We want to show that $u \in \mathrm{frac}\,(B[[x]])$. Since $u \in \mathrm{frac}\,(C[[x]])$, there exists $v \neq 0$ and w in $C[[x]]$ such that $w = vu \in C[[x]]$. Let $v = \sum_{j=0}^{\infty} c_j x^j$ and $w = \sum_{k=0}^{\infty} c'_k x^k$, where the $c_j,\, c'_j \in C$. Then for each $m \geq 0$, we have that

$$(*) \qquad \sum_{j+k=m} c_j \beta_k = c'_m.$$

Choose j_0 such that $c_{j_0} \neq 0$ and choose $f : C \to B$, B-linear, such that $f(c_{j_0}) \neq 0$ in B. Extend f to a map $C[[x]]$ to $B[[x]]$ by letting it act on coefficients. Then we may multiply the equation $(*)$ by b to get

$$\sum_{j+k=m} c_j(b\beta_k) = bc'_m,$$

and now the B-linearity of f implies that

$$\sum_{j+k=m} f(c_j)b\beta_k = bf(c'_m).$$

Now we may use the fact that b is not a zerodivisor in B to conclude that

$$\sum_{j+k=m} f(c_j)\beta_k = f(c'_m),$$

as we wanted to show. These equations show that $f(v)u = f(w)$, and $f(v) \neq 0$ because $f(c_{j_0}) \neq 0$. Since $f(v)$, $f(w) \in B[[x]]$, we have that $u = f(w)/f(v) \in \mathrm{frac}\,(B[[x]])$, as required. $\square$

We can now prove part (b) of the Theorem on p. 7 of the Lecture Notes from October 17.

Proof of the theorem on intersections of fraction fields of formal power series rings. We prove the theorem by induction on n. If $n = 1$ it follows from the uniqueness of coefficients in the Laurent expansion of an element of

$$\mathrm{frac}\,(\mathcal{K}_j([[x]]) = \mathcal{K}_j[[x]][x^{-1}].$$

Now assume the result for $n-1$ variables. For every j, we have

$$\mathcal{K}_j((x_1, \ldots, x_n)) \subseteq \mathcal{K}_j((x_1, \ldots, x_{n-1}))((x_n)).$$

It follows from the one variable case that

$$\bigcap_j \mathcal{K}_j((x_1, \ldots, x_n)) \subseteq \big(\bigcap_j \mathcal{K}_j((x_1, \ldots, x_{n-1}))\big)((x_n)),$$

and from the induction hypothesis that

$$\bigcap_j \mathcal{K}_j((x_1, \ldots, x_{n-1})) = \mathcal{K}((x_1, \ldots, x_{n-1})).$$

Hence,

$$\bigcap_j \mathcal{K}_j((x_1, \ldots, x_n)) \subseteq \mathcal{K}((x_1, \ldots, x_{n-1}))((x_n)).$$

Fix any element j_0 in the index set. Then we have

$$(*) \quad \bigcap_j \mathcal{K}_j((x_1, \dots, x_n)) \subseteq \mathcal{K}_{j_0}((x_1, \dots, x_n)) \cap \mathcal{K}((x_1, \dots, x_{n-1}))((x_n)).$$

We now want to apply the Lemma from the preceding page. Let $B = \mathcal{K}[[x_1, \dots, x_{n-1}]]$ and $C = \mathcal{K}_{j_0}[[x_1, \dots, x_{n-1}]]$. Since $\mathcal{K}_{j_0}$ is $\mathcal{K}$-free, it embeds in a direct sum of copies of $\mathcal{K}$ and, hence, in a product of copies of $\mathcal{K}$. Thus, $\mathcal{K}_{j_0}$ is injectively free over $\mathcal{K}$, and it follows that C is injectively free over B. The Lemma from p. 2 applied with $x = x_n$ then asserts precisely that

$$(**) \quad \mathcal{K}_{j_0}((x_1, \dots, x_n)) \cap \mathcal{K}((x_1, \dots, x_{n-1}))((x_n)) =$$

$$\mathrm{frac}\,(C[[x]]) \cap \big(\mathrm{frac}\,(B)\big)((x_n)) = \mathrm{frac}\,(B[[x_n]]) = \mathcal{K}((x_1, \dots, x_n)).$$

From $(*)$ and $(**)$, we have that

$$\bigcap_i \mathcal{K}_i((x_1, \dots, x_n)) \subseteq \mathcal{K}((x_1, \dots, x_n)).$$

The opposite inclusion is obvious. $\square$

Corollary. *Let K be a field of characteristic $p > 0$ and let Λ be a p-base for K. Let A be the formal power series ring $K[[x_1, \dots, x_n]]$. Then*

$$\bigcap_{\Gamma \text{ cofinite in } \Lambda} \mathrm{frac}\,(A^\Gamma) = \mathrm{frac}\,(A).$$

Proof. Since the completion of A^Γ is $K^\Gamma[[x_1, \dots, x_n]]$, we have that

$$(*) \quad \bigcap_{\Gamma \text{ cofinite in } \Lambda} \mathrm{frac}\,(A^\Gamma) \subseteq \bigcap_{\Gamma \text{ cofinite in } \Lambda} \mathrm{frac}\,(K^\Gamma[[x_1, \dots, x_n]]).$$

Since

$$\bigcap_{\Gamma \text{ cofinite in } \Lambda} K^\Gamma = K$$

by the Lemma on p. 6 of the Lecture Notes from October 17 and part (b) of the Theorem on p. 7 of the Lecture Notes from October 17 we have that the right hand term in $(*)$ is $\mathrm{frac}\,(K[[x_1, \dots, x_n]])$. This proves one of the inclusions needed, while the opposite inclusion is obvious. $\square$

We also want to observe the following:

Lemma. *Let $\mathcal{L}$ be any field of characteristic $p > 0$, and let Ω be any field finitely generated over $\mathcal{L}$. Then there exists a field $\Omega' \supseteq \Omega$ finitely generated over $\mathcal{L}$ such that Ω' is a finite separable algebraic extension of a pure transcendental extension $\mathcal{L}'(y_1, \ldots, y_h)$ of a field $\mathcal{L}'$ that is a finite purely inseparable algebraic extension of $\mathcal{L}$.*

Proof. Let h be the transcendence degree of Ω over $\mathcal{L}$. Then Ω is a finite algebraic extension of a pure transcendental extension $\mathcal{F} = \mathcal{K}(z_1, \ldots, z_h)$, where $z_1, \ldots, z_h$ is a transcendence basis for Ω over $\mathcal{L}$. Suppose that $\Omega = \mathcal{F}[\theta_1, \ldots, \theta_s]$ where every θ_j is algebraic over $\mathcal{F}$. Within the algebraic closure $\overline{\Omega}$ of Ω, we may form $\mathcal{F}^\infty[\theta_1, \ldots, \theta_s]$, where $\mathcal{F}^\infty$ is the perfect closure of $\mathcal{F}$ in $\overline{\Omega}$. Since $\mathcal{F}^\infty$ is perfect, every θ_i is separable over $\mathcal{F}^\infty$, and so every θ_i satsfies a separable equation over $\mathcal{F}^\infty$. Let $\alpha_1, \ldots, \alpha_N$ be all the coefficients of these equations. Then every θ_i is separable over $\mathcal{F}[\alpha_1, \ldots, \alpha_N]$, and every α_j has a q_j th power in $\mathcal{F}$. Hence, we can choose a single $q = p^e$ such that $\alpha_j^q \in \mathcal{F} = \mathcal{L}(z_1, \ldots, z_h)$ for every j. Every α_j^q can be written in the form

$$\frac{f_j(z_1, \ldots, z_h)}{g_j(z_1, \ldots, z_h)}$$

where $f_j, g_j \in \mathcal{L}[z_1, \ldots, z_h]$ and $g_j \neq 0$. Hence, α_j can be written as a rational function in the elements $z_1^{1/q}, \ldots, z_h^{1/q}$ in which the coefficients are the q th roots of the coefficients occurring in f_j and g_j. Let $\mathcal{L}'$ be the field obtained by adjoining all the q th roots of all coefficients of all of the f_j and g_j to $\mathcal{L}$. Let $y_j = z_j^{1/q}$, $1 \leq j \leq h$. Then all of the α_j are in $\mathcal{L}'(y_1, \ldots, y_h)$, and every θ_i satsifies a separable equation over $\mathcal{L}'(y_1, \ldots, y_h)$. But then we may take

$$\Omega' = \mathcal{L}'(y_1, \ldots, y_h)[\theta_1, \ldots, \theta_s],$$

which evdiently contains Ω. $\square$

We are now read to prove the Theorem stated at the top of p. 6 of the Lecture Notes from October 17.

Proof that $\mathrm{frac}\,(A^\Gamma) \otimes_A \Omega$ *is a field for* $\Gamma \ll \Lambda$. We recall that, as usual, K is a field of characteristic $p > 0$, and Λ is p-base for K. Let $\mathcal{L} = \mathrm{frac}\,(A)$, and $\mathcal{L}_\Gamma = \mathrm{frac}\,(A^\Gamma)$. Let Ω be a field finitely generated over $\mathcal{L}$. We want to show that for all $\Gamma \ll \Lambda$, $\mathcal{L}_\Gamma \otimes_{\mathcal{L}} \Omega$ is a field. Since every element of $\mathcal{L}_\Gamma$ has a q th power in $\mathcal{L}$, it is equivalent to show that this ring is reduced: it is purely inseparable over Ω. As in the preceding Lemma, we can choose $\Omega' \supseteq \Omega$ such that Ω' is separable over $\mathcal{L}'(y_1, \ldots, y_h)$, where $\mathcal{L}'$ is a finite purely inseparable extension of $\mathcal{L}$ and $y_1, \ldots, y_h$ are indeterminates over $\mathcal{L}'$. Since $\mathcal{L}_\Gamma$ is flat over the field $\mathcal{L}$, we have that

$$\mathcal{L}_\Gamma \otimes_{\mathcal{L}} \Omega \subseteq \mathcal{L}_\Gamma \otimes_{\mathcal{L}} \Omega',$$

and so it suffices to consider the problem for Ω'.

By the Corollary on p. 4 and the Theorem stated at the bottom of p. 6 of the Lecture Notes from October 17 (which is proved on p. 1 of the notes from this lecture), for all $\Gamma \ll \Lambda$, we have that $\mathcal{L}_\Gamma \otimes_{\mathcal{L}} \mathcal{L}'$ is a field. The ring $\mathcal{G} = \mathcal{L}_\Gamma \otimes_{\mathcal{L}} \mathcal{L}'(y_1, \ldots, y_h)$ is a localization of the polynomial ring $(L_\Gamma \otimes_{\mathcal{L}} \mathcal{L}')[y_1, \ldots, y_h]$. Hence, it is a domain, and therefore a field. Let $\mathcal{F} = \mathcal{L}'(y_1, \ldots, y_n)$. Then Ω' is a finite separable algebraic extension of $\mathcal{F}$, and it suffices to show that $\mathcal{G} \otimes_{\mathcal{F}} \Omega'$ is reduced. This follows from the second Corollary on *p.* 4 of the Lecture Notes of September 19, but we give a separate elementary argument. We can replace $\mathcal{G}$ by its algebraic closure: assume it is algebraically closed. By the theorem on the primitive element, $\Omega' \cong \mathcal{F}[X]/\bigl(h(X)\bigr)$, where h is a separable polynomial. Then

$$\mathcal{G} \otimes_{\mathcal{F}} \Omega' \cong \mathcal{G}[X]/\bigl(h(X)\bigr),$$

and since h is a separable polynomial, this ring is reduced. $\square$

We have now completed the proof of the Theorem on p. 4 of the Lecture Notes from October 17 concerning properties we can preserve with the gamma construction for Γ sufficiently small but cofinite in Λ.

Math 711: Lecture of October 22, 2007

By the *singular locus* Sing (R) in a Noetherian ring R we mean the set

$$\{P \in \mathrm{Spec}\,(R) : R_P \text{ is not regular}\}.$$

We know that if R is excellent, then Sing (R) is a Zariski closed set, i.e., it has the form $\mathcal{V}(I)$ for some ideal I of R. We say that I *defines* the singular locus in R. Such an ideal I is not unique, but its radical is unique. It follows easily that $c \in \mathrm{Rad}\,(I)$ if and only if R_c is regular.

We next want to prove:

Theorem. *Let K be a field of characteristic p with p-base Λ. Let B be a complete local ring with with coefficient field K. Let R be a ring essentially of finite type over B, and for Γ cofinite in Λ let $R^\Gamma = B^\Gamma \otimes_B R$.*

(a) *If R is regular, then R^Γ is regular for all $\Gamma \ll \Lambda$.*

(b) *If $c \in R$ is such that R_c is regular, then $(R_c)^\Gamma \cong (R^\Gamma)_c$ is regular for all $\Gamma \ll \Lambda$.*

(c) *If I defines the singular locus of R, then for all $\Gamma \ll \Lambda$, IR^Γ defines the singular locus in R^Γ.*

Proof. For every Γ cofinite in Λ, $R \to R^\Gamma$ is purely inseparable, and so we have a homeomorphism Spec (R^Γ)Spec $(R) = X$, given by contraction of primes. The unique prime ideal of R^Γ lying over P in R is Rad (PR^Γ). See the Proposition on p. 2 of the Lecture Notes from October 1. We identify the spectrum of every R^Γ with X. Let Z_Γ denote the singular locus in R^Γ, and Z the singular locus in R. Since all of these rings are excellent, every singular locus is closed in the Zariski topology. If $R \to S$ is faithfully flat and S is regular then R is regular, by the Theorem on p. 2 of the Lecture Notes of September 19. Thus, a prime Q such that S_Q is regular lies over a prime P in R such that R_P is regular. For $\Gamma \subseteq \Gamma'$ we have maps $R \to R^\Gamma \to R^{\Gamma'}$: both maps are faithfully flat. It follows that $Z \subseteq Z_\Gamma \subseteq Z_{\Gamma'}$ for all $\Gamma \subseteq \Gamma'$.

The closed sets in X have DCC, since ideals of R have ACC. It follows that we can choose Γ cofinite in Λ such that Z_Γ is minimal. Since the sets cofinite in Λ are directed under $\supseteq$, it follows that Z_Γ is minimum, not just minimal. We have $Z \subseteq Z_\Gamma$. We want to prove that they are equal. If not, we can choose Q prime in R^Γ lying over P in R such that R^Γ_Q is not regular but R_P is regular. By part (a) of the Theorem at the bottom of p. 4 of the Lecture Notes from October 17, we can choose $\Gamma_0 \subseteq \Gamma$ cofinite in Λ such that PR^{Γ_0} is prime. This prime will be the contraction Q_0 of Q to R^{Γ_0}. Let R_P have Krull dimension d. In R_P, P has d generators. Hence, $Q_0R_P^{\Gamma_0} = PR_P^{\Gamma_0}$ also has d generators, and it follows that Q_0 itself has d generators. Consequently, we have that $R^{\Gamma_0}_{Q_0}$ is regular, and this means that Z_{Γ_0} is *strictly* smaller than Z_Γ: the point corresponding to P is not in Z_{Γ_0}. This contradiction shows that for all $\Gamma \ll \Lambda$, $Z_\Gamma = Z$. It is immediate that for such a choice of Γ, a prime Q of R^Γ is such that R^Γ_Q is not regular if and only if $R_{Q\cap R}$ is not regular. But this holds if and only if $Q \cap R$ contains I, i.e., if and only if $Q \supseteq I$, which is equivalent to $Q \supseteq IR^\Gamma$. This proves (c).

Part (a) is simply the case where Z is empty. Note that for any $c \in R$,

$$(R_c)^\Gamma = B^\Gamma \otimes_B R_c \cong B^\Gamma \otimes_B (R \otimes_R R_c) \cong (B^\Gamma \otimes_B R) \otimes_R R_c \cong (R^\Gamma)_c.$$

Thus, (b) follows from (a) applied to R_c. $\square$

We are now in a position to fill in the details of the proof of the Theorem on the existence of completely stable big test elements stated on p. 2 of the Lecture Notes from October 12. The proof was sketched earlier to motivate our development of the gamma construction.

We need one small preliminary result.

Lemma. *If R is essentially of finite type over B and $B \to C$ is geometrically regular, then $C \otimes_B R$ is geometrically regular over R.*

Proof. This is a base change, so the map is evidently flat. Let P be a prime ideal of R lying over $\mathfrak{p}$ in B. Then

$$\kappa_P \otimes_R (R \otimes_B C) \cong \kappa_P \otimes_B C \cong \kappa_P \otimes_{\kappa_\mathfrak{p}} (\kappa_\mathfrak{p} \otimes_B C).$$

Let $T = \kappa_\mathfrak{p} \otimes_B C$, which is a geometrically regular $\kappa_\mathfrak{p}$-algebra by the hypothesis on the fibers. Then all we need is that every finite algebraic purely inseparable extension field extension $\mathcal{L}$ of κ_P, the ring $\mathcal{L} \otimes_{\kappa_\mathfrak{p}} T$ is regular. We may replace $\mathcal{L}$ by a larger field finitely generated over $\kappa_\mathfrak{p}$. By the Lemma at the top of p. 5 of the Lecture Notes of October 19, we may assume this larger field is a finite separable algebraic extension of $\mathcal{K}(y_1, \dots, y_h)$, where $\mathcal{K}$ is a finite algebraic purely inseparable extension of $\kappa_\mathfrak{p}$ and $y_1, \dots, y_h$ are indeterminates. Then $\mathcal{K} \otimes_{\kappa_\mathfrak{p}} T$ is regular by the hypothesis of geometric regularity of the fiber T over $\kappa_\mathfrak{p}$. Therefore, $\mathcal{K}(y_1, \dots, y_h) \otimes_{\kappa_\mathfrak{p}} T$ is regular because it is a localization of the polynomial ring $(\mathcal{K} \otimes_{\kappa_\mathfrak{p}} T)[y_1, \dots, y_h]$. Since $\mathcal{L}$ is finite separable algebraic over $\mathcal{K}(y_1, \dots, y_h)$, the result now follows from the second Corollary on p. 4 of the Lecture Notes from September 19. $\square$

We now restate the result that we want to prove.

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$. Suppose that R is reduced and essentially of finite type over an excellent semilocal ring B. Then there are elements $c \in R^\circ$ such that R_c is regular, and every such element c has a power that is a completely stable big test element.*

Proof. By the Lemma above, $\widehat{B} \otimes_B R$ is geometrically regular over R. Moreover, the localization at c may be viewed as has a regular base R_c, and the fibers of $R_c \to \widehat{B} \otimes_R R_c$

are still regular: they are a subset of the original fibers, corresponding to primes of R that do not contain c. By the first Corollary at the top of p. 4 of the Lecture Notes of September 19, $(\widehat{B} \otimes_B R)_c$ is regular. Since R is reduced and $c \in R^\circ$, c is not a zerodivisor in R, i.e., $R \subseteq R_c$. It follows that $\widehat{B} \otimes_B R \subseteq \widehat{B} \otimes_B R_c$, and so $\widehat{B} \otimes_B R$ is reduced. Since $R \to \widehat{B} \otimes_B R$ is faithfully flat, it suffices to prove the result for $\widehat{B} \otimes_B R$, by part (b) of the Proposition at the bottom of p. 8 of the Lecture Notes from September 17.

Thus, we may replace B by its completion. Henceforth, we assume that B is complete. B is now a product of local rings. R is a product in a corresponding way, and every R-module is a product of R-modules over the factors. The hypotheses are preserved on each factor ring, and all of the issues under consideration reduce to consideration of the factors separately. Therefore we need only consider the case where B is a complete local ring.

Choose a coefficient field K for B, and a p-base Λ for K, so that we may use the gamma construction on B. For all $\Gamma \ll \Lambda$, we have that $R^\Gamma = B^\Gamma \otimes_B R$ is reduced, and that

$$B^\Gamma \otimes_B R_c \cong R_c^\Gamma$$

is regular. Since R^Γ is faithfully flat over R, it suffices to consider R^Γ instead of R. Since R^Γ is F-finite, the result is now immediate from the Theorem at the bottom of p. 4 of the Lectture Notes of October 1. $\square$

We want to improve the result above: it will turn out that it suffices to assume that R_c is Gorenstein and weakly F-regular. We will need some further results about weak F-regularity in the Gorenstein case. In particular, we want to prove that when the ring is F-finite, weak F-regularity implies strong F-regularity.

We first note the following fact:

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$. Then the following conditions are equivalent:*

(a) *If $N \subseteq M$ are arbitary modules (with no finiteness condition), then N is tightly closed in M.*

(b) *For every maximal ideal m of R, 0 is tightly closed (over R) in $E_R(R/m)$.*

(c) *For every maximal ideal m of R, if u generates the socle in $E(R/m)$, then u is not in the tight closure (over R) of 0 in $E_R(R/m)$.*

Proof. Evidently (a) $\Rightarrow$ (b) $\Rightarrow$ (c). But $(c) \Rightarrow$ (b) is clear, because if if the tight closure of 0 is not 0, it must contain the socle: $R/m \hookrightarrow E_R(R/m)$ is essential, and every nonzero submodule of $E_R(R/m)$ therefore contains u.

Now suppose that $N \subseteq M$ and $u \in M$ is such that $u \in N^*_M - N$. We may replace N by a submodule of M maximal with respect to containing N and not containing u, by Zorn's Lemma. Then we may replace u and $N \subseteq M$ by the image of u in M/N and $0 \subseteq M/N$. Hence, we may assume that $u \in 0^*_M - \{0\}$ and that u is in every nonzero submodule of M. We may now apply the Lemma on p. 1 of the Lecture Notes from September 17 to conclude that for every finitely generated nonzero submodule of M, there is only one associated prime, m, which is maximal, and that the socle is one-dimensional and generated by u. But then the same conclusion applies to M itself, and so M is an essential extension of $Ru \cong Ku$, where $K = R/m$. Hence, M embeds in $E_R(R/m) = E$ so that u generates the socle in E, and $u \in 0^*_M$ implies that $u \in 0^*_E$. $\square$

We next want to prove the following:

Theorem. *Let $(R,\, m,\, K)$ be a Gorenstein local ring of prime characteristic $p > 0$. Then the conditions of the preceding Proposition hold if and only if R is weakly F-regular.*

Moreover, if R is weakly F-regular and F-finite, then R is strongly F-regular.

It will be a while before we can give a complete proof of this result. Our proof of the Theorem requires understanding $E_R(K)$ when R is a Gorenstein local ring.

Calculation of the injective hull of a Gorenstein local ring

Theorem. *Let $(R,\, m,\, K)$ be a Gorenstein local ring with system of parameters $x_1,\, \ldots\,, x_n$. For every integer $t \geq 1$, let $I_t = (x_1^t,\, \ldots\,, x_n^t)R$. Let $y = x_1 \cdots x_n$. Then*

$$E_R(K) \cong \varinjlim_t R/I_t,$$

where the map $R/I_t \to R/I_{t+1}$ is induced by multiplication by y on the numerators.

Moreover, if $u \in R$ represents a socle generator in $R/(x_1,\, \ldots\,, x_n)R$, then for every t, $y^{t-1}u \in R/I_t$ represents the socle generator in R/I_t and in $E_R(K)$.

Proof. Let $E = E_K(R)$ be a choice of injective hull for K. Then $E_t = \mathrm{Ann}_E I_t$ is an injective hull for K over R/I_t, and so is isomorphic to R/I_t. Since every element of E is killed by a power of m, each element of E is some E_t. Then

$$E = \bigcup_t E_t$$

shows that there is some choice of injective maps

$$\theta_t : R/I_t \to R/I_{t+1}$$

such that

$$E = \varinjlim_t E_t,$$

using the maps θ_t. One injection of R/I_t into R/I_{t+1} is given by the map η_t induced by multiplication by y on the numerators: see the Theorem at the bottom of p. 5 of the

Lecture Notes from October 8, applied to $x_1, \ldots, x_n$ and $x_1^t, \ldots, x_n^t$, with the matrix $A = \mathrm{diag}(x_1^{t-1}, \ldots, x_n^{t-1})$. (See also the last statement of the Proposition near the top of p. 8 in the same lecture, which will prove the final statement of the Theorem.) Since the modules have finite lengths, an injection of E_t into E_{t+1} must have image $E_t = \mathrm{Ann}_E I_t$, since the image is clear contained in E_t, and so there must be an automorphism α_t of E_t such that $\theta_t = \alpha_t \circ \eta_t$. In fact, $\alpha_t \in \mathrm{Hom}_{R/I_t}(E_t, E_t) \cong R_t$ must be multiplication by a unit of R_t. Thus, every α_t lifts to a unit $a_t \in R$. Let $b_1 = 1$, and let $b_t = a_1 \cdots a_{t-1}$.

We can now construct a commutative diagram

$$\begin{array}{ccccccccccc}
E_1 & \xrightarrow{\eta_1} & E_2 & \xrightarrow{\eta_2} & \cdots & \xrightarrow{\eta_{t-1}} & E_t & \xrightarrow{\eta_t} & E_{t+1} & \xrightarrow{\eta_{t+1}} & \cdots \\
{\scriptstyle b_1}\big\downarrow & & {\scriptstyle b_2}\big\downarrow & & & & {\scriptstyle b_t}\big\downarrow & & {\scriptstyle b_{t+1}}\big\downarrow & & \\
E_1 & \xrightarrow{\theta_1} & E_2 & \xrightarrow{\theta_2} & \cdots & \xrightarrow{\theta_{t-1}} & E_t & \xrightarrow{\theta_t} & E_{t+1} & \xrightarrow{\theta_{t+1}} & \cdots
\end{array}$$

Commutativity follows from the fact that on E_t, $b_{t+1}\eta_t$ is induced by multiplication by $b_{t+1}y = a_t b_t y = (a_t y)b_t$, and θ_t is induced by multiplication by $a_t y$ on E_t. Since the vertical arrows are isomorphisms, the direct limits are isomorphic. The direct limit of the top row is the module that we are trying to show is isomorphic to E, while the direct limit of the bottom row is E. $\square$

Math 711: Lecture of October 24, 2007

The action of Frobenius on the injective hull of the residue class field of a Gorenstein local ring

Let (R, m, K) be a Gorenstein local ring of prime characteristic $p > 0$, and let $x_1, \ldots, x_n$ be a system of parameters. Let $I_t = (x_1^t, \ldots, x_n^t)R$ for all $t \geq 1$, and let $u \in R$ represent a socle generator in R/I, where $I = I_1 = (x_1, \ldots, x_n)R$. Let $y = x_1 \cdots x_n$. We have seen that

$$E = \varinjlim_t R/I_t$$

is an injective hull of $K = R/m$ over R, where the map $R/I_t \to R/I_{t+1}$ is induced by multiplication by y acting on the numerators. Each of these maps is injective. Note that the map from $R/I_t \to R/I_{t+k}$ in the direct limit system is induced by multiplication by y^k acting on the numerators.

Let $e \in \mathbb{N}$ be given. We want to understand the module $\mathcal{F}^e(E)$, and we also want to understand the qth power map $v \mapsto v^q$ from E to $\mathcal{F}^e(E)$. If $r \in R$, we shall write $\langle r;\, x_1^t, \ldots, x_n^t\rangle$ for the image of r under the composite map $R \twoheadrightarrow R/I_t \hookrightarrow E$, where the first map is the quotient surjection and the second map comes from our construction of E as the direct limit of the R/I_t. With this notation,

$$\langle r;\, x_1^t, \ldots, x_n^t\rangle = \langle y^k r;\, x_1^{t+k}, \ldots, x_n^{t+k}\rangle$$

for every $k \in \mathbb{N}$.

Since tensor products commute with direct limit, we have that

$$\mathcal{F}^e(E) = \varinjlim_t \mathcal{F}^e(R/I_t) = \varinjlim_t R/(I_t)^{[q]} = \varinjlim_t R/I_{tq}.$$

In the rightmost term, the map from $R/I_{tq} \to R/I_{(t+1)q} = I_{tq+q}$ is induced by multiplication by t^q acting on the numerators. The rightmost direct limit system consists of of a subset of the terms in the system $\varinjlim_t R/I_t$, and the maps are the same. The indices that occur are cofinal in the positive integers, and so we may idenitfy $\mathcal{F}^e(E)$ with E. Under this identification, if $v = \langle r;\, x_1^t, \ldots, x_n^t\rangle$, then $v^q = \langle r^q;\, x_1^{qt}, \ldots, x_n^{qt}\rangle$.

We can now prove the assertions in the first paragraph of the Theorem on p. 4 of the Lecture Notes from October 22.

Proof that 0 *is tightly closed in* $E_R(K)$ *for a weakly F-regular Gorenstein local ring.* Let (R, m, K) be a Gorenstein local ring of prime characteristic $p > 0$. We want to determine when $v = \langle u;\, x_1, \ldots, x_n\rangle$ is in 0^* in E. This happens precisely when there is an element $c \in R^\circ$ such that $cv^q = 0$ in $\mathcal{F}^e(E)$ for all $q \gg 0$. But $cv^q = \langle cu^q;\, x_1^q, \ldots, x_n^q\rangle$, which is 0 if and only if $cu^q \in I_q = I^{[q]}$ for all $q \gg 0$. Thus, 0 is tightly closed in E if and only if I is tightly closed in R. This gives a new proof of the result that in a Gorenstein local ring, if I is tightly closed then R is weakly F-regular. But it also proves that if I is tightly closed, every submodule of every module is tightly closed. In particular, if R is weakly F-regular then every submodule over every module is tightly closed. $\square$

It remains to show that when a Gorenstein local ring is F-finite, it is strongly F-regular. We first want to discuss some issues related to splitting a copy of local ring from a module to which it maps.

Splitting criteria and approximately Gorestein local rings

Many of the results of this section do not depend on the characteristic.

Theorem. *Let (R, m, K) be a local ring and M an R-module. Let $f : R \to M$ be an R-linear map. Suppose that R is complete or that M is finitely generated. Let E denote an injective hull for the residue class field $K = R/m$ of R. Then $R \to M$ splits if and only if the map $E = E \otimes_R R \to E \otimes_R M$ is injective.*

Proof. Evidently, if the map splits the map obtained after tensoring with E (or any other module) is injective: it is still split. This direction does not need any hypothesis on R or M. For the converse, first consdider the case where R is complete. Since the map $E \otimes_R R \to E \otimes_R M$ is injective, if we apply $\mathrm{Hom}_R(\_\,, E)$, we get a surjective map. We switch the order of the modules in each tensor product, and have that

$$\mathrm{Hom}_R(R \otimes_E E,\, E) \to \mathrm{Hom}_R(M \otimes_R E,\, E)$$

is surjective. By the adjointness of tensor and Hom, this is isomorphic to the map

$$\mathrm{Hom}_R\big(M,\, \mathrm{Hom}_R(E,\, E)\big) \to \mathrm{Hom}_R(R,\, \mathrm{Hom}_R(E,\, E).$$

By Matlis duality, we have that $\mathrm{Hom}_R(E, E)$ may be naturally identified with R, since R is complete, and this yields that the map $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(R, R)$ induced by composition with $f : R \to M$ is surjective. An R-linear homomorphism $g : M \to R$ that maps to the identity in $\mathrm{Hom}_R(R, R)$ is a splitting for f.

Now supppose that R is not necessarily complete, but that M is finitely generated. By part (b) of the Theorem on p. 3 of the Lecture Notes from Septmeber 24, completing does not affect whether the map splits. The result now follows from the complete case, because E is the same for R and for $\widehat{R}$, and $E \otimes_{\widehat{R}} (\widehat{R} \otimes_R \_\,)$ is the same as $E \otimes_R \_$ by the associativity of tensor. $\square$

This result takes a particularly concrete form in the Gorenstein case.

Theorem (splitting criterion for Gorenstein rings). *Let (R, m, K) be a Gorenstein local ring, and let $x_1, \dots, x_n$ be a system of parameters for R. Let $u \in R$ represent a socle generator in R/I, where $I = (x_1, \dots, x_n)$, let $y = x_1 \cdots, y_n$, and let $I_t = (x_1^t, \dots, x_n^t)R$ for $I \geq 1$. Let $f : R \to M$ be an R-linear map with $f(1) = w \in M$, and assume either that R is complete or that M is finitely generated. Then the following conditions are equivalent:*

(1) *$f : R \to M$ is split.*

(2) *For every ideal J of R, $R/J \to M/JM$ is injective, where the map is induced by applying $(R/J) \otimes_R \_$.*

(3) *For all $t \geq 1$, $R/I_t \to M/I_tM$ is injective.*

(4) *For all $t \geq 1$, $y^{t-1}uw \notin I_tM$.*

Moreover, if $x_1, \dots, x_n$ is a regular sequence on M, then the following two conditions are also equivalent:

(5) *$R/I \to R/IM$ is injective.*

(6) *$uw \notin IM$.*

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (5) is clear. The map $R/I_t \to M/I_tM$ has a nonzero kernel if and only if the socle element, which is the image of $y^{t-1}u$, is killed, and this element maps to $y^{t-1}uw$. Thus, the statements in (3) and (4) are equivalent for every value of t, and the equivalence (5) $\Leftrightarrow$ (6) is the case $t = 1$. We know from the preceding Theorem that $R \to M$ is split if and only if $E \to E \otimes_R M$ is injective, and this map is the direct limit of the maps $R/I_t \to (R/I_t) \otimes_R M$ by the Theorem on p. 2. This shows that (3) $\Rightarrow$ (1). Thus, (1), (2), (3), and (4) are all equivalent and imply (5) and (6), while (5) and (6) are also equivalent. To complete the proof it suffices to show that (6) $\Rightarrow$ (4) when $x_1, \dots, x_n$ is a regular sequence on M. Suppose $y^t uw \in (x_1^t, \dots, x_n^t)M$. Then $uw \in (x_1^t, \dots, x_n^t)M :_M y^t = (x_1, \dots, x_n)M$ by the Theorem on p. 3 of the Lecture Notes from October 8. $\square$

Remark. If $M = S$ is an R-algebra and the map $R \to S$ is the structural homomorphism, then the condition in part (2) is that every ideal J of R is contracted from S. Similarly, the condition in (4) (respectively, (5)) is that I_t (respectively, I) be contracted from S.

We define a local ring (R, m, K) to be *approximately Gorenstein* if there exists a decreasing sequence of m-primary ideals $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_t \supseteq \cdots$ such that every R/I_t is a Gorenstein ring (i.e., the socle of every R/I_t is a one-dimensional K-vector space) and the I_t are cofinal with the powers of m. That is, for every $N > 0$, $I_t \subseteq m^N$ for all $t \gg 1$. Evidently, a Gorenstein local ring is approximately Gorenstein, since we may take $I_t = (x_1^t, \dots, x_n^t)R$, where $x_1, \dots, x_n$ is a system of parameters.

Note that the following conditions on an m-primary ideal I in a local ring (R, m, K) are equivalent:

(1) R/I is a 0–dimensional Gorenstrein.

(2) The socle in R/I is one-dimensional as a K-vector space.

(3) I is an irreducible ideal, i.e., I is not the intersection of two strictly larger ideals.

Note that (2) $\Rightarrow$ (3) because when (2) holds, any two larger ideals, considered modul I, must both contain the socle of R/I. Conversely, if the socle of R/I has dimension 2 or more, it contains nonzero vector subspaces V and V' whose intersection is 0. The inverse iamges of V and V' in R are ideals strictly larger than I whose intersection is I. $\square$

If R itself has dimension 0, the chain I_t is eventually 0, and so in this case an approximately Gorenstein ring is Gorenstein. In higher dimension, it turns out to be a relatively weak condition on R.

Theorem. *Let (R, m, K) be a local ring. Then R is approximately Gorenstein if and only if $\widehat{R}$ is approximately Gorenstein. Moreover, R is approximately Gorenstein provided that at least one of the following conditions holds:*

(1) *$\widehat{R}$ is reduced.*

(2) *R is excellent and reduced.*

(3) *R has depth at least 2.*

(4) *R is normal.*

The fact that the condition holds for R if and only it holds for $\widehat{R}$ is obvious. Moreover, (2) $\Rightarrow$ (1) and (4) $\Rightarrow$ (3). We shall say more about why the Theorem given is true in the sequel. For a detailed treatment see [M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977) 463–488.], which gives the following precise characterization: a local ring of dimension at least one is approximately Gorenstein if and only if R has positive depth and there is no associated prime P of the completion $\widehat{R}$ such that $\dim(\widehat{R}/P) = 1$ and $(\widehat{R}/P) \oplus (\widehat{R}/P)$ embeds in $\widehat{R}$.

Before studying characterizations of the property of being approximately Gorenstein further, we want to note the folliwing.

Propositon. *Let (R, m, K) be an approximately Gorenstein local ring and let $\{I_t\}_t$ be a descending chain of m-primary irreducible ideals cofinal with the powers of m. Then an injective hull $E = E_R(K)$ is an increasing union $\bigcup_t \mathrm{Ann}_{I_t} E$, and $\mathrm{Ann}_E I_t \cong R/I_t$, so that E is the direct limit of a system in which the modules are the R/I_t and the maps are injective.*

Proof. Since every element of E is killed by a power of m, every element of E is in $\mathrm{Ann}_E I_t$ for some t. We know that $\mathrm{Ann}_E I_t$ is an injective hull for K over R/I_t. Since R/I_t is 0-dimensional Gorenstein, this ring itself is an injective hull over itself for K. $\square$

This yields:

Theorem. *Let (R, m, K) be an approximately Gorenstein local ring and let $\{I_t\}_t$ be a descending chain of m-primary irreducible ideals cofinal with the powers of m. Let $u_t \in R$*

represent a socle generator in R/I_t. Let $f : R \to M$ be an R-linear map with $f(1) = w \in M$. Then the following conditions are equivalent:

(1) *$f : R \to M$ splits over R.*

(2) *For all $t \geq 1$, $R/I_t \to M/I_tM$ is injective.*

(3) *For all $t \geq 1$, $u_t w \notin I_tM$.*

Proof. Since $E = E_R(K)$ is the direct limit of the R/I_t, we may argue exactly as in the proof of the Theorem at the top of p 3. □

When is a ring approximately Gorenstein?

To prove a sufficient condition for a local ring to be approximately Gorenstein, we want to introduce a corresponding notion for modules. Let (R, m, K) be local and let M be a finitely generated R-module. We shall say that $N \subseteq M$ is *cofinite* if M/N is killed by power of m. (The reader should be aware that the term "cofinite module" is used by some authors for a module with DCC.) The following two conditions on a cofinite submodule are then equivalent, just as in the remark at the bottom of p. 3 and top of p. 4.

(1) The socle in M/N is one-dimensional as K-vector space.

(2) N is in irreducible submodule of M, i.e., it is not the intersection of two strictly larger submodules of M.

We shall say that M has *small cofinite irreducibles* if for every positive integer t there is an irreducible cofinite submodule N of M such that $N \subseteq m^tM$. Thus, a local ring R is approximately Gorenstein if and only if R itself has small cofinite irreducibles.

Note the the question of whether $(R,\, m,\, K)$ is approximately Gorenstein or whether M has small cofinite irreducibles is unaffected by completion: there is a bijection between the cofinite submodules N of M and those of $\widehat{M}$ given by letting N correspond to $\widehat{N}$. The point is that if N' is cofinite in $\widehat{M}$, $\widehat{M}/N'$ is a finitely generated R-module (in fact, it has finite length) and $M \to \widehat{M}/N'$ is surjective, since $M/m^tM \cong \widehat{M}/m^t\widehat{M}$ for all t, so that N' is the completion of $N' \cap M$. Moreover, when N and N' correspond, $M/N \cong \widehat{M}/N'$ since M/N is already a complete R-module. In particular, irreducibility is preserved by the correspondence.

We have already observed that Gorenstein local rings are approximately Gorenstein. We next note:

Proposition. *Let $(R,\, m,\, K)$ be a local ring. If M is a finitely generated R-module that has small cofinite irreducibles, then every nonzero submodule of M has small cofinite irreducibles.*

Proof. Suppose that $N \subseteq M$ is nonzero. By the Artin-Rees lemma there is a constant $c \in \mathbb{N}$ such that $m^t M \cap N \subseteq m^{t-c}N$ for all $t \geq c$. If M_{t+c} is cofinite in M and such that $M_{t+c} \subseteq m^{t+c}M$ and M/M_{t+c} has a one-dimensional socle, then $N_t = M_{t+c} \cap N$ is cofinite in N, contained in $m^t N$ (so that N/N_t is nonzero) and has a one-dimensional socle, since N/N_t embeds into M/M_{t+c}. $\square$

Before giving the main result of this section, we note the following fact, due to Chevalley, that will be needed in the argument.

Theorem (Chevalley's Lemma). *Let M be a finitely generated module over a complete local ring (R, m, K) and let $\{M_t\}_t$ denote a nonincreasing sequence of submodules. Then $\bigcap_t M_t = 0$ if and only if for every integer $N > 0$ there exists t such that $M_t \subseteq m^N M$.*

Proof. The "if" part is clear. Suppose that the intersection is 0. Let $V_{t,N}$ denote the image of M_t in $M/m^N M$. Then the $V_{t,N}$ do not increase as t increases, and so are stable for all large t. Call the stable image V_N. Then the maps $M/m^{N+1}M \to M/m^N M$ induce surjections $V_{N+1} \twoheadrightarrow V_N$. The inverse limit W of the V_N may be identified with a submodule of the inverse limit of the $M/m^N M$, i.e. with a submodule of M, and any element of W is in

$$\bigcap_{t,N}(M_t + m^N M) = \bigcap_t\big(\bigcap_N(M_t + m^N M)\big) = \bigcap_t M_t.$$

If any V_{N_0} is not zero, then since the maps $V_{N+1} \twoheadrightarrow V_N$ are surjective for all N, the inverse limit W of the V_N is not zero. But V_N is zero if and only if $M_t \subseteq m^N M$ for all $t \gg 0$. $\square$

The condition given in the Theorem immediately below for when a finitely generated module of positive dimension over a complete local ring has small cofinite irreducibles is necessary as well as sufficient: we leave the necessity as an exercise for the reader. The proof of the equivalence is given in [M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977) 463–488.]

Theorem. *Suppose that M is a finitely generated module over a complete local ring (R, m, K) such that* $\dim M \geq 1$. *Suppose that m is not an associated prime of M and that if P is an associated prime of M such that* $\dim R/P = 1$ *then $R/P \oplus R/P$ is not embeddable in M. Then M has small cofinite irreducibles.*

Proof. We use induction on $\dim M$. First suppose that $\dim M = 1$. We represent the ring R as a homomorphic image of a complete regular local ring S of dimension d. Because R is catenary and $\dim M = 1$, the annihilator of M must have height $d-1$. Choose part of a system of parameters $x_1,\, \ldots\,, x_{d-1}$ in the annihilator. Now view M as a module over $R' = S/(x_1,\, \ldots\,, x_{d-1})$. We change notation and simply write R for this ring. Then

R is a one-dimensional complete local ring, and R is Gorenstein. It follows that R has small cofinite irreducibles, and we can complete the argument, by the Proposition on the preceding page, by showing that M can be embedded in R. Note that for any minimal prime $\mathfrak{p}$ in R, $R_\mathfrak{p}$ is a (zero-dimensional) Gorenstein ring. (In fact, any localization of a Gorenstein local ring at a prime is again Gorenstein: but we have not proved this here. However, in this case, we may view $R_\mathfrak{p}$ as the quotient of the regular ring $S_\mathfrak{q}$, where $\mathfrak{q}$ is the inverse image of $\mathfrak{p}$ in S, by an ideal generated by a system of parameters for $S_\mathfrak{q}$, and the result follows.)

To prove that we can embed M in R, it suffices to show that if $W = R^\circ$, then $W^{-1}M$ can be embedded in $W^{-1}R$. One then has $M \subseteq W^{-1}M \subseteq W^{-1}R$, and the values of the injective map $M \hookrightarrow W^{-1}R$ on a finite set of generators of M involve only finitely many elements of W. Hence, one can multiply by a single element of W, and so arrange that $M \hookrightarrow W^{-1}R$ actually has values in R.

But $W^{-1}R$ is a finite product of local rings $R_\mathfrak{p}$ as $\mathfrak{p}$ runs through the minimal primes of R, and so it suffices to show that if $\mathfrak{p}$ is a minimal prime of R in the support of M, then $M_\mathfrak{p}$ embeds in $R_\mathfrak{p}$. Now, $M_\mathfrak{p}$ has only $\mathfrak{p}R_\mathfrak{p}$ as an associated prime, and since only one copy of $R/\mathfrak{p}$ can be embedded in M, only one copy of $\kappa_\mathfrak{p} = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ can be embedded in $M_\mathfrak{p}$. Thus, $M_\mathfrak{p}$ is an essential extension of a copy of $\kappa_\mathfrak{p}$. Thus, it embeds in the injective hull of the residue field of $R_\mathfrak{p}$, which, since $R_\mathfrak{p}$ is a zero-dimensional Gorenstein ring, is the ring $R_\mathfrak{p}$ itself.

Now suppose that $\dim M = d > 1$ and that the result holds for modules of smaller dimension. Choose a maximal family of prime cyclic submodules of M, say $Ru_1, \dots, Ru_s$, such that $\mathrm{Ann}_R u_i$ is a prime Q_i for every i and the sum $N = Ru_1 \oplus \cdots \oplus Ru_s$ is direct. Then M is an essential extension of N: if $v \in M$, it has a nonzero multiple rv that generates a prime cyclic module, and if this prime cyclic module does not meet N we can enlarge the family. Since M is an essential extension of N, M embeds in the injective hull of N, which we may identify with the direct sum of the $E_i = E_R(Ru_i)$. Note that a prime ideal of R may occur more than once among the Q_i, but not if $\dim(R/Q_i) = 1$, and R/m does not occur. Take a finite set of generators of M. The image of each generator only involves finitely many elements from a given E_i. Let M_i be the submodule of E_i generated by these elements. Then $M_i \subseteq E_i$, so that $\mathrm{Ass}(M_i) = Q_i$, and M_i is an essential extension of R/Q_i. What is more $M \subseteq \oplus_{i=1}^s M_i$.

By the Propositiion at the bottom of p. 5, it suffices to show that this direct sum, which satisfies the same hypotheses as M, has small cofinite irreducibles. Thus, by we need only consider the case where $M = \bigoplus_{i=1}^s M_i$ as described. We assume that, for $i \le h$, $\mathrm{Ass}\, M_i = \{Q_i\}$ with $\dim(R/Q_i) = 1$ and with the Q_i *mutually distinct*, while for $i > h$, $\dim(R/Q_i) > 1$, and these Q_i need not all be distinct. Now choose primes $P_1, \dots, P_s$ such that, for every i, $\dim R/P_i = 1$, such that $P_1, \dots, P_s$ are all distinct, and such that for all i, $P_i \supseteq Q_i$. We can do this: for $1 \le i \le h$, the choice $P_i = Q_i$ is forced. For $i > h$ we can solve the problem recursively: simply pick P_i to be any prime different from the others alreaday selected and such that $P_i \supseteq Q_i$ and $\dim R/P_i = 1$. (We are using the fact that a local domain R/Q of dimension two or more contains infinitely many primes P such that $\dim R/P = 1$. To see this, kill a prime to obtain a ring of dimension exactly two. We then need to see that there are infinitely many height one primes. But if there are only finitely many, their union cannot be the entire maximal ideal, and a minimal prime of an element of the maximal ideal not in their union will be another height one prime.)

Fix a positive integer t. We shall construct a submodule N of M contained in m^tM and such that M/N is cofinite with a one-dimensional socle. We shall do this by proving that for every i there is a submodule N_i of M_i with the following properties:

(1) $N_i \subseteq m^t M_i$

(2) $\mathrm{Ass}\, M_i/N_i = \{P_i\}$ and M_i/N_i is an essential extension of R/P_i.

It then follows that $\overline{M} = M/(\bigoplus_i N_i)$ is a one-dimensional module with small cofinite irreducibles, and so we can choose $\overline{N} \subseteq m^t\overline{M}$ such that $\overline{M}/\overline{N}$ has finite length and a one-dimensional socle. We can take N to be the inverse image of $\overline{N}$ in M. This shows that the problem reduces to the construction of the N_i with the two properties listed.

If $i \leq h$ we simply take $N_i = 0$. Now suppose that $i > h$. To simplify notation we write M, Q and P for M_i, Q_i and P_i, respectively. Let $D_k \subseteq M$ be the contraction of $P^k M_P$ to $M \subseteq M_P$. Since $\bigcap_k P^k M_P = 0$ (thinking over R_P), we have that $\bigcap_k D_k = 0$. Since M is complete, by Chevalley's Lemma, we can choose k so large that $D_k \subseteq m^t M$.

We shall show that the completion of M_P over the completion of R_P satisfies the hypothesis of the Theorem. But then, since M_P and its completion have dimension strictly smaller than M, it follows from the induction hypothesis that, working over R_P, M_P has small cofinite irreducibles. Consequently, we may choose a cofinite irreducible $N' \subseteq P^k M_P$, and the contraction of N' to M will have all of the properties that we want, since it will be contained in $D_k \subseteq m^t M$.

Thus, we need only show that the completion of M_P over the completion of R_P satisfies the hypothesis of the Theorem. Since $\mathrm{Ass}\,(M) = \{Q\}$, we have that $\mathrm{Ass}\,(M_P) = \{QR_P\}$, and so PR_P is not an associated prime of M_P. Thus, the depth of M_P is at least one, and this is preserved when we complete. By Problem 2(b) of Problem Set #3, $\mathrm{Ass}\,(\widehat{M_P})$ is the same as the set of associated primes of the completion of R_P/QR_P, which we may identify with $\widehat{R_P}/Q\widehat{R_P}$. Since this ring is reduced, the primes $\mathfrak{q}$ that occur are minimal primes of $Q\widehat{R_P}$. For such a prime $\mathfrak{q}$,

$$\mathrm{Ann}_{\widehat{M_P}}\mathfrak{q} \subseteq \mathrm{Ann}_{\widehat{M_P}}Q \cong \widehat{R_P} \otimes_{R_P} \mathrm{Ann}_{M_P}QR_P,$$

since $\widehat{R_P}$ is flat over R_P. From the hypothesis, we know that $\mathrm{Ann}_{M_P}QR_P$ has torsion free rank one over R_P/QR_P, and so it embeds in R_P/QR_P. It follows that $\mathrm{Ann}_{\widehat{M_P}}\mathfrak{q}$ embeds in $\widehat{R_P}/Q\widehat{R_P}$. Since this ring is reduced with $\mathfrak{q}$ as one of the minimal primes, its total quotient ring is a product of fields. Hence, it is not possible to embed the direct sum of two copies of $(\widehat{R_P}/Q\widehat{R_P})/\mathfrak{q}$ in $\widehat{R_P}/Q\widehat{R_P}$. This completes the proof of the Theorem. $\square$

Math 711, Fall 2007 **Problem Set #3**
Due: Wednesday, November 7

1. Let R be a domain in which the test ideal has height two, and let P be a height one prime ideal of R. Suppose that $u \in N^*_M$, where $N \subseteq M$ are finitely generated R-modules. Let $R \to S$ be a homomorphism to a domain S with kernel P. Show that $1 \otimes u$ is in the tight closure of the image of $S \otimes_R N$ in $S \otimes_R M$ over S, i.e., in $\langle S \otimes_R N \rangle^*_{S \otimes_R M}$.

2. Let R be a Noetherian ring of prime characteristic $p > 0$.

(a) Let $I \subseteq R$ be an ideal, and let $W \subseteq R$ be a multiplicative system disjoint from every associated prime of every ideal of the form $I^{[q]}$. Show that $(IW^{-1}R)^*$ over $W^{-1}R$ may be identified with $W^{-1}I^*$.

(b) Let R be a reduced Cohen-Macaulay ring, and let $x_1, \ldots, x_n$ be a regular sequence in R such that $I = (x_1, \ldots, x_n)R$ is tightly closed in R. Let P be a minimal prime of I. Prove that R_P is F-rational. (Suggestion: first localize at the multiplicative system W consisting of the complement of the union of the minimal primes of I. After this localization, P expands to a maximal ideal.)

(c) Let (R, m, K) be F-rational and P a prime ideal of R. Show that R_P is F-rational.

3. (a) If M is a finitely generated module over a Noetherian ring R, show that M has a finite filtration such that every factor is a finitely generated torsion-free (R/P)-module N for some prime $P \in \mathrm{Ass}\,(M)$, and each such module N embeds in $(R/P)^{\oplus h}$ for some h.

(b) Let $R \to S$ be flat, where R and S are Noetherian rings, and let M be an R-module. Show that $\mathrm{Ass}_S(S \otimes_R M) = \bigcup_{P \in \mathrm{Ass}_R(M)} \mathrm{Ass}_S(S/PS)$.

4. Let (R, m, K) be a Gorenstein local ring of prime characteristic $p > 0$, and let $x_1, \ldots, x_n$ be a system of parameters for R. Suppose that every x_i is a test element. Let $I = (x_1, \ldots, x_n)R$. Show that $I :_R I^*$ is the test ideal $\tau(R)$ for R.

5. (a) Let (R, m, K) be a Gorenstein local ring of prime characteristic $p > 0$ that is F-finite or complete, and let $x_1, \ldots, x_n$ be a system of parameters for R. Let $u \in R$ represent a generator of the socle in $R/(x_1, \ldots, x_n)$. Show that R is F-split if and only if $u^p \notin (x_1^p, \ldots, x_n^p)R$.

(b) Let K be a perfect field of characteristic $p > 0$, where $p \neq 3$. Determine for which primes p the ring $K[[x, y, z]]/(x^3 + y^3 + z^3)$ is F-split.

6. (a) Let R be ring of prime characteristic $p > 0$, and W be a multipllicative system in R, and let $S = W^{-1}R$. Let M be an S-module. Show that $\mathcal{F}^e_R(M) \cong \mathcal{F}^e_S(M)$.

(b) Let R be a Noetherian ring of prime characteristic $p > 0$. Show that if every submodule of every R-module is tightly closed, then the same holds for $W^{-1}R$ for every multiplicative system W in R. [Suggestion: it suffices to consider injective hulls of quotients of the ring by prime ideals.]

Math 711: Lecture of October 26, 2007

It still remains to prove the final assertion of the Theorem from p. 3 of the Lecture Notes of October 22: that if R is F-finite and weakly F-regular, then R is strongly F-regular. Before doing so, we want to note some consequences of the theory of test elements, and also of the theory of approximately Gorenstein rings.

Theorem. *Let $(R,\, m,\, K)$ be a local ring of prime characteristic $p > 0$.*

(a) *If R has a completely stable test element, then $\widehat{R}$ is weakly F-regular if and only if R is weakly F-regular.*

(b) *If R has a completely stable big test element, then $\widehat{R}$ has the property that every submodule of every module is tightly closed if and only if R does.*

Proof. We already know that if a faithfully flat extension has the relevant property, then R does. For the converse, it suffices to check that 0 is tightly closed in every finite length module over $\widehat{R}$ (respectively, in the injective hull E of the residue class field over $\widehat{R}$, which is the same as the injective hull of the residue class field over R). A finite length $\widehat{R}$-module is the same as a finite length R-module. We can use the completely stable (big, for part (b)) test element $c \in R$ in both tests, which are then bound to have the same outcome for each element of the modules. For a module M supported only at m,

$$\mathcal{F}^e_{\widehat{R}}(M) \cong \mathcal{F}^e_{\widehat{R}}(\widehat{R} \otimes_R M) \cong \widehat{R} \otimes_R \mathcal{F}^e_R(M) \cong \mathcal{F}^e_R(M). \qquad \square$$

Proposition. *Let R have a test element (respectively, a big test element) c and let $N \subseteq M$ be finitely generated (respectively, arbitrary) R-modules. Let $d \in R^\circ$ and suppose $u \in M$ is such that $cu^q \in N^{[q]}$ for infinitely many values of q. Then $u \in N^*_M$.*

Proof. Suppose that $du^q \in N^{[q]}$ and that $p^{e_1} = q_1 < q$, so that $q = q_1 q_2$. Then $(du^{q_1})^{q_2} = d^{q_2-1}du^q \in (N^{[q_1]})^{[q_2]} = N^{[q]}$, and it follows that for all q_3, $(du^{q_1)})^{q_2 q_3} \in (N^{[q_1]})^{[q_2 q_3]}$. Hence, $du^{q_1} \in (N^{[q_1]})^*$ in $\mathcal{F}^{e_1}(M)$ whenever $q_1 \leq q$. Hence, if $du^q \in N^{[q]}$ for arbitrarily large values of q, then $du^q \in (N^{[q]})^*$ in $\mathcal{F}^e(M)$ for all q and it follows that $cdu^q \in N^{[q]}$ for all q, so that $u \in N^*_M$. $\square$

Theorem. *Let R be a Noetherian ring of prime characteristic $p > 0$.*

(a) *If every ideal of R is tightly closed, then R is weakly F-regular.*

(b) *If R is local and $\{I_t\}_t$ is a descending sequence of irreducible m-primary ideals cofinal with the powers of m, then R is weakly F-regular if and only if I_t is tightly closed for all $t \geq 1$.*

Proof. (a) We already know that every ideal is tightly closed if and only if every ideal primary to a maximal ideal is tightly closed, and this is not affected by localization at a maximal ideal. Therefore, we may reduce to the case where R is local. The condition that every ideal is tightly closed implies that R is normal and, hence, approximately Gorenstein. Therefore, it suffices to prove (b). For (b), we already know that R is weakly F-regular if and only if 0 is tightly closed in every finitely generated R-module that is an essential extension of K. Such a module is killed by I_t for some $t \gg 0$, and so embeds in $E_{R/I_t}(K) \cong R/I_t$ for some t. Since I_t is tightly closed in R, 0 is tightly closed in R/I_t, and the result follows. $\square$

We next want to establish a result that will enable us to prove the final assertion of the Theorem from p. 3 of the Lecture Notes of October 22.

Theorem. *Let (R, m, K) be a complete local ring of prime characteristic $p > 0$. If R is reduced and $c \in R^\circ$, let $\theta_{q,c} : R \to R^{1/q}$ denote the R-linear map such that $1 \mapsto c^{1/q}$. Then the following conditions are equivalent:*

(1) *Every submodule of every module is tightly closed.*

(2) *0 is tightly closed in the injective hull $E = E_R(K)$ of the residue class field $K = R/m$ of R.*

(3) *R is reduced, and for every $c \in R^\circ$, there exists q such that the $\theta_{q,c}$ splits.*

(4) *R is reduced, and for some c that has a power which is a big test element for R, there exists q such that $\theta_{q,c}$ splits.*

(5) *R is reduced, and for some c such that R_c is regular, there exists q such that $\theta_{q,c}$ splits.*

Proof. Note that all of the conditions imply that R is reduced.

We already know that conditions (1) and (2) are equivalent. Let u denote a socle generator in E. Then we have an injection $K \to E$ that sends $1 \mapsto u$, and we know that 0 is tightly closed in E if and only if u is in the tight closure of 0 in E. This is the case if and only if for some $c \in R^\circ$ (respectively, for a single big test element $c \in R^\circ$), $cu^q = 0$ in $\mathcal{F}^e(E)$ for all $q \gg 0$. We may view $\mathcal{F}^e : R \to R$ as $R \subseteq R^{1/q}$ instead. Then $\mathcal{F}^e(E)$ is identified with $R^{1/q} \otimes_R E$, and R acts via the isomorphism $R \cong R^{1/q}$ such that $r \mapsto r^{1/q}$. Then u^q corresponds to $1 \otimes u$, and cu^q corresponds to $c^{1/q} \otimes u$.

Then $u \in 0^*_E$ if and only if for every $c \in R^\circ$ (respectively, for a single big test element $c \in R^\circ$), the map $K \to R^{1/q} \otimes_R E$ that sends $1 \mapsto c^{1/q} \otimes u$ is 0 for all $q \gg 0$. We may now apply the functor $\mathrm{Hom}_R(\_\,, E)$ to obtain a dual condition. Namely, $u \in 0^*_E$ if and only if for every $c \in R^0$ (respectively, for a single big test element $c \in R^\circ$), the map

$$\mathrm{Hom}_R(R^{1/q} \otimes_R E,\, E) \to \mathrm{Hom}_R(K,\, E)$$

is 0 for all $q \gg 0$. The map is induced by composition with $K \to R^{1/q} \otimes_R E$. By the adjointness of tensor and Hom, we may identify this map with

$$\mathrm{Hom}_R\big(R^{1/q},\, \mathrm{Hom}_R(E,\, E)\big) \to \mathrm{Hom}_R(K,\, E).$$

This map sends f to the composition of $K \to R^{1/q} \otimes_R E$ with the map such that $s \otimes v \mapsto f(s)(v)$. Since $\mathrm{Hom}_R(E,\, E) \cong R$ by Matlis duality and $\mathrm{Hom}_R(K,\, E) \cong K$, we obtain the map

$$\mathrm{Hom}_R(R^{1/q},\, R) \to K$$

that sends f to the image of $f(c^{1/q})$ in R/m.

Thus, $u \in 0^*_E$ if and only if for every $c \in R^0$ (respectively, for a single big test element $c \in R^\circ$), every $f : R^{1/q} \to R$ sends $c^{1/q}$ into m for every $q \gg 0$. This is equivalent to the statement that $\theta_{q,c} : R \to R^{1/q}$ sending $1 \to c^{1/q}$ does not split for every $q \gg 0$, since if $f(c^{1/q}) = a$ is a unit of R, $a^{-1}f$ is a splitting.

Note that if $R \to R^{1/q}$ sending $1 \mapsto c^{1/q}$ splits, then $R \to R^{1/q}$ splits as well: the argument in the Lecture Notes from September 21 (see pages 4 and 5) applies without any modification whatsoever. Moreover, the second Proposition on p. 5 of those notes shows that if one has the splitting for a given q, one also has it for every larger q.

We have now shown that $u \in 0^*_E$ if and only if for every $c \in R^0$ (respectively, for a single big test element $c \in R^\circ$), $\theta_{q,c} : R \to R^{1/q}$ sending $1 \to c^{1/q}$ does not split for every q.

Hence, 0 is tightly closed in E if and only if for every $c \in R^0$ (respectively, for a single big test element $c \in R^\circ$) the map $\theta_{q,c}$ splits for some q.

We have now shown that conditions (1), (2), and (3) are equivalent, and that (4) is equivalent as well provided that c is a big test element.

Now suppose that we only know that c has a power that is a big test element. Then this is also true for any larger power, and so we can choose $q_1 = p^{e_1}$ such that c^{q_1} is a test element. If the equivalent conditions (1) , (2), and (3) hold, then we also know that the map $R \to R^{1/qq_1}$ sending $1 \mapsto (c^{q_1})^{1/qq_1} = c^{1/q}$ splits for all $q \gg 0$, and we may restrict this splitting to $R^{1/q}$. Thus, (1) through (4) are equivalent.

Finally, (5) is equivalent as well, because we know that if $c \in R^\circ$ is such that R_c is regular, then c has a power that is a big test element. $\square$

Remark. It is not really necessary to assume that R is reduced in the last three conditons. We can work with $R^{(e)}$ instead of $R^{1/q}$, where $R^{(e)}$ denotes R viewed as an R-algebra via the structural homomorphism $\mathcal{F}^e$. We may then define $\theta_{q,c}$ to be the R-linear map $R \to R^{(e)}$ such that $1 \mapsto c$. The fact that this map is split for some some $c \in R^\circ$ and some q implies that R is reduced: if r is a nonzero nilpotent, we can replace it by a power which is nonzero but whose square is 0. But then the image of r is $r^q c = 0$, and the map is not even injective, a contradiction. Once we know that R is reduced, we can identify $R^{(e)}$ with $R^{1/q}$ and c is identified with $c^{1/q}$.

We want to apply the preceding Theorem to the F-finite case. We first observe:

Lemma. *Let $(R,\, m,\, K)$ be an F-finite reduce local ring. Then $\widehat{R}^{1/q} \cong \widehat{R^{1/q}} \cong \widehat{R} \otimes_R R^{1/q}$ for all $q = p^e$.*

Proof. $R^{1/q}$ is a local ring module-finite over R. Hence, the maximal ideal of R expands to an ideal primary to the maximal ideal of $R^{1/q}$, and it follows that $\widehat{R^{1/q}}$ is the $mR^{1/q}$-adic completion of $R^{1/q}$. Thus, we have an isomorphism $\alpha : \widehat{R^{1/q}} \cong \widehat{R} \otimes_R R^{1/q}$. Since R is reduced, so is $R^{1/q}$. Since R is F-finite, so is $R^{1/q}$, and $R^{1/q}$ is consequently excellent. Hence, the completion $\widehat{R^{1/q}}$ is reduced. If we use the identification α to write a typical element of $u \in \widehat{R^{1/q}}$ as a sum of terms of the form $s \otimes r^{1/q}$, where $s \in \widehat{R}$ and $r \in R$, we see that $u^q \in \widehat{R}$. This shows that we have $\widehat{R^{1/q}} \subseteq \widehat{R}^{1/q}$. On the other hand, if $r_0, r_1, \ldots, r_k, \ldots$ is a Cauchy sequence in R with limit s, then $r_0^{1/q}, r_1^{1/q}, \cdots, r_k^{1/q}, \cdots$ is a Cauchy sequence in $R^{1/q}$, and its limit is $s^{1/q}$. This shows that $\widehat{R}^{1/q} \subseteq \widehat{R^{1/q}}$. $\square$

From the preceding Theorem we then have:

Corollary. *If R is F-finite, then R is strongly F-regular if and only if every submodule of every module is tightly closed.*

Proof. We need only show that if every submodule of every module is tightly closed, then R is strongly F-regular. We know that both conditions are local on the maximal ideals of R (cf. problem 6. of Problem Set #3). Thus, we may assume that (R, m, K) is local. We know that R has a completely stable big test element c. By part (b) of the Theorem on the first page, $\widehat{R}$ has the property that every submodule of every module is tightly closed: in particular, 0 is tightly closed in $E = E_{\widehat{R}}(K) \cong E_R(K)$. By the equivalence of (2) and (4) in the preceding Theorem, we have that the $\widehat{R}$-linear map $\widehat{\theta} : \widehat{R} \to \widehat{R^{1/q}}$ that sends $1 \mapsto c^{1/q}$ splits for some q. This map arises from the R-linear map $\theta : R \to R^{1/q}$ that sends $1 \mapsto c^{1/q}$ by applying $\widehat{R} \otimes_R \_$. Since $\widehat{R}$ is faithfully flat over R, the map θ is split if and only if $\widehat{\theta}$ is split, and so θ is split as well. $\square$

Finally, we can prove the final statement in the Theorem on p. 4 of the Lecture Notes from October 22.

Corollary. *If R is Gorenstein and F-finite, then R is weakly F-regular if and only if R is strongly F-regular.*

Proof. The issue is local on the maximal ideals of R. We have already shown that in the local Gorenstein case, (R, m, K) is weakly F-regular if and only if 0 is tightly closed in $E_R(K)$. By the Corollary just above, this implies that R is strongly F-regular in the F-finite case. $\square$

This justifies extending the notion of *strongly F-regular* ring as follows: the definition agrees with the one given earlier if the ring is F-finite.

Definition. Let R be a Noetherian ring of prime characteristic $p > 0$. We define R to be *strongly F-regular* if every submodule of every module (whether finitely generated or not) is tightly closed.

Math 711: Lecture of October 29, 2007

We want to study flat local homomorphism $(R, m, K) \to (S, \mathfrak{n}, L)$ to obtain information about S from corresponding information about the base R and the closed fiber S/mS. We recall one fact of this type from p. 3 of the Lecture Notes from September 19:

Proposition. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a flat local homomorphism of local rings. Then*

(a) $\dim(S) = \dim(R) + \dim(S/mS)$*, the sum of the dimensions of the base and of the closed fiber.*

(b) *If R is regular and S/mS is regular, then S is regular.*

Part (a) is generalized in the Theorem given below. We first want to note the following.

Lemma. *Let R a ring, and S a flat R-algebra.*

(a) *If M is a finitely generated R-module, then*

$$\mathrm{Ann}_S(S \otimes_R M) = (\mathrm{Ann}_R M)S \cong S \otimes (\mathrm{Ann}_R M).$$

Hence, if $N, N' \subseteq W$ are R-modules with N' finitely generated, $S \otimes_R N :_S S \otimes_R N' = (N :_R N')S$.

(b) *If I is a finitely generated ideal of R, M is any R-module, and N is a flat R-module, then then*

$$\mathrm{Ann}_{M \otimes_R N} I \cong (\mathrm{Ann}_M I) \otimes_R N.$$

Proof. (a) Let $u_1, \ldots, u_n$ be generators of M. Then there is a map $\alpha : R \to M^n$ that sends $r \mapsto (ru_1, \ldots, ru_n)$. The kernel of this map is evidently $\mathrm{Ann}_R M$, so that

$$0 \to \mathrm{Ann}_R M \to R \xrightarrow{\alpha} M^n$$

is exact. Since S is flat, we may apply $S \otimes_R \_$ to get an exact sequence:

$$(*) \quad 0 \to S \otimes_R (\mathrm{Ann}_R M) \to S \xrightarrow{\beta} (S \otimes_R M)^n$$

where the map $\beta = \mathbf{1}_S \otimes \alpha$ sends $s \in S$ to $s(1 \otimes u_1, \ldots, 1 \otimes u_n)$. Since the elements $1 \otimes u_j$ generate $S \otimes_R M$, the kernel of β is $\mathrm{Ann}_S(S \otimes_R M)$, while the kernel is also $S \otimes_R (\mathrm{Ann}_R M)$ by the exactness of the sequence $(*)$. For the final statement, one may simply observe that $N :_R N' = \mathrm{Ann}_R (N + N')/N$.

(b) Let $f_1, \ldots, f_n$ be generators for I, and consider the map $\gamma : M \to M^n$ such that $u \mapsto (f_1 u, \ldots, f_n u)$. Then

$$0 \to \mathrm{Ann}_M I \to M \xrightarrow{\gamma} M^n$$

is exact. It follows that

$$(**) \quad 0 \longrightarrow (\mathrm{Ann}_M I) \otimes_R N \longrightarrow M \otimes_R N \xrightarrow{\delta} (M \otimes_R N)^n$$

is exact, where $\delta = \gamma \otimes \mathbf{1}_N$ sends $u \otimes v \mapsto (f_1 u \otimes v, \ldots, f_n u \otimes v)$. Therefore the kernel is $\mathrm{Ann}_{M \otimes_R N} I$, but from $(**)$ the kernel is also $(\mathrm{Ann}_M I) \otimes_R N$.

□

Comparison of depths and types for flat local extensions

In the Theorem below, the main case is when $N = S$, and the reader should keep this case in mind. When N is an S-module, we refer to N/mN as the *closed* fiber of N over R. When we refer to the *depth* of a finitely generated nonzero module over a local ring, we always mean the depth on the maximal ideal of the local ring, unless otherwise specified.

Theorem. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a local homomorphism of local rings, and let N be a finitely generated nonzero S-module that is R-flat. Let M be a nonzero finitely generated R-module. Then:*

(a) $\dim(N) = \dim(R) + \dim(N/mN)$.

More generally, $\dim(M \otimes_R N) = \dim(M) + \dim(N/mN)$.

(b) *N is faithfully flat over R.*

(c) *If $y_1, \ldots, y_k \in \mathfrak{n}$ form a regular sequence on the closed fiber N/mN, then they form a regular sequence on $W \otimes_R N$ for every nonzero R-module W. In particular, they form a regular sequence on N/IN for every proper ideal I of R, and on N itself. Moreover, $N/(y_1, \ldots, y_k)N$ is faithfully flat over R.*

(d) $\mathrm{depth}(M \otimes_R N) = \mathrm{depth}(M) + \mathrm{depth}(N/mN)$. *In particular,* $\mathrm{depth}(N) = \mathrm{depth}(R) + \mathrm{depth}(N/mN)$.

(e) *N is Cohen-Macaulay if and only if both R and N/mN are Cohen-Macaulay.*

More generally, if M is any finitely generated R-module, then $M \otimes_R N$ is Cohen-Macaulay if and only if both M and N/mN are Cohen-Macaulay.

(f) *If N is Cohen-Macaulay, then the type of N is the product of the type of R and the type of N/mN. More generally, if $M \otimes_R N$ is Cohen-Macaulay, the type of $M \otimes_R N$ is the product of the type of M and the type of N/mN.*

If M is 0-dimensional and N/mN is 0-dimensional, then the socle of $M \otimes_R N$ is the same as the socle of $\mathrm{Ann}_M m \otimes_K N/mN$.

Proof. We use induction on $\dim(R)$ to prove the first statement. If J is the nilradical of R, we may make a base change and replace R, S, and N by R/J, S/JS, and N/JN. The dimensions of R and N do not change, and the closed fiber does not change. Thus, we may assume that R is reduced. If $\dim(R) = 0$, then R is a field, $m = 0$, and the result is obvious. If $\dim(R) > 0$ then m contains a nonzerodivisor x, which is also a nonzerodivisor on N, because N is R-flat. We may make a base change to R/xR. The dimensions of R and N decrease by one, and the closed fiber does not change. Hence, the validity of the statement in (a) is not affected by this base change. The result now follows from the induction hypothesis.

To prove the second statement, note that M has a finite filtration whose factors are cyclic modules R/I_j, and so $M \otimes_R N$ has a corresponding filtration whose factors are the $(R/I_j) \otimes_R N$. Thus, we can reduce to the case where $M = R/I$. But this case follows from what we have already proved by base change from R to R/I.

(b) To see that a flat module N is faithfully flat over any ring R, it suffices to see that $Q \otimes_R N \neq 0$ for every nonzero R-module Q. If $u \in Q$ is a nonzero element, then $Ru \hookrightarrow Q$, and so it suffices to see that $Ru \otimes_R N \neq 0$ when $Ru \neq 0$. But $Ru \cong R/I$ for some proper ideal I of R, and $Ru \otimes_R M \cong Q/IQ$. Thus, it suffices to see that $IQ \neq Q$ for every proper ideal I of R. Since any proper ideal I is contained in a maximal ideal, it suffices to see that $mQ \neq Q$ when m is maximal in R. In the local case, there is only one maximal ideal to check. In the situation here, $mN \subseteq \mathfrak{n}N \neq N$ by Nakayama's Lemma, since N is finitely generated and nonzero.

(c) By a completely straightforward induction on k, part (c) reduces at once to the case where $k = 1$. (Note that an important element in making this inductive proof work is that we know that N/y_1N is again R-flat.)

Write y for y_1. To see that N/yN is R-flat, it suffices by the local criterion for flatness, p. 1 of the Lecture Notes from October 1, to show that $\mathrm{Tor}^1_R(R/m,\, N/yN) = 0$. The short exact sequence

$$(*) \quad 0 \longrightarrow N \xrightarrow{y\cdot} N \longrightarrow N/yN \longrightarrow 0$$

yields a long exact sequence part of which is

$$0 = \mathrm{Tor}_1^R(R/m,\, N) \longrightarrow \mathrm{Tor}_1^R(R/m,\, N/yN) \longrightarrow N/mN \xrightarrow{y\cdot} N/mN$$

where the 0 on the left is a consequence of the fact that N is R-flat. Since y is not a zerodivisor on N/mN, we have that $\mathrm{Tor}_1^R(R/m,\, N/yN) = 0$. Faithful flatness is then immediate from part (b).

Note that if $M \neq 0$, we have that $M \otimes_R (N/yN) \neq 0$ because N/yN is faithfully flat over R. To show that y is not a zerodivisor on $M \otimes_R N$, we may use the long exact sequence for Tor arising from the short exact sequence $(*)$ displayed above when one applies $M \otimes_R \_$. The desired result follows because $\mathrm{Tor}_1^R(M,\, N/yN) = 0$.

(d) We use induction on $\mathrm{depth}(M) + \mathrm{depth}(N/mN)$. Suppose that both depths are 0. Because $\mathrm{depth}(M) = 0$, m is an associated prime of M, and there is an injection $R/m \hookrightarrow M$. We may apply $\_ \otimes_R N$ to obtain an injection $N/mN \hookrightarrow M \otimes_R N$. Since $\mathrm{depth}(N/mN) = 0$, there is an injection $S/\mathfrak{n} \hookrightarrow N/mN$, and the composite

$$S/\mathfrak{n} \hookrightarrow N/mN \hookrightarrow M \otimes_R N$$

shows that $\operatorname{depth}(M \otimes_R N) = 0$, as required. If $\operatorname{depth}(M) > 0$ we may choose $x \in m$ not a zerodivisor on M. Then x is not a zerodivisor on $M \otimes_R N$ because N is R-flat. We may replace M by M/xM. The depths of M and $M \otimes_R N$ decrease by 1, while the closed fiber does not change. The result now follows from the induction hypothesis. Finally, suppose $\operatorname{depth}(N/mN) > 0$. Choose $y \in \mathfrak{n}$ not a zerodivisor on N/mN. Then we may replace N by N/yN. This module is still flat over R by part (c). The depths of N and N/mN decrease by one, while M is unaffected. Again, the result follows from the induction hypothesis.

(e) $M \otimes_R N$ is Cohen-Macaulay if and only if $\dim(M \otimes_R N) = \operatorname{depth}(M \otimes_R N)$, and by parts (a) and (c), we have that

$$\begin{aligned}\dim(M\otimes_R N)-\operatorname{depth}(M\otimes_R N) &= \dim(M)+\dim(N/mN)-\big(\operatorname{depth}(M)+\operatorname{depth}(N/mN)\big)\\ &= \big(\dim(M)-\operatorname{depth}(M)\big)+\big(\dim(N/mN)-\operatorname{depth}(N/mN)\big).\end{aligned}$$

The last sum is 0 if and only if both summands vanish, since both summands are nonnegative. This proves (e).

(f) Choose a maximal regular sequence $x_1, \ldots, x_h \in m$ on M. This is also a regular sequence on $M \otimes_R N$, and so we may replace M by $M/(x_1, \ldots, x_h)M$. Both types are unaffected by this replacement. Similarly, we may choose $y_1, \ldots, y_k \in \mathfrak{n}$ that form a maximal regular sequence on N/mN, and replace N by $N/(y_1, \ldots, y_k)N$. Hence, we have reduced to the case where M and N/mN both are 0-dimensional.

We next want to establish the final statement, from which the calculation of the type will follow. We have that $\operatorname{Ann}_{\mathfrak{n}}(M \otimes_R N) \subseteq \operatorname{Ann}_m(M \otimes_R N) \cong (\operatorname{Ann}_M m) \otimes_R N$, by part (b) of the Lemma from p. 1. Since m kills the module $\operatorname{Ann}_M m$, this tensor product may be identified with $(\operatorname{Ann}_M m) \otimes_R (N/mN) \cong (\operatorname{Ann}_M m) \otimes_K (N/mN)$. Then $\operatorname{Ann}_M n \cong K^s$ where s is the type of M, and this module is $(N/mN)^{\oplus s}$. Clearly the socle is the direct sum of s copies of the socle in N/mN, whose dimension over L is the type of N/mN, and the statement about the product of the types is immediate. □

Corollary. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a flat local homomorphism of local rings.*

(a) *S is Gorenstein if and only if R and S/mS are both Gorenstein.*

(b) *If I is an irreducible m-primary ideal in R and $y_1, \ldots, y_k \in \mathfrak{n}$ have images that are a system of parameters in S/mS, then for every integer t, $IS + (y_1^t, \ldots, y_k^t)S$ is an irreducible m-primary ideal of S.*

Proof. Part (a) is immediate from parts (e) and (f) of the preceding Theorem, since the type of S is the product of the types of R and S/mS, and so the type of S will be 1 if and only if and only if both R and S/mS are of type 1.

For part (b), make a base change to R/I, which is 0-dimensional Gorenstein ring. Thus, S/IS is Gorenstein, the images of $y_1^k, \ldots, y_t^k$ are a system of parameters and, hence, a maximal a regular sequence. Thus, the quotient of S/I by the ideal they generate is a 0-dimensional Gorenstein ring. □

We can now prove:

Theorem. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a flat local homomorphism of local rings of prime characteristic $p > 0$ such that the closed fiber S/m is regular. Suppose that $c \in R^\circ$ is a test element for both R and S. If R is weakly F-regular, then S is weakly F-regular.*

Proof. It suffices to show that a sequence of irreducible ideals cofinal with the powers of $\mathfrak{n}$ is tightly closed. Since R is weakly F-regular, it is normal, and, hence, approximately Gorenstein. Given t, choose $I \subseteq m^t$ that is m-primary and irreducible. Let $u \in m$ represent a socle generator in R/I. Choose $y_1, \dots, y_k$ whose images in the regular local ring S/mS are a minimal set of generators of the maximal ideal. Then $(y_1 \cdots y_k)^{t-1}$ represents a socle generator in $(S/mS)/(y_1^t, \dots, y_k^t)(S/mS)$. It follows from part (f) of the preceding Theorem that

$$w_t = (y_1 \cdots y_k)^{t-1}u$$

represents a socle generator in

$$S/\big((IS + (y_1^t, \dots, y_k^t)S\big);$$

this ideal is irreducible by the preceding Corollary. Note that $IS + (y_1^t, \dots, y_k^t)S \subseteq \mathfrak{n}^t$. It will therefore suffice to prove that every ideal J of the form $IS + (y_1^t, \dots, y_k^t)S$ is tightly closed, and for this it suffices to check that w_t is not in the tight closure. Since c is a test element for both rings, if w_t were in the tight closure of J we would have

$$c\big((y_1 \cdots y_k)^{t-1}u\big)^q \in I^{[q]}S + (y_1^{qt}, \dots, y_k^{qt})S$$

for all $q \gg 0$. By part (c) of the Theorem on p. 2, $y_1, \dots, y_k$ is regular sequence on $S/I^{[q]}S$. Hence, modulo $I^{[q]}S$, cu^q is in

$$(y_1^{qt}, \dots, y_k^{qt})(S/I^{[q]}S) :_{S/I^{[q]}S} y_1^{tq-q} \cdots y_k^{tq-q} = (y_1^q, \dots, y_k^q)(S/I^{[q]}S),$$

and so

$$cu^q \in I^qS + (y_1^q, \dots, y_k^q)S$$

for all $q \gg 0$. Now work modulo $(y_1^q, \dots, y_k^q)S$ instead. Since $T = S/(y_1^q, \dots, y_k^q)S$ is faithfully flat over R by the part (c) of the Theorem on p. 2, we may think of R as a subring of T. But then we have that $cu^q \in I^{[q]}T \cap R = I^{[q]}$ for all $q \gg 0$, and so $u \in I^*_R = I$, a contradiction, because u represents a socle generator in R/I. $\square$

We next want to prove a corresponding result for strong F-regularity: this works in just the same way, except that we need to assume that c is a big test element. However, the proof involves some understanding of the injective hull of the residue class field of S in this situation.

Math 711: Lecture of October 31, 2007

Discussion: local cohomology. Let $y_1, \ldots, y_d$ be a sequence of elements of a Noetherian ring S and let N be an S-module, which need not be finitely generated. Let J be an ideal whose radical is the same as the radical of $(y_1, \ldots, y_d)S$. Then the dth local cohomology module of N with supports in J, denoted $H^d_J(N)$, may be obtained as

$$\varinjlim_k \frac{N}{(y_1^k, \ldots, y_d^k)N}$$

where the map from

$$N_k = \frac{N}{(y_1^k, \ldots, y_d^k)N}$$

to N_{k+h} is induced by multiplication by z^h, where $z = y_1 \cdots y_d$, on the numerators.. If $u \in N$, $\langle u;\, y_1^k, \ldots, y_d^k\rangle$ denotes the image of the class of u in N_k in $H^d_J(N)$. With this notation, we have that

$$\langle u;\, y_1^k, \ldots, y_d^k\rangle = \langle z^h u;\, y_1^{k+h}, \ldots, y_d^{k+h}\rangle$$

for every $h \in \mathbb{N}$.

If $y_1, \ldots, y_d$ is a regular sequence on N, these maps are injective. We also know from the seminar that if $(S, \mathfrak{n}, L)$ is a Gorenstein local ring and $\underline{y} = y_1, \ldots, y_d$ is a system of parameters for S, then $H^d_{(\underline{y})}(S) = H^d_{\mathfrak{n}}(S)$ is an injective hull for the residue class field $L = S/\mathfrak{n}$ of S over S. In the sequel, we want to prove a relative form of this result when $R \to S$ is a flat local homomorphism whose closed fiber is Gorenstein.

Theorem. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a flat local homomorphism such that the closed fiber S/mS is Gorenstein. Let $\dim(R) = n$ and let $\dim(S/mS) = d$. Let $\underline{y} = y_1, \ldots, y_d \in \mathfrak{n}$ be elements whose images in S/mS are a system of parameters. Let $E = E_R(K)$ be an injective hull for the residue class field $K = R/m$ of R over R. Then $E \otimes_R H^d_{(\underline{y})}(S)$ is an injective hull for $L = S/\mathfrak{n}$ over S.*

In the case where the rings are of prime characteristic $p > 0$,

$$\mathcal{F}^e_S\big(E \otimes_R H^d_{(\underline{y})}(S)\big) \cong \mathcal{F}^e_R(E) \otimes_R H^d_{(\underline{y})}(S),$$

and if $u \in E$ and $s \in S$, then

$$(u \otimes \langle s;\, y_1^k, \ldots, y_d^k\rangle)^q = u^q \otimes \langle s^q;\, y_1^{qk}, \ldots, y_d^{qk}\rangle.$$

Proof. We first give an argument for the case where R is approximately Gorenstein, which is somewhat simpler. We then treat the general case. Suppose that $\{I_t\}$ is a descending sequence of m-primary ideals of R cofinal with the powers of M. We know that $E = \varinjlim_t R/I_t$ for any choice of injective maps $R/I_t \to R/I_{t+1}$. Let $\mathfrak{A}_{t,k} = I_tS + J_k$, where $J_k = (y_1^k, \ldots, y_d^k)S$. For every k we may tensor with the faithfully flat R-algebra S/J_k to obtain an injective map $S/\mathfrak{A}_{t,k} \to S/\mathfrak{A}_{t+1,k}$. Since $y_1, \ldots, y_d$ is a regular sequence on S/I_tS for every I_t, we also have an injective map $S/\mathfrak{A}_{t,k} \to S/\mathfrak{A}_{t,k+1}$ induced by multiplication by $z = y_1 \cdots y_d$ on the numerators. The ideals $\mathfrak{A}_{t,k}$ are $\mathfrak{n}$-prinary irreducible ideals and as t, k both become large, are contained in aribtrarily large powers of $\mathfrak{n}$. (Once $I_t \subseteq m^s$ and $k \geq s$, we have that $\mathfrak{A}_{t,\,k} \subseteq m^sS + \mathfrak{n}^s \subseteq \mathfrak{n}^s$.) Thus, we have

$$E_S(L) \cong \varinjlim_{t,k} \frac{S}{\mathfrak{A}_{t,k}} = \varinjlim_{t,k} \left(\frac{R}{I_t} \otimes_R \frac{S}{J_k}\right) \cong \varinjlim_k \left(\varinjlim_t \Big(\frac{R}{I_t} \otimes_R \frac{S}{J_k}\Big)\right) \cong$$

$$\varinjlim_k \left(\Big(\varinjlim_t \frac{R}{I_t}\Big) \otimes_R \frac{S}{J_k}\right) \cong \varinjlim_k \left(E \otimes_R \frac{S}{J_k}\right) \cong E \otimes_R \left(\varinjlim_k \frac{S}{J_t}\right) \cong E \otimes_R H^d_{(\underline{y})}(S).$$

We now give an alternative argument that works more generally. In particular, we do not assume that R is approximately Gorenstein. Let E_t denote $\mathrm{Ann}_E m^t$. We first claim that that $E_{t,k}$, which we define as $E_t \otimes_R (S/J_k)$, is an injective hull of L over $S_{t,k} = (R/m^t) \otimes_R (S/J_k)$. By part (f) of the Theorem on p. 2 of the Lecture Notes from October 29, it is Cohen-Macaulay of type 1, since that is true for E_t and for the closed fiber of S/J_k, since S/mS is Gorenstein. Hence, $E_{t,k}$ is an essential extension of L, and it is killed by $\mathfrak{A}_{t,k} = m^tS + J_k$. To complete the proof, it suffices to show that it has the same length as $S_{t,k}$. Let M denote either R/m^t or E_t. Note that M has a filtration with $\ell(M)$ factors, each of which is $\cong K = R/m$. Since S/J_k is R-flat, this gives a filtration of $M \otimes_R S/J_k$ with $\ell(M)$ factors each of which is isomorphic with $K \otimes_R S/J_k = S/(mS + J_k)$. Since $\ell(R/m^t) = \ell(E_t)$, it follows that $S_{t,k}$ and $E_{t,k}$ have the same length, as required.

If $t \leq t'$ we have an inclusion $E_t \hookrightarrow E_{t'}$, and if $k \leq k'$, we have an injection $S/J_k \to S/J_{k'}$ induced by multplication by $z^{k'-k}$ acting on the numerators. This gives injections $E_t \otimes_R S_k \to E_{t'} \otimes S_k$ (since S_k is R-flat) and $E_{t'} \otimes_R S_k \to E_{t'} \otimes_R S'_k$ (since $y_1, \ldots, y_d$ is a regular sequence on $E_{t'} \otimes_R S$). The composites give injections $E_{t,k} \hookrightarrow E_{t',k'}$ and the direct limit over t, k is evidently $E \otimes_K H^d_{(\underline{y})}(S)$. The resulting module is clearly an essential extension of L, since it is a directed union of essential extensions. Hence, it is contained in a maximal essential extension $E_S(L)$ of L over S. We claim that this inclusion is an equality. To see this, suppose that $u \in E_S(L)$ is any element. Then u is killed by $\mathfrak{A} = \mathfrak{A}_{t,k} = m^tS + J_k$ for any sufficiently large choices of t and k. Hence $u \in \mathrm{Ann}_{E_S(L)}\mathfrak{A} = N$, which we know is an injective hull for L over $S/\mathfrak{A}$. But $E_t \otimes_R S/J_k$ is a submodule of N contained in $E \otimes_R H^d_{(\underline{y})}(S)$, and is already an injective hull for L over $S/\mathfrak{A}$. It follows, since they have the same length, that we must have that $E_t \otimes_R S/J_k \subseteq N$ is all of N, and so $u \in E_t \otimes_R S/J_k \subseteq E \otimes_R H^d_{(\underline{y})}(S)$.

To prove the final statement about the Frobenius functor, we note that by the first problem of Problem Set #4, one need only calculate $\mathcal{F}^e_S\big(H^d_{(\underline{y})}(S)\big)$, and this calculation is the precisely the same as in third paragraph of p. 1 of the Lecture Notes from October 24. $\square$

We are now ready to prove the analogue for strong F-regularity of the Theorem at the top of p. 5 of the Lecture Notes from October 29, which treated the weakly F-regular case.

Theorem. *Let $(R, m, K) \to (S, \mathfrak{n}, L)$ be a local homomorphism of local rings of prime characteristic $p > 0$ such that the closed fiber S/m is regular. Suppose that $c \in R^\circ$ is a big test element for both R and S. If R is strongly F-regular, then S is strongly F-regular.*

Proof. Let u be a socle generator in $E = E_R(K)$, and let $\underline{y} = y_1, \ldots, y_d \in \mathfrak{n}$ be elements whose images in the closed fiber S/mS form a minimal set of generators of the maximal ideal $\mathfrak{n}/mS$. Let $z = y_1 \cdots y_d$. Then the image of 1 in $S/\bigl(mS + (y_1, \ldots, y_d)S\bigr)$ is a socle generator, and it follows that $v = u \otimes \langle 1; y_1, \ldots, y_d\rangle$ generates the socle in $E_S(L) \cong E \otimes_R H^d_{(\underline{y})}(S)$. Since c is a big test element for S, it can be used to test whether v is in the tight closure of 0 in $E \otimes_R H^d_{(\underline{y})}(S)$.

This occurs if and only if for all $q \gg 0$, $c(u \otimes \langle 1; y_1, \ldots, y_d\rangle)^q = 0$ in $\mathcal{F}^e_R(E) \otimes_R H^d_{(\underline{y})}(S)$, and this means that $cu^q \otimes \langle 1; y_1^q, \ldots, y_d^q\rangle = 0$ in $\mathcal{F}^e_R(E) \otimes_R H^d_{(\underline{y})}(S)$. By part (c) of the Theorem on p. 2 of the Lecture Notes from October 29, $y_1, \ldots, y_d$ is a regular sequence on $E \otimes_R S$, from which it follows that the module $\mathcal{F}^e_R(E) \otimes_R \bigl(S/(y_1^q, \ldots, y_d^q)\bigr)$ injects into $\mathcal{F}^e_R(E) \otimes_R H^d_{(\underline{y})}(S)$. Since $\overline{S} = S/(y_1^q, \ldots, y_d^q)S$ is faithfully flat over R, the map $\mathcal{F}^e_R(E) \to \mathcal{F}^e_R(E) \otimes_R S/(y_1^q, \ldots, y_d^q)S$ sending $w \mapsto w \otimes 1$ is injective. The fact that $cu^q \otimes \langle 1; y_1^q, \ldots, y_d^q\rangle = 0$ implies that $cu^q \otimes 1_{\overline{S}}$ is 0 in $\mathcal{F}^e_R(E) \otimes_R \overline{S}$, and hence that $cu^q = 0$ in R. Since this holds for all $q \gg 0$, we have that $u \in 0^*_E$, a contradiction. □

The following result will be useful in studying algebras essentially of finite type over an excellent semilocal ring that are not F-finite but are strongly F-regular: in many instances, it permits reductions to the F-finite case.

Theorem. *Let R be a reduced Noetherian ring of prime characteristic $p > 0$ that is essentially of finite type over an excellent semilocal ring B.*

(a) *Let $\widehat{B}$ denote the completion of B with respect to its Jacobson radical. Suppose that R is strongly F-regular. Then $\widehat{B} \otimes_B R$ is essentially of finite type over $\widehat{B}$ and is strongly F-regular and faithfully flat over R.*

(b) *Suppose that $B = A$ is a complete local ring with coefficient field K. Fix a p-base Λ for K. For all $\Gamma \ll \Lambda$, let $R^\Gamma = A^\Gamma \otimes_A R$. We nay identify* $\mathrm{Spec}\,(R^\Gamma)$ *with $X =$* $\mathrm{Spec}\,(R)$ *as topological spaces, and we let Z_Γ denote the closed set in* $\mathrm{Spec}\,(R)$ *of points corresponding to primes P such that R^Γ_P is not strongly F-regular. Then Z_Γ is the same for all sufficiently small $\Gamma \ll \Lambda$, and this closed set is the locus in X consisting of primes P such that R_P is not strongly F-regular.*

   In particular, if R is strongly F-regular, then for all $\Gamma \ll \Lambda$, R^Γ is strongly F-regular.

Proof. (a) Since $B \to \widehat{B}$ is faithfully flat with geometrically regular fibers, the same is true for $R \to \widehat{B} \otimes_B R$. Choose $c \in R^\circ$ such that R_c is regular. Then we also have that

$(\widehat{B} \otimes_B R)_c$ is regular. Hence, c has a power that is a completely stable big test element in both rings. Let Q be any prime ideal of $S = \widehat{B} \otimes_B R$ and let P be its contraction to R. We may apply the preceding Theorem to the map $R_P \to S_Q$, and so S_Q is strongly F-regular for all Q. It follows that S is strongly F-regular.

(b) For all choices of $\Gamma' \subseteq \Gamma$ cofinite in Λ, we have that $R \subseteq R^{\Gamma'} \subseteq R^{\Gamma}$, and that the maps are faithfully flat and purely inseparable. Since every R^{Γ} is F-finite, we know that every Z_Γ is closed. Since the map $R^{\Gamma'} \subseteq R^{\Gamma}$ is faithfully flat, Z_Γ decreases as Γ decreases. We may choose Γ so that $Z = Z_\Gamma$ is minimal, and, hence, minimum, since a finite intersection of cofinite subsets of Λ is cofinite.

We shall show that Z must be the set of primes P in $\mathrm{Spec}\,(R)$ such that R_P is strongly F-regular. If Q is a prime of R^{Γ} not in Z_Γ lying over P in R, the fact that $R_P \to R^{\Gamma}_Q$ is faithfully flat implies that P is not in Z. Thus, $Z \subseteq Z_\Gamma$. If they are not equal, then there is a prime P of R such that R_P is strongly F-regular but R^{Γ}_Q is not strongly F-regular, where Q is the prime of R^{Γ} corresponding to P. Choose $\Gamma' \subseteq \Gamma$ such that $Q' = PR^{\Gamma'}$ is prime. It will suffice to prove that $S = R^{\Gamma'}_{Q'}$ is strongly F-regular, for this shows that $Z_{\Gamma'} \subseteq Z_\Gamma - \{P\}$ is strictly smaller than Z_Γ. Since S is F-finite, we may choose a big test element c_1 for S. Then c_1 has a q_1 th power c in R_P for some q_1, and c is still a big test element for S. The closed fiber of $R_P \to S$ is $S/PS = S/Q'$, a field. Hence, by the preceding Theorem, S is strongly F-regular. $\square$

Using this result, we can now prove:

Theorem. *Let R be reduced and essentially of finite type over an excellent semilocal ring B. Then the strongly F-regular locus in R is Zariski open.*

Proof. We first consider the case where $B = A$ is a complete local ring. Choose a coefficient field K for A and a p-base Λ for it. Then the result is immediate from part (b) of the preceding Theorem by comparison with R^{Γ} for any $\Gamma \ll \Lambda$.

In the general case, let $S = \widehat{B} \otimes_B R$. Since $\widehat{B}$ is a finite product of complete local rings, S is a finite product of algebras essentially of finite type over a complete local ring, and so the non-strongly F-regular locus is closed. Let J denote an ideal of S that defines this locus.

Now consider any prime ideal P of R such that R_P is strongly F-regular. Let $W = R - P$. Then we may apply part (a) of the preceding Theorem to $R_P \to \widehat{B} \otimes_B R_P$ to conclude that $\widehat{B} \otimes_R R_P = W^{-1}S$ is strongly F-regular. It follows that W must meet J: otherwise, we can choose a prime Q of S containing J but disjoint from W, and it would follow that S_Q is strongly F-regular even though $J \subseteq Q$, a contradiction. Choose $c \in W \cap J$. Then S_c is strongly F-regular, and since $R_c \to S_c$ is faithfully flat, so is R_c. Thus, the set of primes of R not containing c is a Zariski open nieghborhood of P that is contained in the strongly F-regular locus. $\square$

Math 711: Lecture of November 5, 2007

The following result is one we have already established in the F-finite case. We can now extend it to include rings essentially of finite type over an excellent semilocal ring.

Theorem. *Let R be a reduced ring of prime characteristic $p > 0$ essentially of finite type over an excellent semilocal ring B. Suppose that $c \in R^\circ$ is such that R_c is strongly F-regular. Then c has a power that is a completely stable big test element in R.*

Proof. If c is a completely stable big test element in a faithfully flat extension of R, then that is also true for R by part (b) of the Proposition at the bottom of p. 8 of the Lecture Notes from September 17.

The hypothesis continues to hold if we replace R by $\widehat{B} \otimes_B R$, and it holds in each factor of this ring. We may therefore assume that R is essentially of finite type over a complete local ring A. As usual, choose a coefficient field K for A and a p-base Λ for K. Again, the hypotheis continues to hold is we replace R by R^Γ for $\Gamma \ll \Lambda$, and R^Γ is faithfully flat over R. But now we are done, since R^Γ is F-finite. $\square$

We next want to backtrack and prove that certain rings are approximately Gorenstein in a much simpler way than in the lengthy and convoluted argument given in the Lecture Notes from October 24. While the result we prove is much weaker, it does suffice for the case of an excellent normal Cohen-Macaulay ring, and, hence, for excellent weakly F-regular rings.

We first note:

Lemma. *Let M and N be modules over a Noetherian ring R and let x be a nonzerodivisor on N. Suppose that M is R-free or, much more generally, that $\mathrm{Ext}^1_R(M, N) = 0$. Then*

$$(R/xR) \otimes_R \mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{R/xR}(M/xM, N/xN).$$

Proof. The right hand module is evidently the same as $\mathrm{Hom}_R(M/xM, N/xN)$, and also the same as $\mathrm{Hom}_R(M, N/xN)$, since any map $M \to N/xN$ must kill xM. Apply $\mathrm{Hom}_R(M, \_\,)$ to the short exact sequence

$$0 \to N \xrightarrow{x\cdot} N \to N/xN \to 0.$$

This yields a long exact sequence which is, in part,

$$0 \to \mathrm{Hom}_R(M, N) \xrightarrow{x\cdot} \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N/xN) \to \mathrm{Ext}^1_R(M, N) = 0,$$

and the result follows. $\square$

Theorem. *Let (R, m, K) be an excellent, normal, Cohen-Macaulay ring, or, more generally, any Cohen-Macaulay local ring whose completion is a Cohen-Macaulay local domain. Then R is approximately Gorenstein.*

Proof. We may replace R by its completion and then R is module-finite over a regular local ring $A \subseteq R$. Because R is Cohen-Macaulay, it is free of some rank h as an A-module, i.e., $R \cong A^h$. Then $\omega = \mathrm{Hom}_A(R, A)$ is also an R-module, and is also isomorphic to A^h as an A-module. (We shall see later that ω is what is called a *canonical module* for R. Up to isomorphism, it is independent of the choice of A.) Then ω is, evidently, also a Cohen-Macaulay module over R. We want to see that it has type one. This only uses the Cohen-Macaulay property of R: it does not use the fact that R is a domain.

From the Lemma above, we see that the calculation of ω commutes with killing a parameter in A. We may choose a system of parameters for A (and R) that is a minimal set of generators for the maximal ideal of A. By killing these one at a time, we reduce to seeing this when $A = K$ is a field and R is a zero-dimensional local ring with coefficient field K. We claim that in this case, $\omega = \mathrm{Hom}_K(R, K)$ is isomorphic with $E_R(K)$. In fact, ω is injective because for any R-module M,

$$\mathrm{Hom}_R(M, \omega) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_K(R, K)) \cong \mathrm{Hom}_K(M \otimes_R R, K) \cong \mathrm{Hom}_K(M, K)$$

by the adjointness of tensor and Hom. This is, in fact, a natural isomorphism of functors. Since $\mathrm{Hom}_K(\_, K)$ is exact, so is $\mathrm{Hom}_R(\_, \omega)$. Thus, ω is a direct sum of copies of $E_R(K)$. But its length is the same as its dimension as a K-vector space, and this is the same as the dimension of R as a K-vector space, which is the length of R. Thus, ω has the same length as $E_R(K)$, and it follows that $\omega \cong E_R(K)$.

We now return to the situation where R is a domain. Since every nonzero element of R has a nonzero multiple in A, we have that ω is torsion-free as an R-module. Thus, if w is any nonzero element of ω, we have an embedding $R \to \omega$ sending $1 \mapsto w$. Let $I_t = (x_1^t, \ldots, x_n^t)$, where $x_1, \ldots, x_n$ is a system of parameters for R. Then $I_t\omega \cap Rw$ must have the form $J_t w$ for some m-primary ideal J_t of R. Then

$$R/J_t \cong Rw/(I_t\omega \cap Rw) \subseteq \omega/I_t\omega.$$

Since $\omega/I_t\omega$ is an injective hull of the residue class field for R/I_t, it is an essential extension of its socle. Therefore, R/J_t is an essential extension of its socle as well. Consequently, $J_t \subseteq R$ is irreducible and m-primary. It will now suffice to show that the ideals J_t are cofinal with the powers of m.

By the Artin-Rees Lemma there exists a constant integer $a \in \mathbb{N}$ such that

$$m^{N+a}\omega \cap Rw \subseteq m^N(Rw) = m^N w$$

for all N. But then $J_{N+a} \subseteq m^n$, since $I_{N+a} \subseteq m^{N+a}$. $\square$

We next want to prove some additional results on openness of loci, such as the Cohen-Macaulay locus. The following fact is very useful.

Lemma on openness of loci. *Let $X = \mathrm{Spec}\,(R)$, where R is a Noetherian ring. Then $S \subseteq X$ is open if and only if the following two conditions hold:*

(1) *If $P \subseteq Q$ and $Q \in S$ then $P \in S$.*

(2) *For all $P \in S$, $S \cap \mathcal{V}(P)$ is open in $\mathcal{V}(P)$.*

The second condition can be weakened to:

(2°) *For all $P \in S$, S contains an open neighborhood of P in $\mathcal{V}(P)$.*

Proof. It is clear that (1), (2), and (2°) are necessary for S to be open. Since (2°) is weaker than (2), and it suffices to show that (1) and (2°) imply that S is open. Suppose otherwise. Since R has DCC on prime ideals, if S is not open there exists a minimal element P of S that has no open neighborhood entirely contained in S. For all primes Q strictly contained in P, choose an open neighborhood U_Q of Q contained entirely in S. Let U be the union of these open sets: the U is an open set contained entirely in S, and contains all primes Q strictly smaller than P.

Let $Z = X - U$, which is closed. It follows that Z has finitely many minimal elements, one of which must be P. Call them $P = P_0,\, P_1,\, \ldots\,, P_k$. Then

$$Z = \mathcal{V}(P_0) \cup \cdots \mathcal{V}(P_k).$$

Finally, choose U' open in X such that $P \in U'$ and $U' \cap \mathcal{V}(P) \subseteq S$. We claim that

$$U'' = U \cup U' - \big(\mathcal{V}(P_1) \cup \cdots \cup \mathcal{V}(P_k)\big)$$

is the required neighborhood of P. It is evidently an open set that contains P. Suppose that $Q \in U''$. If $Q \in U$ then $Q \in S$. Otherwise, Q is in

$$X - U = \mathcal{V}(P) \cup \mathcal{V}(P_1) \cup \cdots \cup \mathcal{V}(P_k),$$

and this implies that $Q \in \mathcal{V}(P)$. But Q must also be in U', and $U' \cap \mathcal{V}(P) \subseteq S$. $\square$

We can use this to show:

Theorem. *Let R be an excellent ring. Then the Cohen-Macaulay locus*

$$\{P \in \mathrm{Spec}\,(R) : R_P \text{ is Cohen-Macaulay}\}$$

is Zariski open.

Proof. It suffices to estabish (1) and (2) of the preceding Lemma. We know (1) because if $P \subseteq Q$ then R_P is a localization of the Cohen-Macaulay ring R_Q. Now suppose that R_P is Cohen-Macaulay. Choose a maximal regular sequence in PR_P. After multiplying by suitable units in R_P, we may assume that this regular sequence consists of images of elements $x_1,\, \ldots\,, x_d \in P$. We can choose $c_i \in R - P$ that kills the annihilator of x_{i+1} in

$R/(x_1, \dots, x_i)$, $0 \le i \le d-1$. Let c be the product of the c_i. Then we may replace R by R_c (we may make finitely many such replacements, each of which amounts to taking a smaller Zariski open neighborhood of P).

Then $x_1, \dots, x_d$ is a regular sequence in P, and is therefore a regular sequence in Q and in QR_Q for all primes $Q \supseteq P$. Hence, in considering property (2), it suffices to work with $R_1 = R/(x_1, \dots, x_d)R$: whether R_Q is Cohen-Macaulay or not is not affected by killing a regular sequence. Consequently, we need only show that if P is a minimal prime of an excellent ring R, then there exists $c \notin P$ such that R_c is Cohen-Macaulay. We may assume by localizing at one element in the other minimal primes but not in P that P is the only minimal prime of R.

First, we may localize at one element $c \notin P$ such that $(R/P)_c$ is a regular domain, because R/P is an excellent domain: the localization at the prime ideal (0) is a field, and, hence, regular, and so (0) has a Zariski open neighborhood that is regular. Henceforth, we assume that R/P is regular. It would suffice in the argument that follows to know that it is Cohen-Macaulay.

Finally, choose a filtration $P = P_1 \supseteq \cdots \supseteq P_n = (0)$ such that every P_i/P_{i+1} is killed by P. We can do this because P is nilpotent. (If $P^n = 0$, we may take $P_i = P^i$, $1 \le i \le n$. Alternatively, we may take $P_i = \mathrm{Ann}_P P^{n-i}$.) Second, we can localize at one element $c \in R - P$ such that each of the (R/P)-modules P_i/P_{i+1}, $1 \le i \le n-1$, is free over R/P. Here, we are writing R for the localized ring. We claim that the ring R is now Cohen-Macaulay.

To see this, suppose that we take any local ring of R. Then we may assume that (R, m, K) is local with unique minimal prime P, that R/P is Cohen-Macaulay, and that P has a finite filtration whose factors are free (R/P)-modules: all this is preserved by localization. Let $x_1, \dots, x_h$ be a system of parameters for R. The images of these elements form a system of parameters in R/P. Then $x_1, \dots, x_d$ is a regular sequence on R/P. But P has a finite filtration in which the factors are free (R/P)-modules, and so does R: one additional factor, R/P, is needed. Since $x_1, \dots, x_d$ is a regular sequence on every factor of this filtration, by the Proposition near the bottom of the first page of the Lecture Notes from October 8, it is a regular sequence on R. Hence, R is Cohen-Macaulay. $\square$

Remark. It is also true that if M is a finitely generated module over an excellent ring R, then

$$\{P \in \mathrm{Spec}\,(R) : M_P \text{ is Cohen-Macaulay}\}$$

is Zariski open in $\mathrm{Spec}\,(R)$. This comes down to establishing property (2), and we may make the same initial reduction as in the ring case, killing a regular sequence in P on M whose image in PR_P is a maximal regular sequence on M_P. Therefore may assume that P is minimal in the support of M, and, after one further localization, that P is the only minimal prime in the support of M. We may assume as above that R/P is regular: again R

is Cohen-Macaulay suffices for the argument. We have $P^n M = 0$ for some n, and we may construct a filtration $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = 0$ such that evey M_i/M_{i+1} is killed by P. We may then localize once more such that every M_i/M_{i+1} becomes (R/P)-free over the localization. The rest of the argument is the same as in the case where $M = R$. □

There are several ways to prove that the type of a Cohen-Macaulay module cannot increase when one localizes. In particular, a Gorenstein ring remains Gorenstein when one localizes. One way is to make use of canonical modules. Here, we give a proof that is, in some sense, more elementary. Part of the argument is left as an exercise.

Theorem. *Let M be a module over a local ring (R, m, K), and let P be any prime of R. Then the type of M_P is at most the type of M.*

Proof. We shall reduce to the case where R is a complete local domain of dimension one, M is a finitely generated torsion-free module, and $P = (0)$, so that the type of M_P is its dimension as a vector space over $\operatorname{frac}(R)$. We leave this case as an exercise: see Problem 5 of Problem Set #4.

Let S be the completion of R, and let Q be a minimal prime of PS, which will lie over P. The closed fiber of $R_P \to S_Q$ is 0-dimensional because Q is minimal over PS, and so $M_P \otimes_{R_P} S_Q$ is Cohen-Macaulay and its type is the product of the type of M_P and the type of S_Q/PS_Q. This shows that the type of M_P is at most the type of $M_P \otimes_{R_P} S_Q \cong M \otimes_R S_Q = (\widehat{M})_Q$. Since M and $\widehat{M}$ have the same type, it will suffice to show that type can not increase under localization in the complete case.

Second, we can choose a saturated chain of primes joining P to Q, and successively localize at each in turn. Thus, we can also reduce to the case where $\dim(R/Q) = 1$. Third, we can choose a maximal regular sequence on M in Q, and replace M by its quotient by this sequence. Thus, there is no loss of generality in assuming the Q is minimal in the support of M. We may also replace R by $R/\mathrm{Ann}_R M$ and so assume that M is fatihful. Let $N = \mathrm{Ann}_M Q$. Let x be a system of parameters for R: it only has one element. In particular, $x \notin Q$. Then x is not a zerodivisor on M, since M is Cohen-Macaulay, nor on N, since $N \subseteq M$. But x is also is not a zerodivisor on M/N, for if $xu \in N$, then $xuQ = 0$, which implies that $uQ = 0$, and so $u \in N$. It follows that when we apply $(R/xR) \otimes_R \_$ to the short exact sequence

$$0 \to N \to M \to M/N \to 0$$

we get an exact sequence. Hence, $N/xN \to M/xM$ is injective, which shows that the type of N is at most the type of M. However, $N_Q \subseteq M_Q$ is evidently the socle in M_Q, and so the type of M_Q is the same as the type of N_Q. It follows that is suffices to show that the type of N_Q is at most the type of N. Here, N is a torsion-free module over R/Q, and so we have reduced to the case described in the first paragraph. □

Math 711: Lecture of November 7, 2007

Our current theory of test elements permits the extension of many results proved under other hypotheses, such as the condition that the ring under consideration be a homomorphic image of a Cohen-Macaulay ring, to the case of excellent local rings or, more generally, rings for which we have completely stable test elements (or completely stable big test elements, depending on whether the result being proved is for finitely generated modules or for arbitrary modules).

Here is one example:

Theorem (colon-capturing). *Let $(R,\, m,\, K)$ be an excellent reduced equidimensional local ring of prime characteristic $p > 0$, and let $x_1, \, \ldots \, , x_{k+1}$ be part of a system of parameters. Let $I_k = (x_1, \, \ldots \, , x_k)R$. Then $I_k^* :_R x_{k+1} = I_k^*$. In particular, $I_k :_R x_{k+1} \subseteq I_k^*$.*

Proof. Note that R has a completely stable test element c. Suppose that $ux_{k+1} \in I_k$ but $u \in R - I_k$. This is also true when we pass to $\widehat{R}$, which is a homomorphic image of a regular ring and, hence, of a Cohen-Macaulay ring. Therefore, from the result on colon-capturing from p. 9 of the Lecture Notes from October 5, we have that $u \in (I_k\widehat{R})^*$, whence $cu^q \in (I\widehat{R})^{[q]} = I^{[q]}\widehat{R}$ for all q, and it follows that $cu^q \in I^{[q]}\widehat{R} \cap R = I^{[q]}$ for all q. Thus, $u \in I^*$.

Now suppose that $ux_{k+1} \in I_k^*$. Then $u^q x_{k+1}^q \in (I_k^*)^{[q]} \subseteq (I_k^{[q]})^*$ for all q, and so $cu^q x_{k+1}^q \in I_k^{[q]}$ for all q, and $cu^q \in I_k^{[q]} :_R x_{k+1}^q \subseteq (I_k^{[q]})^*$ by the result of the first paragraph applied to $x_1^q, \, \ldots \, , x_{k+1}^q$. Hence, $c^2u^q \in (I_k)^{[q]}$ for all q, so $u \in I_k^*$. The opposite conclusion is obvious. □

A Noetherian ring is called *locally excellent* if its localization at every maximal ideal (equivalently, at every prime ideal) is excellent.

Corollary. *If R is weakly F-regular and locally excellent, then R is Cohen-Macaulay.*

Proof. Both weak F-regularity and the Cohen-Macaulay property are local on the maximal ideals of R. Hence, we may assume that R is local. Since weakly F-regular rings are normal, R is certainly equidimensional. Since colon-capturing holds for systems of parameters in R, the result is immediate. □

We can also prove a global version of this Theorem above that is valid even in case the ring is not equidimensional. We need one additional fact.

Lemma. *Let $(R,\, m,\, K)$ be an excellent local ring and let I be an ideal of R that has height at least k modulo every minimal prime of R. Then $I\widehat{R}$ has height at least k modulo every minimal prime of $\widehat{R}$.*

Proof. If $\mathfrak{p}_i$ is a minimal prime of R, $\mathfrak{p}_i\widehat{R}$ is a radical ideal and is the intersection of certain minimal primes $\mathfrak{q}_{ij}$. The intersection of all $\mathfrak{q}_{ij}$ is the same as the intersection of the $\mathfrak{p}_i\widehat{R}$. Since finite intersection commutes with flat base change, this is 0. Thus, it will suffice to show that the height of I is at least k modulo every $\mathfrak{q}_{ij}$. To this end, we can replace R by $R/\mathfrak{p}_i$. Thus, it is enough to show the result when R is an excellent local domain. In this case, $\widehat{R}$ is reduced and equidimensional. Any prime Q of $\widehat{R}$ containing $I\widehat{R}$ lies over a prime P of R containing I. The height of Q is at least the height of Q_0 where Q_0 is a minimal prime of $P\widehat{R}$. Hence, it suffices to show that if Q is a minimal prime of $P\widehat{R}$ then height $(Q) =$ height (P). Since R and $\widehat{R}$ are equidimensional and catenary,

$$\text{height}\, P = \dim(R) - \dim(R/P) = \dim(\widehat{R}) - \dim(\widehat{R}/P\widehat{R}).$$

Since the completion of R/P is equidimensional,

$$\dim(\widehat{R}/P\widehat{R}) = \dim\big(\widehat{R}/Q\big).$$

Hence,

$$\text{height}\,(P) = \dim(\widehat{R}) - \dim\big(\widehat{R}/Q\big) = \text{height}\,(Q),$$

as required. □

Theorem (colon-capturing). *Let R be a reduced Noetherian ring of prime characteristic $p > 0$ that is locally excellent and has a completely stable test element c . This holds, for example, if R is reduced and essentially of finite type over an excellent semilocal ring. Let $x_1, \dots, x_{k+1}$ be elements of R. Let I_t denote the ideal $(x_1, \dots, x_t)R$, $0 \le t \le k+1$. Suppose that the image of the ideal I_k has height k modulo every minimal prime of R, and that the image of the ideal $I_{k+1}R$ has height $k+1$ modulo every minimal prime of R. Then $I_k^* :_R x_{k+1} = I_k^*$.*

Proof. We first prove that $I_k :_R x_{k+1} \subseteq I_k^*$. The stronger conclusion then follows exactly as in the Theorem above because c is a test element.

If $x_{k+1}u \in I_k$ but $u \notin I_k^*$, we can choose q so that $cu^q \notin I_k^{[q]}$. This is preserved when we localize at a maximal ideal in the support of $(I_k^{[q]} + cu^q)/I_k^{[q]}$. We have therefore reduced to the case of an excellent local ring R_m. By the Lemma above, the hypotheses are preserved after completion, and we still have $cu^q \notin I_k^{[q]}S = (I_kS)^{[q]}$, where S is the completion of R_m. Since c is a test element in S, we have that $u \notin (I_kS)^*$. Since S is a homomorphic image of a Cohen-Macaulay ring, this contradicts the Theorem on colon-capturing from p. 9 of the Lecture Notes from October 5. □

We next want to use the theory of test elements to prove results on persistence of tight closure.

Persistence

Let $\mathcal{R}$ (respectively, $\mathcal{R}_{\text{big}}$) denote the class of Noetherian rings S such that for every domain $R = S/P$, the normalization R' of R is module-finite over R and has the following two properties:

(1) The singular locus in R' is closed.

(2) For every element $c \in R' - \{0\}$ such that R'_c is regular, c has a power that is a test element (respectively, a big test element) in R'.

Of course, $\mathcal{R}_{\text{big}} \subseteq \mathcal{R}$, and $\mathcal{R}_{\text{big}}$ includes both the class of F-finite rings and the class of rings essentially of finite type over an excellent semilocal ring.

Theorem (persistence of tight closure). *Let R be in $\mathcal{R}$ (respectively,in $\mathcal{R}_{\text{big}}$). Let $R \to S$ be a homomorphism of Noetherian rings and suppose that $N \subseteq M$ are finitely generated (respectively, arbitrary) R-modules. Let $u \in N^*_M$. Then $1 \otimes u \in \langle S \otimes_R N\rangle^*_{S\otimes_R M}$.*

Proof. It suffices to prove the result after passing to $S/\mathfrak{q}_j$ as $\mathfrak{q}_j$ runs through the minimal primes of S. Therefore, we may assume that S is a domain. Let P denote the kernel of $R \to S$. Then P contains a minimal prime $\mathfrak{p}$ of R. Tight closure persists when we kill $\mathfrak{p}$ because the element c used in the tight closure test is not in $\mathfrak{p}$. Hence, we may make a base change to $R/\mathfrak{p}$, and so we may assume that $R \to S$ is a map of domains with kernel P. It suffices to prove that tight closure is preserved when we pass from R to R/P, since the injective map of domains $R/P \hookrightarrow S$ always preserves tight closure. Henceforth we may assume that S has the form R/P.

Choose a saturated chain of primes

$$(0) = P_0 \subseteq P_1 \subseteq \cdots \subseteq P_h = P.$$

Then it suffices to show that tight closure persists as we make successive base changes to R/P_1, then to R/P_2, and so forth, until we reach $R/P_h = R/P$. Therefore, we need only prove the result when $S = R/P$ and P has height one.

Let R' be the normalization of R and let Q be a prime of R' lying over P. We have a commutative diagram

$$\begin{array}{ccc} R/P & \longrightarrow & R'/Q \\ \uparrow & & \uparrow \\ R & \longrightarrow & R' \end{array}$$

where the horizontal arrows are module-finite extensions and the vertical arrows are quotient maps. Tight closure is preserved by the base change from R to R' because it is an inclusion of domains. If R' is regular, then the element is in the image of the submodule, and this is preserved when we pass to R'/Q. If not, because R' is normal, the defining ideal of the singular locus has depth at least two, and we can find a regular sequence b, c in R' such that R'_b and R'_c are both regular. Then b and c are not both in Q, and hence at least one of them has nonzero image in R/Q: say that c has nonzero image. For some s, c^s is a test element (respectively, big test element) in R, and it has nonzero image in R'/Q. It follows that the base change $R' \to R'/Q$ preserves tight closure, and, hence, so does the composite base change $R \to R'/Q$.

Now suppose that the base change $R \to R/P$ fails to preserve tight closure. By the argument above, the further base change $R/P \hookrightarrow R'/Q$ restores the image of the element to the tight closure. This contradicts the fourth problem in Problem Set #4. Hence, $R \to R/P$ preserves tight closure. $\square$

Corolllary. *Let $R \to S$ be a homomorphism of Noetherian rings such that S has a completely stable (respectively, completely stable big) test element c and suppose that $N \subseteq M$ are finitely generated (respectively, arbitrary) R-modules. Let $u \in N^*_M$. Then $1 \otimes u \in \langle S \otimes_R N\rangle^*_{S\otimes_R M}$.*

Proof. Suppose that we have a counterexample. Then for some q, $c(1 \otimes u)^q \notin \langle S \otimes_R N\rangle^{[q]}$. This continues to be the case after localization at a suitable maximal Q ideal of S, and after completing the local ring S_Q. Hence, we obtain a counterexample such that $(S, \mathfrak{n}, L)$ is a complete local ring. Let m be the contraction of $\mathfrak{n}$ to R and let let R_1 be the completion of R_m. Then the initial instance of tight closure is preserved by the base change from R to R_1 but not by the base change $R_1 \to S$. This is a contradiction, since R_1 is in $\mathcal{R}_{\text{big}}$. $\square$

Although the theory of test elements that we have developed thus far is reasonably satisfactory for theoretical purposes, it is useful to have theorems that assert that specific elements of the ring are test elements: not only that some unknown power is a test element.

For example, the following result is very useful.

Theorem. *Let R be a geometrically reduced, equidmensional algebra finitely generated over a field K of prime characteristic $p > 0$. Then the elements of the Jacobian ideal $\mathcal{J}(R/K)$ that are in R° are completely stable big test elements for R.*

It will be a while before we can prove this. We shall discuss the definition and properties of the Jacobian ideal in detail later. For the moment, we make only two comments. First, the Jacobian ideal defines the geometrically regular locus in R. Second, if $R = K[x_1, \ldots, x_n]/(f)$ is a hypersurface, then $\mathcal{J}(R/K)$ is simply the ideal generated by the images of the partial derivatives $\partial f/\partial x_i$ in R.

For example, suppose that K has characteristic $p > 0$ with $p \neq 3$. The Theorem above tells us that if $R = K[x, y, z]/(x^3+y^3+z^3)$ then the elements x^2, y^2, and z^2 are completely stable big test elements (3 is iinvertible in K). This is not the best possible result: the test ideal turns out to be all of $m = (x, y, z)$. But it gives a good starting point for computing $\tau(R)$.

The situation is essentially the same in the local case, where we study R_m instead. In this case, once we know that x^2, y^2 are test elements, we can calculate the test ideal as $(x^2,\, y^2) :_R (x^2, y^2)^*$, since this ring is Gorenstein and we may apply problem 4 of Problem Set #3. The socle generator modulo $I = (x^2,\, y^2)$ turns out to be xyz^2, and the problem of showing that the test ideal is mR_m reduces to showing that the ideal $(x^2,\, y^2, xyz^2)$ is tightly closed in R_m. The main point here is that the Theorem above can sometimes be used to make the calculation of the test ideal completely down-to-earth.

The proof of the Theorem above involves several ingredients. One is the Lipman-Sathaye Jacobian Theorem, which we will state but not prove. The Theorem is proved in [J. Lipman and A. Sathaye, *Jacobian ideals and a theorem of Briançon-Skoda,* Michigan Math. J. **28** (1981) 199–222]. Moreover, a complete treatment of the Lipman-Sathaye argument is given in the Lecture Notes from Math 711, Fall 2006. See specifically, the Lectures of September 25, 27, and 29, as well as the Lectures of October 2, 4, 6, 9, 11, and 13.

Another ingredient is the Theorem stated just below. We shall say that an extension of a domain S of a field $\mathcal{K}$ is *étale* if S is a finite product of finite separable algebraic extension fields of $\mathcal{K}$. We shall say that an extension $A \to R$ of a domain A is *generically étale* if the generic fiber is étale, i.e., $\mathrm{frac}\,(A) \otimes_A R$ is a finite product of finite separable algebraic extension fields of $\mathrm{frac}\,(A)$.

Theorem. *Let R be a module-finite and generically étale extension of a regular ring A of prime characteristic $p > 0$. Let $r \in R^\circ$ be such that $cR^\infty \subseteq R[A^\infty]$. Then c is a completely stable big test element for R.*

We shall see that elements c as above exist, and that the Lipman-Sathaye Theorem can be used to find specific elements like this. The reason that it is very helpful that $cR^\infty \subseteq R[A^\infty]$ is that it turns out that $R[A^\infty] \cong R \otimes_A A^\infty$ is faithfully flat over R, since A^∞ is faithfully flat over A. This makes it far easier to work with $R[A^\infty]$ than it is to work with R^∞, and multiplication by c can be used to "correct" the error in replacing R^∞ by $R[A^\infty]$.

We begin by proving the following preliminary result.

Lemma. *Let $(A,\, m_A,\, K)$ be a normal local domain and let R be a module-finite extension domain of A that is generically étale over A. Let* ord *be a $\mathbb{Z}$-valued valuation on A that is nonnegative on A and positive on m_A. Then* ord *extends uniquely to A^∞ by letting* $\mathrm{ord}\,(a^{1/q}) = (1/q)\mathrm{ord}\,(a)$ *for all $a \in A - \{0\}$. The extended valuation takes values in* $\mathbb{Z}[1/p]$.

Let $\mathfrak{m}$ be a proper ideal of R. Let d be the torsion-free rank of R as an A-module. Let $u \in \mathfrak{m}R[A^\infty] \cap A^\infty$. Then $\mathrm{ord}\,(u) \geq 1/d!$.

Proof. We know that $\mathrm{frac}\,(R)$ is separable of degree d over $\mathrm{frac}\,(A) = \mathcal{K}$. Let θ be a primitive element. The splitting field $\mathcal{L}$ of the minimal polynomial f of θ is generated by the roots of f, and is Galois over $\mathcal{K}$, with a Galois group that is a subgroup of the permutations on d, the roots of f. We may replace R by the possibly larger ring which is the integral closure of A in $\mathcal{L}$. Hence, we may assume that the extension of fraction fields is Galois with Galois group G, and $|G| = D \le d!$. The action of G on R extends to $R[A^\infty]$, fixing A^∞. Let $x_1, \dots, x_n \in R$ generate $\mathfrak{m}$. We have an equation

$$u = \sum_{i=1}^{n} a_i x_i$$

where the $a_i \in A^\infty$. The action of G then yields $|G|$ such equations:

$$(*_g) \quad u = \sum_{i=1}^{n} a_i g(x_i)$$

one for each element $g \in G$. Let $\underline{\nu} = (\nu_1, \dots, \nu_n)$ run through n-tuples in $\mathbb{N}^n$ such that $\nu_1 + \cdots + \nu_n = D$, and let $\underline{\mathcal{P}}$ run through ordered partitions $(\mathcal{P}_1, \dots, \mathcal{P}_n)$ of G into n sets. we use the notation $|\underline{\mathcal{P}}|$ for

$$(|\mathcal{P}_1|, \dots, |\mathcal{P}_n|) \in \mathbb{N}^n.$$

Let

$$y_\nu = \sum_{|\underline{\mathcal{P}}| = \underline{\nu}} \left(\prod_{g \in \mathcal{P}_j} g(x_j) \right).$$

Then multiplying the elements $(*_g)$ together yields

$$u^D = \sum_{\underline{\nu}} a_1^{\nu_1} \cdots a_n^{\nu_n} y_{\underline{\nu}}.$$

Each $y_{\underline{\nu}}$ is invariant under the action of G, and is therefore in $R^G = A$. Since each $y_{\underline{\nu}}$ is a sum of products involving at least one of the x_i, each $y_j \in \mathfrak{m} \cap A \subseteq m_A$, and every $\operatorname{ord}(y_{\underline{\nu}}) \ge 1$. Hence,

$$D \operatorname{ord}(u) = \operatorname{ord}(u^D) \ge \min_\nu \operatorname{ord}(a_1^{\nu_1} \cdots a_n^{\nu_n} y_\nu) \ge \min_\nu \operatorname{ord}(y_\nu) \ge 1,$$

and we have that

$$\operatorname{ord}(u) \ge \frac{1}{D} \ge \frac{1}{d!},$$

as required. $\square$

Math 711, Fall 2007 **Problem Set #4**
Due: Wednesday, November 28

1. Let $R \to S$ be a homomorphism of rings of prime characteristic $p > 0$, let M be an R-module, and let N be an S-module. Prove that $\mathcal{F}_S^e(M \otimes_R N) \cong \mathcal{F}_R^e(M) \otimes_R \mathcal{F}_S^e(N)$, and that with this identification, $(u \otimes v)^q = u^q \otimes v^q$ for $u \in M$ and $v \in N$.

2. Let R be a Noetherian ring and I a nilpotent ideal. Suppose that I has a filtration $I = I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n = 0$ such that I_t/I_{t+1} is (R/I)-free for $1 \le i \le n-1$.

(a) Show that $x \in R$ is a nonzerodivisor if and only if it is a nonzerodivisor on R/I, in which case $I/xI \hookrightarrow R/xR$ and there is a corresponding filtration of I/xI given by the images if the I_t in which the factors are the modules $(R/xR) \otimes_R (I_t/I_{t+1})$.

(b) Prove that R is Cohen-Macaulay if and only if R/I is Cohen-Macaulay.

3. (a) Let R be a Noetherian ring and P a height 0 prime ideal of R. Show that we can localize at one element $c \in R - P$ such that R_c is Cohen-Macaulay if and only if $(R/P)_c$ is Cohen-Macaulay. [Show that we may reduce to the case where P is the only minimal prime. Consider a filtration of P by ideals P_i such that $P = P_1$, P_i/P_{i+1} is killed by P, and $P_n = 0$ for some n. (If $P^n = 0$, we may take $P_i = P^i$. Alternatively, we may take $P_i = \mathrm{Ann}_P P^{n-i}$.) Localize at one element c such that all of the factors P_i/P_{i+1} are R_c free. The "if" direction was done in class.]

(b) Let R be a local ring that is a homorphic image of a Cohen-Macaulay ring. Prove that the Cohen-Macaulay locus in R is open.

4. Let $R \hookrightarrow S$ be a module-finite extension of Noetherian domains of prime characteristic $p > 0$. Let $N \subseteq M$ be R-modules and let $u \in M$. Show that if $1 \otimes u \in \langle S \otimes_R N \rangle^*_{S \otimes_R M}$ then $u \in N^*_M$.

5. Let (R, m, K) be a complete one-dimensional local domain with $\mathrm{frac}\, R = \mathcal{L}$, and let M be a finitely generated torsion free R-module. Show that the type of $\mathcal{L} \otimes_R M$, which is the same as its vector space dimension over $\mathcal{L}$ (this is also the torsion-free rank of M) is at most the type of M. (The latter may be described as the K-vectcor space dimension of M/xM, where $x \in m$ is a parameter, or as the K-vector space dimension of $\mathrm{Ext}^1_R(K, M)$.)

6. Let R be either an excellent ring or a local ring that is a homomorphic image of a Gorenstein ring. Prove that the locus where R is Cohen-Macaulay of type at most t is open. In particular, prove that the locus where R is Gorenstein is open.

Math 711: Lecture of November 9, 2007

We note the following fact from field theory:

Proposition. *Let $\mathcal{K}$ be a field of prime characteristic $p > 0$, let $\mathcal{L}$ be a separable algebraic extension of $\mathcal{K}$, and let $\mathcal{F}$ be a purely inseparable algebraic extension of $\mathcal{K}$. Then the map $\mathcal{F} \otimes_{\mathcal{K}} \mathcal{L}$ to the compositum $\mathcal{L}[\mathcal{F}]$ (which may be formed within a perfect closure or algebraic closure of $\mathcal{L}$) such that $a \otimes b \mapsto ab$ is an isomorphism.*

Proof. The map is certainly onto. It suffices to show that $\mathcal{F} \otimes_{\mathcal{K}} \mathcal{L}$ is a field: every element has a q th power in $\mathcal{L}$, and so if the ring is reduced it must be a field, and the injectivity of the map follows. $\mathcal{L}$ is a direct limit of finite separable algebraic extensions of $\mathcal{K}$, and so there is no loss of generality in assuming that the $\mathcal{L}$ is fnite over $\mathcal{K}$. The result now follows from the second Corollary on p. 4 of the Lecture Notes from September 19, or the argument given at the bottom of p. 6 of the Lecture Notes from October 19. $\square$

This fact is referred to as the *linear disjointness* of separable and purely inseparable field extensions.

In consequence:

Corollary. *Let $\mathcal{L}$ be a separable algebraic extension of $\mathcal{K}$, a field of prime characteristic $p > 0$. Then for every $q = p^e$, $\mathcal{L}[\mathcal{K}^{1/q}] = \mathcal{L}^{1/q}$.*

Proof. We need to show that every element of $\mathcal{L}$ has a q th root in $\mathcal{L}[\mathcal{K}^{1/q}]$. Since $\mathcal{L}$ is a directed union of finite separable algebraic extensions of $\mathcal{K}$, it suffices to prove the result when $\mathcal{L}$ is a finite separable algebraic field extension of $\mathcal{K}$. Let $[\mathcal{L} : \mathcal{K}] = d$. The field extension $\mathcal{K}^{1/q} \subseteq \mathcal{L}^{1/q}$ is isomorphic with the field extension $\mathcal{K} \subseteq \mathcal{L}$. Consequently, $[\mathcal{L}^{1/q} : \mathcal{K}^{1/q}] = d$ also. Since $\mathcal{K}^{1/q} \subseteq \mathcal{L}[\mathcal{K}^{1/q}] \subseteq \mathcal{L}^{1/q}$, to complete the proof it suffices to show that $[\mathcal{L}[\mathcal{K}^{1/q}] : \mathcal{K}^{1/q}] = d$ as well. But $\mathcal{L}[\mathcal{K}^{1/q}] \cong \mathcal{K}^{1/q} \otimes_{\mathcal{K}} \mathcal{L}$, and so its dimension as a $\mathcal{K}^{1/q}$-vector space is the same as the dimension of $\mathcal{L}$ as a $\mathcal{K}$-vector space, which is d. $\square$

We next prove:

Proposition. *Let R be module-finite, torsion-free, and generically étale over a regular domain A of prime characteristic $p > 0$.*

(a) *R is reduced.*

(b) *For every q, then map $A^{1/q} \otimes_A R \to R[A^{1/q}]$ is an isomorphism. Likewise, $A^\infty \otimes_A R \to R[A^\infty]$ is an isomorphism.*

(c) *For every q, $R[A^{1/q}]$ is faithfully flat over R. Moreover, $R[A^\infty]$ is faithfully flat over R.*

Proof. Let $\mathcal{K} = \mathrm{frac}\,(A)$. Then $\mathcal{K} \otimes_A R = \prod_{i=1}^h \mathcal{L}_i$, where every $\mathcal{L}_i$ is a finite separable algebraic extension of $\mathcal{K}$.

(a) Since R is torsion-free as an A-module, $R \subseteq \mathcal{K} \otimes_A R = \prod_{i=1}^h \mathcal{L}_i$, from which the result follows.

(b) We have an obvious surjection $A^{1/q} \otimes_A R \twoheadrightarrow R[A^{1/q}]$. Since R is torsion-free over A, each nonzero element $a \in A$ is a nonzerodivisor on R. Since $A^{1/q}$ is A-flat, this remains true when we apply $A^{1/q} \otimes_A \_$. It follows that $A^{1/q} \otimes_A R$ is a torsion-free A-module. Hence, we need only check that the map is injective after applying $\mathcal{K} \otimes_A \_$: if there is a kernel, it will not be killed. The left hand side becomes $\mathcal{K}^{1/q} \otimes_{\mathcal{K}} \prod_{i=1}^h \mathcal{L}_i$ and the right hand side becomes $\prod_{i=1}^h \mathcal{L}_i[\mathcal{K}^{1/q}]$. The map is the product of the maps $\mathcal{K}^{1/q} \otimes \mathcal{L}_i \to \mathcal{L}_i[\mathcal{K}^{1/q}]$, each of which is an isomorphism by the Proposition at the top of p. 1.

(c) This is immediate from part (b), since $A^{1/q}$ is faithfully flat over A for every q: this is equivalent to the flatness of $F^e : A \to A$. Since A^∞ is the directed union of the $A^{1/q}$, it is likewise flat over A, and since it is purely inseparable over A, it is faithfully flat. Hence, $R[A^\infty]$ is faithfully flat over R as well, by part (b). $\square$

Theorem. *Let R be module-finite, torsion-free, and generically étale over a regular domain A of prime characteristic $p > 0$. Then there exist nonzero elements $c \in A$ such that $cR^{1/p} \subseteq R[A^{1/p}]$. For such an element c, we have that $c^2 R^{1/q} \subseteq R[A^{1/q}]$ for all q, and, hence, also that $c^2 R^\infty \subseteq R[A^\infty]$.*

Proof. Consider the inclusion $R[A^{1/p}] \subseteq R^{1/p}$, which is a module finite extension: even $A^{1/p} \subseteq R^{1/p}$ is module-finite, because it is isomorphic with $A \subseteq R$. If we apply $\mathcal{K} \otimes_A \_$, on the left hand side R becomes $\prod_{i=1}^h \mathcal{L}_i$ and $A^{1/p}$ becomes $\mathcal{K}^{1/p}$. Hence, the left hand side becomes

$$(\prod_{i=1}^h \mathcal{L}_i)[\mathcal{K}^{1/p}] \cong \prod_{i=1}^h \mathcal{L}_i[\mathcal{K}^{1/p}] = \prod_{i=1}^h \mathcal{L}_i^{1/p}$$

by the Corollary on p. 1, and the right hand side also becomes $\prod_{i=1}^h \mathcal{L}_i^{1/p}$. Hence, if we take a finite set of generators for $R^{1/p}$ as an $R[A^{1/p}]$-module, each generator is multiplied into $R[A^{1/p}]$ by an element $c_i \in A^\circ$. The product c of the c_i is the required element.

Now suppose $c \in A^\circ$ is such that $cR^\infty \subseteq R[^\infty]$. Let

$$c_e = c^{1+\frac{1}{p}+\cdots+\frac{1}{p^e}}$$

and note that

$$c_{e+1} = c c_e^{1/p}$$

for $e \geq 1$. We shall show by induction on e that $c_e R^{1/q} \subseteq R[A^{1/q}]$ for every $e \in \mathbb{N}$. Note that $c_0 = c$, and this base case is given. Now suppose that $c_e R^{1/q} \subseteq R[A^{1/q}]$. Taking pth roots, we have that $c_e^{1/p} R^{1/pq} \subseteq R^{1/p}[A^{1/pq}]$. We multiply both sides by c to obtain

$$c_{e+1} R^{1/pq} = c c_e^{1/p} R^{1/pq} \subseteq cR^{1/p}[A^{1/pq}] \subseteq R[A^{1/p}][A^{1/pq}] = R[A^{1/pq}],$$

as required.

Since
$$1 + \frac{1}{p} + \cdots + \frac{1}{p^e} \leq 1 + \frac{1}{2} + \cdots + \frac{1}{2^e} < 2,$$
c^2 is a multiple of c_e in $A^{1/q}$ and in $R[A^{1/q}]$, and the stated result follows. □

Also note:

Lemma. *Let R be module-finite, torsion-free, and generically étale over a domain A.*

(a) *If $A \hookrightarrow B$ is flat, injective homomorphism of domains, then $B \otimes_A R$ is module-finite, torsion-free and generically étale over B.*
In particular, if $\mathcal{K} \to \mathcal{L}$ is a field extension and $\mathcal{F}$ is an étale extension of $\mathcal{K}$, then $\mathcal{L} \otimes_{\mathcal{K}} \mathcal{F}$ is an étale extension of $\mathcal{L}$.

(b) *With the same hypothesis as in the first assertion in part (a), if $c \in R$ is such that $cR^\infty \subseteq R[A^\infty]$, then $c(B \otimes_A R)^\infty \subseteq (B \otimes_A R)[B^\infty]$.*

(c) *If $\mathfrak{q}$ is a minimal prime of R, then $\mathfrak{q}$ does not meet A and $A \hookrightarrow R/\mathfrak{q}$ is again module-finite, torsion-free, and generically étale over A.*

Proof. (a) We prove the second statement first. Since $\mathcal{F}$ is a product of finite separable algebraic extensions of $\mathcal{K}$, we reduce at once to the case where $\mathcal{F}$ is a finite separable algebraic field extension of K, and then $\mathcal{F} \cong \mathcal{K}[x]/(g)$, where x is an indeterminate and g is an irreducible monic polynomial of positive degree over $\mathcal{K}$ whose roots in an algebraic closure of $\mathcal{K}$ are mutually distinct. Let $g = g_1 \cdots g_s$ be the factorization of g into monic irreducible polynomials over $\mathcal{L}$. These are mutually distinct, and any two generate the unit ideal. Hence, by the Chinese Remainder Theorem,
$$\mathcal{L} \otimes_{\mathcal{K}} \mathcal{F} \cong \mathcal{L}[x]/(g) \cong \prod_{j=1}^{s} \mathcal{L}[x]/(g_j),$$
and every $\mathcal{L}_j[x]/g_j)$ is a finite separable algebraic extension of $\mathcal{L}$.

It is obvious that $B \otimes_A R$ is module-finite over A. By the Lemma on the first page of the Lecture Notes from October 12, the fact that R is module-finite and torsion-free over A implies that we have an embedding of $R \hookrightarrow A^{\oplus h}$ for some h. Because B is A-flat, we have injection $B \otimes_A R \hookrightarrow B^{\oplus h}$, and so $B \otimes_A R$ is torsion-free over B. The fact that the condition of being generically étale is preserved is immediate from the result of the first paragraph above, with $\mathcal{K} = \mathrm{frac}\,(A)$, $\mathcal{L} = \mathrm{frac}\,(B)$, and $\mathcal{F} = \mathcal{K} \otimes_A R$.

(b) Every element of $B \otimes_A R)^{1/q} \cong B^{1/q} \otimes_{A^{1/q}} R^{1/q}$ is a sum of elements of the form $b^{1/q} \otimes r^{1/q}$, while $c(b^{1/q} \otimes r^{1/q}) = b^{1/q} \otimes cr^{1/q}$. Since $cr^{1/q} \in R[A^\infty]$, it follows that $c(B \otimes_A R)^{1/q} \subseteq (B \otimes_A R)[A^\infty][B^{1/q}] \subseteq (B \otimes_A R)[B^\infty]$.

(c) $\mathfrak{q}$ cannot meet A° because R is torsion-free over A. Thus, $\mathfrak{q}$ corresponds to one of the primes of the generic fiber $\mathcal{K} \otimes_A R$, which is a product of finite algebraic separable field extensions of $\mathcal{K}$. It follows that $\mathcal{K} \otimes_A (R/\mathfrak{p})$ is one of these finite algebraic separable field extensions. $\square$

We can now prove the result on test elements, which we state again.

Theorem. *Let R be module-finite, torsion-free, and generically étale over a regular domain A. Let $c \in R^\circ$ be any element such that $cR^\infty \subseteq R[A^\infty]$. Then c is a completely stable big test element for R.*

Proof. Let Q be any prime ideal of R, and let P be its contraction to A. Then $A_P \to R_P$ satisfies the same hypothesis by parts (a) and (b) of the Lemma on p. 3, and so we may assume that A is local and that Q is a maximal ideal of R. We may now apply $B \otimes_A \_$, where $B = \widehat{A}$. By the same Lemma, the hypotheses are preserved. B becomes a product of complete local rings, one of which is the completion of R_Q. The hypotheses hold for each factor, and so we may assume without loss of generality that $(A, m, K) \to (R, \mathrm{frac}\, m, L)$ is a local map of complete local rings as well. Now suppose that $H \subseteq G$ are R-modules and $u \in H^*_G$. We may assume, as usual, that G is free. (This is not necessary, but may help to make the argument more transparent.) We are not assuming, however, that G or H is finitely generated.

We know that $u \in H^*_G$. Hence, there is an element r of R°, such that $ru^{q'} \in H^{[q']}$ for all $q' \gg 0$. Since $r \in R^\circ$, $\dim(R/rR) < \dim(R)$. Since R/rR is a module finite extension of $A/(rR \cap A)$, we must have that $\dim(A/(rR \cap A) < \dim(A)$, and it follows that $rR \cap A \neq (0)$, i.e., that r has a nonzero multiple $a \in A$. Then $au^{q'} \in H^{[q']}$ for all $q' \gg 0$. We may take q'th roots and obtain $a^{1/q'} \in R^{1/q'}H$ for all $q' \gg 0$. We are using the notation $R^{1/q'}H$ for the expansion of H to $R^{1/q'} \otimes_R G$, i.e., for the image of $R^{1/q'} \otimes H$ to $R^{1/q'} \otimes_R G$.

Let ord denote any valuation on A with values in $\mathbb{Z}$ that is nonnegative on A and positive on m. Then ord extends uniquely to a valuattion on A^∞ with values in $\mathbb{Z}[1/p]$ such that $\mathrm{ord}\,(b^{1/q'}) = (1/q')\mathrm{ord}\,(b)$ for all $b \in A^\circ$ and q'.

To complete the argument, we shall prove the following:

(#) Suppose that $\{\delta_n\}_n$ is asequence of elements of $A^\infty - \{0\}$ such that $\delta_n u \in R^\infty H$ for all n and $\mathrm{ord}\,(\delta_n) \to 0$ as $n \to \infty$. Then $cu^q \in H^{[q]}$ for all q, and so $u \in H^*_G$.

This not only proves that c is a big test element, it also gives a new characterization of tight closure which is stated as a Corollary of this proof in the sequel.

Moreover, we will have proved that c is a completely stable big test element in every completed local ring of R, and so it will follow that c is a completely stable big test element for R.

If the statement (#) is false, fix q such that $cu^q \notin H^{[q]}$. For every n, we have

$$\delta_n u \in R^\infty H$$

and, hence,

$$\delta_n^q u^q \in R^\infty H^{[q]}.$$

Let $S = R[A^\infty]$, which we know is flat over R. We multiply by $c \in R$ to obtain $\delta_n^q(cu^q) \in SH^{[q]}$, i.e., that

$$\delta_n^q \in SH^{[q]} :_S cu^q = (H^{[q]} :_R cu^q)S,$$

by the second statement in part (a) of the Lemma on p. 1 of the Lecture Notes from October 29 and the flatness of S over R. Since $cu^q \notin H^{[q]}$, $H^{[q]} :_R cu^q$ is a proper ideal J of R, amd so $\delta_n^q \in JR[A^\infty]$ for all n. Now J is contained in some maximal ideal $\mathcal{M}$ of R. $\mathcal{M}$ contains a minimal prime $\mathfrak{q}$ of R. By part (c) of the Lemma on p. 3, A injects into $\overline{R}$, where $\overline{R}$ is module-finite domain extension of A generically étale over A, and $\mathfrak{m} = J\overline{R}$ is a proper ideal of $\overline{R}$. We can map $R[A^\infty]$ onto $\overline{R}[A^\infty]$ Then for all n, $\delta_n^q \in \mathfrak{m}\overline{R}[A^\infty] \cap A^\infty$. Let d denote the torsion-free rank of $\overline{R}$ over A. By the Lemma at the bottom of p. 5 of the Lecture Notes from November 7, we have that

$$q\,\mathrm{ord}\,(\delta_n) = \mathrm{ord}\,(\delta_n^q) \geq \frac{1}{d!}$$

for all n, and so

$$\mathrm{ord}\,\delta_n \geq \frac{1}{qd!}$$

for all n. Since q and d are both fixed and $n \to \infty$, this contradicts the assumption that $\mathrm{ord}\,(\delta_n) \to 0$ as $n \to \infty$. □

Remark. The Theorem also holds when the regular ring A is not assumed to be a domain, if the hypothesis that R be torsion-free over A is taken to mean that every element of A° is a nonzero divisor on R, and the condition that R be generically étale over A is taken to mean that $R_\mathfrak{p}$ is étale over $A_\mathfrak{p}$ for every minimal prime $\mathfrak{p}$ of A. In this case, A is a finite product of regular domains, there is a corresponding product decomposition of R, and each factor of R is module-finite, torsion-free, and generically étale over the corresponding factor of A. The result follows at once from the results for the individual factors. □

In the course of the proof of the Theorem we have demonstrated the following:

Corollary. *Let (A, m, K) be a complete regular local ring, let R be module-finite, torsion-free and generically étale over A, and let* ord *by a $\mathbb{Z}$-valued valuation on A nonnegative on A and positive on m. Extend* ord *to a $\mathbb{Z}[1/p]$-valued valuation on A^∞. Let $N \subseteq M$ by R-modules and let $u \in M$. Then the following two conditions are equivalent:*

(1) $u \in N^*_M$.

(2) *There exists an infinite sequence of elements $\{\delta_n\}_n$ of $A^\infty - \{0\}$ such that* $\mathrm{ord}\,(\delta_n) \to 0$ *as $n \to \infty$ and for all n, $\delta_n \otimes u$ is in the image of $R^\infty \otimes_R N$ in $R^\infty \otimes_R M$.* □

This result is surprising: in the standard definition of tight closure, the δ_n are all q th roots of a single element c. Here, they are permitted to be entirely unrelated. We shall soon prove a better result in this direction, in which the multipliers are allowed to be arbitrary elements of R^+ whose orders with respect to a valuation are approaching 0.

Math 711: Lecture of November 12, 2007

Before proceeding further with our treatment of test elements, we note the following consequence of the theory of approximately Gorenstein rings. We shall need similar splitting results in the proof of the generalization, stated in the first Theorem on p. 2, of the Corollary near the bottom of p. 5 of the Lecture Notes from November 9.

Theorem. *Let R be a weakly F-regular ring. Then R is a direct summand of every module-finite extension ring S. Moreover, if R is a complete local ring as well, R is a direct summand of R^+. In particular, these results hold when R is regular.*

Proof. Both weak F-regularity and the issue of whether $R \to S$ splits are local on the maximal ideals of R. Therefore, we may assume that (R, m, K) is local. Since R is approximately Gorenstein, there is a descending chain $\{I_t\}_t$ of m-primary irreducible ideals cofinal with the powers of m. By the splitting criterion in the Theorem at bottom of p. 4 and top of p. 5 of the Lecture Notes from October 24, R is a direct summand of S (or R^+ in case R is complete local) if and only if I_t is contracted for all t. In fact, $I_tS \cap R \subseteq I_t^*$ by the Theorem near the bottom of *p.* 1 of the Lecture Notes of October 12, and, by hypothesis, $I_t^* = I_t$. □

It is an open question whether a locally excellent Noetherian domain R of prime characteristic $p > 0$ is weakly F-regular if and only if $(*)$ R is a direct summand of every module-finite extension ring. The issue is local on the maximal ideals of R, and reduces to the excellent local case. By the main result of [K. E. Smith, *Tight Closure of Parameter Ideals,* Inventiones Math. **115** (1994) 41–60], the tight closure of an ideal generated by part of a system of parameters is the same as its plus closure. From this result, it is easy to see that $(*)$ implies that R is F-rational. In the Gorenstein case, F-rational is equivalent to F-regular, so that the equivalence of the two conditions holds in the locally excellent Gorenstein case. We shall prove Smith's result that tight closure is the same as plus closure for parameter ideals. The argument depends on the use of local cohomology, and also utiliuzes general Néron desingularization. We shall also need the main result of [M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras,* Annals of Math. bf 135 (1992) 53–89], that if R is an excellent local domain, then R^+ is a big Cohen-Macaulay algebra over R. We shall prove this using a recent idea method of Huneke and Lyubeznik: cf. [C. Huneke and G. Lyubeznik, *Absolute integral closure in positive characteristic,* Advances in Math. **210** (2007) 498–504].

Our next immediate goal is to prove a strengthened version of the Corollary on p. 5 of the Lecture Notes from November 9. First note that if A is a regular local ring, we can choose a $\mathbb{Z}$-valued valuation ord that is nonnegative on A and positive on m. For example, if $a \neq 0$ we can let $\mathrm{ord}\,(a)$ be the largest integer k such that $a \in m^k$. We thus have an inclusion $A \subseteq V$ where V is a Noetherian discrete valuation ring. Now assume that A is complete, and complete V as well. That is, we have a local injection $A \hookrightarrow V$. We also have an injection $A^+ \hookrightarrow V^+$

For every module-finite extension domain R of A, where we think of R as a subring of A^+, we may form $V[R]$ within V^+. $V[R]$ is a complete local domain of dimension one that contains V. Its normalization, which we may form within V^+, is a complete local normal domain of dimension one, and is therefore a discrete valuation ring V_R. The generator of the maximal ideal of V is a unit times a power of the generator of the maximal ideal of V_R. Hence, ord extends to a valuation on R with values in the abelian group generated by $\frac{1}{h}$, where h is the order of the generator of the maximal ideal of V in V_R. Since A^+ is the union of all of these rings R, ord extends to a $\mathbb{Q}$-valued valuation on R^+ that is nonnegative on R^+ and postive on the maximal ideal of R^+.

If R is any complete local domain, we can represent R as a module-finite extension of a complete regular local ring A. Hence, we can choose a complete discrete valuation ring V_R and a local injection $R \to V_R$, and extend the corresponding $\mathbb{Z}$-valued valuation to a $\mathbb{Q}$-valued valuation that is nonnegative on R^+ and positive on the maximal ideal of R^+.

Theorem (valuation test for tight closure). *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$ and let* ord *be a $\mathbb{Q}$-valued valuation on R^+ that is nonnegative on R^+ and positive on the maximal ideal of R^+. Let $N \subseteq M$ be arbitary R-modules and $u \in M$. Then the following two conditions are equivalent:*

(1) $u \in N^*_M$.

(2) *There exists a sequence $\{v_n\}$ of elements of $R^+ - \{0\}$ such that* $\mathrm{ord}\,(v_n) \to 0$ *as $n \to \infty$ and $v_n \otimes u$ is in the image of $R^+ \otimes_R N$ in $R^+ \otimes_R M$ for all n.*

We need several preliminary results in order to prove this.

The following generalization of colon-capturing can be further generalized in several ways. We only give a version sufficient for our needs here.

Theorem. *Let (R, m, K) be a reduced excellent local ring of prime characteristic $p > 0$. Let $x_1, \ldots, x_k \in m$ be part of a system of parameters modulo every minimal prime of R. Let $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{N}$, and assume that $a_i < b_i$ for all i. Then*

$$(x_1^{b_1}, \ldots, x_k^{b_k})^* :_R x_1^{a_1} \cdots x_k^{a_k} = (x_1^{b_1-a_1}, \ldots, x_k^{b_i-a_i})^*.$$

Proof. Let $d_i = b_i - a_i$. It is easy to see that each $x_i^{d_i}$ multiplies $x_1^{a_1} \cdots x_k^{a_k}$ into

$$(x_1^{b_1}, \ldots, x_k^{b_k}) \subseteq (x_1^{b_1}, \ldots, x_k^{b_k})^*,$$

since $d_i + a_i = b_i$ for every i. But if I is tightly closed, so is any ideal of the form $I :_R y$. (This is equivalent to the statement that if 0 is tightly closed in R/I, then it is also tightly closed in the smaller module $y(R/I) \cong R/(I :_R y)$.) Since

$$(x_1^{d_1}, \ldots, x_k^{d}) \subseteq (x_1^{b_1}, \ldots, x_k^{b_k})^* :_R x_1^{a_1} \cdots x_k^{a_k},$$

we also have

$$(x_1^{d_1},\,\dots,\,x_k^{d_k})^* \subseteq (x_1^{b_1},\,\dots,\,x_k^{b_k})^* :_R x_1^{a_1}\,\cdots\,x_k^{a_k}$$

Thus, it suffices to prove the opposite inclusion. By induction on the number of a_i that are not 0, we reduce at once to the case where only one of the a_i is not 0, because, quite generally,

$$I :_R (yz) = (I :_R y) :_R z.$$

By symmetry, we may assume that only $a_k \neq 0$. We write $x_k = x$, $a_k = a$, $b_k = b$ and $d_k = d$. Let $J = (x_1^{b_1},\,\dots,\,x_{k-1}^{b_{k-1}})$. Suppose $x^a u \in (J + x^b R)^*$. Let $c \in R^\circ$ be a test element. Then $cx^{qa}u^q \in J^{[q]} + x^{qb}R$ for all $q \gg 0$, and for such q, we can write $cx^{qa}u^q = j_q + x^{qb}r_q$, where $j_q \in J^{[q]}$ and $r_q \in R$. Then $x^{qa}(cu^q - r_q x^{qd}) \in J^*$, and by the form of colon-capturing already established, we have that $cu^q - r_q x^{qd} \in (J^{[q]})^*$, and, hence,

$$c^2u^q - cr_q x^{qd} \in J^{[q]}.$$

Consequently,

$$c^2u^q \in J^{[q]} + x^{qd}R = (J + x^d R)^q$$

for all $q \gg 0$, and so $u \in (J + x^d R)^*$, as required. $\square$

Theorem. *Let $(A,\,m,\,K)$ be a complete regular local ring of characteristic p and let* ord *be a $\mathbb{Q}$-valued valuation nonnegative on A^+, and positive on the maximal ideal of A^+. Let $v \in A^+ - \{0\}$ be an element such that* $\mathrm{ord}\,(v)$ *is strictly smaller than the order of any element of m (it suffices to check the generators of m). Then the map $A \to A^+$ such that $1 \mapsto v$ splits, i.e., there is A-linear map $\theta : A^+ \to A$ such that $\theta(v) = 1$.*

Proof. Let $x_1,\,\dots,x_n$ be minimal generators of m. Since A is complete and Gorenstein, it suffices, by the Theorem at the top of p. 3 of the Lecture Notes from October 24 to check that for all t,

$$x_1^t \cdots x_n^t v \notin (x_1^{t+1},\,\dots,x_n^{t+1})A^+.$$

Suppose that

$$x_1^t \cdots x_n^t v = \sum_{i=1}^n s_i x_i^{t+!}.$$

Let $S = A[v,\,s_1,\,\dots,s_i]$. In S we have

$$v \in (x_1^{t+1},\,\dots,x_n^{t+1})S :_S x_1^t\,\cdots\,x_k^t,$$

and so $v \in \big((x_1,\,\dots,x_n)S\big)^*$, by the preceding Theorem on colon-capturing. But then v is in the integral closure of $(x_1,\,\dots,x_n)S$, and this contradicts $\mathrm{ord}\,(v) < \min_i \mathrm{ord}\,(x_i)$. $\square$

Theorem. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$ and let $N \subseteq M$ be R-modules (not necessarily finitely generated). Let $u \in M$. Then the following conditions are equivalent:*

(1) $u \in N^*_M$.

(2) *There exist a fixed integer $s \in \mathbb{N}$ and arbitrarily large integers q such that $N^{[q]} :_R u^q$ meets $R - m^s$.*

(3) *There exist a fixed integer $s \in \mathbb{N}$ such that $N^{[q]} :_R u^q$ meets $R - m^s$ for all q.*

The following two conditons are also equivalent:

(1′) $u \notin N^*_M$.

(2′) *For all s, $N^{[q]} :_R u^q \subseteq m^s$ for all $q \gg 0$.*

Proof. Let $J_q = (N^{[q]})^* :_R u^q$, where $(N^{[q]})^* = (N^{[q]})^*_{\mathcal{F}^e(M)}$. Then the sequence of ideals J_q is descending. To see this, suppose that $r \in J_{pq}$. Then $ru^{pq} \in (N^{[pq]})^*$. Let c be a big test element for R. Then for all $q' \gg 0$,

$$cr^{q'}u^{pqq'} \in N^{[pqq']},$$

from which we have $c(ru^q)^{pq'} \in (N^{[q]})^{[pq']}$ since $r^{pq"}$ is a multiple of $r^{q'}$. This shows that $ru^q \in (N^{[q]})^*$ as well, and so $J_{pq} \subseteq J_q$ for every q.

Let $J = \bigcap_q J_q$. We shall show that whether $J \neq (0)$ or $J = (0)$ governs whether $u \notin N^*_M$ or $u \in N^*M$.

If $J \neq 0$ let $d \in J - \{0\}$. Then $du^q \in (N^{[q]})^*$ for all q, and then $(cd)u^q \in N^{[q]}$ for all q, and so $u \in N^*_M$.

If $J = (0)$, then by Chevalley's Lemma (see p. 6. of the Lecture Notes from October 24) we have that for all s the ideal $J :^{[q]} \subseteq m^s$ for al $q \gg 0$, and it follows as well that $N^{[q]} :_R u^q \subseteq m^s$ for all $q \gg 0$,

If $u \in J$ we have that $c \in N^{[q]} :_R u^q$ for all q. (3) obviously holds, since we can choose s such that $c \notin m^s$, and (3) $\Rightarrow$ (2). Now suppose (2) holds. If $u \notin N^*_M$, we have contradicted the result of the preceding paragraph. Hence, (1), (2), and (3) are equivalent.

The equivalence of (1′) and (2′) is the contrapositive of the equivalence of (1) and (2). □

Math 711: Lecture of November 14, 2007

We continue to develop the preliminary results needed to prove the Theorem stated on p. 2 of the Lecture Notes from November 12. Only one more is needed.

Theorem. *Let $(R,\, m,\, K)$ be a complete local domain of prime characteristic $p > 0$, and let* ord *be a $\mathbb{Q}$-valued valuation nonnegative R^+ and positive on the maximal ideal of R^+. Then there exist an integer $s \geq 1$ and a positive rational number δ such that if $v \in R^+$ and* $\mathrm{ord}\,(v) < \delta$, *then there exists an R-linear map $\phi : R^+ \to R$ such that $\phi(v) \in R - m^s$.*

Proof. R is module-finite over a complete regular local ring A. Note that we may identify $R^+ = A^+$. Let δ be the minimum value of ord on a finite set of generators of the maximal m_A of A.

The module $\omega = \mathrm{Hom}_A(R,\, A)$ is a finitely generated A-module, but also has the structure of an R-module. Evidently, it is a finitely generated R-module. ω is torsion-free over A since its elements are functions with values in A. Since every nonzero element of R has a nonzero multiple in A, it is also torsion-free over R. Let $\mathcal{K} = \mathrm{frac}\,(A)$. Then $\mathcal{K} \otimes_A R = \mathcal{L}$ is the fraction field of R: let h be its degree, i.e., the torsion-free rank of R over A. Then

$$\mathcal{K} \otimes_A \omega \cong \mathrm{Hom}_{\mathcal{K}}(\mathcal{K} \otimes_A R,\, \mathcal{K}) \cong \mathrm{Hom}_{cK}(\mathcal{L}, \mathcal{K})$$

also has dimension d as a $\mathcal{K}$-vector space. Hence, as an $\mathcal{L}$-vector space, it must have dimension 1. Therefore, ω is a rank one torsion-free R-module, and so there exists an isomorphism $\omega \cong J \subseteq R$, where J is a nonzero ideal of R. Now $m_A R$ is primary to m, and so $m^k \subseteq m_A R$ for some k. We may apply the Artin-Rees Lemma to $J \subseteq R$ to conclude that

$$m^s \cap J = m^s R \cap J \subseteq m^k J$$

for s sufficiently large. Choose one such value of s. Then

$$m^s \cap J \subseteq m^k J \subseteq (m_A R)J = m_A J.$$

We shall prove that the desired conclusion holds for the values of δ and s that we have chosen. We may think of R^+ as A^+ and apply the Theorem on p. 3 of the Lecture Notes from November 12 to choose an A-linear map $\theta : R^+ \to A$ such that $\theta(v) = 1$. We then have an induced map

$$\mathrm{Hom}_A(R,\, R^+) \xrightarrow{\theta_*} \mathrm{Hom}_A(R,\, A)$$

which is R-linear, and hence a composite map

$$R^+ \xrightarrow{\mu} \mathrm{Hom}_A(R,\, R^+) \xrightarrow{\theta_*} \mathrm{Hom}_A(R,\, A) \xrightarrow{\cong} J \xrightarrow{\subseteq} R$$

where the first map μ is the map that takes $u \in R^+$ to the map $f_u : R \to R^+$ such that $f_u(r) = ur$ for all $r \in R$. Note that μ is R-linear using the R-module structure on $\mathrm{Hom}_A(R, R^+)$ that comes from R, since $r'u$ maps to $f_{r'u}$ and

$$f_{r'u}(r) = r'ur = u(r'r) = f_u(r'r) = (r'f_u)(r).$$

Call the composite map ϕ.

We shall prove that ϕ has the required property. First note that $(\theta_* \circ \mu)(v) \in \mathrm{Hom}_A(R, A)$ is very special: its value on 1 is $\theta(v \cdot 1) = \theta(v) = 1$. Thus, it is a splitting of the inclusion map $A \hookrightarrow R$. But this means that $(\theta_* \circ \mu)(v) \notin m_A\mathrm{Hom}(R, A)$, for maps in $m_A\mathrm{Hom}_A(R, A)$ can only take on values that are in m_A. It follows that $\phi(v) \notin m_A J \subseteq R$. Since $m^s \cap J \subseteq m_A J$, it also follows that $\phi(v) \notin m^s$, as required. $\square$

We are now ready to prove the first Theorem stated on p. 2 of the Lecture Notes from November 12.

Proof of the valuation test for tight closure. We may assume without loss of generality that $M = G$ is free, that $N = H \subseteq G$, and that $u \in G$. We fix a basis for G, and identify $\mathcal{F}^e(G) \cong G$. We identify H with its image $1 \otimes H \subseteq R^+ \otimes_R G$, and write R^+H for $\langle R^+ \otimes_R H \rangle$ which we may think of as all R^+-linear combinations of elements of H in $R^+ \otimes_R G$. We shall simply write wg for $w \otimes g$ when $w \in R^+$ and $g \in G$.

Suppose that we have $v_n u \in R^+H$ for all n and $\mathrm{ord}\,(v_n) \to 0$. Choose s and δ as in the preceding Theorem. Fix q, and choose n so large that $\mathrm{ord}\,(v_n) < \delta/q$, so that $\mathrm{ord}\,(v_n^q) < \delta$. Choose an R-linear map $\phi : R^+ \to R$ such that $\phi(v_n^q) \in R - m^s$. Then tensoring with G yields an R-linear map $R^+ \otimes_R G \to G$ such that $wg \mapsto \phi(w)g$ for every $w \in R^+$ and $g \in G$.

Since $v_n u \in R^+H$, we may apply $\mathcal{F}^e$ to obtain that

$$v_n^q u^q \in R^+H^{[q]}.$$

We may now apply $\phi \otimes \mathbf{1}_G$ and conclude that

$$\phi(v_n^q)u^q \in H^{[q]},$$

where $\phi(v_n^q) \in R - m^s$. Hence, for every q, $H^{[q]} :_R u^q$ meets $R - m^s$. By the Theorem at the top of p. 4 of the Lecture Notes from November 12, $u \in H^*_G$, as required. $\square$

Capturing normalizations using discriminants

Consider $A \to R$ where A is a normal or possibly even regular Noetherian domain and R is module-finite, torsion-free, and generically étale over A. In this situation, we know that R is reduced. It has a normalization R' in its total quotient ring $\mathcal{T}$. Under these hypotheses, $\mathcal{T}$ may be identified with $\mathcal{K} \otimes_A R$, which is a finite product of finite separable algebraic field extensions $\mathcal{L}_1 \times \cdots \times \mathcal{L}_h$ of $\mathcal{K}$. R' is the product of the normalizations R'_i of the domains $R_i = R/\mathfrak{p}_i$ obtained by killing a minimal prime $\mathfrak{p}_i$ of R. There is one minimal prime for each $\mathcal{L}_i$, namely, the kernel of the composite homomorphism

$$R \to \mathcal{K} \otimes_A R \cong \prod_{i=1}^{h} \mathcal{L}_i \twoheadrightarrow \mathcal{L}_i,$$

and $\mathcal{L}_i$ is the fraction field of the domain R_i.

We want to develop methods of finding elements $c \in R^\circ$ that "capture" the normalization R' in the sense that $cR' \subseteq R$. Moreover, we want a construction such that c continues to have this property after a flat injective base change $A \hookrightarrow B$ of regular domains. We shall see that whenever we have such an element $c \in R^\circ$, it is a big completely stable test element.

There are two methods for constructing such elements c. One is to take c to be a discriminant for R over A: we explain this idea in the immediate sequel. The other is to use the Lipman-Sathaye Jacobian Theorem.

The use of discriminants is much more elementary, and we explore this method first.

Discussion: discriminants. Let A be a normal Noetherian domain and let R be a module-finite torsion-free generically étale extension of A. Let $\mathcal{K} = \mathrm{frac}\,(A)$ and

$$\mathcal{T} = \mathcal{K} \otimes_A R \cong \prod_{i=1}^{h} \mathcal{L}_i,$$

where the $\mathcal{L}_i$ are finite separable algebraic field extensions of $\mathcal{K}$. We first note that we have a trace map $\mathrm{Trace}_{\mathcal{T}/\mathcal{K}} : \mathcal{T} \to \mathcal{K}$ that is $\mathcal{K}$ linear. Such a map is defined whenever $\mathcal{T}$ is a $\mathcal{K}$-algebra that is finite-dimensional as as $\mathcal{K}$-vector space. The *trace* of $\lambda \in \mathcal{T}$ is defined to be the trace of the linear transformation $f_\lambda : \mathcal{T} \to \mathcal{T}$ that sends $\alpha \mapsto \lambda\alpha$. To calculate the trace, one takes a basis for $\mathcal{T}$ over $\mathcal{K}$, finds the matrix of multiplication by λ, and then takes the sum of the diagonal entries of the matrix. The trace is independent of how one chooses the $\mathcal{K}$-basis for $\mathcal{T}$. We summarize thes properties as follows.

Proposition. *Let $\mathcal{T}$ be a $\mathcal{K}$-algebra that is finite-dimensional as a $\mathcal{K}$-vector space. Then* $\mathrm{Trace}_{\mathcal{T}/\mathcal{K}} : \mathcal{T} \to \mathcal{K}$ *is a $\mathcal{K}$-linear map.*

If $\mathcal{K}'$ is any field extension of $\mathcal{K}$ and $\mathcal{T}' = \mathcal{K}' \otimes_{\mathcal{K}} \mathcal{T}$, then

$$\mathrm{Trace}_{\mathcal{T}'/\mathcal{K}'} = \mathbf{1}_{\mathcal{K}'} \otimes_{\mathcal{K}} \mathrm{Trace}\mathcal{T}/\mathcal{K},$$

i.e., if $\beta \in \mathcal{K}'$ and $\lambda \in \mathcal{T}$, then

$$\mathrm{Trace}_{\mathcal{T}'/\mathcal{K}'}(\beta \otimes \lambda) = \beta\,\mathrm{Trace}_{\mathcal{T}/\mathcal{K}}(\lambda).$$

Proof. The previous discussion established the first statement, while the second statement is a consequence of the following two observations. First, if $\theta_1, \ldots, \theta_n$ is a basis for $\mathcal{T}$ over $\mathcal{K}$, then the images $1\otimes\theta_1, \ldots, 1\otimes\theta_n$ of these elements in $\mathcal{K}'\otimes_{\mathcal{K}}\mathcal{T}$ form a basis for $\mathcal{K}'\otimes_{\mathcal{K}}\mathcal{T}$ over $\mathcal{K}'$. Second, If the matrix for multiplication by λ with respect to the basis $\theta_1, \ldots, \theta_n$ is $\mathcal{M}$, the matrix for multiplication by $\beta\otimes\lambda$ with respect to the basis $1\otimes\theta_1, \ldots, 1\otimes\theta_n$ is $\beta\mathcal{M}$, from which the stated result is immediate. □

Because A is normal, the restriction of the trace map to R takes values in A, not just in $\mathcal{K}$. One may argue as follows: a normal Noetherian domain is the intersecftion of the discrete valuation domains V of the form $A_P \subseteq \mathcal{K}$, where P is a height one prime of A. Thus, we may make a base change from A to such a ring V, and it suffices to prove the result when $A = V$ is a Noetherian discrete valuation ring. In this case, because R is torsion-free, it is free, and we may choose a free basis for R over V. This will also be a basis for $\mathcal{L}$ over $\mathcal{K}$. If we compute trace using this basis, all entries of the matrix are in V, and so it is obvious that the trace is in V.

We note that when $\mathcal{T} = \prod_{i=1}^{h}\mathcal{L}_i$ is a finite product of finite separable algebraic field extensions, the map $B : \mathcal{T}\times\mathcal{T} \to \mathcal{K}$ that sends $(\lambda, \lambda') \mapsto \mathrm{Trace}_{\mathcal{T}/\mathcal{K}}(\lambda\lambda')$ is a nondegenerate symmetric bilinear form. This is a well known characterization of separability of finite algebraic field extensions if there is only one $\mathcal{L}_i$. See the Lecture Notes from December 3 from Math 614, Fall 2003, pp. 4–6. In the general case, choose a basis for each $\mathcal{L}_i$ and use the union as a basis for $\mathcal{T}$. It follows at once that

$$\mathrm{Trace}_{\mathcal{T}/\mathcal{K}}(\lambda_1, \ldots, \lambda_h) = \sum_{i=1}^{h}\mathrm{Trace}_{\mathcal{T}_i/\mathcal{K}}(\lambda_i),$$

since the matrix of multiplication by $(\lambda_1, \ldots, \lambda_h)$ is the direct sum of the matrices of multiplciation by the individual λ_i. To show non-degeneracy, consider a nonzero element $\lambda = (\lambda_1, \ldots, \lambda_h)$. Then some λ_i is not 0: by renumbering, we may assume that $\lambda_1 \neq 0$. Since $\mathrm{Trace}_{\mathcal{L}_1/\mathcal{K}}$ yields a nondegenerate bilinear form on $\mathcal{L}_1$, we can choose $\lambda_1' \in \mathcal{L}_1$ such that

$$\mathrm{Trace}_{\mathcal{L}_1/\mathcal{K}}(\lambda_1'\lambda_1) \neq 0.$$

Let $\lambda' \in \mathcal{L}$ be the element $(\lambda_1', 0, \ldots, 0)$. Then

$$\mathrm{Trace}_{\mathcal{T}/\mathcal{K}}(\lambda'\lambda) = \mathrm{Trace}_{\mathcal{L}_1/\mathcal{K}}(\lambda_1'\lambda_1) \neq 0.$$

By a *discriminant* for R over A we mean an element of A obtained as follows: choose $\underline{\theta} = \theta_1, \ldots, \theta_n \in R$ whose images in $\mathcal{L}$ are a basis for $\mathcal{T}$ over $\mathcal{K}$, and let

$$D = D_{\underline{\theta}} = \det\bigl(\mathrm{Trace}_{\mathcal{L}/\mathcal{K}}(\theta_i\theta_j)\bigr).$$

Since every $\theta_i\theta_j \in R$, the matrix has entries in A, and the determinant is in A. Since the corresponding bilinear form is nondegenerate, D is a nonzero element of A. The following result is very easy.

Proposition. *Let R be module-finite, torsion-free, and generically étale over a normal Noetherian domain A. Let $A \hookrightarrow B$ be a flat injective map of normal Noetherian domains.*

(a) *$B \to B \otimes_A R$ is module-finite, torsion-free, and generically étale.*

(b) *If the images of $\theta_1, \ldots, \theta_n \in R$ in $\mathcal{K} \otimes_A R$ are a $\mathcal{K}$ basis for $\mathcal{K} \otimes_A R$, then their images $\underline{\theta}' = 1 \otimes \theta_1, \ldots, 1 \otimes \theta_n$ in $B \otimes_A R$ are a basis for* $\mathrm{frac}\,(B) \otimes_B (B \otimes_A R)$ *over* $\mathrm{frac}\,(B)$.

(c) *The image of the discriminant $D_{\underline{\theta}}$ in B is the discriminant $D_{\underline{\theta}'}$ of the basis $\theta' = 1 \otimes \theta_1, \ldots, 1 \otimes \theta_n$ for the extension $B \to B \otimes_A R$.*

Proof. We have already proved part (a): this is part (a) of the Lemma on p. 3 of the Lecture Notes from November 9. Part (b) is obvious, and part (c) follows from part (b), the definition of the discriminant, and the second statement of the Proposition on p. 3. □

The key property of discriminants for us is:

Theorem. *Let R be module-finite, torsion-free, and generically étale over a normal Noetherian doman A with fraction field $\mathcal{K}$. Let $\theta_1, \ldots, \theta_n \in R$ give a $\mathcal{K}$-vector space basis for $\mathcal{T} = \mathcal{K} \otimes_A R$. Let R' denote the normalization of R in its total quotient ring $\mathcal{A} \otimes_A R$. Then $D_{\underline{\theta}}$, the discriminant of $\theta_1, \ldots, \theta_n$, is a nonzero element of A such that $D_{\underline{\theta}} R' \subseteq R$. In consequence, R' is module-finite over R.*

Proof. Let $s \in R'$. Then $s \in \mathcal{K} \otimes R$, and so we can write s uniquely in the form

$$(\#) \quad s = \sum_{j=1}^{n} \alpha_j \theta_j,$$

where the $\alpha_i \in \mathcal{K}$. For every θ_i we have that

$$\theta_i s = \sum_{j=1}^{n} \alpha_i \theta_i \theta_j.$$

Let Trace denote $\mathrm{Trace}_{\mathcal{T}/\mathcal{K}}$, and apply the $\mathcal{K}$-linear operator Trace to both sides of the equation. Since $\theta_i s$ is integral over R, its trace a_i is in A. This gives n equations

$$a_i = \sum_{j=1}^{n} \alpha_j \mathrm{Trace}(\theta_i \theta_j), \ 1 \leq i \leq n.$$

Let $\mathcal{M}$ denote the matrix $\big(\mathrm{Trace}(\theta_i \theta_j)\big)$, which has entries in A. Then these equations give a matrix equation

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \mathcal{M} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Let adj($\mathcal{M}$) denote the classical adjoint of $\mathcal{M}$, the transpose of the matrix of cofactors. Then $\operatorname{adj}(\mathcal{M})\mathcal{M} = D\boldsymbol{I}_n$ where $D = \det(\mathcal{M}) = D_{\underline{\theta}}$, and $\boldsymbol{I}_n$ is the size n identity matrix. Note that adj($\mathcal{M}$) has entries in A. Then

$$\begin{pmatrix} D\alpha_1 \\ \vdots \\ D\alpha_n \end{pmatrix} = D\boldsymbol{I}_n \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \operatorname{adj}(\mathcal{M})\mathcal{M} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \operatorname{adj}(\mathcal{M}) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

and the rightmost column matrix clearly has entries in A. Hence, every $D\alpha_i \in A$, and it follows from the displayed formula (#) on the preceding page that $Ds \in R$. Since $s \in R'$ was arbitrary, we have proved that $DR' \subseteq R$, as requried.

The final statement follows because $R' \cong DR' \subseteq R$ as A-modules, and so R' is finitely generated over A and, hence, over R. $\square$

Math 711: Lecture of November 16, 2007

We next observe:

Lemma. *Let A be a regular Noetherian domain of prime characteristic $p > 0$, and let $A \to R$ be module-finite, torsion-free, and generically étale. Then for every q, $R^{1/q}$ is contained in the normalization of $R[A^{1/q}]$.*

Proof. Fix $q = p^e$, and let
$$S = R[A^{1/q}] \cong A^{1/q} \otimes_A R.$$
Since every element of $R^{1/q}$ has its qth power in $R \subseteq S$, the extension is integral. Let $\mathcal{K} = \mathrm{frac}\,(A)$. We can write
$$\mathcal{K} \otimes_A R = \prod_{i=1}^{h} \mathcal{L}_i$$
where every $\mathcal{L}_i$ is finite separable algebraic extension field $\mathrm{frac}\,(A) = \mathcal{K}$. Then
$$\mathcal{K} \otimes_A R^{1/q} = \mathcal{K}^{1/q} \otimes_{A^{1/q}} R^{1/q},$$
since $R^{1/q}$ contains $A^{1/q}$ and inverting every element of $A - \{0\}$ makes every element of $A^{1/q} - \{0\}$ invertible. Hence,
$$\mathcal{K} \otimes_A R^{1/q} \cong \prod_{i=1}^{h} \mathcal{L}_i^{1/q}.$$
This is the total quotient ring of $R^{1/q}$. On the other hand,
$$\mathcal{K} \otimes_A (A^{1/q} \otimes_A R) \cong \mathcal{K}^{1/q} \otimes_{\mathcal{K}} (\mathcal{K} \otimes_A R) \cong \mathcal{K}^{1/q} \otimes_{\mathcal{K}} \prod_{i=1}^{h} \mathcal{L}_i \cong \prod_{i=1}^{h} (\mathcal{K}^{1/q} \otimes_{\mathcal{K}} \mathcal{L}_i) \cong \prod_{i=1}^{h} \mathcal{L}_i^{1/q}$$
where the rightmost isomorphism follows from the Corollary on p. 1 of the Lecture Notes from November 9. Thus, $R^{1/q}$ is contained in the total quotient ring of $R[A^{1/q}]$. $\square$

We can now show that discriminants yield test elements.

Theorem. *Let A be a regular Noetherian domain of prime characteristic $p > 0$, and let $A \to R$ be module-finite, torsion-free, and generically étale. Let $\mathcal{K} = \mathrm{frac}\,(A)$, let $\underline{\theta} = \theta_1, \ldots, \theta_n$ be elements of R that form a basis for $\mathcal{T} = \mathcal{K} \otimes_{\mathcal{K}} R$, and let $D = D_{\underline{\theta}} \in A^\circ$ be the discriminant. Then D is a competely stable big test element for R.*

Moreover, if $A \to B$ is an injective flat homomorphism of regular domains, then the image of D in $B \otimes_A R$ is a completely stable big test element for $B \otimes_A R$.

Proof. It follows from the Lemma above and the Theorem on p. 5 of the Lecture Notes of November 14 that $DR^{1/q} \subseteq R[A^{1/q}]$ for all q, Hence, by the Theorem on p. 4 of the Lecture Notes of November 9, D is a completely stable big test element for R.

The final statement now follows because, by parts (a) and (b) of the Lemma on p. 3 of the Lecture Notes from November 9 and the Proposition at the top of p. 5 of the Lecture Notes from November 14, the hypotheses are preserved by the base change from A to B. □

We next want to show that the Lipman-Sathaye Jacobian Theorem produces test elements in an entirely similar way: it also provides elements that "capture" the normalization of an extension of A and are stable under suitable base change.

Test elements using the Lipman-Sathaye Jacobian Theorem

Until further notice, A denotes a Noetherian domain with fraction field $\mathcal{K}$, and R denotes an algebra essentially of finite type over A such that R is torsion-free and *generically étale* over A, by which we mean that $\mathcal{T} = \mathcal{K} \otimes_R S$ is a finite product of finite separable algebraic field extensions of $\mathcal{K}$. Note that $\mathcal{T}$ may also be described as the total quotient ring of S. We shall denote by R' the integral closure of R in $\mathcal{T}$.

We shall write $\mathcal{J}_{R/A}$ for the *Jacobian ideal* of R over A. If R is a finitely generated A-algebra, so that we may think of R as

$$A[X_1, \dots, X_n]/(f_1, \dots, f_h),$$

then $\mathcal{J}_{R/A}$ is the ideal of R generated by the images of the size n minors of the Jacobian matrix $(\partial f_j/\partial x_i)$ under the surjection $A[X] \to R$. This turns out to be independent of the presentation, as we shall show below. Moreover, if $u \in R$, then $\mathcal{J}_{R_u/A} = \mathcal{J}_{R/A}R_u$. From this one sees that when R is essentially of finite type over A and one defines $\mathcal{J}_{S/R}$ by choosing a finitely generated subalgebra R_0 of R such that $R = W^{-1}R_0$ for some multiplicative system W of R_0, if one takes $\mathcal{J}_{R/A}$ to be $\mathcal{J}_{R_0/A}R$, then $\mathcal{J}_{R/A}$ is independent of the choices made. We shall consider the definition in greater detail later. We use Jacobian ideals to state the following result, which we shall use without proof here.

Theorem (Lipman-Sathaye Jacobian theorem). *Let A be regular domain with fraction field $\mathcal{K}$ and let R be an extension algebra essentially of finite type over A such that R is torsion-free and generically étale over A. Let $\mathcal{T} = \mathcal{K} \otimes_A R$ and let R' be the integral closure[1] of R in $\mathcal{L}$. If $\theta \in \mathcal{T}$ is such that $\theta \mathcal{J}_{R'/A} \subseteq R'$ then $\theta \mathcal{J}_{R/A} R' \subseteq R$.*

In particular, we may take $\theta = 1$. Thus, if $c \in \mathcal{J}_{R/A}$, then $cR' \subseteq R$.

In other words, elements of $\mathcal{J}_{R/A}$ "capture" the integral closure of R: as in the case of discriminants, this will enable us to prove the existence of completely stable big test elements.

[1] One can show that R' is module-finite over R.

In constructing test elements, we shall only use the Theorem in the case where R is module-finite over A as well. In this case, we already know from our treatment of discriminants that R' is module-finite over R. The result that R' is module-finite over R in the more general situation is considerably more difficult: see the Theorem at the bottom of p. 1 of the Lecture Notes from October 4 from Math 711, Fall 2006.

The Lipman-Sathaye Theorem is proved in [J. Lipman and A. Sathaye, *Jacobian ideals and a theorem of Briançon-Skoda,* Michigan Math. J. **28** (1981) 199–222], although it is assumed that R is a domain in that paper. The argument works without essential change in the generality stated here. See also [M. Hochster, *Presentation depth and the Lipman-Sathaye Jacobian theorem*, Homology, Homotopy and Applications (International Press, Cambridge, MA) **4** (2002) 295–314] for this and further generalizations. As mentioned earlier, the proof of the Jacobian Theorem is given in the Lecture Notes from Math 711, Fall 2006, especially the Lecture Notes from September 25, 27, and 29, as well as the Lectures of October 2, 4, 6, 9, 11, and 13.

We note that the hypotheses of the Lipman-Sathaye are stable under flat base change.

Proposition. *Let R be essentially of finite type, torsion-free, and generically étale over the regular domain A, and let $A \hookrightarrow B$ be a flat injective homomorphism to a regular domain B. Then $B \otimes_A R$ is essentially of finite type, torsion-free, and generically étale over B.*

Morever, $\mathcal{J}_{(B\otimes_A R)/B} = \mathcal{J}_{R/A}(B \otimes_A R)$.

Proof. The proof that $B \otimes_A R$ is essentially of finite type over B is completely straightforward. The proof that the extension remains generically étale is the same as in the Lemma on p. 3 of the Lecture Notes from Novermber 9. The proof that $B \otimes_A R$ is torsion-free over B needs to be modified slightly. R is a directed union of finitely generated torsion-free A-modules N. Each such N is a submodule of a finitely generated free A-module. Hence, each $B \otimes_A N$ is a submodule of a finitely generated free B-module. Since $B \otimes_A R$ is the directed union of these, it is torsion-free over B.

The proof of the last statement reduces at once to the case where R is finitely generated over A. Suppose that

$$R = A[x_1, \ldots, x_n]/(f_1, \ldots, f_m).$$

Then

$$B \otimes_A R \cong B[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$$

(the ideal in the denominator now an ideal of a larger ring, but it has the same generators). The result is now immediate form the definition. $\square$

Why the Jacobian ideal is well-defined

We next want to explain why the Jacobian ideal is well-defined. We assume first that R is finitely generated over A. Suppose that $R = A[x_1, \ldots, x_n]/I$. To establish independence of the presentation we first show that the Jacobian ideal is independent of the choice of generators for the ideal I. Obviously, it can only increase as we use more generators. By enlarging the set of generators still further we may assume that the new generators are obtained from the orginal ones by operations of two kinds: multiplying one of the original generators by an element of the ring, or adding two of the original generators together. 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 R is 0, it follows that the image of $\nabla(gf)$ in R 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 R. 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.

Now consider two different sets of generators for R over A. 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 $h \in A[X_1, \ldots, X_s]$ 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 $\mathcal{M}$ over a ring R such that the last row is $(0\ 0\ \ldots\ 0\ u)$, where u is a unit of R. Let $\mathcal{M}_0$ be the h by s matrix in the upper left corner of $\mathcal{M}$ obtained by omitting the last row and the last column. Then $I_s(\mathcal{M}_0) = I_{s+1}(\mathcal{M})$.*

Proof. If we expand a size $s+1$ minor with respect to its last column, we get an R-linear combination of size s minors of $\mathcal{M}_0$. Therefore, $I_{s+1}(\mathcal{M}) \subseteq I_s(\mathcal{M}_0)$. To prove the other inclusion, consider any s by s submatrix Δ_0 of $\mathcal{M}_0$. We get an $s+1$ by $s+1$ submatrix Δ of $\mathcal{M}$ by using as well the last row of $\mathcal{M}$ and the appropriate entries from the last column of $\mathcal{M}$. 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 $I_s(\mathcal{M}_0) \subseteq I_{s+1}(\mathcal{M})$. $\square$

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

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 $u \in R$, where u is the image of $h(X_1, \dots, X_s) \in A[X_1, \dots, X_s]$, where we have chosen an A-algebra surjection $A[X_1, \dots, X_s] \twoheadrightarrow R$. 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, $X_{s+1}h(X_1, \dots, X_s) - 1$, 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 $h(X_1, \dots, X_s)$. Since the image of this entry is u and so invertible in $R[u^{-1}]$, the Lemma above shows that the new Jacobian ideal is generated by the original Jacobian ideal. We have proved:

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

If R is essentially of finite type over A, and $R_0 \subseteq R$, $R_1 \subseteq R$ are two finitely generated A-subalgebras such that $R = W_0^{-1}R_0$ and $R = W_1^{-1}R_1$, then $\mathcal{J}_{R_0/A}R = \mathcal{J}_{R_1/A}R$. Thus, we may define $\mathcal{J}_{R/A}$ to be $\mathcal{J}_{R_0/A}R$ for any choice of such an R_0.

To see why $\mathcal{J}_{R_i/A}R$ does not depend on the choice of $i = 0, 1$, first note that each generator of R_1 is in $(R_0)_w$ for some $w \in W_1$. Hence, we can choose $w \in W_1$ such that $R_1 \subseteq (R_0)_w$. Replacing R_0 by $(R_0)_w$ does not affect $\mathcal{J}_{R_0/A}R$, by the Proposition above. Therefore, we can assume that $R_1 \subseteq R_0$. Similarly, we can choose y in W_1 such that each generator of R_0 is in $(R_1)_y$. Then $(R_0)_y = (R_1)_y$ and replacing R_i by $(R_i)_y$ does not affect $\mathcal{J}_{R_i/A}R$. $\square$

We now obtain the existence of test elements.

Theorem (existence of test elements via the Lipman-Sathaye theorem). *Let R be a domain module-finite and generically smooth over the regular domain A of characteristic p. Then every element c of $J = \mathcal{J}(R/A)$ is such that $cR^{1/q} \subseteq A^{1/q}[R]$ for all q, and, in particular, $cR^{\infty} \subseteq A^{\infty}[R]$. Thus, if $c \in J \cap R^{\circ}$, it is a completely stable big test element.*

Moreover, if $A \hookrightarrow B$ is a flat injective homomorphism of A into a regular domain B, the image of c is a completely stable big test element for $B \otimes_A R$.

Proof. Since $A^{1/q}[R] \cong A^{1/q} \otimes_A R$, the image of c is in $\mathcal{J}(A^{1/q}[R]/A^{1/q})$, and so the Lipman-Sathaye theorem implies that c multiplies the normalization S' of $S = A^{1/q}[R]$ into $A^{1/q}[R]$. But $R^{1/q} \subseteq S'$ by the Lemma on p. 1. $\square$

Geometrically reduced K-algebras

Let K be a field, and let R be a K-algebra. For the purpose of this discussion, we do not need to impose any finiteness condition on R.

Proposition. *The following conditions on R are equivalent.*

(1) *For every finite purely inseparable extension L of K, $L \otimes_K R$ is reduced.*

(2) *$K^\infty \otimes_K R$ is reduced, where K^∞ is the perfect closure of K.*

(3) *$\overline{K} \otimes_K R$ is reduced, where $\overline{K}$ is an algebraic closure of K.*

(4) *For some field L containing K^∞, $L \otimes_K R$ is reduced.*

(5) *For every field extension L of K, $L \otimes_K R$ is reduced.*

Proof. If $K \subseteq L \subseteq L'$ are field extensions, then $L' \otimes_K R = L' \otimes_L (L \otimes_K R)$ is free and, in particular, faithfully flat over R. Hence, $L \otimes_K R \subseteq L' \otimes_K R$, and $L \otimes_K R$ is reduced if $L' \otimes_K R$ is reduced. Hence (5) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (4) $\Rightarrow$ (2) $\Rightarrow$ (1), while (1) $\Rightarrow$ (2) because $K^\infty \otimes_K R$ is the directed union of the rings $L \otimes_K R$ as L runs though the subfields of K^∞ that are finite algebraic over R. Thus, it will suffice to show that (2) $\Rightarrow$ (5).

For a fixed field extension L of K, $L \otimes_K R$ is reduced if and only if $L \otimes_K R_0$ is reduced for every finitely generated K-subalgebra R_0 of R. Hence, to prove the equivalence of (2) and (5), it suffices to consider the case where R is finitely generated over K. In either case, R itself is reduced. Let W be the multiplicative system of all nonzerodivisors in R. These are also nonzerodivisors in $L \otimes_K R$, and $W^{-1}(L \otimes_K R) \cong L \otimes_K (W^{-1}R)$. Therefore, in proving the equivalence of (2) and (5), we may replace R by its total quotient ring, which is a product of fields finitely generated as fields over K. Thus, we may assume without loss of generality that R is a field finitely generated over K. In this case, $L \otimes_K R$ is a zero-dimensional Noetherian ring, and so $L \otimes_K R$ is reduced if and only if it is regular, and the result follows from our treatment of geometric regularity: see page 2 of the Lecture Notes from September 19. $\square$

We define R to be *geometrically reduced* over K if it satisfies the equivalent conditions of this Proposition. If R is essentially of finite type over K or if R is Noetherian and L is a finitely generated field extension of K, $L \otimes_K R$ will be Noetherian. Our main interest is in the case where R is finitely generated over K.

The Jacobian ideal of a finitely generated K-algebra

Let R be a finitely generated K-algebra such that the quotient by every minimal prime has dimension d. Suppose that $R = K[x_1, \ldots, x_n]/I$. Then we define the Jacobian ideal $\mathcal{J}_{R/K}$ as the ideal generated by the images of the $n-d$ size minors of the matrix $\big(\partial f_i/\partial x_j\big)$ in R. This ideal is independent of the choice of presentation: the argument is the same as in the treatment of $\mathcal{J}_{R/A}$ on p. 3. If K is algebraically closed, this ideal defines the singular locus. We give the argument.

Theorem. *Let K be an algebraically closed field. Let R be a finitely generated K-algebra such that the quotient by every minimal prime has dimension d. For a given prime ideal P of R, R_P is regular if and only if P does not contain $\mathcal{J}_{R/K}$.*

Proof. We first consider the case where $P = m$ is maximal. By adjusting the constant terms, we can pick generators for R that are in m. Then we can write $R = K[x_1, \ldots, x_n]/I$ and assume without loss of generality that $m = (x_1, \ldots, x_n)R$. Let $f_1, \ldots, f_m$ generate I. Then R_m is regular if and only if R_m/m^2R_m has K-vector space dimension d. Since R/m^2 is already local, $R/m^2 \cong R_m/m^2R_m$, and $m/m^2 \cong mR_m/m^2R_m$. The K-vector space dimension of m/m^2 is $n-r$, where r is the K-vector space dimension of the K-span V of the linear forms that occur in the f_j: in fact, m/m^2 is the quotient of $Kx_1 + \cdots + Kx_n$ by V. The K-vector space V is isomorphic with the column space of the matrix

$$\left(\frac{\partial f_j}{\partial x_i}\right)\Big|_{(0,\ldots,0)},$$

where the partial derivative entries are evaluated at the origin: the j th column corresponds to the vector of coefficients of the linear form occurring in f_j. Thus, the ring R_m is regular if and only if the evaluated matrix has rank $n-d$: the rank cannot be larger than $n-d$, since R_m has dimension d. This will be the case if and only if some $n-d$ size minor does not vanish at the origin, and this is equivalent to the statement that $\mathcal{J}_{R/K}$ is not contained in m.

In the general case, if P does not contain J, let $f \in J - P$. Choose a maximal ideal of R_f that contains PR_f. The quotient R_f/PR_f is K, and so this maximal ideal corresponds to a maximal ideal m of R containing P and not containing f. Since R_m is regular, so is its localization R_P.

Now suppose that P contains $\mathcal{J}_{R/K}$ but R_P is regular. Then PR_P is generated by height (P) elements, and we can choose $f \in R-P$ such that PR_f is generated by height (P) elements. Choose a maximal ideal of $(R/P)_f$ such that the localization at this maximal ideal is regular. This will correspond to a maximal ideal m of R containing P and not f. Since PR_m is generated by height (P) elements (f is inverted in this ring) and $m(R/P)_m$

is generated by by $\dim\big((R/P)_m\big)$ elements, mR_m is generated by $\dim(R_m)$ elements, and so R_m is regular. But this contradicts $\mathcal{J}_{R/K} \subseteq P \subseteq m$. $\square$

We want to use the Lipman-Sathaye Theorem to produce specific test elements for finitely generated algebras over a field. We need some preliminary results.

Lemma. *Let $X \to Y$ be a morphism of affine varities over an algebraically closed field K such that the image of X is dense in Y. Then the image of every Zariski dense open subset U of X contains a dense Zariski open subset of Y.*

Proof. The morphism corresponds to a map of domains finitely generated over K. If the map has a kernel P, the image of the morphism would be contained in $\mathcal{V}(P)$, a proper closed set. Hence, we have an injection of domains $A \to B$, and B is finitely generated over K and, hence, over A. U contains an open subset of X of the form $X - \mathcal{V}(f)$, where $f \neq 0$, and so we might as well assume that $U = X - \mathcal{V}(f)$. This amounts to replacing B by B_f, which is still finitely generated over A. After localizing A at one element $a \in A - \{0\}$, we have that B_a is a module-finite extension of a polynomial ring C over A_a, by Noether normalization over a domain. Then $\mathrm{Spec}(B_a) \to \mathrm{Spec}(C)$ and $\mathrm{Spec}(C) \to \mathrm{Spec}(A_a)$ are both surjective, so that the image of the morphism contains $Y - \mathcal{V}(a)$. $\square$

Theorem. *Let K be an algebraically closed field and R a finitely generated K-algebra of dimension d. Let $\underline{x} = x_1, \ldots, x_n$ be generators of R over K, and let $\mathrm{GL}(n, K)$ act so that γ replaces these generators by the entries of the column*

$$\gamma \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

We use $\gamma(\underline{x})$ to denote this sequence of n elements of R, which also generates R over K, and use $\gamma_i(\underline{x})$ to denote its i th entry.

(a) *There is a dense Zariski open subset U of $\mathrm{GL}(n, K)$ such that for all $\gamma \in U$, R is module-finite over the ring generated over K by $\gamma_{i_1}(\underline{x}), \ldots, \gamma_{i_d}(\underline{x})$ for every choice of d mutually distinct indices $i_1, \ldots, i_d$ in $\{1, \ldots, n\}$. Moreover, for every choice of the d elements, $\gamma_{i_1}(\underline{x}), \ldots, \gamma_{i_d}(\underline{x})$ are algebraically independent over K.*

(b) *Assume in, addition, that R is reduced, and that the quotient of R by every minimal prime has dimension d. Then there is a dense Zariski open subset U_0 of $\mathrm{GL}(n, K)$ such that, in addition, R is torsion-free and generically étale over the polynomial ring $K[\gamma_{i_1}(\underline{x}), \ldots, \gamma_{i_d}(\underline{x})]$ for every choice of $i_1, \ldots, i_d$ in $\{1, \ldots, n\}$.*

Proof. (a) This is a variant of Noether normalization. It suffices to show that there is a dense Zariski open subset such that R is module-finite over $K[\gamma_1(\underline{x}), \ldots, \gamma_d(\underline{x})]$. By symmetry, we obtain a dense open subset for each of the $\binom{n}{d}$ possible choices of $i_1, \dots, i_d$, and we may intersect them all.

In this paragraph we allow K to be any infinite field, not necessarily algebraically closed. Note that if $n > d$ there is a nontrivial polynomial relation $F(X_1, \dots, X_n)$ on $x_1, \dots, x_n$ over K, i.e., $F(x_1, \dots, x_n) = 0$. Let $\underline{y} = y_1, \dots, y_n$ be the image of $\underline{x}$ under γ. Then $\delta = \gamma^{-1}$ maps $\underline{y}$ to $\underline{x}$, and the elements $\underline{y}$ have the relation $F\bigl(\delta(\underline{Y})\bigr) = 0$. Let $h = \deg(F)$ and let G be the degree $h > 0$ form in F. The key point is that for δ in a dense open set of $\mathrm{GL}(n, K)$ ($\gamma = \delta^{-1}$ will also vary in a dense open set), $G\bigl(\delta(\underline{Y})\bigr)$ will be monic in every Y_i. To see this for, for example, Y_n, it suffices to see that G does not become 0 when we specialize all the Y_j for $j < n$ to 0. But this yields a power of Y_n times the value of G on the nth column of δ, and the polynomial G obviously vanishes only on a proper closed subset of $\mathrm{GL}(n, K)$. Hence, for every j, y_j is integral over the subring generated by the other y_i.

From now on we assume that K itself is algebraically closed. If we enlarge K by adjoining n^2 algebraically indeterminates $t_{ij}^{(1)}$, and let $K_1 = K(t_{ij}^{(1)} : i, j)$, we may carry through the procedure of the preceding paragraph over K_1, letting the matrix $\bigl(t_{ij}^{(1)}\bigr)^{-1}$ act, so that $\delta = \bigl(t_{ij}^{(1)}\bigr)$. It is clear that G does not vanish on the nth column of δ, which is a matrix of indeterminates. Let $\underline{y}^{(1)}$ denote the image of $\underline{x}$.

If $n - 1 > d$, we continue in this way, next adjoining $(n-1)^2$ indeterminates $t_{ij}^{(2)}$ to K_1 to produce a field K_2, and letting the matrix $\bigl(t_{ij}^{(2)}\bigr)^{-1}$ act. This matrix is in $\mathrm{GL}(n-1, K_2)$, but we view it as an element of $\mathrm{GL}(n, K_2)$ by taking its direct sum with a 1×1 identity matrix. Thus, it acts on $\underline{y}^{(1)}$ to produce a new sequence of generators $\underline{y}^{(2)}$ for $K_2 \otimes_K R$ over K_2. We now have that $y_{n-1}^{(2)}$ and $y_n^{(2)}$ are integral over the ring $K_2[y_1^{(2)}, \dots, y_{n-2}^{(2)}]$.

We iterate this procedure to produce a sequence of fields K_h and sets of generators $\underline{y}^{(h)}$, $1 \le h \le n - d$. Once K_h and $\underline{y}^{(h)}$ have been constructed so that $K_h \otimes_K R$ is integral over $K[y_1^h, \dots, y_{n-h}^h]$, we construct the next field and set of generators as follows. Enlarge the field K_h to K_{h+1} by introducing $(n-h+1)^2$ new indeterminates $t_{ij}^{(h+1)}$, view the matrix $\bigl(t_{ij}^{(h+1)}\bigr)^{-1}$, which is *a priori* in $\mathrm{GL}(n-h+1, K_{h+1})$, as an element of $\mathrm{GL}(n, K_{h+1})$ by taking its direct sum with an identity matrix of size $h-1$, and let its inverse act on $\underline{y}^{(h)}$ to produce $\underline{y}^{(h+1)}$. We will then have that $K_{h+1} \otimes_K R$ is integral over $K_{h+1}[y_1^{(h+1)}, \dots, y_{n-h-1}^{(h+1)}]$. Thus, we eventually construct a field K_{n-d} such that $K_{n-d} \otimes_K R$ is module-finite over $K_{n-d}[y_1^{(n-d)}, \dots, y_d^{(n-d)}]$. Let $K[\underline{t}]$ denote the polynomial ring in all the indeterimates $t_{ij}^{(h)}$ that we have adjoined to K in forming K_{n-d}. Thus, K_{n-d} is the fraction field $K(\underline{t})$ of the polynomial ring $K[\underline{t}]$. It follows that each of the original generators x_j satisfies a monic polynomial with coefficients in $K(\underline{t})[y_1^{(n-d)}, \dots, y_d^{(n-d)}]$. We can choose a single polynomial $H = H(\underline{t}) \in K[\underline{t}] - \{0\}$ that is a common denominator for all of the coefficients in $K(\underline{t})$ occurring in these monic equations of integral dependence for the various x_j, and such that all the $y_i^{(h)}$ are elements of $K[\underline{t}][1/H] \otimes_K R$. It follows that $K[\underline{t}][1/H] \otimes_K R$ is module-finite over $K[\underline{t}][1/H][y_1^{(n-d)}, \dots, y_d^{(n-d)}]$.

We want to specialize the variables $t_{ij}^{(h)}$ to elements of K in such a way that, first, the matrices $\bigl(t_{ij}^{(h)}\bigr)$ specialize to invertible matrices, and, second, H does not vanish. Such values of $t_{ij}^{(h)}$ correspond to points over K of the open set in

$$G = \mathrm{GL}(n-d+1,\, K) \times \cdots \times \mathrm{GL}(n,\, K)$$

where H does not vanish. (Here, each $\mathrm{GL}(s,\, K)$ for $s \leq n$ is thought of a subgroup of $\mathrm{GL}(n,\, K)$ by identifying $\eta \in \mathrm{GL}(s,\, K)$ with the direct sum of η and a size $n-s$ identity matrix.) Call this point $(\gamma^{(n-d+1)}, \dots, \gamma^{(n)})$. For any such point, the result of specializing all of the $t_{ij}^{(h)}$ in the equations of integral dependence for the x_j shows that R is module-finite over the ring generated over K by the images of $y_1^{n-d}, \dots, y_d^{n-d}$. These images are the first d coordinates of $\gamma(\underline{x})$, where $\gamma = \gamma^{(n-d+1)} \cdots \gamma^{(n)}$. The map of $G \to \mathrm{GL}(n,\, K)$ is surjective. By the preceding Lemma, the image of $G - \mathcal{V}(H)$ contains a dense open subset U of $\mathrm{GL}(n,\, K)$, which completes the proof of part (a).

(b) Since R has pure dimension d, when it is represented as a finite module over a polynomial ring of dimension d, it must be torsion-free: if there were a torsion element u, Ru would be a submodule of R of dimension strictly smaller than d, and R would have an associated prime Q with $\dim(R/Q) < d$. But R is reduced, so that all associated primes are minimal, and these have quotients of dimension d.

To show that there is an open set U_0 such that R is generically étale over every $K[\gamma_{i_1}(\underline{x}), \dots, \gamma_{i_d}(\underline{x})]$ it suffices to show this for $R/\mathfrak{p}$ for each minimal prime $\mathfrak{p}$ of R: we can then intersect the finitely many open sets for the various minimal primes. Thus, we may assume that R is a domain of dimension d.

We want each d element subset of the image of $x_1, \dots, x_n$, call it $y_1, \dots, y_n$, to be such that R is generically étale over every polynomial ring in the d elements of the chosen subset. It suffices to get such an open set for $y_1, \dots, y_d$: by symmetry, there will be an open set of every d element subset of $y_1, \dots, y_n$, and we may intersect these. This condition is precisely that $y_1, \dots, y_d$ be a separating transcendence basis for the fraction field $\mathcal{L}$ of R over K. The fact that K is algebraically closed implies that $\mathcal{L}$ has some separating transcendence basis over K, by the Theorem on p. 4 of the Lecture Notes from September 19. There are now several ways to argue. To give a specific one, we may apply, for example, Theorem 5.10 (d) of [E. Kunz, *Kähler differentials*, Friedr. Vieweg & Sohn, Braunschweig, 1986], which asserts that a necessary and sufficient condition for $y_1, \dots, y_d$ to be a separating transcendence basis is that the differentials of these elements $dy_1, \dots, dy_d$ in the module of Kähler differentials $\Omega_{\mathcal{L}/K} \cong \mathcal{L}^d$ be a basis for $\Omega_{\mathcal{L}/K}$ as an $\mathcal{L}$-vector space. Since the differentials of the original variables span $\Omega_{\mathcal{L}/K}$ over $\mathcal{L}$, it is clear that the set of elements of $\mathrm{GL}(n,\, K)$ for which all d element subsets of the new variables have differentials that span $\Omega_{\mathcal{L}/K}$ contains a Zariski dense open set. $\square$

Theorem (test elements for affine K-algebras via the Lipman-Sathaye theorem). *Let K be a field of characteristic p and let R be a finitely generated d-dimensional geometrically reduced K-algebra such that the quotient by every minimal prime has dimension d. Then $\mathcal{J}_{R/K}$ is generated by its intersection with R°, and the elements in this intersection are completely stable big test elements for R.*

Proof. Let L be an algebraic closure of K. From the definition, $\mathcal{J}_{R/K}$ expands to give $\mathcal{J}_{(L\otimes_K R)/L}$. Since $L \otimes_K R$ is reduced, its localization at any minimal prime is a field and, in particular, is regular. It follows that $\mathcal{J}_{R/K}$ expands to an ideal of $L \otimes_K R$ that is not contained in any minimal prime of $L \otimes_K R$, and so $\mathcal{J}_{R/K}$ cannot be contained in a minimal prime of R. It follows from the Lemma on p. 10 of the Lecture Notes from September 17 that it is generated by its intersection with R°. To show that the specified elements are completely stable big test elements, it suffices to prove this after making a base change to $L \otimes_K R$, by part (b) of the Proposition at the bottom of p. 8 of the Lecture Notes from September 17. Hence, we may assume without loss of generality that K is algebraically closed.

The calculation of the Jacobian ideal is independent of the choice of indeterminates. We are therefore free to make a linear change of coordinates, which corresponds to choosing an element of $G = GL(n, K) \subseteq K^{n^2}$ to act on the one-forms of $K[x_1, \ldots, x_n]$. For a dense Zariski open set U of $G \subseteq K^{n^2}$, if we make a change of coordinates corresponding to an element $\gamma \in U \subseteq G$ then, for every choice of d of the (new) indeterminates, if A denotes the K-subalgebra of R that these d new indeterminates generate, by parts (a) and (b) of the Theorem above, the two conditions listed below will hold:

(1) R is module-finite over A (and the d chosen indeterminates will then, per force, be algebraically independent) and

(2) R is torsion-free and generically étale over A.

Now suppose that a suitable change of coordinates has been made, and, as above, let A be the ring generated over K by some set of d of the elements x_i. Then the $n-d$ size minors of $(\partial f_j/\partial x_i)$ involving the $n-d$ columns of $(\partial f_j/\partial x_i)$ that correspond to the variables not chosen as generators of A precisely generate $\mathcal{J}_{R/A}$. The result is now immediate from the Theorem on p. 8: as we vary the set of d variables, so that A varies as well, every $n-d$ size minor occurs as a generator of some $\mathcal{J}(R/A)$ $\square$

Math 711: Lecture of November 19, 2007

Summary of Local Cohomology Theory

The following material and more was discussed in seminar but not in class. We give a summary here.

Let I be an ideal of a Noetherian ring R and let M be any R-module, not necessarily finitely generated. We define

$$H^j_I(M) = \varinjlim_t \mathrm{Ext}^j_R(R/I^t,\, M).$$

This is called the i th *local cohomology module of* M *with support in* I.

$$H^0_I(M) = \varinjlim_t \mathrm{Hom}_R(R/I^t,\, M)$$

which may be identified with $\bigcup_t \mathrm{Ann}_M I^t \subseteq M$. Every element of $H^j_I(M)$ is killed by a power of I. Evidently, if M is injective then $H^j_I(M) = 0$ for $j \geq 1$. By a taking a direct limit over t of long exact sequences for Ext, we see that if

$$0 \to M' \to M \to M'' \to 0$$

is exact there is a functorial long exact sequence for local cohomology:

$$0 \to H^0_I(M') \to H^0_I(M) \to H^0_I(M'') \to \cdots \to H^j_I(M') \to H^j_I(M) \to H^j_I(M'') \to \cdots .$$

It follows that $H^j_I(\_)$ is the j th right derived functor of $H^0_I(\_)$. In the definition we may use instead of the ideals I^t any decreasing sequence of ideals cofinal with the powers of I. It follows that if I and J have the same radical, then $H^i_I(M) \cong H^i_J(M)$ for all i.

Theorem. *Let M be a finitely generated module over the Noetherian ring R, and I and ideal of R. Then $H^i_I(M) \neq 0$ for some i if and only if $IM \neq M$, in which case the least integer i such that $H^i_I(M) \neq 0$ is* $\mathrm{depth}_I M$.

Proof. $IM = M$ iff $I + \mathrm{Ann}_R M = R$, and every element of every $H^j_I(M)$ is killed by some power I^N of I and by $\mathrm{Ann}_R M$: their sum must be the unit ideal, and so all the local cohomology vanishes in this case.

Now suppose that $IM \neq M$, so that the depth d is a well-defined integer in $\mathbb{N}$. We use induction on d. If $d = 0$, some nonzero element of M is killed by I, and so $H^0_I(M) \neq 0$. If $d > 0$ choose an element $x \in I$ that is not a zerodivisor on M, and consider the long exact sequence for local cohomology arising from the short exact sequence

$$0 \to M \xrightarrow{x} M \to M/xM \to 0.$$

From the induction hypothesis, $H^j_I(M/xM) = 0$ for $j < d-1$ and $H^{d-1}_I(M/xM) \neq 0$. The long exact sequence therefore yields the injectivity of the map

$$H^{j+1}_I(M) \xrightarrow{x} H^{j+1}_I(M)$$

for $j < d-1$. But every element of $H^{j+1}_I(M)$ is killed by a power of I and, in particular, by a power of x. This implies that $H^{j+1}_I(M) = 0$ for $j < d-1$. Since

$$0 = H^{d-1}_I(M) \to H^{d-1}_I(M/xM) \to H^d_I(M)$$

is exact, $H^{d-1}_I(M/xM)$, which we know from the induction hypothesis is not 0, injects into $H^d_I(M)$. $\square$

If $A^\bullet$ and $B^\bullet$ are two right complexes of R-modules with differentials d and d', the *total tensor product* is the right complex whose n th term is

$$\bigoplus_{i+j=n} A^i \otimes_R B^j$$

and whose differential d'' is such that $d''(a_i \otimes b_j) = d(a_i) \otimes b_j + (-1)^i a_i \otimes d'(b_j)$.

Now let $\underline{f} = f_1, \ldots, f_n$ generate an ideal with the same radical as I. Let $\mathcal{C}^\bullet(\underline{f}^\infty;\, R)$ denote the total tensor product of the complexes $0 \to R \to R_{f_j} \to 0$, which gives a complex of flat R-modules:

$$0 \to R \to \bigoplus_j R_{f_j} \to \bigoplus_{j_1<j_2} R_{f_{j_1}f_{j_2}} \to \cdots \to \bigoplus_{j_1<\cdots<j_t} R_{f_{j_1}\cdots f_{j_t}} \to \cdots \to R_{f_1\cdots f_n} \to 0.$$

The differential restricted to R_g where $g = f_{j_1}\cdots f_{j_t}$ takes u to the direct sum of its images, each with a certain sign, in the rings $R_{gf_{j_{t+1}}}$, where j_{t+1} is distinct from $j_1, \ldots, j_t$.

Let

$$\mathcal{C}^\bullet(\underline{f}^\infty;\, M) = \mathcal{C}^\bullet(\underline{f}^\infty;\, R) \otimes_R M,$$

which looks like this:

$$0 \to M \to \bigoplus_j M_{f_j} \to \bigoplus_{j_1<j_2} M_{f_{j_1}f_{j_2}} \to \cdots \to \bigoplus_{j_1<\cdots<j_t} M_{f_{j_1}\cdots f_{j_t}} \to \cdots \to M_{f_1\cdots f_n} \to 0.$$

We temporarily denote the cohomology of this complex as $\mathcal{H}^\bullet_{\underline{f}}(M)$. It turns out to be the same, functorially, as $H^\bullet_I(M)$. We shall not give a complete argument here but we note several key points. First,

$$\mathcal{H}^0_{\underline{f}}(M) = \mathrm{Ker}\,(M \to \bigoplus_j M_{f_j})$$

is the same as the submodule of M consisting of all elements killed by a power of f_j for every j, and this is easily seen to be the same as $H^0_I(M)$. Second, by tensoring a short exact sequence of modules

$$0 \to M' \to M \to M'' \to 0$$

with the complex $\mathcal{C}^\bullet(\underline{f}^\infty;\, R)$ we get a short exact sequence of complexes. This leads to a functorial long exact sequence for $\mathcal{H}^\bullet_{\underline{f}}(\_)$. These two facts imply an isomorphism of the functors $H^\bullet_I(\_)$ and $\mathcal{H}^\bullet_{\underline{f}}(\_)$ provided that we can show that $\mathcal{H}^j_{\underline{f}}(M) = 0$ for $j \geq 1$ when M is injective. We indicate how the argument goes, but we shall assume some basic facts about the structure of injective modules over Noetherian rings.

First note that if one has a map $R \to S$ and an S-module M, then if $\underline{g}$ is the image of $\underline{f}$ in S, we have $H^\bullet_{\underline{f}}(M) = H^\bullet_{\underline{g}}(M)$. This has an important consequence for local cohomology once we establish that the two theories are the same: see the Corollary below.

Every injective module over a Noetherian ring R is a direct sum of injective hulls $E(R/P)$ for various primes P. $E(R/P)$ is the same as the injective hull of the reisdue class field of the local ring R_P. This, we may assume without loss of generality that $(R,\, m,\, K)$ is local and that M is the injective hull of K. This enables to reduce to the case where M has finite length over R, and then, using the long exact sequence, to the case where $M = K$, since M has a finite filtration such that all the factors are K. Thus, we may assume that $M = K$. The complex $\mathcal{C}^\bullet(\underline{f}^\infty;\, R)$ is then a tensor product of complexs of the the form $0 \to R \to R \to 0$ and $0 \to R \to 0 \to 0$. If we have only the latter the complex has no terms in higher degree, while if there are some of the former we get a cohomogical Koszul complex $\mathcal{K}^\bullet(g_1,\, \ldots\,, g_n; K)$ where at least one $g_j \neq 0$. But then $(g_1,\, \ldots\,, g_n)K = K$ kills all the Koszul cohomology. Thus, we get vanishing of higher cohomology in either case. It follows that $\mathcal{H}^\bullet_{\underline{f}}(\_)$ and $H^\bullet_I(\_)$ are isomorphic functors, and we drop the first notation, except in the proof of the Corollary just below.

Corollary. *If $R \to S$ is a homomorphism of Noetherian rings, M is an S-module, and ${}_RM$ denotes M viewed as an R-module via restriction of scalars, then for every ideal I of R, $H^\bullet_I({}_RM) \cong H^\bullet_{IS}(M)$.*

Proof. Let $f_1,\, \ldots\,, f_n$ generate I, and let $g_1,\, \ldots\,, g_n$ be the images of these elements in S: they generate IS. Then we have

$$H^\bullet_I({}_RM) \cong \mathcal{H}^\bullet_{\underline{f}}({}_RM) \cong \mathcal{H}^\bullet_{\underline{g}}(M) \cong H^\bullet_{IS}(M)\,. \qquad \square$$

We note that the complex $0 \to R \to R_f \to 0$ is isomorphic to the direct limit of the cohomological Koszul complexes $\mathcal{K}^\bullet(f^t; R)$, where the maps between consecutive complexes are given by the identity on the degree 0 copy of R and by multiplication by f on the degree 1 copy of R — note the commutativity of the diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R & \xrightarrow{f^{t+1}} & R & \longrightarrow & 0 \\ & & \mathrm{id}\uparrow & & \uparrow f & & \\ 0 & \longrightarrow & R & \xrightarrow{f^t} & R & \longrightarrow & 0 \end{array}.$$

Tensoring these Koszul complexes together as f runs through $f_1, \ldots, f_n$, we see that

$$\mathcal{C}^\bullet(\underline{f}^\infty;\, M) = \varinjlim_t \mathcal{K}^\bullet(f_1^t, \ldots, f_n^t;\, M).$$

Hence, whenever $f_1, \ldots, f_n$ generate I up to radicals, taking cohomology yields

$$H_I^\bullet(M) \cong \varinjlim_t H^\bullet(f_1^t, \ldots, f_n^t;\, M).$$

When R is a local ring of Krull dimension d and $x_1, \ldots, x_d$ is a system of parameters, this yields

$$H_m^d(R) = \varinjlim_t R/(x_1^t, \ldots, x_d^t)R.$$

Likiewise, for every R-module M,

$$H_m^d(M) = \varinjlim_t M/(x_1^t, \ldots, x_d^t)M \cong H_m^d(R) \otimes_R M.$$

We next recall that when (R, m, K) is a complete local ring and $E = E_R(K)$ is an injective hull of the residue class field (this means that $K \subseteq E$, where E is injective, and every nonzero submodule of E meets K), there is duality between modules with ACC over R and modules with DCC: if M satsifies one of the chain conditions then $M^\vee = \mathrm{Hom}_R(M, E)$ satisfies the other, and the canonical map $M \to M^{\vee\vee}$ is an isomorphism in either case. In particular, when R is complete local, the obvious map $R \to \mathrm{Hom}_R(E, E)$ is an isomorphism. An Artin local ring R with a one-dimensional socle is injective as a module over itself, and, in this case, $E_R(K) = R$. If R is Gorenstein and $x_1, \ldots, x_d$ is a system of parameters, one has that each $R_t = R/(x_1^t, \ldots, x_d^t)R$ is Artin with a one-dimensional socle, and one can show that in this case $E_R(K) \cong H_M^d(R)$. When R is local but not complete, if M has ACC then $M^\vee$ has DCC, and $M^{\vee\vee}$ is canonically isomorphic with $\widehat{M}$. If M has DCC, $M^\vee$ is a module with ACC over $\widehat{R}$, and $M^{\vee\vee}$ is canonically isomorphic with M.

We can make use of this duality theory to gain a deeper underrstanding of the behavior of local cohomology over a Gorenstein local ring.

Theorem (local duality over Gorenstein rings). *Let (R, m, K) be a Gorenstein local ring of Krull dimension d, and let $E = H^d_m(R)$, which is also an injective hull for K. Let M be a finitely generated R-module. Then for every integer j, $H^j_m(M) = \mathrm{Ext}^{d-j}_R(M, R)^\vee$.*

Proof. Let $x_1, \ldots, x_d$ be a system of parameters for R. In the Cohen-Macaulay case, the local cohomology of R vanishes for $i < d$, and so $\mathcal{C}^\bullet(\underline{x}^\infty; R)$, numbered backwards, is a flat resolution of E. Thus,

$$H^j_m(M) \cong \mathrm{Tor}^R_{d-j}(M, E).$$

Let $G_\bullet$ be a projective resoultion of M by finitely generated projective R-modules. Then

$$\mathrm{Ext}^{d-j}_R(M, R)^\vee \cong H^{d-j}\big(\mathrm{Hom}_R(G_\bullet, R), E\big)$$

(since E is injective, $\mathrm{Hom}_R(\_, E)$ commutes with the calculation of cohomology). The functor $\mathrm{Hom}_R\big(\mathrm{Hom}_R(\_, R), E\big)$ is isomorphic with the functor $\_ \otimes E$ when restricted to finitely generated projective modules G. To see this, observe that for every G there is an R-bilinear map $G \times E \to \mathrm{Hom}_R\big(\mathrm{Hom}_R(G, R), E\big)$ that sends (g, u) (where $g \in G$ and $u \in E$) to the map whose value on $f : G \to R$ is $f(g)u$. This map is an isomorphism when $G = R$, and commutes with direct sum, so that it is also an isomorphism when G is finitely generated and free, and, likewise, when G is a direct summand of a finitely generated free module. But then

$$\mathrm{Ext}^{d-j}_R(M, R)^\vee \cong H_{d-j}(G_\bullet \otimes E) \cong \mathrm{Tor}^R_{d-j}(M, E),$$

which is $\cong H^j_m(M)$, as already observed. $\square$

Corollary. *Let M be a finitely generated module over a local ring (R, m, K). Then the modules $H^i_m(M)$ have DCC.*

Proof. The issues are unchanged if we complete R and M. Then R is a homomorphic image of a complete regular local ring, which is Gorenstein. The problem therefore reduces to the case where the ring is Gorenstein. By local duality, $H^i_m(M)$ is the dual of the Noetherian module $\mathrm{Ext}^{n-i}_R(M, R)$, where $n = \dim(R)$. $\square$

The action of the Frobenius endomorphism on local cohomolgy

Let R be a ring of prime characteristic $p > 0$, and let $I = (f_1, \ldots, f_n)R$. Consider the complex $\mathcal{C}^\bullet = \mathcal{C}^\bullet(\underline{f}^\infty; R)$, which is

$$0 \to R \to \bigoplus_j R_{f_j} \to \bigoplus_{j_1<j_2} R_{f_{j_1}f_{j_2}} \to \cdots \to \bigoplus_{j_1<\cdots<j_t} R_{f_{j_1}\cdots f_{j_t}} \to \cdots \to R_{f_1\cdots f_n} \to 0.$$

This complex is a direct sum of rings of the form R_g each of which has a Frobenius endomorphism $F_{R_g} : R_g \to R_g$. Given any homomorphism $h : S \to T$ of rings of prime characteristic $p > 0$, there is a commutative diagram:

$$\begin{array}{ccc} S & \xrightarrow{h} & T \\ {\scriptstyle F_S}\uparrow & & \uparrow{\scriptstyle F_T} \\ S & \xrightarrow{h} & T \end{array}$$

The commutativity of the diagram follows simply because $h(s)^p = h(s^p)$ for all $s \in S$. Since every $\mathcal{C}^i$ is a direct sum of R-algebras, each of which has a Frobenius endomorphism, collectively these endomorphism yield an endomorphism of $\mathcal{C}^i$ that stabilizes every summand and is, at least, $\mathbb{Z}$-linear. This gives an endomorphism of $\mathcal{C}^\bullet$ that commutes with differentials $\delta^i : \mathcal{C}^i \to \mathcal{C}^{i+1}$ in the complex. The point is that the restriction of the differential to a term R_g may be viewed as a map to a product of rings of the form R_{gf}. Each component map is either h or $-h$, where $h : R_g \to R_{gf}$ is the natural localization map, and is a ring homomorphism. The homomorphism h commutes with the actions of the Frobenius endomorphisms, and it follows that $-h$ does as well.

This yields an action of F on the complex and, consequently, on its cohomology, i.e., an action of F on the local cohomology modules $H^i_I(R)$. It is not difficult to verify that this action is independent of the choice of generators for I. This action of F is more than $\mathbb{Z}$-linear. It is easy to check that for all $r \in R$, $F(ru) = r^p F(u)$. This is, in fact, true for the action on $\mathcal{C}^\bullet$ as well as for the action on $H^\bullet_I(R)$.

If $R \to S$ is any ring homomorphism, there is an induced map of complexes

$$\mathcal{C}^\bullet(\underline{f}^\infty;\, R) \to \mathcal{C}^\bullet(\underline{f}^\infty;\, S).$$

It is immediate that the actions of F are compatible with the induced maps of local cohomology, i.e., that the diagrams

$$\begin{array}{ccc} H^i_I(R) & \longrightarrow & H^i_I(S) \\ {\scriptstyle F}\uparrow & & \uparrow{\scriptstyle F} \\ H^i_I(R) & \longrightarrow & H^i_I(S) \end{array}$$

commute.

We now want to use our understanding of local cohomology to prove the Theorem of Huneke and Lyubeznik.

Discussion. We are primarily interested in studying R^+ when $(R,\, m,\, K)$ is a local domain that is a homomorphic image of a Gorenstein ring A. If $\mathcal{M}$ is the inverse image of m in A, we may replace A by $A_{\mathcal{M}}$ and so assume that A is local.

Note, however, that when we take a module-finte extension domain of R, the ring that we obtain is no longer local: it is only semilocal. Therefore, we shall frequently have the hypothesis that R is a semilocal domain that is a module-finite extension of a homomorphic image of a Gorenstein local ring.

Let $(A, \mathfrak{m}, K)$ denote a Gorenstein local ring, $\mathfrak{p}$ a prime ideal of this ring, and R a local domain that is a module-finite extension of $B = A/\mathfrak{p}$. R is semilocal in this situation. The maximal ideals of R are the same as the prime ideals m that lie over $\mathfrak{m}/\mathfrak{p}$, since R/m is a module finite extension of $B/(m \cap B)$, and so R/m has dimension 0 if and only if $B/(m \cap B)$ has dimension 0, which occurs only when $m \cap B$ is the maximal ideal $\mathfrak{m}/\mathfrak{p}$ of B. Note that since A is Gorenstein, it is Cohen-Macaulay, and therefore universally catenary. Hence, so is R. The Jacobson radical $\mathfrak{A}$ of R will be the same as the radical of $\mathfrak{m}R$.

By the dimension formula, which is stated on p. 3 of the Lecture Notes from September 18 for Math 711, Fall 2006, and proved in the Lecture Notes from September 20 from the same course on pp. 3–5, we have that $\text{height}\,(m) = \text{height}\,(\mathfrak{m}/\mathfrak{p})$ for every maximal ideal m of R: thus, the height of every maximal ideal is the same as $\dim(R) = \dim(A/\mathfrak{p})$.

We next observe the following fact:

Proposition. *Let R be a domain and let W be a multiplicative system of R that does not contain 0.*

(a) *If T is an extension domain of $W^{-1}R$ and $u \in T$ is integral over $W^{-1}R$, then there exists $w \in W$ such that wu is integral over R.*

(b) *If T is module-finite (respectviely, integral) extension domain of R then there exists a module-finite (respectively, integral) extension domain S of R within T such that $T = W^{-1}S$.*

(c) *If $W^{-1}(R^+)$ is an absolute integral closure for $W^{-1}R$, i.e., we may write $W^{-1}(R^+) \cong (W^{-1}R)^+$.*

(d) *If I is any ideal of R, $I(W^{-1}R)^+ \cap W^{-1}R = W^{-1}(IR^+ \cap R)$. That is, plus closure commutes with localization.*

Proof. (a) Consider an equation of integral dependence for u on T. We may multiply by a common denominator $w \in W$ for the coefficients that occur to obtain an equation

$$wu^k + r_1u^{k-1} + \cdots + r_iu^{k-i} + \cdots + r_{k-1}u + r_k = 0,$$

where the $r_i \in R$. Multiply by w^{k-1}. The resulting equation can be rewritten as

$$(wu)^k + r_1(wu)^{k-1} + \cdots + w^{i-1}r_i(wu)^{k-i} + \cdots + w^{k-2}r_{k-1}(wu) + w^{k-1}r_k = 0,$$

which shows that wu is integral over R, as required.

(b) If T is module-finite over R, choose a finite set of generators for T over R. In the case where T is integral, choose an arbitrary set of generators for T over R. For each generator t_i, choose $w_i \in W$ such that $w_i t_i$ is integral over R. Let S be the extension of R generated by all the $w_i t_i$.

(c) We have that $W^{-1}R^+$ is integral over $W^{-1}R$ and so can be enlarged to a plus closure T. But each element $u \in T$ is integral over $W^{-1}R$, and so has there exists $w \in W$ such thtat wu is integral over R, which means that $wu \in R^+$. But then $u = w^{-1}(wu) \in W^{-1}R^+$, and it follows that $T = W^{-1}R^+$.

(d) Note that $\supseteq$ is obvious. Now suppose that $u \in I(W^{-1}R)^+ = IW^{-1}(R^+)$ by part (c). Then we can choose $w \in W$ such that $wu \in IR^+$, and the result follows. $\square$

Remark. Part (d) may be paraphrased as asserting that plus closure for ideals commutes with arbitrary localization. I.e., $(IW^{-1}R)^+ = W^{-1}(I^+)$. Here, whenever J is an ideal of a domain S, $J^+ = (JS^+) \cap S$.

Remark: plus closure for modules. If R is a domain we can define the plus closure of $N \subseteq M$ as the set of elements of M that are in $\langle R^+ \otimes_R N\rangle$ in $R^+ \otimes_R M$. It is easy to check that the analogue of (d) holds for modules as well.

We are now ready to begin the proof of the following result.

Theorem (Huneke-Lyubeznik). *Let R be a semilocal domain of prime characteristic $p > 0$ that is a module-finite extension of a homomorphic image of a Gorenstein local ring $(A, \mathfrak{m}, K)$. Let $\mathfrak{A}$ denote the Jacobson radical in R, which is the same as the radical of $\mathfrak{m}R$. Let d be the Krull dimension of R. Then there is a module-finite extension domain S of R such that for all $i < d$, the map $H^i_{\mathfrak{m}R}(R) \to H^i_{\mathfrak{m}S}(S)$ is 0. If $\mathfrak{B}$ denotes the Jacobson radical of S, we may rephrase this by saying that $H^i_{\mathfrak{A}}(R) \to H^i_{\mathfrak{B}}(S)$ is 0 for all $i < d$.*

Proof. Let n denote the Krull dimension of the local Gorenstein ring $(A, \mathfrak{m}, K)$. Since R is a module-finite extension of $A/\mathfrak{p}$, we have that the height of $\mathfrak{p}$ is $n - d$.

Recall from the discussion above that $\mathfrak{A}$ (respectively, $\mathfrak{B}$) is the radical of $\mathfrak{m}R$ (respectively, $\mathfrak{m}S$). This justifies the rephrasing. We may think of the local cohomology modules as $H^i_{\mathfrak{m}}(R)$ and $H^i_{\mathfrak{m}}(S)$.

It suffices to solve the problem for one value of i. The new ring S satisfies the same hypotheses as R. We may therefore repeat the process d times, if needed, to obtain a module-finite extension such that all local cohomology maps to 0: once it maps to 0 for a given S, it also maps to 0 for any further module-finite extension. In the remainder of the proof, i is fixed.

It follows from local duality over A that is suffices to choose a module-finite extension S of R such that the map

$$(*) \quad \mathrm{Ext}^{n-i}_A(S, A) \to \mathrm{Ext}^{n-i}_A(R, A)$$

is 0, since the map of local cohomology is the dual of this map. Note that both of the modules in $(*)$ are finitely generated as A-modules. We shall use induction on $\dim(R)$ to reduce to the case where the image of the map has finite length over A: we then prove a theorem to handle that case. Let V_S denote the image of the map.

Let $P_1, \dots, P_h$ denote the associated primes over A of the image of this map that are not the maximal ideal of A. Note that as S is taken successively larger, the image V_S cannot increase. Also note that since since V_S is a submodule of $N = \mathrm{Ext}_A^{n-i}(R, A)$, any associated prime of V_S is an associated prime of N. We show that for each P_i, we can choose a module-finite extension S_i of R such that P is not an associated prime of V_{S_i}. This will remain true when we enlarge S_i further. By taking S so large that it contains all the S_i, we obtain V_S which, if it is not 0, can only have the associated prime $\mathfrak{m}$. This implies that V_S has finite length over A, as required.

We write P for P_i. Let $W = A - P$. Then $W^{-1}R = R_P$ is module-finite over the Gorenstein local ring A_P. Let P have height s in A, where $s < n$. By local duality over A_P, we have that the dual of $\mathrm{Ext}_{A_P}^{n-i}(M_P, A_P)$ is, functorially, $H_{PA_P}^{s-(n-i)}(M_P)$ for every finitely generated A-module M. Since $i < d$,

$$s - (n - i) < s - (n - d) = s - \mathrm{height}\,(\mathfrak{p}) = s - \mathrm{height}\,(\mathfrak{p}A_P) = \dim\,(A_P/\mathfrak{p}A_P).$$

By the induction hypothesis we can choose a module-finite extension T of R_P such that

$$H_{PA_P}^{s-(n-i)}(T) \to H_{PA_P}^{s-(n-i)}(R_P)$$

is 0. By part (b) of the Proposition on p. 7, we can choose a module-finite extension S of R such that $T = S_P$. Then we have the dual statement that

$$\mathrm{Ext}_{A_P}^{n-i}(S_P, A_P) \to N_P$$

is 0, which shows that $(V_S)_P = 0$. But then P is not an associated prime of V_S, as required.

Thus, we can choose a module-finite extension S of R such that V_S has finite length as an A-module. Taking duals, we find that the image of $H_{\mathfrak{m}}^i(R) \to H_{\mathfrak{m}}^i(S)$ has finite length as an A-module, Since Frobenius acts on both of these local cohomology modules so that the action is compatible with this map, it follows that the image W of the map is stable under the action of Frobenius. Moreover, W is a finitely generated A-module, and, consequently, a finitely generated S-module. It suffices to show that we can take a further module-finite extension T of S so as to kill the image of W in $H_{\mathfrak{m}}^i(T)$. This follows from the Theorem below. □

Theorem. *Let $I \subseteq S$ be an ideal of a Noetherian domain S of prime characteristic $p > 0$, and let W be a finitely generated submodule of $H_I^i(S)$ that is stable under the action of the Frobenius endomorphism F. Then there is a module-finite extension T of S such that the image of W in $H_I^i(T)$ is 0.*

Notice that there is no restriction on i in this Theorem. We shall, in fact, prove a somewhat stronger fact of this type.

Math 711: Lecture of November 21, 2007

We are aiming to prove the Theorem stated at the bottom of the last page of the Lecture Notes from November 19, which will complete the proof of the Huneke-Lyubeznik Theorem. We first want to make an observation about local cohomology when the ring is not Noetherian, and then we prove a Lemma that does most of the work.

Discussion. Let R be a ring that is not necessarily Noetherian and let I be an ideal of R that is the radical of a finitely generated ideal. Let M be any R-module. We shall still use the notation $H^i_I(M)$ for

$$H^i\bigl(\mathcal{C}^\bullet(\underline{f}^\infty;\, M)\bigr),$$

where $\underline{f} = f_1, \, \ldots \, , f_n$ are elements of R that generate an ideal whose radical is the same as the radical of I. Tht is, we are relaxing the restriction that the base ring be Noetherian.

Note that if R_0 is any subring of R that is finitely generated over the prime ring and contains $f_1, \, \ldots \, , f_n$, then we may view M as an R_0-module, and

$$H^i\bigl(\mathcal{C}^\bullet(\underline{f}^\infty;\, M)\bigr) \cong H^i_{(\underline{f})R_0}(M).$$

If $\underline{g} = g_1, \, \ldots \, , g_s$ is another set of elements generating an ideal whose radical is the same as $Rad(I)$, then every f_i has a power in $(g_1, \, \ldots \, , g_s)R$, say

$$f_i^{h_i} = \sum_{j=1}^{s} r_{ij} g_j$$

and every g_j has a power in $(f_1, \, \ldots \, , f_n)R$, say

$$g_j^{k_j} = \sum_{i=1}^{n} r'_{ji} f_i.$$

These equations will evidnetly hold in any subring R_0 of R finitely generated over the prime ring that is sufficiently large to contain $\underline{f}$, $\underline{g}$ and all of the r_{ij} and r'_{ji}. With such a choice of R_0, we see that $H^i_{(\underline{f})R_0}(M) = H^i_{(\underline{g})R_0}(M)$ for all i. Thus, even when R is not Noetherian, this cohomology is independent of the choice of $\underline{f}$.

However, when R is not Noetherian, we do not have available the result that this is the same cohomology theory one gets using Ext.

Notation: polynommial operators in the Frobenius endomorphism. Let R be a ring of prime characteristic $p > 0$, and let $\mathcal{G} = \mathcal{G}(Z)$ be a monic polynomial in one indeterminate Z with coefficients in R, say

$$\mathcal{G} = Z^e + r_1 Z^{e-1} + \cdots + r_{e-1} Z + r_e.$$

Then we may view

$$\mathcal{G}_F = F^e + \cdots + r_1 F^{e-1} + \cdots + r_{e-1}F + r_e\mathbf{1}$$

as an operator on every R-algebra S whose value on $s \in S$ is

$$s^{p^e} + rs^{p^{e-1}} + \cdots + r_1 s^p + r_0 s.$$

$\mathcal{G}_F$ acts on the complexes $\mathcal{C}^\bullet(\underline{f}^\infty; S)$ just as F does: it stabilizes every component summand S_g, and is value on u is

$$F^e(u) + r_1 F^{e-1}(u) + \cdots + r_{e-1}F(u) + r_0 u.$$

Both F and multiplication by an element r of R act on $\mathcal{C}^\bullet(\underline{f}^\infty;\, S)$ so that:

(1) The action is $\mathbb{Z}$-linear.

(2) The action stabilizes every component summand S_g, where g is a product $f_{i_1} \cdots f_{i_h}$.

(3) The action commutes with the differential.

The operators on the complex with these three properties are closed under addition and composition, from which it follows that $\mathcal{G}_F$ is a $\mathbb{Z}$-linear endomorphism of $\mathcal{C}^\bullet(\underline{f}^\infty;\, S)$ that stabilizes every component summand and commutes with the differential. Hence, this operator also acts on the cohomology of the complex.

Lemma. *Let S be a domain of prime characteristic $p > 0$ and $f_1, \ldots, f_n \in S$. Let $I = (f_1, \ldots, f_h)S$. Let $\mathcal{G} = \mathcal{G}(Z)$ be a monic polynomial in one indeterminate Z with coefficients in S. Let $u \in H^i_I(S)$ be such that $\mathcal{G}_F$ kills u. Then S has a module-finite extension domain T such that the image of u under the map $H^i_I(S) \to H^i_I(T)$ is 0.*

Proof. Let $v \in \mathcal{C}^i(\underline{f}^\infty;\, S)$ be a cycle that represents u. Then $\mathcal{G}_F(v)$ is a coboundary, say $\mathcal{G}_F(v) = \delta(w)$, where δ is the diffferential in the complex. Let w_0 be one component of w: it is an element of a ring of the form S_g. The equation

$$\mathcal{G}_F(Y) - w_0 = 0$$

is monic in Y, and so has a solution in a module-finite extension domain of S_g. By part (b) of the Lemma on p. 7 of the Lecture Notes from November 19, there is a module-finite extension domain T_0 of S such that this equation has a solution in $(T_0)_g$. We can find such a module-finite extension for every component summand of $\mathcal{C}^\bullet(\underline{f}^\infty;\, S)$. Since there are only finitely many, we can find a module-finite extension T_1 of S sufficiently large that there is an element w' of $\mathcal{C}^{i-1}(\underline{f}^\infty;\, T_1)$ such that $\mathcal{G}_F(w') = w$. We then have that

$$\mathcal{G}_F(v) = \delta(w) = \delta\bigl(\mathcal{G}_F(w')\bigr) = \mathcal{G}_F\bigl(\delta(w')\bigr)$$

and so

$$\mathcal{G}_F\bigl(v - \delta(w')\bigr) = 0.$$

It follows that every component of $v - \delta(w')$ is a fraction in some $(T_1)_g$ that satisfies a monic polynomial over T_1. Therefore, we may choose a module-finite extension T of T_1 within its fraction field such that all components of $v' = v - \delta(w')$ are in T. It will now suffice to show that v' is a coboundary in $\mathcal{C}^i(\underline{f}^\infty; T)$.

Each component T_g of the complex $\mathcal{C}^\bullet(\underline{f}^\infty; T)$ contains a copy of T. These copies of T form a subcomplex, and this subcomplex contains v'. It will therefore suffice to show that this subcomplex is exact. But this subcomplex is the complex

$$\mathcal{C}^\bullet(\underline{1}^\infty; T)$$

where $\underline{1}$ denotes a string $1, 1, \ldots, 1$ of n elements all of which are 1. Hence, its cohomology is $H^\bullet_T(T)$, which is killed by T and, consequently, is 0. □

We now restate the Theorem we are trying to prove, in a slightly generalized form, and give the argument. In the earlier version, R and S were the same.

Theorem. *Let $I \subseteq S$ be a finitely generated ideal of a domain S of prime characteristic $p > 0$, let $R \subseteq S$ be a Noetherian ring, and and let M be a finitely generated R-submodule of $H^i_I(S)$ that is stable under the action of the Frobenius endomorphism F on $H^i_I(S)$. Then there is a module-finite extension T of S such that the image of M in $H^i_I(T)$ is 0.*

Proof. Let $u \in M$. Consider the ascending chain of R-submodules of M spanned by the initial segments of the sequence

$$u,\ F(u),\ F^2(u),\ \cdots,\ F^k(u),\ ldots.$$

Since M is Noetherian, these submodules stabilize, and so some $F^e(u)$ is an R-linear combination of its predecessors. This yields an equation

$$F^e(u) + s_1 F^{e-1} u + \cdots + s_e u = 0,$$

where the $s_i \in R$. However, the argument makes no further use of this fact.

We may apply the preceding Lemma with

$$G = Z^e + s_1 Z^{e-1} + \cdots + s_e.$$

This shows that there is a module-finite extension T_0 of S such that u maps to 0 in $H^i_I(T_0)$. We can choose such a module-finite extension for every u_j in a finite set of generators $u_1, \ldots, u_h$ for M over R. We may then choose a module-finite extension T that contains all of these. Then M maps to 0 in $H^i_I(T)$. □

Corollary. *Let R be a semilocal domain of Krull dimension d with Jacobson radical $\mathfrak{A}$ that is module-finite over a Gorenstein local ring. Then $H^i_{\mathfrak{A}}(R^+) = 0$, $0 \le i \le d-1$.*

Proof. $H^i_{\mathfrak{A}}(R^+)$ is the direct limit of the modules $H^i_{\mathfrak{A}}(S)$ as S runs through all module-finite extensions of R. But each $H^i_{\mathfrak{A}}(S)$ maps to 0 in $H^i_{\mathfrak{A}}(T)$ for some further module-finite extension domain T of S, by the Huneke-Lyubeznik Theorem, and so each $H^i_{\mathfrak{A}}(S)$ maps to 0 in $H^i_{\mathfrak{A}}(R^+)$. □

Corollary. *Let (R, m, K) be a local domain of Krull dimension d that is module-finite over a Gorenstein local ring. Then $H^i_m(R^+) = 0$, $0 \le i \le d-1$.* $\square$

Theorem. *Let (R, m, K) be a local domain of Krull dimension d that is module-finite over a Gorenstein local ring. Then R^+ is a big Cohen-Macaulay algebra. That is, every system of parameters for R is a regular sequence in R^+.*

Proof. It is clear that $mR^+ \ne R^+$: since R^+ is integral over R, it has a prime ideal that lies over m.

Let $x_1, \ldots, x_d$ be part of a system of parameters: we must show that it is a regular sequence on R^+. We use induction on $\dim(R)$, and also on d. The result is trivial if $d = 1$, since R^+ is a domain. Assume that $d > 1$ and that we have a counterexample. Then $x_1, \ldots, x_{d-1}$ is a regular sequence but we can choose $u \in R^+$ such that $ux_d \in (x_1, \ldots, x_{d-1})R^+$ while $u \notin (x_1, \ldots, x_{d-1})R^+ = J$. Choose a minimal prime P of R in the support of $(J + Ru)/J$. Then we still have a counterexample when we pass to R_P and $(R_P)^+ \cong (R^+)_P$. By the induction hypothesis we may assume that $P = m$. Then $H^0_m(R^+/J) = 0$.

We can get a contradiction by proving that for every integer h with $0 \le h \le d-1$,

$$H^i_m(R^+/(x_1, \ldots, x_h)R^+) = 0$$

when $x_1, \ldots, x_h$ is part of a system of parameters and $i < d - h$. We then have a contradiction, taking $h = d-1$ in the paragraph just above.

We use induction on h. We already know this when $h = 0$. Now suppose that $S = R^+/(x_1, \ldots, x_h)R^+$ and that we know that $H^i_m(S) = 0$ for $i < d-h$. Let $x = x_{h+1}$. We want to show that $H^i(S/xS) = 0$ for $i < d-h-1$. From the short exact sequence

$$0 \to S \xrightarrow{x\cdot} S \to S/xS \to 0,$$

we obtain a long exact sequence part of which is

$$H^i_m(S) \to H^i_m(S/xS) \to H^{i+1}_m(S).$$

For $i < d-h-1$ we also have $i+1 < d-h$, and so both the leftmost term and the rightmost term vanish, which implies that the middle term vanishes as well, as required. $\square$

We shall next expend a considerable effort proving the following Theorem of K. E. Smith:

Theorem. *Let R be a locally excellent Noetherian domain of prime characteristic $p > 0$, and let $x_1, \ldots, x_d \in R$ be such that $I = (x_1, \ldots, x_d)R$ has height d. Then $I^* = I^+$.*

We give, in outline, the steps of the proof.

(1) Work with a counterexample with d minimum.

(2) Reduce to the case where R is local, normal, and $x_1, \ldots, x_d$ is a system of parameters. This requires the theorem that R^+ is a big Cohen-Macaulay algebra.

(3) Show that if R is normal local excellent domain, $u \in R$, $I \subseteq R$, and $u \in IT$ for a module-finite extension domain T of $\widehat{R}$, then $u \in IS$ for a module-finite extension domain S of R. This permits a reduction to the case where R is complete. This requires a generalization of Artin approximation that may be deduced from a very difficult Theorem of Popescu.

(4) Reduce to the case where R is Gorenstein.

(5) Let $I_t = (x_1^t, \ldots, x_d^t)R$. Consider $\varinjlim_t I_t^*/I_t$, which may be thought of as 0^* in $H_m^d R)$, as well as $\varinjlim_t I_t^+/I_t$, which may be thought of as 0^+ in $H_m^d(R)$. Also consider the respective annihilators J_* and J_+ of these submodules of $H_m^d(R)$. Show that it suffices to prove that $0^*/0^+$ is 0, and that this module is the Matlis dual of J_+/J_*.

(6) Show that J_+/J_* has finite length. This involves proving that J_* is the test ideal for R, and that formation of the test ideal in an excellent Gorenstein local ring commutes with localization. Then use the induction hypothesis: in proper localizations of R at primes, one knows that tight closure of parameter ideals is the same as plus closure.

(7) Once it is known that J_+/J_* has finite length, it follows that $0^*/0^+$ has finite length, and this module may be identified with the image M of 0^* in $H_m^d(R^+)$. It then follows from the Theorem on p. 3 that M is 0, from which the desired result follows.

Needless to say, it will take quite some time to fill in the details.

Math 711: Lecture of November 26, 2007

Étale and pointed étale homomorphisms and a generalization of Artin approximation

Let R be a Noetherian ring. We shall say that $R \to S$ is *étale* if S is essentially of finite type over R, flat, and the fibers are étale field extensions, so that for all $P \in \mathrm{Spec}\,(R)$, $\kappa_P \otimes_R S$ is a finite product of finite separable field extensions of κ_P. An equivalent conditiions is that S is essentially of finite type over R and flat with 0-dimensional geometrically regular fibers. There are many other characterizations: a detailed treatment is given in the Lecture Notes from Math 711, Fall 2004.

A local homomorphism if local rings $(R, m, K) \to (S, \mathfrak{n}, L)$ is called *pointed étale* if it is étale and the induced map of residue class fields $K \to L$ is an isomorphism. There is a structure theorem for pointed étale extensions:

Theorem. *Let (R, m, K) be a local ring. S is a pointed étale extension of R if and only if there is a monic polynomial $f \in R[X]$ in one variable such that the image $\overline{f}$ of f in $K[X]$ has a simple root $\lambda \in K$, and*

$$S \cong \frac{R[X]_{\mathcal{M}}}{(f)},$$

where $\mathcal{M}$ is the kernel of the composite map $R[X] \twoheadrightarrow K[X] \twoheadrightarrow K$ and the right hand surjection is the evaluation map $g(X) \mapsto g(\lambda)$.

If r in R is such that $r \equiv \lambda$ modulo m, then the maximal ideal $\mathcal{M}$ may alternatively be described as $mR[X] + (x - r)R[X]$. Note that the image of the formal derivative f' of the polynomial f with respect to X is inveritble in S: because λ is a simple root of $\overline{f}$, $\overline{f}'(\lambda) \neq 0$, i.e., $f'(r) \in R - m$.

The Theorem above and many other results about the structure of étale, smooth, and umramified homomorphisms may be found in the Lecture Notes from Math 711, Fall 2004.

Here, we shall not use much more than the fact that a pointed étale extension is a localization at a maximal ideal of a module-finite extension. But we do mention a few properties to help give the reader some feeling for what may be expected from such an extension.

Let (R, m, K) be local and let $(S, \mathfrak{n}, L)$ be a pointed étale extension.

(1) S is fatihfully flat over R.

(2) $\mathfrak{n} = mS$, so that the closed fiber is $S/mS = S/\mathfrak{n} = L \cong K$.

(3) There is a unique local R-algebra embedding of S into $\widehat{R}$, and $\widehat{R}$ is also the completion of S.

(4) If R is excellent and normal, so is S.

(5) If $R \to R'$ is local, then $S' = R' \to R' \otimes_R S$ is a pointed étale extension of R'. In particular, for every proper ideal I of R, S/IS is a pointed étale extension of S/I.

Propertiers (1), (2), and (5) are immediate from the Theorem above. The proof of (3) uses Hensel's Lemma, which implies that the factorization $\overline{f} = (X - \lambda)g$, where $x - \lambda$ and g are relatively prime, lifts uniquely to a factorization $f = (x - \rho)G$ over $\widehat{R}$; here, $\rho \in \widehat{R}$. The embedding maps the image of X in S to ρ. Since S is essentially of finite type over R it is excellent, while the normality of S follows, for example, from the normality of $\widehat{R}$, which is faithfully flat over S.

We shall need the following generalization of the Artin approximation theorem.

Theorem. *Let $F_i(Z_1, \dots, Z_n) = 0$, $1 \le i \le k$, be a finite system of polynomial equations with coefficients in an excellent local ring (R, m, K). Let N be a positive integer. Suppose that the equations have a solution $\widehat{z}_1, \dots, \widehat{z}_n$ in $\widehat{R}$. Then they also have a solution $s_1, \dots, s_n$ in a pointed étale extension S of R such that $s_i \equiv \widehat{z}_i$ mod $m^N\widehat{R}$, $0 \le i \le n$.*

If one states the theorem without the congruence condition mod $m^N\widehat{R}$, one can still deduce that condition easily. Let $u_1, \dots, u_t$ be generators of m^N in R. Choose $r_i \in R$ such that $r_i \cong \widehat{z}_i$ mod $m^N\widehat{R}$ for every i. Then the congruence condition can be expressed equationally by introducing auxiliary variables Z_{ij} and auxiliary equations

$$Z_i - r_i - \sum_{j=1}^{t} u_j Z_{ij} = 0$$

for $1 \le i \le n$.

The theorem was first proved by M. Artin in the case of a local ring essentially of finite type over a field or over an excellent DVR, and also in the case of an analytic local ring (i.e., for a quotient of the ring of convergent power series in n variables over the complex numbers — analytic local rings are Henselian). The more general result follows from a theorem of D. Popescu called General Néron Desingularization: for a considerable time there was some disagreement about whether Popescu's argument, which certainly had gaps, was essentially correct. The conflict was resolved in an expository paper by R. Swan which gave all details of a complete and correct proof. Swan's version was based in turn on a paper by T. Ogoma which also gave an exposition of the proof of Popescu's theorem. We refer the reader to [M. Artin, *On the solutions of analytic equations*, Invent. Math. **5** (1968) 277–291], [M. Artin, *Algebraic approximation of structures over complete local rings*, Publ. Math. I.H.E.S. (Paris) 36 (1969) 23–56], [T. Ogoma,*General Néron desingularization based on the idea of Popescu*, J. Algebra **167** (1994) 57–84], [D. Popescu, *General Néron desingularization* Nagoya Math. J. **100** (1985) 97–126], [D. Popescu, *General Néron desingularization and* *approximation*, Nagoya Math. J. **104** (1986) 85–115], and, especially, [Swan, R. G. *Néron-Popescu desingularization*, in Algebra and geometry (Taipei, 1995), 135–192, Lect. Algebra Geom. **2** Int. Press, Cambridge, MA, 1998].

We next want to observe the following:

Lemma. *Let R be a normal Noetherian ring, and let S be the integral closure of R in a finite normal algebraic extension $\mathcal{L}$ of the fraction field $\mathcal{K}$ of R. Then the group $G = Aut(\mathcal{L}/\mathcal{K})$ stabilizes S, fixes R, and acts transitively on the set of prime ideals of S lying over a given prime P of R. If (R, m, K) is local, G acts transitively on the maximal ideals of S.*

Proof. If we replace R by $R^{1/q}$, which is a normal local ring isomorphic with R, for sufficiently large q, and $\mathcal{L}$ by $\mathcal{L}[\mathcal{K}^{1/q}]$, then S is replaced by a ring purely inseparable over S, which will have the same spectrum. Now the extension of fraction fields is separable, and so Galois, and the group of field automorphisms is unaffected. Hence, we may assume without loss of generality that the extension of fraction fields is Galois, and then S is module-finite over R. We may replace R by R_P and so assume that (R, m, K) is local.

G fixes R and therefore stabilizes the set of elements of $\mathcal{L}$ integral over R, which is S. The fixed ring S^G must consist of elements of $\mathcal{K}$ that are integral over R. Since R is normal, $S^G = R$. Let $m_1, \ldots, m_k$ be the maximal ideals of S. They all lie over m. Choose $s \in m_1 - \bigcup_{j=2}^k m_j$. Consider $r = \prod_{g \in G} g(s)$. Since it is fixed by G, it is in R. In fact, it is in $m_1 \cap R = m$. But then, for every i, $r \in m_i$. It follows that at leat one of the elements $g(s)$ is in m_i, since their product is. Since s is contained in exactly one maximal ideal, m_1, of S, and g is an automorphism of S, $g(s)$ is contained in exactly one maximal ideal, $g(m_1)$, of s. But $g(s) \in m_i$, and so we must have that $g(m_1) = m_i$, as required. □

The following result will enable us to reduce the problem of proving that tight closure is the same as plus closure for parameter ideals to the complete case.

Theorem. *Let (R, m, K) be an excellent, normal local ring. Let $u \in R$, and let $x_1, \ldots, x_d$ be generators of an ideal I of R. Suppose that there is a module-finite extension domain T of $\widehat{R}$ such that $u \in IT$. Then there is a module-finite extension domain S of R such that $u \in IS$.*

Proof. It suffices to construct a module-finite extension S_1 of R such that $u \in IS_1$. We may then get a domain S by killing a minimal prime of S_1 disjoint from $R - \{\{0\}$.

The idea of the argument is to encode the problem of giving a module-finite extension T of a ring R_1 with $R \subseteq R_1 \subseteq \widehat{R}$ such that $u \in IT$ into solving a finite system of polynomial equations in finitely many variables with coefficients in R (but whose solutions we think of as in R_1). Once we have such a system, from the fact that the equations have a solution in $\widehat{R}$, we can deduce that they have a solution in a pointed étale extension of R. We then need to do some further work to show that R itself has a module-finite extension S such that $u \in IS$.

Fix generators for the module-finite extension T of R_1: call them $\theta_1, \ldots, \theta_h$. We choose h from the module-finite extension domain of $\widehat{R}$ such that u is in the expansion of I. We may assume without loss of generality that θ_1 is taken to be 1. The structure of T as a module-finite R_1-algebra, the fact that $u \in IT$, and the condition that T is an extension of R_1 provided that R_1 is a domain are consequences of the equational conditions described in the following seven paragraphs.

(1) We keep track of the relations on the θ_k over R_1: think of these as given by an $h \times s$ unknowns $\bigl(Z_{ij}\bigr)$. The values z_{ij} of these coefficients determine the structure of T as an R_1-module: we assume that $\sum_i z_{ij}\theta_i = 0$ for every j, so that the module is the cokernel of the matrix $\bigl(z_{ij}\bigr)$.

(2) For each θ_i and θ_j, we keep track of the coefficients needed to write $\theta_i\theta_j$ as an R_1-linear combination of $\theta_1, \ldots, \theta_h$. Specifically,

$$(\#) \quad \theta_i\theta_j = \sum_{k=1}^{h} z_{ijk}\theta_k.$$

Think of the Z_{ijk} as h^3 additional unknowns whose values z_{ijk} determine the multiplication.

(3) We require that $Z_{ijk} = Z_{jik}$ for all i, j, so that the multiplication will be commutative, and that $Z_{1ik} = Z_{1ki}$ be 1 if $i = k$ and 0 otherwise, which will imply the θ_1 will be the identity element.

(4) In order for the multiplication to be well-defined, we also need equations which assert that for every column of the matrix of relations on $\theta_1, \ldots, \theta_h$, when we multiply the relation the column gives by θ_ν, and then rewrite each $\theta_\nu\theta_k$ as a linear combination of $\theta_1, \ldots, \theta_1 k$ using the equations (#) displayed in (2), the resulting linear combination of $\theta_1, \ldots, \theta_h$ is 0, i.e., the vector of coefficients is in the column space of the matrix of relations. It should be clear that we can formulate a system of equations in auxiliary variables which does exactly this. Solving the equations we have specified so far in an R-algebra R_1 gives just the information we need to construct a symmetric R_1-bilinear form (i.e., a multiplication) from the cokernel of the relation matrix, call it T, to T, such that $\theta_1, \ldots, \theta_h$ is a set of generators for T and θ_1 is an identity element.

(5) We next want to address the problem of using equational conditions to guarantee that we have an associative multiplication. We can use the values of the Z_{ijk} in (2) to work out $(\theta_\mu\theta_\nu)\theta_\rho$. We first use the equations given in (2) to write $\theta_\mu\theta_\nu$ as a linear combination of the θ_k. We then multiply by θ_ρ and use several applications of the equations in (2) to write this as a linear combination of the θ_k. We proceed similarly to expand $\theta_\mu(\theta_\nu\theta_\rho)$. We get two different expressions, each of which is a linear combination of the θ_k, whose coefficients are polynomials in the variables Z_{ijk}. The difference should be a relation on the θ_k. The vector of coefficients from such a difference must therefore be a linear combination of the relations on the θ_k specified in (1). Thus, for each choice of μ, ν, and ρ, we write down equations that represent the difference vector of coefficients described above as a

linear combination, using new unknowns for coefficients, of the column vectors given in (1).

(6) Recall that $x_1, \ldots, x_d$ generate I. The fact that $u \in IT$ can be expressed as follows. Consider $u\theta_1$ minus a linear combination of the θ_k, where each of the coefficients in the subtrahend is a linear combination of $x_1, \ldots, x_d$ with new unknown coefficients. Write the vector of coefficients of the θ_k arising in this difference as an unknown linear combination of the relation vectors from (1) using new unknowns again.

(7) One can express the condition that the map $R_1 \to T$ be injective (in the case where, as here, circumstances are forcing R_1 to be a domain) by requiring that there exist a map $T \to R_1$ whose value on θ_1 (the identity) is not 0. The map is determined by its values on the θ_k. Use new unknowns Z'_k for those values. The Z'_k must satisfy the same relations imposed on the θ_k in (1), which leads to a new system of equations. In the case we are considering, the original solution of the equations will be in $\widehat{R}$ and the new solution in a pointed étale extension of R. We get a linear map from T to $\widehat{R}$ that is nonzero on 1 because T is a finitely generated torsion-free module over $\widehat{R}$: it can be embedded in a finitely generated free $\widehat{R}$-module, the value of 1 will have a nonzero coordinate, and the projection map to $\widehat{R}$ corresponding to this coordinate will be the required map. Suppose that this map has nonzero value z'_1 on 1. Then we can choose N so large that $z'_1 \notin m^N\widehat{R}$. When we apply the generalized Artin approximation theorem, we can require that the value of Z'_1 be congruent to z'_1 modulo $m^N\widehat{R}$.

A module-finite extension domain T of $\widehat{R}$ such that $u \in IT$ gives a solution of the equations and congruence condition specified in (1) – (7) in $\widehat{R}$. By the Artin-Popescu approximation theorem, there is a solution in a pointed étale extension R_1 of R. Then $R_1 \subseteq \widehat{R}$. Since R is excellent and normal, R_1 is excellent and normal. In particular, R_1 is a domain. The solution in R_1 gives a ring S_1 module-finite over R_1 in which $u \in IS_1$. It is an extension ring because there is an R_1-linear map f to R_1 whose value on 1 is not 0. If $c \in R_1^\circ$ were mapped to 0 in S_1, i.e., if $c\theta_1 = 0$, then we would have

$$0 = f(0) = f(c \cdot \theta_1) = cf(\theta_1) = cz'_1 \neq 0,$$

a contradiction.

It is not clear that S_1 is a domain. But we may kill a minimal prime disjoint from $S_1 - \{0\}$ and so we get a module-finite extension domain S_2 of R_1 such that $u \in IS_2$.

Now, S_2 is a domain module-finite over a localization at a maximal ideal of a module-finite extension domain of R. We can replace S_2 by its localization at a maximal ideal. The resulting ring can be obtained as the localization at a maximal ideal m_3 of a module-finite extension domain S_3 of R. There is no harm in replacing S_3 by a larger domain that is integral over it. Choose a finite algebraic field extension $\mathcal{L}$ of $\mathcal{K} = \mathrm{frac}\,(R)$ containing $\mathrm{frac}\,(S_3)$ that is normal. Let S be the integral closure of R in this field. We know that $u \in IS_{\mathcal{M}}$ for a maximal ideal $\mathcal{M}$ of S lying over m_3 in S_3. We claim that $u \in IS$.

To prove this, it suffices to show that it is true after localization at every maximal ideal of S. By the Lemma near the bottom of p. 2, the Galois group G of the extension of fraction fields between R and S acts transitively on the maximal ideals of S, while fixing R. But for every $g \in G$, we have that $u \in IS_g(\mathcal{M})$, since g fixes u and I. $\square$

In consequence, we can extend the Theorem that R^+ is a big Cohen-Macaulay algebra to the excellent case.

Theorem (Hochster-Huneke). *Let R be an excellent semi-local domain of prime characteristic $p > 0$ such that all maximal ideals of R have height $d = \dim(R)$. Let $\mathfrak{A}$ be the Jacobson radical of R, and $x_1, \dots, x_d$ elements of $\mathfrak{A}$ such that $\mathfrak{A} = \mathrm{Rad}\,(x_1, \dots, x_d)$. Then $x_1, \dots, x_d$ is a regular sequence in R^+.*

In particular, if R is an excellent local domain of prime characteristic $p > 0$, then R^+ is a big Cohen-Macaulay algebra for R.

Proof. Suppose that $ux_{k+1} \in (x_1, \dots, x_k)R^+$. We must show that $u \in (x_1, \dots, x_k)R^+$. We may replace R by a module-finite extension domain. Thus, we may assume that $u \in (x_1, \dots, x_k)R$ and that R is normal. If $u \notin (x_1, \dots, x_k)R^+$, this remains true when we localize at a suitable maximal ideal $\mathcal{M}$ of R^+: suppose that $\mathcal{M}$ lies over m in R. Then R_m is a normal excellent local domain, $x_1, \dots, x_d$ is a system of parameters, $ux_{k+1} \in (x_1, \dots, x_k)R$, and $u \notin (x_1, \dots, x_k)R^+$. The completion whR is again a normal local domain in which $x_1, \dots, x_d$ is a system of parameters. Since whR is a homomorphic image of a regular local ring, we know that $\widehat{R}^+$ is a big Cohen-Macaulay algebra for $\widehat{R}$. It follows that there is a module-finite extension domain T of $\widehat{R}$ such that $u \in (x_1, \dots, x_d)T$. We may now apply the preceding Theorem to replace T by a module-finite extension domain S of R. $\square$

We can now begin our treatment of the proof the Theorem stated at the bottom of p. 4 of the Lecture Notes of November 21. We follows the steps listed on p. 5 of those Lecture Notes.

Step 1.. Choose a counterexample in which d is minimum.

Step 2.: reduction to the case where R is excellent, local, normal, of Krull dimension d, and $x_1, \dots, x_d$ is a system of parameters. First, we may replace R by its normalization. $(x_1, \dots, x_d)$ still has height height d, and R^+ does not change. The element u remains in $(x_1, \dots, x_d)^*$ and it is still true that $u \notin (x_1, \dots, x_d)R^+ = \mathfrak{A}$. Choose a minimal prime P in R of the support of $(\mathfrak{A} + Ru)/\mathfrak{A}$. We can replace u by a multiple ru in Ru whose image in $(\mathfrak{A} + Ru)/\mathfrak{A}$ has annihilator P. We still have that $ru \notin \big((x_1, \dots, x_d)R_P\big)^+$, since plus closure commutes with localization. Now R_P is excellent, local, and normal. We have, moreover, $Pu \subseteq (x_1, \dots, x_d)^+$. We claim that P must be a minimal prime of $(x_1, \dots, x_d)$. If not, P is not contained in the union of the minimal primes of $(x_1, \dots, x_d)$. Then we can choose $x_{d+1} \in P$ such that $x_1, \dots, x_d, x_{d+1}$ is part of a system of parameters for R_P. Then $x_{d+1}ru \in (x_1, \dots, x_d)R^+ = f\mathfrak{A}$. Since R^+ is a big Cohen-Macaulay algebra, we have that $ru \in \mathfrak{A}$ after all, a contradiction. Thus, P is a minimal prime of $(x_1, \dots, x_d)R$.

We have now reduced to the case where R is excellent, local, normal, of Krull dimension d, and $x_1, \dots, x_d$ is a system of parameters.

Math 711: Lecture of November 28, 2007

Step 3. Reduction to the complete local case. Now suppose that the result holds for ideals of height k of the form $(x_1, \ldots, x_k)R$ whenever $k < d$. Also suppose that (R, m, K) is a normal excellent local ring of prime characteristic $p > 0$ of dimension d, that $I = (x_1, \ldots, x_d)R$ where $x_1, \ldots, x_d$ is a system of parameters for R, and that $u \in I^* - I^+$. We next want to show that there is a counterexample such that R is also complete. Over $\widehat{R}$, we still have that $u \in (I\widehat{R})^*$. If

$$u \in (I\widehat{R})^+,$$

then there is a module-finite extension domain T of $\widehat{R}$ such that $u \in IT$. By the Theorem at the bottom of p. 3 of the Lecture Notes from November 26, there is also a module-finite extension S of R such that $u \in IS$, a contradiction. Henceforth, we may assume that our minimal counterexample is such that R is complete. $\square$

For the next reduction, we need the following fact.

Lemma. *Let A be a normal domain, and let S be a domain extension of A generated by one element u that is integral over A, so that $S = A[u]$. Let $f = f(X)$ be the minimal polynomial of u over $\mathcal{K} = \mathrm{frac}\,(A)$. Then f has coefficients in A, and $S \cong A[x]/(f)$.*

Proof. Let $\deg(f) = n$. Let $\mathcal{L}$ be a splitting field for f over $\mathcal{K}$. Let g be a monic polynomial over A such that $g(u) = 0$. Then $f|g$ working in $\mathcal{K}[X]$. It follows that every root ρ of f satisfies $g(\rho) = 0$. Hence, all of the roots of f in $\mathcal{L}$ are integral over A. We can write

$$f = \prod_{i=1}^{n}(X - \rho_i)$$

where the ρ_i are the roots of f. The coefficients of f are elementary symmetric functions of $\rho_1, \ldots, \rho_n$, and so are integral over A. Since they are also in $\mathcal{K}$ and A is normal, the coefficients of f are in A, i.e., $f \in A[x]$.

Now suppose that $h \in A[X]$ is any polynomial such that $h(u) = 0$. Then $h|f$ working over $\mathcal{K}[X]$. Because f is monic, we can carry out the division algorithm, dividing h by f and obtaining a remainder of degree strictly less than n, entirely over $A[X]$, and the result will be the same as if we had carried out the dvision algorithm over $\mathcal{K}[X]$. Since the remainder is 0 when we carry out the division over $\mathcal{K}[X]$, the remainder is also 0 when we carry out the division over $A[X]$. Consequently, $h \in fA[X]$. It follows that the kernel of the A-algebra surjection $A[X] \twoheadrightarrow A[u] = S$ such that $X \mapsto u$ is precisely $fA[X]$, and the stated result follows. $\square$

Step 4. Reducction the case where R is complete and Gorenstein. Choose a coeffiicient field K for the complete counterexample R. Then R is module-finite over its subring

$A = K[[x_1, \dots, x_d]]$, which is regular, and, in paritcular, normal. Let $S = A[u]$. A domain module-finite over a complete local domain is again local. In S, we still have that

$$u \in \big((x_1, \dots, x_n)S\big)^*,$$

since this becomes true when we make the module-finite extension to R: cf. Problem 4 of Problem Set #4. Moreover, since R is module-finite over S, we may identify $R^+ = S^+$, so that we still have

$$u \notin (x_1, \dots, x_d)S^+.$$

Thus, S also gives a counterexample. By the preceding Lemma, $S \cong A[X]/f$ where f is monic polynomial. Since u is not a unit, the constant term of f is in the maximal ideal of A. It follows that $S \cong A[[X]]/(f)$ as well. Since $A[[X]]$ is regular, $A[[X]]/(f)$ is Gorenstein. We therefore have a minimal counterexample to the Theorem in which the ring is a complete local Gorenstein domain. □

Remark. Until this point in the proof, we have been concerned with keeping R normal. In doing the reduction just above, normality is typically lost. But the remainder of the proof will be carried through for the Gorenstein case, without any further refernce to or need of normality.

We shall soon carry through an investigation that requires the study of the tight closure of 0 in the injective hull of the residue class field of a Gorenstein local ring (R, m, K), which may also be thought of as the highest nonvanishing local cohomology module of the ring with support in m. We shall therefore digress briefly to study some aspects of the behavior $0^*_{H^d_m(R)}$.

Comparison of finitistic tight closure and tight closure

Let R be a Noetherian ring of prime characteristic $p > 0$. When $N \subseteq M$ are modules that are not necessarily finitely generated, we have a notion of tight closure N^*_M.

There is an alternative notion, $N^{*\mathrm{fg}}_M$, defined as follows:

$$N^{*\mathrm{fg}}_M = \bigcup_{N \subseteq M_0 \subseteq M \text{ with } M_0/N \text{ finitely generated}} N^*_{M_0}.$$

As with tight closure, studying this notion can be reduced to the case where $N = 0$, and in this case

$$0^{*\mathrm{fg}}_M = \bigcup_{M_0 \subseteq M \text{ with } M_0 \text{ finitely generated}} 0^*_{M_0}$$

It is not known whether, under mild conditions on R, these two notions are always the same. There has been particularly great interest in the case where the module M is

Artinian, for reasons that we shall discuss in the sequel. The result that $0^{*\mathrm{fg}}_M = 0^*_M$ is known in the following cases:

(1) $M = H^d_m(R)$, where (R, m, K) is a reduced, equidimensional excellent local ring and $d = \dim(R)$.

(2) R is $\mathbb{N}$-graded with $R_0 = K$ and M is a graded Artinian module.

(3) R is excellent, equidimensional reduced local with an isolated singularity, and M is an arbitrary Artinian module.

(4) (R, m, K) is excellent, local, R_P is Gorenstein if $P \neq m$, and M is the injective hull of the residue class field.

(5) R is excellent local, W is a finitely generated R-module such that W_P has finite injective dimension if $P \neq m$, and M is the Matlis dual of W.

(1) was proved by K. E. Smith, and (2), (3), and (4) by G. Lyubeznik and K. E. Smith. See [G. Lyubeznik and K. E. Smith, *Strong and weak F-regularity are equivalent for graded rings*, Amer. J. Math. **121** (1999), 1279–1290] and [G. Lyubeznik and K. E. Smith, *On the commutation of the test ideal with localization and completion* Trans. Amer. Math. Soc. **353** (2001) 3149–3180]. (5) is a recent result of J. Stubbs in his thesis (University of Michigan, expected May, 2008), whose full results greatly extend (2), (3), and (4), as well as related results in [H. Eltizur, *Tight closure in Artinian modules*, Thesis, University of Michigan, 2003].

We shall prove (1), shortly. We first want to note that the following questions are all open:

Let (R, m, K) be an excellent local reduced ring of prime characteristic $p > 0$.

(a) Does $0^{*\mathrm{fg}}_M = 0^*_M$ in every Artinian R-module M?

(b) Does $0^{*\mathrm{fg}}_E = 0^*_E$ in the injective hull E of the residue class field of R?

(c) If R is weakly F-regular, does $0^{*\mathrm{fg}}_E = 0^*_E$ in the injective hull of the residue class field? Equivalently, if R is weakly F-regular, is $0^*_E = 0$ in the injective hull E of the residue class field?

(d) If R is weakly F-regular, is R strongly F-regular?

Obviously, an affirmative answer to each of (a), (b), or (c) implies an affirmative answer to the next on the list. Note that in (c), the two formulations are equivalent because in a weakly F-regular ring, $0^{*\mathrm{fg}} = 0$ in every module M, since 0 is tightly closed in every finitely generated module.

What is more, (c) and (d) are equivalent, by the Proposition on p. 3 of the Lecture Notes from October 22.

Hence, an affirmative answer to any one of the statements (a), (b), (c) and (d) implies an affirmative answer to all of the questions following it on the list, while affirmative answers for (c) and (d) are equivalent.

Math 711, Fall 2007 **Problem Set #5**
Due: Wednesday, December 12

1. Let K be a field of characteristic $p > 0$ with $p \neq 3$. Let X, Y, and Z be indeterminates over K, and let $R = K[X, Y, Z]/(X^3 + Y^3 + Z^3) = K[x, y, z]$.

(a) Show that R is module-finite, torsion-free, and generically étale over $A = K[x, y]$, and find the discriminant D of R over A with respect to the basis $1, z, z^2$.

(b) Use the Jacobian ideal to show that $(x^2, y^2, z^2) \subseteq \tau_{\mathrm{b}}(R)$.

2. Continue the notation of problem 1. Show that xyz^2 is a socle generator modulo $I = (x^2, y^2)R$. Show that $I^* = (x^2, y^2, xyz^2)R$. Conclude using problem 4. of Problem Set #3 that the test ideal of R is m.

3. Let $x_1, \ldots, x_k$ be part of a system of parameters in an excellent local domain (R, m, K) of prime characteristic $p > 0$, and let $I = (x_1, \ldots, x_k)R$. Prove that for every multiplicative system W in R, $(IW^{-1}R)^* = I^*W^{-1}R$. That is, tight closure commutes with localization for such an ideal I.

4. Let R be a locally excellent domain of prime characteristic $p > 0$ that is a direct summand of every module-finite extension domain. Prove that R is F-rational. In particular, it follows that R is Cohen-Macaulay.

5. Let (R, m, K) be a complete weakly F-regular local ring of Krull dimension d of prime characteristic $p > 0$. Let S be a Noetherian R-algebra such that the height of mS in S is d. Prove that R is a direct summand of S.

6. Let R be an $\mathbb{N}$-graded domain over an algebraically closed field K of prime characteristic $p > 0$, where $R_0 = K$, and let I be an ideal generated by forms of degree $\geq d \geq 1$. Let G be a form of degree d that is not in I. Prove that $G \notin I^*$.

Math 711: Lecture of November 30, 2007

Theorem (K. E. Smith). *Let $(R,\, m,\, K)$ be an excellent, reduced, equidimensional local ring of Krull dimension d, and let $H = H^d_m(R)$. Then $0^*_H = 0^{*\mathrm{fg}}_H$. If $x_1, \, \ldots \, , x_d$ is a system of parameters for R, $I_t = (x_1^t, \, \ldots \, , x_d^t)R$, and $y = x_1 \cdots x_d$, then $y(I_t^*) \subseteq I_{t+1}^*$, and both 0^*_H and $0^{*\mathrm{fg}}_H$ may be thought of as*

$$\varinjlim_t \frac{I_t^*}{I_t},$$

where the map between consecutive terms is induced by multiplication by y on the numerators.

Hence, if $(R,\, m,\, K)$ is an excellent, reduced Gorenstein local ring and E is the injective hull of its residue class field, $0^*_E = 0^{*\mathrm{fg}}_E$.

Proof. Note that $yI_t \subseteq I_{t+1}$, and so $(yI_t)^* \subseteq I^*_{t+1}$. In general, for any ideal J, $y(J^*) \subseteq (yJ)^*$, since if $cj^q \in J^{[q]}$, then $c(yj)^q \subseteq y^q J^{[q]} = (yJ)^{[q]}$. Thus, $y(I_t)^* \subseteq I^*_{t+1}$ for all t.

To prove that $0^*_H = 0^{*\mathrm{fg}}_H$, we need only show $\subseteq$. Let $v \in 0^*_H$. The for some t, v is represented by the class of an element $u \in R$ in R/I_t. We then have that for some $c \in R^\circ$ and for all $q \gg 0$, cv^q is 0 in

$$\mathcal{F}^e(H) \cong \varinjlim_t \frac{R}{(I_t)^{[q]}} \cong H^d_m(R)$$

and this means that for all $q \gg 0$, the element of H represented by the class of cu^q in R/I_{tq} maps to 0 in H. In the generality in which we are working, the maps $R/I_{tq} \to H$ are not necessarily injective. However, this means that for all $q \gg 0$, there exists k_q such that

$$y^{k_q} cu^q \in I_{tq+k_q},$$

and so for all $q \gg 0$,

$$cu^q \in I_{tq+k_q} : y^{k_q}.$$

By the Theorem near the bottom of p. 2 of the Lecture Notes from November 12, the colon ideal on the right is contained in the tight closure of I_{tq}. Note that if $x_1, \, \ldots \, , x_d$ were a regular sequence, this colon ideal would be equal to I_{tq}. Hence, for all $q \gg 0$,

$$cu^q \in I^*_{tq}.$$

We may multiply by a test element $c' \in R^\circ$ to obtain that for all $q \gg 0$,

$$c' cu^q \in I_{tq} = (I_t)^{[q]},$$

and so $u \in I_t^*$. This means that the image of u is in the tight closure of 0 in R/I_t, and hence v is in the tight closure of 0 in the image M of R/I_t in H. Hence, $v \in 0_H^{*\mathrm{fg}}$, as required. We have also established the assertion in the final statement of the first paragraph of the Theorem. The assertion in the second paragraph is immediate. $\square$

Remark. Of course, we have a commutative diagram:

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & \dfrac{R}{I_t} & \xrightarrow{y\cdot} & \dfrac{R}{I_{t+1}} & \longrightarrow & \cdots \; H^d_m(R) \\
 & & \uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & \dfrac{I_t^*}{I_t} & \xrightarrow{y\cdot} & \dfrac{I_{t+1}^*}{I_t} & \longrightarrow & \cdots \; 0^*_{H^d_m(R)}
\end{array}$$

where the vertical arrows are inclusions. Note that if R is Cohen-Macaulay, then all of the arrows, both horizontal and vertical, are inclusions, and so we may think of $0^*_{H^d_m(R)}$ as the ascending union of the modules $\dfrac{I_t^*}{I_t}$. In particular, these remarks apply when R is Gorenstein.

Discussion: the plus closure of 0 in local cohomology. . Let $(R,\, m,\, K)$ be a local domain of prime characteristic $p > 0$, and let $d = \dim(R)$. Let $H = H^d_m(R)$. The 0^+_H is, by definition, the kernel of the map

$$H^d_m(R) \to R^+ \otimes_R H^d_m(R)$$

and the latter is $H^d_m(R^+)$. Let $x_1, \ldots, x_d$ be a system of parameters for R, let $I_t = (x_1^t, \ldots, x_d^t)R$, and let $y = x_1 \cdots x_d$. Then $y(I_t^+) \subseteq (yI_t)^+$ for all t, simply because $y(I_tR^+) = (yI_t)R^+$, and since $yI_t \subseteq I_{t+1}$ we have as well that $y(I_t)^+ \subseteq I_{t+1}^+$. Hence, we can consider

$$\varinjlim_t \frac{I_t^+}{I_t}$$

where the maps are induced by multiplication by y on numerators, and the direct limit is a submodule of $H^d_m(R)$. This submodule is the same as 0^+_H.

To see this, first note that because R^+ is a big Cohen-Macaulay algebra over R, $x_1, \ldots, x_d$ is a regular sequence on R^+, and so the maps in the direct limit system

$$\varinjlim_t \frac{R^+}{I_tR^+}$$

are injective, and each R^+/I_tR^+ injects into $H^d_m(R^+)$. It follows that if $v \in H^d_m(R)$ is represented by the class of $u \in R$ in R/I_t, then v maps to 0 in $H^d_m(R^+)$ if and only if $u \in I_tR^+$ if and only if $u \in I_tR^+ \cap R = I_t^+$, from which the result follows.

Moreover, we have a commutative diagram

$$
\begin{array}{ccccccc}
\cdots & \longrightarrow & \dfrac{R^{+}}{I_tR^{+}} & \xrightarrow{y\cdot} & \dfrac{R^{+}}{I_{t+1}R^{+}} & \longrightarrow & \cdots \; H^d_m(R^{+}) \\
 & & \big\uparrow & & \big\uparrow & & \big\uparrow \\
\cdots & \longrightarrow & \dfrac{R}{I_t} & \xrightarrow{y\cdot} & \dfrac{R}{I_{t+1}} & \longrightarrow & \cdots \; H^d_m(R) \\
 & & \big\uparrow & & \big\uparrow & & \big\uparrow \\
\cdots & \longrightarrow & \dfrac{I_t^*}{I_t} & \xrightarrow{y\cdot} & \dfrac{I_{t+1}^*}{I_t} & \longrightarrow & \cdots \; 0^*_{H^d_m(R)} \\
 & & \big\uparrow & & \big\uparrow & & \big\uparrow \\
\cdots & \longrightarrow & \dfrac{I_t^{+}}{I_t} & \xrightarrow{y\cdot} & \dfrac{I_{t+1}^{+}}{I_t} & \longrightarrow & \cdots \; 0^{+}_{H^d_m(R)}
\end{array}
$$

where the vertical maps, except those to the top row, are injective, and so $0^+_H \subseteq 0^*_H \subseteq H$. It also follows that

$$\frac{0^*_H}{0^+_H} = \varinjlim_t \frac{I_t^*}{I_t^+}$$

for every choice of system of parameters $x_1, \ldots, x_d$ for R.

When R is Cohen-Macaulay and, in particular, when R is Gorenstein, all of the horizontal maps in the commutative diagram just above are injective, as well as the vertical maps other than those to the top row.

Step 5. Reformulation of the problem in terms of $0^*_{H^d_m(R)}/0^+_{H^d_m(R)}$ *and its dual.* In consequence of the discussion above, we can assert the following:

Proposition. *The following three conditions on an excellent Gorenstein domain* (R, m, K) *of prime characteristic* $p > 0$ *of Krull dimension* d *are equivalent.*

(1) *For every system of parameters* $x_1, \ldots, x_d \in m$*, if* $I = (x_1, \ldots, x_d)R$*, then* $I^* = I^+$*.*

(2) *For some system of parameters* $x_1, \ldots, x_d \in m$*, if* $I_t = (x_1^t, \ldots, x_d^t)R$*, then* $I_t^* = I_t^+$ *for all* $t \geq 1$*.*

(3) *If* $H = H^d_m(R)$*, then* $0^*_H/0^+_H = 0$*, i.e.,* $0^*_H = 0^+_H$*.*

Proof. It is obvious that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). We need only show that (3) $\Rightarrow$ (1). Assume (3). If $x_1, \ldots, x_d$ is a system of parameters and I_t is defined as in (2), we may use this system to calculate

$$\frac{0^*_H}{0^+_H} = \varinjlim_t \frac{I_t^*}{I_t^+}.$$

The maps in the direct limit system are all injective. Hence, if $I^* \neq I^+$, we cannot have $0^*_H = 0^+_H$. This contradiction proves that (3) $\Rightarrow$ (1). $\square$

We next note the following easy consequence of Matlis duality.

Proposition. *Let* (R, m, K) *be a local ring, and let* $E = E_R(K)$ *be an injective hull of the residue class field. Let* $\_^\vee$ *denote the functor* $\mathrm{Hom}_R(\_, E)$.

(a) *If* R *is complete, there is a bijective order-reversing correspondence between submodules* $N \subseteq E$ *and ideals of* R *under which* $N \subseteq E$ *corresponds to* $\mathrm{Ann}_R N$ *and* $J \subseteq R$ *corresponds to* $\mathrm{Ann}_E J$. *In particular, if* $N \subseteq E$, $\mathrm{Ann}_E(\mathrm{Ann}_R N) = N$, *and if* $J \subseteq R$, *then* $\mathrm{Ann}_R(\mathrm{Ann}_E J) = J$. N *corresponds to* J *if and only if* N *is the Matlis dual* $(R/J)^\vee$ *of* R/J, *in which case* $N \cong E_{R/J}(K)$.

(b) *Whether* R *is complete or not, if* $J \subseteq R$ *is any ideal,* $\mathrm{Ann}_R(\mathrm{Ann}_J E) = J$.

Proof. (a) Note that if M has ACC or DCC, we have that $\mathrm{Ann}_R(M) \subseteq \mathrm{Ann}_R(M^\vee)$, and $\mathrm{Ann}_R(M^\vee) \subseteq \mathrm{Ann}_R(M^{\vee\vee}) = \mathrm{Ann}_R M$ in turn, since $M^{\vee\vee} \cong M$. Thus, M and $M^\vee$ have the same annihilator.

There is a bijection between injections $N \hookrightarrow E$ and surjections $N^\vee \twoheadleftarrow R$ obtained by applying $\_^\vee$ (this is used in both directions). Thus, $N \hookrightarrow E$ is dual to $R/J \twoheadleftarrow R$ for some ideal of J of R that is uniquely determined by N. Since N and R/J have the same annihilator, $J = \mathrm{Ann}_R N$. The dual of R/J is evidently $\mathrm{Hom}_R(R/J, E) \cong \mathrm{Ann}_E J$.

(b) Let $\mathrm{Ann}_E J = \mathrm{Ann}_E(J\widehat{R})$, and so the annihilator of $\mathrm{Ann}_{\widehat{R}}(\mathrm{Ann}_J E) = J\widehat{R}$. It follows that the annihilator of $\mathrm{Ann}_E J$ in R is $J\widehat{R} \cap R = J$, since whR is faithfully flat over R. □

For the rest of the proof of Theorem that plus closure and tight closure agree for ideals generated by a system of parameters, if R is a complete local Gorenstein domain of prime characteristic $p > 0$ of Krull dimension d, we shall write write $H = H^d_m((R)$, and we shall write J_* for $\mathrm{Ann}_R(0^*_H)$ and J_+ for $\mathrm{Ann}_R(0^+_H)$. We shall see that $J_* = \tau(R) = \tau_{\mathrm{b}}(R)$ in the Gorenstein case. Our objective is to show that $0^*_H = 0^+_H$. We make use of the following fact.

Corollary. *With notation as above,* $0^*_H/0^+_H$ *is the Matlis dual of* J_+/J_*.

Proof. Since R is Gorenstein, $H = E$ is an injective hull for R and we may take the Matlis dual to of a given module M to be $M^\vee = \mathrm{Hom}_R(M, H)$. We have a short exact sequence

$$0 \to 0^+_H \to 0^*_H \to 0^*_H/0^+_H \to 0$$

whose dual is

$$0 \leftarrow R/J_+ \leftarrow R/J_* \leftarrow (0^*_H/0^*_H)^\vee \leftarrow 0.$$

The kernel of the map on the left is evidently J_+/J_*, from which the result follows at once. □

We next want to establish the connection between J_* and the test ideal of R. Part (d) of the result just below was also discussed in the solution of problem 4. in Problem Set #3.

Theorem. *Let R be a reduced Noetherian ring of prime characteristic $p > 0$. Let $E_R(M)$ denote an injective hull of M over R. Note that if m is a maximal ideal, $E_R(R/m) \cong E_{R_m}(R_m/MR_m)$.*

(a) $\tau(R) = \displaystyle\bigcap_{m \in \mathrm{MaxSpec}(R)} \mathrm{Ann}_R(0^{*\mathrm{fg}}_{E_R(R/m)})$.

(b) $\tau_{\mathrm{b}}(R) = \displaystyle\bigcap_{m \in \mathrm{MaxSpec}(R)} \mathrm{Ann}_R(0^{*}_{E_R(R/m)})$.

(c) *Hence, if (R, m, K) is local and $E = E_R(K)$, then $\tau(R) = \mathrm{Ann}_R(0^{*\mathrm{fg}}_E)$ and $\tau_{\mathrm{b}}(R) = \mathrm{Ann}_R(0^*_E)$.*

(d) *If R is local and approximately Gorenstein with I_t a descending sequence of m-primary irreducible ideals cofinal with the powers of m, then*

$$\tau(R) = \bigcap_t I_t :_R I_t^*.$$

(e) *If R is local, excellent, and Gorenstein, then $\tau(R) = \tau_{\mathrm{b}}(R) = \mathrm{Ann}(0^*_H)$, where $H = H^d_m(R)$.*

Proof. Part (c) is just a restatement of (a) and (b) in the local case.

In all of (a), (b), and (d), $\subseteq$ is clear. Suppose that c is in the specified intersection but that we have modules $N \subseteq M$ such that $u \in N^*_M$ and $cu \notin N$, and assume as well that these modules are finitely generated in cases (a) and (d). We are free to replace N with a submodule of M containing N and maximal with respect to not containing cu, and we ma then kill N. The image of cu is then killed by some maximal ideal m of R, and generates a module $V \cong R/m = K$ in a module M that is an essential extension of V. In case (a), M is a finitely generated submodule of $E = E_R(R/m)$, with $u \in 0^*$, and so $u \in 0^{*\mathrm{fg}}_E$, which implies that $cu = 0$, a contradiction. In case (d), M is killed by I_t for some t, and so may be viewed as an essential extension of K over the Gorenstein Artin local ring R/I_t. But then M injects into R/I_t. The image v of u is in the tight closure of 0 in R/I_t, but cv is not 0. If we represent v by an element $r \in R$, we have that $r \in I_t^*$ but that $cr \notin I_t$, a contradiction. Finally, in case (b), M embeds in E, and $u \in 0^*_E$ while $cu \neq 0$, a contradiction.

Part (e) is then immediate from the fact that in the local, excellent, Gorenstein case, $H = E$ and $0^*_E = 0^{*\mathrm{fg}}_E$. $\square$

We shall now complete the proof by showing that J_+/J_* and, hence, $0^*_H/0^+_H$, has finite length in the case of a minimal counterexample, and then applying the Theorem on p. 3 of the Lecture Notes from November 21 on killing finitely generated submodules of local cohomology by making a suitable module-finite extension. A key point is that information about J_+/J_* can be obtained by localizing at a proper prime ideal P of R, which is not directly true for $0^*_H/0^+_H$.

Math 711: Lecture of December 3, 2007

Step 6. Proof that J_+/J_* has finite length when d is minimum. We first prove that the test ideal commutes with localization for a reduced excellent Gorenstein local ring of prime characteristic $p > 0$. In order to do so, we introduce a new notion. Let (R, m, K) be a reduced excellent Gorenstein local ring of prime characteristic $p > 0$. We say that an ideal $J \subseteq R$ is *F-stable* provided that J is the annihilator of a submodule N of $H = H^d_m(R)$ that is stable under the action of F on H. We first note:

Lemma. *Let notation be as above.*

(a) *$J \subseteq R$ is F-stable if and only if for every ideal I of R generated by a system of parameters $x_1, \ldots, x_d$, $(*)$ if $Ju \subseteq I$ then $Ju^p \subseteq I^{[p]}$. Moreover, for J to be F-stable, it suffices that for a single system of parameters $x_1, \ldots, x_d$ for R, with $I_t = (x_1^t, \ldots, x_d^t)R$ we have that $Ju \subseteq I_t$ implies that $Ju^p \subseteq I_t^{[p]}$ for all t.*

(b) *If J is F-stable and P is any prime ideal of R, then JR_P is F-stable.*

(c) *If J is an F-stable ideal of R that contains a nonzerodivisor, then $\tau(R) \subseteq J$.*

Proof. (a) Each element of H is represented by the class v of $u \in R$ in $R/I_t \hookrightarrow H$ for some t. The maps in the direct limit system for H are injective, and so J kills the class of u if and only if $Ju \subseteq I_t$. Then $F(v)$ is represented by v^p in R/I_{pt}, and $I_{pt} = I_t^{[p]}$. It is immediate both that condition $(*)$ for all I_t is necessary and sufficient for J to be F-stable, and since we may choose I to be any ideal generated by a system of parameters, we must have $(*)$ for all parameter ideals.

(b) Let $h = \mathrm{height}\,(P)$ and choose a system of parameters $x_1, \ldots, x_d \in m$ such that $x_1, \ldots, x_h \in P$, and such that the images of $x_1, \ldots, x_h$ form a system of parameters in R_P. It suffices to check that if $u/w \in R_P$, where $u \in R$ and $w \in R - P$, and $J(u/w)^p \in (x_1, \ldots, x_h)R_P$, then $J(u/w) \in (x_1^p, \ldots, x_h^p)R_P$. From the first condition we can choose $w' \in R - P$ such that $w'Ju \subseteq (x_1, \ldots, x_h)R$, and the latter ideal is contained in $(x_1, \ldots, x_h, x_{h+1}^N, \ldots, x_d^N)R$ for all $N \geq 1$. Since J is F-stable, and $J(w'u) \subseteq (x_1, \ldots, x_h, x_{h+1}^N, \ldots, x_d^N)R$, we have that

$$J(w'u)^p \subseteq (x_1^p, \ldots, x_h^p, x_{h+1}^{pN}, \ldots, x_d^{pN})R$$

for all N. Intersecting the ideals on the right as N varies, we obtain that

$$(w')^p Ju^p \subseteq (x_1^p, \ldots, x_h^p),$$

which implies that $J(u/w)^p \in (x_1^p, \ldots, x_h^p)R_P$, as required.

(c) Let $c \in J \cap R^\circ$. Since c kills $N = \mathrm{Ann}_H J$ if $v \in N$ we have that $v^q \in N$ for all e, and so $cv^q = 0$ for all q. It follows that $v \in 0^*_H$. Hence, $N \subseteq 0^*_H$, and so $\tau(R) = \mathrm{Ann}_R 0^*_H \subseteq \mathrm{Ann}(N) = \mathrm{Ann}_R(\mathrm{Ann}_H(J)) = J$. $\square$

We shall need the following fact:

Proposition. *Let (R, m, K) be an excellent reduced equidimensional local ring of prime characteristic $p > 0$, and let $d = \dim(R)$. Let $H = H^d_m(R)$. Then 0^*_H is stable under the action of F. If R is a domain, 0^+_H is stable under the action of F.*

Proof. Let $x_1, \ldots, x_d$ be a system of parameters. The first statement follows from the fact that if $u \in I_t^*$ for some t, then $u^p \in \big((I_t)^{[p]}\big)^*$. In fact, if $u \in I^*$ then $u^p \in (I^{[p]})^*$ in complete generality. The second assertion follows from the fact that if $u \in I_t^+$, then $u^p \in \big(I_t^{[p]}\big)^+$. The corresponding fact for any ideal I in any domain R follows from the fact that the Frobenius endomorphism on R^+ sends u to u^p and IR^+ to $I^{[p]}R^+$ while stabilizing R: hence, $u^p \in I^{[p]}R^+ \cap R$. $\square$

We next note:

Lemma. *Let R be a Noetherian ring of prime characteristic $p > 0$. Let $\mathfrak{A}$ be an ideal whose radical is contained only in maximal ideals of R, and let m be one maximal ideal of R. Then $(\mathfrak{A}R_m)^*$ in R_m is the same as $\mathfrak{A}^*R_m$.*

Proof. It suffices to prove $\subseteq$. Let $m = m_1, \ldots, m_k$ be the maximal ideals of R. If any m_i is also minimal, then $\{m_i\}$ is an isolated point of $\mathrm{Spec}(R)$, and the ring is a product. Every ideal is a product, and tight closure may be calculated separately in each factor. We can reduce to studying a factor where tthere are fewer maximal ideals. Therefore, we may assume that no m_i is minimal.

Then $\mathfrak{A}$ has primary decomposition $\mathfrak{A} = \mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_k$ where $\mathfrak{A}_i$ is primary to m_i. Choose an element w of $\mathfrak{A}_2 \cap \cdots \cap \mathfrak{A}_k$ that is not in P, and not in any minimal prime of the ring.

Now suppose that $u/1 \in (IR_P)^*$ (we may clear denominators to assume the element has this form). By the Proposition on p. 2 of the Lecture Notes from September 17, we can choose $c \in R^\circ$ such that $cu^{[q]}/1 \in (\mathfrak{A}R_m)^{[q]}$ for all $q \gg 0$. Then $(*)\quad wc \in R^\circ \cap (R - m)$, and $c(wu)^q \in \mathfrak{A}^{[q]}$ for all $q \gg 0$. To see this, note that

$$\mathfrak{A}^{[q]} = (\mathfrak{A}_1 \cap \cdots \cap \mathfrak{A}_k)^{[q]} = (\mathfrak{A}_1 \cdots \mathfrak{A}_k)^{[q]}$$

(since the ideals $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ are pairwise comaximal). This becomes $\mathfrak{A}_1^{[q]} \cap \cdots \cap \mathfrak{A}_k^{[q]}$ and, since the ideal m_i is maximal, the ideal $\mathfrak{A}_i^{[q]}$ is primary to m_i. Then cu^q is in the contraction of $(\mathfrak{A}R_m)^{[q]}$ to R, and this is $\mathfrak{A}_1^{[q]}$, while $w^q \in \mathfrak{A}_i^{[q]}$ for $i > 1$. This proves $(*)$, and, hence, $wu \in I^*$ and $u \in W^{-1}I^*$. $\square$

Theorem (K. E. Smith). *Let (R, m, K) be an excellent reduced Gorenstein local ring of prime characteristic $p > 0$. Let P be a prime ideal of R. Then $\tau(R_P) = \tau(R)_P$.*

Proof. We know that both ideals are generated by nonzerodivisors. We first show that $\tau(R)_P \subseteq \tau(R_P)$. Let $c \in \tau(R)$. Let $\mathrm{height}\,(P) = h$ and let $x_1, \ldots, x_h$ be part of a system of parameters for R whose images in R_P give a system of parameters for R_P. Let $\mathfrak{A}_t = (x_1^t, \ldots, x_h^t)R$. By part (d) of the Theorem on p. 5 of the Lecture Notes from November 30, it suffices to show that for every t, $c(\mathfrak{A}_t R_P)^*_{R_P} \subseteq \mathfrak{A}_t R_P$. We claim that $(\mathfrak{A}_t R_P)^* = \mathfrak{A}_t^* R_P$. By Problem 2(a) of Problem Set #3, we can localize at the multiplicative system W which is the complement of the union of the minimal primes of $\mathfrak{A}$, since elements of W are nonzerodivisors on every $\mathfrak{A}^{[q]}$. In the resulting semilocal ring, the expansion of P is maximal, and we may apply the preceding Lemma to obtain that $(\mathfrak{A}_t R_P)^* = \mathfrak{A}_t^* R_P$. But then $c\mathfrak{A}_t^* \subseteq \mathfrak{A}_t$, and so $c(\mathfrak{A}_t R_P)^* = c\mathfrak{A}_t^* R_P \subseteq \mathfrak{A}_t R_P$, as required.

To prove the other direction, let d be the Krull dimension of R and let $H = H^d_m R)$. Then the annihilator of 0^*_H in R is $\tau(R)$. Hence, by the Proposition above, $\tau(R)$ is an F-stable ideal. It follows that $\tau(R)R_P$ is an F-stable ideal of R_P by part (b) of the Lemma on p. 1. It contains a nonzerodivisor, since $\tau(R)$ does. By part (c) of the Lemma on p. 1, $\tau(R_P) \subseteq \tau(R)R_P$. □

We can now prove:

Lemma. *Let (R, m, K) be a complete local Gorenstein domain of Krull dimension d of prime characteristic $p > 0$ such that, for $h < d$, tight closure is the same as plus closure for ideals generated by h elements that are part of a system of parameters. Then J_+/J_* has finite length. Hence, $0^*/0^+$ has finite length.*

Proof. Since J_+/J_* is finitely generated, it suffices to prove that it becomes 0 when we localize at a prime ideal P of R strictly contained in m. Since $J_* = \tau(R)$, we have that $(J_*)_P = J_*R_P = \tau(R_P)$, by the Theorem above. Hence, it suffices to prove that every element of J_+ maps to a test element in R_P. Let $c \in J_+$. Let $h = \text{height}\,(P)$. Let $x_1, \ldots, x_d$ be a system of parameters for R such that $x_1, \ldots, x_h \in P$ and their images in R_P are a system of parameters for R_P. Then it suffices to show that

$$c\big((x_1^t, \ldots, x_h^t)R_P\big)^* \subseteq (x_1^t, \ldots, x_h^t)R_P$$

for all t. We have that

$$\big((x_1^t, \ldots, x_h^t)R_P\big)^* = (x_1^t, \ldots, x_h^t)^* R_P$$

and

$$\big((x_1^t, \ldots, x_h^t)R\big)^* = \big((x_1^t, \ldots, x_h^t)R\big)^+ \subseteq \big((x_1^t, \ldots, x_h^t, x_{h+1}^N, \ldots, x_d^N)R\big)^+$$

for all $N \geq 1$. Since $c \in J_+$, this yields

$$c\big((x_1^t, \ldots, x_h^t)R_P\big)^* \subseteq (x_1^t, \ldots, x_h^t, x_{h+1}^N, \ldots, x_d^N)R$$

for all $N \geq 1$. We may intersect the ideals on the right as N varies to obtain

$$c\big((x_1^t, \ldots, x_h^t)R_P\big)^* \subseteq (x_1^t, \ldots, x_h^t)R,$$

and localizing at P then gives the result that we require. □

Step 7. The dénouement: applying the Theorem on killing local cohomology in a module-finite extension. We can now complete the proof that plus closure is the same as tight closure for parameter ideals. We know that the kernel of the map $H = H^d_m(R) \to H^d_m(R^+)$ is 0^+_H, by the Discussion on p. 2 of the Lecture Notes from November 30. Hence, we may view $M = 0^*_H/0^+_H$ as an R-submodule of $H^d_m(R^+)$. It is stable under F, since this is true for both 0^*_H and 0^+_H in $H^d_m(R)$, by the Proposition at the top of p. 2, and the map $H^d_m(R) \to H^d_m(R^+)$ commutes with the action of F. Hence, by the Theorem on p. 3 of the Lecture Notes of November 21, there is a module finite extension domain T of R^+ such that the map $H^d_m(R^+) \to H^d_m(T)$ kills m. However, R^+ does not have such an extension, unless it is an isomorphism. Hence, M must already be 0 in $H^d_m(R^+)$, which shows that $0^*_H = 0^+_H$. This completes the proof of the Theorem stated at the bottom of p. 4 of the Lecture Notes of November 21, as sketched on p. 5 of those Lecture Notes. □

Characterizing tight closure using solid algebras and big Cohen-Macaulay algebras

We next want to prove the results on characterizing tight closure over complete local domains using solid algebras and big Cohen-Macaulay algebras that were stated on p. 12 of the Lecture Notes of September 7.

We recall that an R-module M over a domain R is *solid* if $\mathrm{Hom}_R(M, R) \neq 0$. That is, there is a nonzero R-linear map $\theta : M \to R$.

Nonzero finitely generated torsion-free modules are solid if and only if they are not torison modules: the quotient by the torsion submodule is finitely generated, nonzero, and torsion free. It can be embedded in a finitely generated free R-module, and one of the coordinate projections will give a nonzero map to R. However,we will be primarily interested in the case where M is an R-algebra. Solidity is much more difficult to understand in this case.

Note that if S is an R-algebra, then S is solid if and only if there is an R-linear module homomorphism $\theta : S \to R$ such that $\theta(1) \neq 0$. For if $\theta_1 : S \to R$ is an R-linear module homomorphism such that $\theta_1(s_0) \neq 0$, we can define θ to be the composition of this map with multiplication by s_0, i.e., define $\theta(s) = \theta(s_0 s)$ for all $s \in S$.

The following is a slight generalization of Problem 1 of Problem Set #1.

Proposition. *Let R be a Noetherian domain of prime characteristic $p > 0$, and let $N \subseteq M$ be R-modules. If $u \in M$ is such that $1 \otimes u \in \langle S \otimes_R N\rangle$ in $S \otimes_R M$, then $u \in N^*_M$.*

Proof. Let $\theta : S \to R$ be an R-linear map such that $\theta(1) = c \neq 0$. Then $u^q \in \langle (S \otimes N)^{[q]}\rangle$ in

$$\mathcal{F}^e_S(S \otimes_R M) \cong S \otimes_R \mathcal{F}^e_R(M),$$

and we may identify $\langle (S \otimes_R N)^{[q]}\rangle$ with $\langle S \otimes_R N^{[q]}\rangle$. Apply $\theta \otimes_R \mathbf{1}_{\mathcal{F}^e(M)}$ to obtain that $cu^q \in N^{[q]}$ in $\mathcal{F}^e_R(M)$ for all q. □

Our objective is to prove a converse for finitely generated modules over complete local domains.

Theorem. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$. Let $N \subseteq M$ be finitely generated R-modules, and let $u \in M$. The following conditions are equivalent.*

(a) $u \in N^*_M$.

(b) *There exists a solid R-algebra S such that $1 \otimes u \in \langle S \otimes_R N \rangle$ in $S \otimes_R M$.*

(c) *There exists a big Cohen-Macaulay R-algebra S such that $1 \otimes u \in \langle S \otimes_R N \rangle$ in $S \otimes_R M$.*

It will be some time before we can prove this. We shall actually prove that there is an R^+-algebra B that is a big Cohen-Macaulay algebra for every module-finite extension R_1 of R within R^+, and the B can be used to test all instances of tight closure in finitely generated modules over such rings R_1.

Before beginning the argument, we want to give quite a different characterization of solid modules over a complete local domain R. In the following result, there is no restriction on the characteristic.

Theorem. *Let (R, m, K) be a complete local domain of Krull dimension d, and let M be any R-module. Then M is solid if and only if $H^d_m(M) \neq 0$.*

Proof. We know that R is a module-finite extension of a regular local ring (A, m_A, K), and for any R-module N, $H^d_m(N) \cong H^d_{m_A}(N)$. First suppose that M is solid, and admits a nonzero map $M \to R$. The long exact sequence for local cohomology yields

$$\cdots \to H^d_{m_A}(M) \to H^d_{m_A}(J) \to 0,$$

where $J \neq (0)$ is some ideal of R, since $H^{d+1}_{m_A}$ vanishes on all A-modules (m_A is generated by d elements). Hence, it suffices to see that $H^d_{m_A}(J) \neq 0$. Since J is a torsion-free A-module, it contains a nonzero free A-submodule, A^h whose quotient is a torsion A-module (take h as large as possible). Then we have $0 \to A^h \to J \to C \to 0$ where C is killed by some element $x \in m_A - \{\{0\}$. Then we also have $J \cong xJ \subseteq A^h \to C' \to 0$, and C' is killed by x since $xA^h \subseteq xJ$. Since C' is a module over A/xA, whose maximal ideal is the radical of an ideal with $d-1$ generators, we have that $H^d_{m_A}(C') = H^d_{m_{A/xA}}(C') = 0$, and so the long exact sequence for local cohomology yields

$$\cdots \to H^d_{m_A}(J) \to H^d_{m_A}(A^h) \to 0.$$

Since $H^d_{m_A}(A^h) \cong H^d_{m_A}(A)^{\oplus h}$ and $H^d_{m_A}(A) \cong E_A(A/m_A) \neq 0$, we have that $H^d_{m_A}(J) \neq 0$ and, hence, $H^d_m(M) \neq 0$, as claimed.

Now suppose that $H^d_m(M) \neq 0$. Let $x_1, \ldots, x_d$ be a system of parameters for A. Let $I_t = (x_1^t, \ldots, x_d^t)A$. Let $E = H^d_{m_A}(A)$, which is also an injective hull for A/m_A over

A. Then $H^d_m(R) = H^d_{m_A}(M) = \varinjlim_t M/I_tM \cong M \otimes_A \varinjlim_t A/I_t \cong M \otimes_A E \neq 0$. Now $\mathrm{Hom}_A(\_\,, E)$ is a faithfully exact functor on A-modules. (To see that it does not vanish on $N \neq 0$, choose a nonzero element $v \in N$. The $Av \cong A/\mathfrak{A}$ for some proper ideal $\mathfrak{A}$, which yields a map $Av \twoheadrightarrow K \hookrightarrow E$. This nonzero map from Av to E extends to N because E is injective over A.) Hence,

$$\mathrm{Hom}_A(M \otimes_A E,\, E) \neq 0.$$

By the adjointness of $\otimes$ and Hom, we have that

$$\mathrm{Hom}_A\big(M,\, \mathrm{Hom}_A(E,\, E)\big) \neq 0,$$

and since A is complete, we have that $\mathrm{Hom}_A(E,\, E) \cong A$. Thus, $\mathrm{Hom}_A(M,\, A) \neq 0$, i.e., M is solid over A.

We have a nonzero A-linear map $\eta : M \to A$. Exactly as in the argument that begins near the bottom of p. 1 in the Lecture Notes from November 14, we have an induced map $\eta_* : \mathrm{Hom}_A(R,\, M) \to \mathrm{Hom}_A(R, A)$, and $\mathrm{Hom}_A(R,\, A)$ is a torsion-free R-module of rank one and, hence, isomorphic with a nonzero ideal $J \subseteq R$. As in the Lecture Notes from November 14, we consequenctly have a composite R-module map

$$M \xrightarrow{\mu} \mathrm{Hom}_A(R,\, M) \xrightarrow{\eta_*} \mathrm{Hom}_A(R,\, A) \xrightarrow{\cong} J \xrightarrow{\subseteq} R$$

where the first map μ is the map that takes $u \in M$ to the map $f_u : R \to M$ such that $f_u(r) = ru$ for all $r \in R$. Call the composite map θ. Let $v \in M$ be such that $\eta(v) \neq 0$. Then $\theta(v) \in R$ is the image under an injection of a map $g : R \to A$ whose value on 1 is $\eta(v) \neq 0$, and so $\theta(v) \neq 0$ and, hence, $\theta \neq 0$. $\square$

Remark. The argument in the last paragraph shows that, in general, if R is a domain that is a module-finite extension of A and M is an R-module that is solid when viewed as an A-module, then M is also solid as an R-module.

Math 711: Lecture of December 5, 2007

From the local cohomology criterion for solidity we obtain:

Corollary. *A big Cohen-Macaulay algebra (or module) B over a complete local domain R is solid.*

Proof. Let $d = \dim(R)$ and let $x_1, \dots, x_d$ be a system of parameters for R. This is a regular sequnece on B, and so the maps in the direct limit system

$$B/(x_1, \dots, x_d)B \to \cdots \to B/(x_1^t, \dots, x_d^t)B \to \cdots$$

are injective. Since $0 \neq B/(x_1, \dots, x_d)B \hookrightarrow H^d_{(\underline{x})}(B) = H^d_m(B)$, B is solid. $\square$

Our next objective is to prove:

Theorem. *Let R be a complete local domain. Then there exists an R^+-algebra B such that for every ring R_1 with $R \subseteq R_1 \subseteq R^+$ such that R_1 is module-finite over R the following two conditions hold:*

(1) *B is a big Cohen-Macaulay algebra for R_1.*

(2) *For every pair of finitely generated R_1-modules $N \subseteq M$ and $u \in N^*_M$, $1 \otimes u \in \langle B \otimes_R N\rangle$ in $B \otimes_R M$.*

The proof will take a considerable effort. The basic idea is to construct an algebra B with the required properties by introducing many indeterminates and killing the relations we need to hold. The difficulty will be to prove that in the resulting algebra, we have that $mB \neq B$.

Forcing algebras

Let T ba ring, u an $h \times 1$ column vector over T, and let α be an $h \times k$ matrix over T. Let $Z_1, \dots, Z_k$ be indeterminates over T and let I be the ideal generated by the entries of the matrix

$$u - \alpha \begin{pmatrix} Z_1 \\ \vdots \\ Z_k \end{pmatrix}$$

By the *forcing algebra*, which we denote $\mathfrak{Force}_\sigma(T)$, of the pair $\sigma = (u, \alpha)$ over T we mean the T-algebra $T[Z_1, \dots, Z_k]/I$. In this algebra, we have "forced" u to be a linear combination (the coefficients are the images of the Z_i) of the columns of α. If M is the cokernel of the matrix α, we have that $1 \otimes u = 0$ in $\mathfrak{Force}_\sigma(T) \otimes_T M$. Given any other

T-algebra T' such that $1 \otimes u = 0$ in $T' \otimes M$ (equivalently, such that the image of u is a T'-linear combination of the images of the columns of α), we have a T-homomorphism $\mathfrak{F}\mathtt{orce}_\sigma(T) \to T'$ that sends the Z_i to the corresponding coeffiicients in T' used to express the image of u as a linear combination of the images of the columns of α. We shall say that $\mathfrak{F}\mathtt{orce}_\sigma(T)$ is obtained from T by *forcing* σ.

It will be technically convenient to allow the matrix α to have size $h \times 0$, i.e., to have no columns. In this case, the forcing algebra is formed by killing the entries of u. (Typically, we are forcing u to be in the span of the columns of α. When $k = 0$, the span of the empty set is the 0 submodule in T^h.)

Now suppose that we are given a set Σ of pairs of the form (u, α) where u is a column vector over T and α is a matrix over T whose columns have the same size as u. We call the set Σ *forcing data* for T. The size of u and of the matrix may vary. By the *forcing algebra* $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ we mean the coproduct of the forcing algebras $\mathfrak{F}\mathtt{orce}_\sigma(T)$ as σ varies in T. One way of constructing this coproduct is to adjoin to T one set of appropriately many indeterminates for every $\sigma \in \Sigma$, all mutually algebraically independent over T, and then impose for every σ the same relations needed to form $\mathfrak{F}\mathtt{orce}_\sigma(T)$. If $\Sigma = \{\sigma_1, \dots, \sigma_n\}$ one may think of this algebra as

$$\bigotimes_{i=1}^{n} \mathfrak{F}\mathtt{orce}_{\sigma_i}(T),$$

where the tensor product is taken over T. When Σ is infinite, one may think of $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ as the direct limit of all the forcing algebras for the finite subsets Σ_0 of Σ.

If Σ is forcing data for T and $h : T \to T'$, we may take the image of Σ to get forcing data over T': one is simply applying the homomorphism h to every entry of every column and every matrix. We write $h(\Sigma)$ for the image of Σ under h. Then

$$\mathfrak{F}\mathtt{orce}_{h(\Sigma)}(T') \cong T' \otimes_T \mathfrak{F}\mathtt{orce}_\Sigma(T).$$

We refer to the process of formation of $\mathfrak{F}\mathtt{orce}_{h(\Sigma)}(T')$ as *postponed* forcing: we have, in fact, postponed the formation of the forcing algebra until after mapping to T'.

In discussing forcing algebras we make the following slight generalization of the notations. Suppose that Σ is a set of forcing data over S and $g : S \to T$ is a homomorphism. We shall also write $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ for $\mathfrak{F}\mathtt{orce}_{h(\Sigma)}(T)$. Thus, our notation will not distinguish between forcing and postponed forcing.

Note that if we partition forcing data Σ for T into two sets, we can form a forcing algebra for the first subset, and then form the forcing algebra for the image of the second subset. We *postponed* the forcing process for the second subset. But the algebra obtained in the two step process is isomorphic to $\mathfrak{F}\mathtt{orce}_\Sigma(T)$.

One can also think of the formation of $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ as an infinite process. Well order the set Σ. Now perform forcing for one (u, α) at a time. Take direct limits at limit ordinals. By transfinite recursion, one reaches the same forcing algebra $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ that one gets by doing all the forcing in one step.

Algebra modifications

Let $g : S \to T$ be a ring homomorphism (which may well be the identity map) and let Γ be a a set whose elements are finite sequences of elements of S. We assume that if a sequence is in Γ, then each initial segment of it is also in Γ. Let $\Sigma_{\Gamma,\,g}$ denote the set of pairs $\big(u,\, (x_1 \ \dots \ x_k)\big)$ such that $x_1, \dots, x_{k+1}$ is a sequence in Γ, $u \in T$, and $x_{k+1}u \in (x_1, \dots, x_k)T$. Thus, if $x_1, \dots, x_{k+1}$ were a regular sequence on T, we would have that $u \in (x_1, \dots, x_k)T$. Let Σ be a subset of $\Sigma_{\Gamma,g}$. We call Σ *modification data* for T over Γ. We refer to $\mathfrak{Force}_\Sigma(T)$ as a *multiple algebra modification* of T over Γ. We write $\mathsf{A}lgmod_{\Gamma,g}(T)$ for the forcing algebra $\mathfrak{Force}_{\Sigma_{\Gamma,g}}(T)$ and refer to it as the *total algebra modification* of T over Γ. If σ is one element of $\Sigma_{\Gamma,g}$ we refer to $\mathfrak{Force}_\sigma(T)$ as an *algebra modification* of T. For emphasis, we also refer to it as a *simple* algebra modification of T. We shall use iterated multiple algebra modifications to construct T-algebras on which the specified sequences in Γ become regular sequences.

Note that if $k = 0$ and $x_1 u = 0$ in T, then we get an algebra modification $\mathfrak{Force}_\sigma(T)$ in which σ is a pair consisting of u and a 1×0 matrix: this algebra modification is simply T/uT.

If we have a homomorphism $h : T \to T'$, and $\sigma = \big(u,\, (x_1 \ \dots \ x_k)\big)$, we write $h(\sigma)$ for $\big(h(u),\, (x_1 \ \dots,\ x_k)\big)$. Note that if $x_{k+1}u \in (x_1, \dots, x_k)T$, then

$$x_{k+1}h(u) \in (x_1, \dots, x_k)T'.$$

Thus,

$$h(\Sigma_{\Gamma,g}) \subseteq \Sigma_{\Gamma,h\circ g)}.$$

With this notation, if Σ is algebra modification data for T over Γ, then $h(\Sigma)$ is modification data for T' over Γ.

Algebra modifications are forcing algebras. As in the general case of a forcing algebra, we may talk about postponed modifications.

The construction of big Cohen-Macaulay algebras that capture tight closure

Let (R, m, K) be a complete local domain. Let Γ consist of all sequences in R^+ that are part of a system of parameters in some ring R_1 with $R \subseteq R_1 \subseteq R^+$ such that R_1 is module-finite over R. Let Σ be the set of all pairs (u, α) consisting, for some ring R_1 as above, of an $h \times 1$ column vector over R_1 and an $h \times k$ matrix over a ring R_1 such that u is in the tight closure over R_1 of the column space of α. Note that we know that whether this condition holds is unaffected by replacing R_1 by a larger ring R_2 such that $R_1 \subseteq R_2 \subseteq R^+$ with R_2 module-finite over R.

Let $B_0 = \mathfrak{Force}_\Sigma(R^+)$. If B_n has been defined for $i \geq 0$, let B_{n+1} be the total algebra modification of $\mathbb{A}lgmod_\Gamma(B_n)$ of B_n over Γ. Then we have a direct limit system

$$B_0 \to B_1 \to \cdots \to B_n \to B_{n+1} \to \cdots .$$

Let $B = \varinjlim_n B_n$. We shall prove that B is the required big Cohen-Macaulay algebra.

Much of this is obvious. Suppose that $N \subseteq M$ are finitely generated R_1-modules and $u \in N^*_M$ over R_1. Choose a finite presentation for M/N over R_1, so that $MN/$ is the cokernel of an $h \times k$ matrix αo over R_1. The image of v in M/N is represented by an element $u \in R_1^k$. Then u is in the tight closure of the column space of α in R_1^h, and it follows from the definition of B_0 that u is a linear combination of the columns of α in B_0 and, hence, in B.

It is likewise easy to see that if $x_1, \ldots, x_d$ is a system of parameters in R_1 then it is a regular sequence on B. Suppose that we have a relation

$$x_{k+1}b_{k+1} = \sum_{i=1l}^{k} x_i b_i$$

on B. Because B is the direct limit of the B_n, we can find n_0 such that B_{n_0} contains elements β_i that map to the b_i. The corresponding relation may not hold in B_{n_0}, but since it holds in B it will hold when we map to B_n for some $n \geq n_0$. Thus, we may assume that we have $\beta_1, \ldots, \beta_{k+1} \in B_n$ such that $x_{k+1}\beta_{k+1} = \sum_{i=1}^k x_i\beta_i$ in B_n and every β_i maps to b_i when we map $B_n \to B$. By the construction of B_{n+1}, we have that the image of β_{k+1} is in $(x_1, \ldots, x_k)B_{n+1}$. We can then map to B to obtain that $b_{k+1} \in (x_1, \ldots, x_k)B$.

There remains only one thing to check: that $mB \neq B$. This is the most difficult point in the proof. This is equivalent to the condition that for some (equivalently, every) system of parameters $x_1, \ldots, x_d$ in every R_1, we have that $(x_1, \ldots, x_d)B \neq B$. To see this, observe that if $IB = B$, then $I^2B = IB = B$, and multiplying by I repeatedly yields by induction that $I^tB = B$ for every $t \geq 1$. If m_1 is the maximal ideal of R_1, then $mR_1 \subseteq m_1$, which is contained in a power of mR_1. Hence, $mB = B$ if and only if $m_1B = B$. Likewise, if $x_1, \ldots, x_d$ is a system of parameters for R_1 generating an ideal I, for some t we have $m_1^t \subseteq I \subseteq m_1$, and so $m_1B = B$ if and only if $IB = B$.

If $(x_1, \ldots, x_d)B = B$, then we have that

$$1 = x_1b_1 + \cdots + x_db_d$$

for some finite set of elements of B.

We shall show that if this happens, it happens for some algebra obtained from some choice of R_1 by a finite sequence of forcing algebra extensions: the first extension is the forcing algebra for a single pair (u, α) such that u is in the tight closure of the column space of α over R_1. The extensions after that are simple algebra modifications with respect to sequences each of which is part of a system of parameters for R_1.

Eventually, we shall have to work even harder to make the problem more "finite": specifically, we aim to replace these algebras by finitely generated submodules. We then use characteristic p methods to get a contradiction. However, the first step is to get to the case where we are only performing the forcing procedure finitely many times. With suffiicient thought about the situation, that one can do this is almost obvious, but it is not quite so easy to give the argument formally..

Descent of forcing algebras

Let $g : S \to T$ be a ring homomorphism. Let Λ be a directed poset and let $\{S_\lambda\}_{\lambda\in\Lambda}$ be a directed family of subrings of S indexed by Λ whose union is S. Let $\{T_\lambda\}_{\lambda\in\Lambda}$ be a directed family of rings such that $\varinjlim_\lambda T_\lambda = T$, and suppose that for every $\lambda \in \Lambda$ we have a homomorphism $g_\lambda : S_\lambda \to T_\lambda$ such that if $\lambda \leq \mu$ the diagram

$$\begin{array}{ccc} S & \xrightarrow{g} & T \\ \uparrow & & \uparrow \\ S_\mu & \xrightarrow{g_\mu} & T_\mu \\ \uparrow & & \uparrow \\ S_\lambda & \xrightarrow{g_\lambda} & T_\mu \end{array}$$

commutes. Thus, $g : S \to T$ is the direct limit of the maps $S_\lambda \to T_\lambda$.

Proposition. *Let notation be as above.*

(a) *Let Σ be forcing data over S. Let Σ_λ denote a subset of Σ such that all entries occurring are in S_λ. Suppose also that if $\lambda \leq \mu$ then $\Sigma_\lambda \subseteq \Sigma_\mu$ and that the union of the sets Σ_λ is Σ. Then $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ is a direct limit of rings each of which is obtained from some T_λ by a finite sequence of such extensions of T_λ each of which is obtained from its immediate predecessor by forcing one element of Σ_λ.*

(b) *Let Γ be a family of finite sequences in S closed under taking initial segments, and $\Sigma \subseteq \Sigma_{\Gamma,g}(T)$. Define Σ_λ to consist of all elements of Σ whose entries are in T_λ, whose corresponding sequence is in S_λ, and such that if the sequence is $x_1, \ldots, x_{k+1}$ and the element is $(u, (x_1 \ \ldots \ x_k))$, then $x_{k+1}u \in (x_1, \ldots, x_k)T_\lambda$. Then the algebra modification $\mathfrak{F}\mathtt{orce}_\Sigma(T)$ is a direct limit of rings, each of which is obtained from T_λ by a simple algebra modification over a subset of Γ.*

Proof. (a) Let $\mathcal{L}$ denote the poset each of whose elements is a pair (λ, Φ) where Φ is a finite subset of Σ_λ. The partial ordering is defined by the condition that $(\lambda, \Phi) \leq (\mu, \Psi)$ precisely if $\lambda \leq \mu$ and $\Phi \subseteq \Psi$. There is an obvious map

$$\mathfrak{F}\mathtt{orce}_\Phi(T_\lambda) \to \mathfrak{F}\mathtt{orce}_\Psi(T_\mu).$$

We claim that $\mathfrak{Force}_\Sigma(T)$ is the direct limit over $\mathcal{L}$ of the algebras $\mathfrak{Force}_\Phi(T\lambda)$ with $(\lambda, \Phi) \in \mathcal{L}$. If we fix any finite set Φ if Σ, it is contained in Σ_λ for all sufficiently large λ, and the direct limit of the $\mathfrak{Force}_\Phi(T_\lambda)$ is evidently $\mathfrak{Force}_\Phi(T)$. The result follows from the fact that the direct limit over Φ of the rings $\mathfrak{Force}_\Phi(T)$ is $\mathfrak{Force}_\Sigma(T)$.

(b) Note that a relation involving a sequence in Γ that holds in one T_λ continues to hold in T_μ for all $\mu \geq \lambda$. Also note that if $\sigma \in \Sigma$, then for all sufficiently large λ then entries will be in T_λ, the elements of the corresponding string $(x_1, \ldots, x_{k+1})$ will be in λ, and since one has $x_{k+1}u \in (x_1, \ldots, x_k)T$, this will also hold with T replaced by T_λ for all sufficiently large λ. From this it is clear that $\Sigma_\lambda \leq \Sigma_\mu$ if $\lambda \leq \mu$ and that the union of the Σ_λ is Σ. Moreover, each time we force T_λ with respect to an element of Σ_λ we are performing a simple algebra modification. The result is now immediate from part (a). □

Lemma. *Let (R, m, K) be a complete local domain of prime characteristic $p > 0$, and let B be the R-algbera constructed at the bottom of p. 3 and the top of p. 4. Then B is a direct limit of rings of that are obtained as follows: start with a module-finite extension R_1 of R within R^+, force finitely many elements $\sigma = (u, \alpha)$ where u is in the tight closure of the column space of α over R_1, and then perform finitely many simple algebra modifications with respect to parts of systems of parameters in R_1.*

Proof. We freely use the notations from the bottome of p. 3 and top of p. 4 where B is defined. We apply part (a) of the preceding Proposition, taking $S = T = R^+$. Both are the directed union of rings of the form R_1. It follows that B_0 is a direct limit of rings that are obtained from a module-finite extension R_1 of R within R^+ by forcing finitely many elements $\sigma = (u, \alpha)$ where u is in the tight closure of the column space of α over R_1. By induction on n and part (b) of the preceding Proposition, every B_n is a direct limit of rings of the form described in the statement of the Lemma. This follows for B as well, since B is the direct limit of the B_n.

Since every R_1 is again a complete local domain, to complete the proof of the Theorem stated on p. 1, we might as well change notation and repalce R by R_1. Now, if one has a finite set of instances of tight closure over R, say u_i is in the tight closure of the column space of α_i for $1 \leq i \leq t$, then the direct sum of the u_i is in the tight closure of the column space of the direct sum of the matrices α_i, $1 \leq i \leq t$. Moreover, the forcing algebra for these direct sums is the coproduct of the t individual forcing algebras for the individual instances of tight closure. While it is not actually necessary to make this reduction, it does simplify the issue a bit. The problem that remains to complete the proof of the Theorem on p. 1 is to establish the following:

> *Let R be a complete local domain of prime characteristic $p > 0$. Let $x_1, \ldots, x_d$ be a system of parameters for R. Let T be a ring obtained from R by first forcing one element $\sigma = (u, \alpha)$ such that u is in the tight closure of the column space of α over R, and then performing finitely many simple algebra modifications with respect to parts of systems of parameters in R. Then $1 \notin (x_1, \ldots, x_d)T$.*

The next step in the argument will involve replacing the sequence of forcing algebras by a sequence of finitely generated R-modules.

Math 711: Lecture of December 7, 2007

We assume that we have the situation of the displayed paragraph near the bottom of p. 6 of the Lecture Notes from December 5. Specifically, let

$$R \to T_0 \to T_1 \to \cdots \to T_r$$

be a sequence of algebras obtained from a complete local domain R of prime characteristic $p > 0$ by successive forcing with respect to $\sigma_0, \sigma_1, \ldots, \sigma_{r-1}$. Here σ_0 forces a column $u \in R^h$ that is in the tight closure of the column space of an $h \times k$ matrix α into the column space of α, and for $i \geq 1$, σ_i yields an algebra modification with repsect to a relation on part of a system of parameters in R. Moreover, we assume that $1 \in (x_1, \ldots, x_d)T_r$, where $x_1, \ldots, x_d$ is a system of parameters for R. We want to obtain a contradiction.

Each T_i is presented as the quotient of polynomial ring over T_{i-1} in finitely many variables Z_{ij} by an ideal generated by polynomials that are linear in the new variables. Putting these presentations together gives a presentation of every T_i as a polynomial ring over R. Thus, we have an increasing sequence of polynomial rings $R \subseteq \mathcal{T}_1 \subseteq \mathcal{T}_2 \subseteq \cdots \subseteq \mathcal{T}_r$ and in each $\mathcal{T}_i$ an ideal $\mathfrak{B}_i$ such that $T_i \cong \mathcal{T}_i/\mathfrak{B}_i$.

For any polynomial ring $\mathcal{T}$ in finitely many variables over R, let $\mathcal{T}_{\leq N}$ denote the span of the monomials of total degree at most N over R. Evidently, $\mathcal{T}_{\leq N}$ is a finitely generated R-module. Let $M_i^{(N)}$ be the image of $(\mathcal{T}_i)_N$ in T_i. Thus, we have a commutative diagram:

$$\begin{array}{ccccccccc}
R & \longrightarrow & T_0 & \longrightarrow & T_1 & \longrightarrow & \cdots & \longrightarrow & T_r \\
{\scriptstyle 1}\uparrow & & \uparrow & & \uparrow & & & & \uparrow \\
R & \longrightarrow & M_0^{(N)} & \longrightarrow & M_1^{(N)} & \longrightarrow & \cdots & \longrightarrow & M_r^{(N)}
\end{array}$$

where the vertical maps are inclusions. The bottom row consists of finitely generated R-modules, and the top row is the ascending union over N of the bottom rows. We refer to the bottom row as a *sequence of partial forcing algebras* over R. Because T_r is the direct limit of the modules $M_r^{(N)}$, we have that (1) the image of $1 \in R$ under the composite map from the bottom row is in $(x_1, \ldots, x_d)M_r^{(N)}$ for any sufficiently large choice of N. We also know that (2) for every i, the elements of T_i occurring in σ_i are in $M_i^{(N)}$ for N sufficiently large. For the rest of the argument, we fix a choice of N sufficiently large that both these conditions hold.

Also fix a $\mathbb{Z}$-valued valuation ord on R that is nonnegative on R and positive on m. In particular, $\mathrm{ord}\,(x_i) \geq 1$ for every x_i. Extend ord to a $\mathbb{Q}$-valued valuation on R^+ that is nonnegative on R^+. We can do this by the argument at the bottom of p. 1 and top of p. 2 of the Lecture Notes from November 12.

We now use characteristic p techniques to obtain a contradiction. Everything that we have done so far is independent of the characteristic, but the final part of the argument depends heavily on the fact that we are in characteristic p.

Here is the key fact:

Lemma. *Let $N_i = N^{i+1}$ for $0 \le i \le r$, which is evidently an ascending sequence of positive integers. For every test element $c \in R$ and every $q = p^e$ there is a commutative diagram of R-linear maps:*

$$\begin{array}{ccccccccc}
R^{+}[1/c^{1/q}] & \xrightarrow{\mathbf{1}} & R^{+}[1/c^{1/q}] & \xrightarrow{\mathbf{1}} & R^{+}[1/c^{1/q}] & \xrightarrow{\mathbf{1}} & \cdots & \xrightarrow{\mathbf{1}} & R^{+}[1/c^{1/q}] \\
{\scriptstyle \iota}\uparrow & & {\scriptstyle \phi_0}\uparrow & & {\scriptstyle \phi_1}\uparrow & & & & {\scriptstyle \phi_r}\uparrow \\
R & \longrightarrow & T_0 & \longrightarrow & T_1 & \longrightarrow & \cdots & \longrightarrow & T_r \\
{\scriptstyle \mathbf{1}}\uparrow & & \uparrow & & \uparrow & & & & \uparrow \\
R & \longrightarrow & M_0^{(N)} & \longrightarrow & M_1^{(N)} & \longrightarrow & \cdots & \longrightarrow & M_r^{(N)}
\end{array}$$

such that ι is the inclusion map, the maps from the middle row to the top row are R-algebra homomorphisms, and such that for every i, $0 \le i \le r$, the image of $M_i^{(N)}$ is contained in the cyclic R^{+} module spanned by $\dfrac{1}{c^{N_i/q}}$.

Before proving the Lemma, we state for emphasis that the values of the integers N_i are independent of the choice of q.

Proof of the Lemma. We construct the ϕ_i recursively. T_0 is formed from R by forcing $(u,\, \alpha)$, where u is in the tight closure of the column space of α. This implies that $c^{1/q}u$ is an $R^{1/q}$-linear combination of the the columns of α, and, hence, an R^{+}-linear combination of the columns of α. This enables us to write u as a linear combination of the columns of α with coefficients in $R^{+}[1/c^{1/q}]$ and so we obtain a map $T_0 \to R^{+}[1/c^{1/q}]$. The elements Z_i are sent into the cyclic R^{+}-module spanned by $1/c^{1/q}$. Hence, $M_0^{(N)}$ maps into the cyclic R^{+}-module spanned by $(1/c^{1/q})^N = 1/c^{N_0/q}$, since $N_0 = N$.

Now suppose that we have constructed $\phi_0,\, \ldots,\, \phi_i$ such that $\phi_j(M_j^{(N)}) \subseteq R^{+}w_j$ for $1 \le j \le i$, where $w_j = 1/c^{N_j/q}$. We want to construct ϕ_{i+1}. Now, T_{i+1} is a modification of T_i with respect to a relation

$$y_{k+1}v_{k+1} = y_1v_1 + \cdots + y_kv_k,$$

where $y_1,\, \ldots\, , y_k$ are part of a system of parameters for R. By our choice of N, the elements $v_1,\, \ldots\, , v_{k+1}$ are in $M_i^{(N)}$. Hence, their images under ϕ_i are expressible in the form s_jw with the $s_j \in R^{+}$ and $w = w_i = 1/c^{N_i/q}$. This means that we can write

$$y_{k+1}\phi_i(v_{k+1}) \in (y_1,\, \ldots\, , y_k)R^{+}w.$$

Since R^{+} is a big Cohen-Macaulay algebra for R, this implies that

$$\phi_i(v_{k+1}) \in (y_1,\, \ldots\, , y_k)R^{+}w,$$

say

$$\phi_i(v_{k+1}) = \sum_{j=1}^{k} y_j s_j w$$

where the $s_j \in R^+$. We can now define ϕ_{i+1} by letting its values on the variables be the elements $s_j w$. Its value on any monomial of degree N in all of the variables that occur up to and including the $i+1$ spot will involve, at worst,

$$\bigl((1/c^{1/q})^{N_i}\bigr)^N = 1/c^{(NN_i)/q} = 1/c^{N_{i+1}/q}$$

as claimed. $\square$

We are now ready for the dénoument, i..e, we can complete the proof of the Theorem stated on p. 1 of the Lecture Notes from December 5.

The final step in the proof of the existence of big Cohen-Macaulay algebras that capture tight closure. We keep the notation of the Lemma above. We have that $1 \in (x_1, \ldots, x_d)M_r^{(N)}$, and that if $w_i = 1/c^{N_i/q}$, $1 \le i \le r$, for every q there is a commutative diagram

$$\begin{array}{ccccccccc}
R^+ & \longrightarrow & R^+w_0 & \longrightarrow & R^+w_1 & \longrightarrow & \cdots & \longrightarrow & R^+w_r \\
\uparrow & & {\scriptstyle \phi_0}\uparrow & & {\scriptstyle \phi_1}\uparrow & & & & {\scriptstyle \phi_r}\uparrow \\
R & \longrightarrow & M_0^{(N)} & \longrightarrow & M_1^{(N)} & \longrightarrow & \cdots & \longrightarrow & M_r^{(N)}
\end{array}$$

where the vertical maps are the restrictions of the ϕ_i and the horizontal maps in the first row are inclusion maps. By can consider the composite map from $R \to R^+w_r$ obtained by iterated composition by traversing two edges of the rectaqngle in two different ways. If we use the leftmost vertical arrow and the top row, we see that the image is simply $1 \in R^+w_r \subseteq R^+[1/c^{1/q}]$. By using the bottom row and the rightmost vertical arrow, as well as the fact that the image of $1 \in R$ is in $(x_1, \ldots, x_d)M_r$, we obtain that $1 \in (x_1, \ldots, x_d)R^+w_r$ for all q. It follows that $c^{N_r/q} \in (x_1, \ldots, x_d)R^+$ for all q, which leads to the conclusion that

$$\frac{1}{q}\mathrm{ord}\,(c^{N_r}) = \mathrm{ord}\,(c^{N_r/q}) \ge \min_j \mathrm{ord}\,(x_j) \ge 1$$

for all q. This is a contradiction, since we can choose $q > \mathrm{ord}\,(c^{N_r})$. $\square$

Note that if S and T are R-algebras, where R is a domain, and there is a map $S \to T$, then S is solid if T is solid. For if T is solid there is an R-linear map $T \to R$ such that $1 \mapsto c \in R^\circ$, and the composition $S \to T \to R$ will also be such a map. We obtain at once:

Corollary. *Let* (R, m, K) *be a complete local domain of prime characteristic* $p > 0$. *Let* $u \in R$, *and let* $I = (f_1, \dots, f_k)R$ *be an ideal of* R. *Then* $u \in I^*$ *if and only if*

$$S = R[Z_1, \dots, Z_k]/(u - \sum_{i=1}^{k} f_i Z_i)$$

is a solid R*-algebra, i.e., if and only if* $H^d_m(S) \neq 0$.

Proof. We know that $u \in I^*$ if and only if there is homomorphism from $R \to T$ such that $u \in IT$ and T is solid. Hence, if S is solid, $u \in I^*$, for $u \in IS$. On the other hand, if $u \in IT$ with T solid, we can map the forcing algebra S to T as an R-algebra, and it follows that S is solid. $\square$

This characterization is the starting point for the work of H. Brenner on tight closure.

Remark. There is an entirely similar criterion for when an element is in the tight closure of a submodule of a finitely generated free module over R.

It appears to be a very difficult problem to determine whether a given finitely generated R-algebra is solid. Any non-trivial result in this direction would be of great interest.

It is an open question whether every solid algebra over a complete local domain R can be mapped as an R-algebra to a big Cohen-Macaulay algebra. (If it can be mapped to a big Cohen-Macaulay algebra, it is solid.) G. Dietz has examples of finitely generated algebras that he conjectures are solid, but which cannot be mapped to a big Cohen-Macaulay algebra. However, it appears difficult to prove that these algebras are solid. See [G. D. Dietz, *Closure operations in positive characteristic and big Cohen-Macaulay algebras*, Thesis, University of Michigan, 2005].

Or next objective will be to study the notion of *phantom homology*. In part of a complex of finitely generated modules (the maps may raise or lower degree), say $G' \to G \to G''$, an element of the homology at the middle spot is called *phantom* if it is represented by a cycle that is in the tight closure of the module of boundaries in G. This notion turns out to have many applications.

Math 711: Lecture of December 10, 2007

We have defined an element of the homology or cohomology of a complex of finitely generated modules over a Noetherian ring R of prime characteristic $p > 0$ to be *phantom* if it is represented by a cycle (or cocycle) that is in the tight closure of the boundaries (or coboundaries) in the ambient module of the complex. We say that the homology or cohomology of a complex of finitely generated modules over R is *phantom* if every element is phantom. A left complex is called *phantom acyclic* if all of its homology is phantom in positive degree.

Discussion: behavior of modules of boundaries under base change. Note the following fact: if

$$G' \xrightarrow{d} G$$

is any R-linear map (in the application, this will be part of a complex), S is any R-algebra, and B denotes the image of d in G, then the image of

$$S \otimes_R G' \xrightarrow{\mathbf{1}_S \otimes d} S \otimes_R G$$

is the same as the image $\langle S \otimes_R B\rangle$ in $S \otimes_R G$. Note that we have a surjection $G' \twoheadrightarrow B$ and an injection $B \hookrightarrow G$, whence

$$S \otimes_R G' \to S \otimes_R G$$

factors as the composition of $S \otimes_R G' \twoheadrightarrow S \otimes_R B$ (this is a surjection by the right exactness of $S \otimes_R \_$) with $S \otimes_R B \to S \otimes_R G$.

From these comments, we obtain the following:

Proposition. *Let $R \to S$ be a homomorphism of Noetherian rings of prime characteristic $p > 0$ for which persistence*[2] *of tight closure holds. Let*

$$G' \to G \to G''$$

be part of a complex, and suppose that η is a phantom element of the homology H at G. Then the image of η in the homology H' of

$$S \otimes_R G' \to S \otimes_R G \to S \otimes_R G''$$

is a phantom element .

Hence, if S is weakly F-regular, the image of η in H' is 0.

[2]See the Theorem on p. 3 and Corollary on p. 4 of the Lecture Notes from November 7.

Proof. Let $z \in G$ represent η, and let B be the image of G' in G. Then $z \in B^*$, and $1 \otimes z$ represents the image of η in H'. By the persistence of tight closure for R to S, $1 \otimes z$ is in the tight closure over S of $\langle S \otimes_R B \rangle$ in $S \otimes_R G$, and by the discussion above, this is the same as the image of $S \otimes_R G'$. The final statement then follows because we can conclude, when the ring is weakly F-regular, that an element in tight closure of the module of boundaries is a boundary. □

There are many circumstances in which one can prove that complexes have phantom homology, and these lead to remarkable results that are difficult to prove by other methods. We shall pursue this theme in seminar next semester. For the moment, we shall only give one result of this type. However, the result we give is already a powerful tool, with numerous applications.

Theorem (Vanishing Theorem for Maps of Tor). *Let $A \to R \to S$ be Noetherian rings of prime characteristic $p > 0$, where A is a regular domain, R is module-finite and torsion-free over A, and S is regular or weakly F-regular and locally excellent.*[3] *Then for every A-module M, the map*

$$\mathrm{Tor}_i^A(M,\, R) \to \mathrm{Tor}_i^A(M,\, S)$$

is 0 for all $i \geq 1$.

This result is also known in equal characteristic 0 when S is regular, but the proof is by reduction to characteristic $p > 0$. It is an open question in mixed characteristic, even in the case where S is the residue class field of R! We discuss this further below.

Proof of the Vanishing Theorem for Maps of Tor. Since M is a direct limit of finitely generated A-modules and Tor commutes with direct limit, it suffices to consider the case where M is finitely generated. If some

$$\mathrm{Tor}_i^A(M,\, R) \to \mathrm{Tor}_i^A(M,\, S)$$

has a nonzero element η in the image, this remains true when we localize at a maximal ideal of S that contains the annihilator of η and complete. Thus, we may assume that $(S,\, \mathcal{M})$ is a complete weakly F-regular local ring, and then persistence of tight closure holds for the map $R \to S$. Let m be the contraction of $\mathcal{M}$ to A. Then we may replace A, M, and R by their localizations at m, and so we may assume that $(A,\, m,\, K)$ is regular local. Let $P_\bullet$ be a finite free resolution of M by finitely generated free A-modules.

To complete the proof, we shall show that the complex $R \otimes_A P_\bullet$ is phantom acyclic over R, i.e., all of its homology modules in degree $i \geq 1$ are phantom. These homology modules are precisely the modules $\mathrm{Tor}_i^A(M,\, R)$. Hence, for $i \geq 1$, the image of this homology in the homology of

$$S \otimes_R (R \otimes_A P_\bullet) \cong S \otimes_A P_\bullet$$

[3] The result holds when the completions of the local rings of R are weakly F-regular, which is a consequence of either of the stated hypotheses.

is 0, by the Proposition at the bottom of p 1. But the i th homology module of the latter complex is $\mathrm{Tor}_i^A(M, S)$, as required.

It remains to show that $R \otimes_A P_\bullet$ is phantom acyclic. Let h be the torsion-free rank of R over A, and let $G \subseteq R$ be a free A-module of rank h. Thus, $G \cong A^h$ as an A-module. Then R/G is a torsion A-module, and we can choose $c \in A^\circ$ such that $cR \subseteq G$. Let $z \in R \otimes_A P_i$ represent a cycle for some $i \geq 1$. Let B_i be the image of $R \otimes P_{i+1}$ in $R \otimes_A P_i$. We shall show that $cz^q \in B_i^{[q]}$ in $\mathcal{F}_R^e(R \otimes_A P_i)$ for all q, which will conclude the proof.

It will suffice to show that, for all e, c kills the homology of $\mathcal{F}_R^e(R \otimes_A P_\bullet)$ in degree $i \geq 1$, since z^q is an element of the homology, and the module of boundaries in $\mathcal{F}_R^e(R \otimes_A P_i)$ is, by another application of the Proposition at the bottom of p. 1, the image of $\mathcal{F}_R^e(B_i)$, which is $B_i^{[q]}$.

By (11) on p. 3 of the Lecture Notes from September 12, we may identify

$$\mathcal{F}_R^e(R \otimes_A P_\bullet) \cong R \otimes_A \mathcal{F}_A^e(P_\bullet).$$

By the flatness of the Frobenius endomorphism of A, the complex $\mathcal{F}_A^e(P_\bullet)$ is acyclic. Since G is A-free, we have that $G \otimes_A \mathcal{F}_A^e(P_\bullet)$ is acyclic, and this is a subcomplex of $R \otimes_A \mathcal{F}_A^e(P_\bullet)$. Because $cR \subseteq G$, we have that c multiplies $R \otimes_A \mathcal{F}_A^e(P_\bullet)$ into the acyclic subcomplex $G \otimes_A \mathcal{F}_A^e(P_\bullet)$. If y is a cycle in $R \otimes_A \mathcal{F}_A^e(P_\bullet)$ in degree $i \geq 1$, then cy is a cycle in $G \otimes_A \mathcal{F}_A^e(P_\bullet)$ in degree i, and consequently is a boundary in $G \otimes_A \mathcal{F}_A^e(P_\bullet)$. But then it is a boundary in the larger complex $R \otimes_A \mathcal{F}_A^e(P_\bullet)$ as well. □

We conclude by giving two consequences of the Vanishing Theorem for Maps of Tor. Both are known in equal characteristic and are open questions in mixed characteristic. Both can be proved by other means in the equal characteristic case, but it is striking that they are consequences of a single theorem.

Theorem. *The Vanishing Theorem for Maps of Tor implies, if it holds in a given characteristic, that direct summands of regular rings are Cohen-Macaulay in that characteristic.*

Before we can give the proof, we need a Lemma that will permit a reduction to the complete local case.

Lemma. *Let R and S be Noetherian rings.*

(a) *Let S be a regular ring and let J be any ideal of S. The the J-adic completion T of S is regular.*

(b) *Let $R \to S$ be a homomorphism and suppose that R is a direct summand of S. Then for every ideal I of R, the I-adic completion of R is a direct summand of the IS-adic completion of S.*

Proof. (a) Every maximal ideal $\mathcal{M}$ of T must contain the image of J, since if $u \in JT$ is not in $\mathcal{M}$, there exists a non-unit $v \in \mathcal{M}$ such that $tu + v = 1$. But $v = 1 - tu$ *is* invertible, since

$$1 + tu + \cdots + t^n u^n + \cdots$$

is an inverse. Hence, every maximal ideal T corresponds to a maximal ideal $\mathcal{Q}$ of S that contains J. Note that $S \to T$ is flat, and $\mathcal{Q}$ expands to $\mathcal{M}$. Hence, $S_{\mathcal{Q}} \to T_{\mathcal{M}}$ is faithfully flat, and the closed fiber is a field. It follows that the image of a regular system of parameters for $S_{\mathcal{Q}}$ is a regular system of parameters for $T_{\mathcal{M}}$.

(b) Let $f_1, \ldots, f_h \in I$ generate I. Let $X_1, \ldots, X_h$ be formal power series indeterminates over both rings. Let $\theta : S \to R$ be an R-linear retraction, Then $R[[X_1, \ldots, X_h]]$ is a direct sumnand of $S[[X_1, \ldots, X_h]]$: we define a retraction $\widetilde{\theta}$ that extends θ by letting θ act on every coefficient of a given power series. Let $\mathfrak{A}$ be the ideal of $R[[x_1, \ldots, x_h]]$ generated by the elements $X_i - f_i$, $1 \leq i \leq h$. Then there is an induced retraction

$$S[[x_1, \ldots, x_h]]/\mathfrak{A}S[[X_1, \ldots, X_h]] \to R[[X_1, \ldots, X_h]]/\mathfrak{A}.$$

The former may be identified with the IS-adic completion of S, and the latter with the I-adic completion of R. $\square$

Proof of the Theorem. Let R be a Cohen-Macaulay ring that is a direct summand of the regular ring S. The issue is local on R, and so we may replace R by its localization at a prime ideal P, and S by S_P. Therefore, we may assume that (R, m, K) is local. Second, we may replace R by its completion $\widehat{R}$ and S by its completion with respect to mS. The regularity of S and the direct summand property are preserved, by the Lemma just above.

Hence, we may assume without loss of generality that (R, m, K) is complete local, and then we may represent it as module-finite over a regular local ring A with system of parameters $x_1, \ldots, x_d$. Let $M = A/(x_1, \ldots, x_d)$. Then the maps

$$f_i : \mathrm{Tor}_i^A(M, R) \to \mathrm{Tor}_i^A(M, S)$$

vanish for $i \geq 1$. Since $S = R \oplus W$ over R (over A is enough), the maps f_i are injective. Hence,

$$\mathrm{Tor}_i^A\big(A/(x_1, \ldots, x_d), R\big) = 0, \quad 1 \leq i \leq d.$$

This means that the Koszul homology $H_i(x_1, \ldots, x_d; R) = 0$ for $i \geq 1$, and, by the self-duality of the Koszul complex, also implies that

$$\mathrm{Ext}_A^i\big(A(x_1, \ldots, x_d)A, R\big) = 0, \quad 0 \leq i < d.$$

It follows that the depth of R on $(x_1, \ldots, x_d)A$ is $d = \dim(A) = \dim(R)$. Hence R is Cohen-Macaulay. $\square$

Theorem. *The Vanishing Theorem for Maps of Tor, if it holds in a given characteristic, implies that the direct summand conjecture holds in that characteristic, i.e., that regular rings are direct summands of their module-finite extensions in that characteristic.*

Proof. Let $A \hookrightarrow R$ be module-finite. We want to show that this map splits. By part (a) of the Theorem on p. 3 of the Lecture Notes from September 24, it suffices to show this when $(A,\, m,\, K)$ is local. By part (b), we may reduce to the case where A is complete. We may kill a minimal prime $\mathfrak{p}$ of R disjoint from A°. If $A \to R/\mathfrak{p}$ has a splitting θ, the composite map $R \twoheadrightarrow R/\mathfrak{p} \xrightarrow{\theta} A$ splits $A \hookrightarrow R$. Hence, we may also assume that R is a domain module-finite over A. Then R is local. Let L be the residue field of R. Let $x_1,\, \ldots\, , x_d$ be a regular sequence of parameters for A. The the image of 1 generates the socle in $A/(x_1,\, \ldots\, , x_d)A = A/m = K$. Hence, the image of $x_1^{t-1} \cdots x_d^{t-1}$ generates the socle in $A/(x_1^t,\, \ldots\, , x_d^t)A$ for all $t \geq 1$. By characterization (4) in the Theorem at the top of p. 3 of the Lecture Notes from October 24, it suffices to show that we cannot have an equation

$$(*) \quad x_1^{t-1} \cdots x_d^{t-1} = y_1 x_1^t + \cdots + y_d x_d^t$$

for any $t \geq 1$ with $y_1,\, \ldots\, , y_d \in R$.

Observe that if $A \to T$ is any ring homomorphism, $f_1,\, \ldots\, , f_h \in A$, and $I = (f_1,\, \ldots\, , f_h)A$, then $\mathrm{Tor}_1^A(A/I,\, T)$ is the quotient of the submodule of T^h whose elements are the relations on $f_1,\, \ldots\, , f_h$ with coefficients in T by the submodule generated by the images of the relations on $f_1,\, \ldots\, , f_h$ over A. (A free resolution of A/I over A begins

$$\cdots \to A^k \xrightarrow{\alpha} A^h \xrightarrow{(f_i)} A \to A/I \to 0$$

where (f_i) is a $1 \times h$ row vector whose entries are $f_1,\, \ldots\, , f_h$ and the column space of the matrix α is the module of relations on $f_1,\, \ldots\, , f_h$ over A. Drop the A/I term, apply the functor $T \otimes \_$, and take homology at the T^h spot.)

Assume that we have the equation $(*)$ for some $t \geq 1$ and $y_1,\, \ldots\, , y_d \in R$ Let I be the ideal of A with generators

$$x_1^{t-1} \cdots x_d^{t-1},\, x_1^t,\, \ldots\, , x_d^t.$$

Then

$$(\#) \quad (1,\, -y_1,\, \ldots\, ,\, -y_d)$$

represents an element of $\mathrm{Tor}_1^A(A/I,\, R)$. Take S to be the residue class field L of R. $S = L$ is certainly regular. Hence, assuming the Vanishing Theorem for Maps of Tor, the image of the relation $(\#)$ in $\mathrm{Tor}_1^A(A/I,\, L)$ is 0. The image of the relation $(\#)$ has the entry 1 in its first coordinate. However, the relations on

$$x_1^{t-1} \cdots x_d^{t-1},\, x_1^t,\, \ldots\, , x_d^t$$

over A all have first entry in m, since $x_1^{t-1} \cdots x_d^{t-1}, \notin (x_1^t,\, \ldots\, , x_d^t)A$. These relations map to elements of L^{d+1} whose first coordinate is 0, and so the image of $(\#)$ cannot be in their span, a contradiction. $\square$

It is worth noting that these two applications of the Vanishing Theorem for Maps of Tor are, in some sense, at diametrically opposed extremes. In the first application, the map to the regular ring S is a split injection. In the second, the map to the regular ring S is simply the quotient surjection of a local ring to its residue class field!

Math 711, Fall 2007 **Problem Set #1 Solutions**

1. Let $\theta(1) = c \neq 0$. If $r \in IS \cap R$, we have $r = f_1 s_1 + \cdots f_n s_n$ with $r \in R$, the $f_i \in I$, and $s_1, \, \dots \, , s_n \in S$. Then for all q, $r^q = f_1^q s_1^q + \cdots f_n^q s_n^q$, and applying the R-linear map θ yields $cr^q = r^q\theta(1) = f_1^q\theta(s_1^q) + \cdots f_n^q\theta(s_n^q) \in I^{[q]}$. Hence, $r \in I^*$. $\square$

2. Since S is weakly F-regular, it is normal, and, hence, a finite product of weakly F-regular domains. It follows that R is reduced. We use induction first on the number of factors of R, if R is a product, and second on the number of factors of S. If R is not a domain, we can partition the minimal primes into two nonempty sets M_1 and M_2. We can construct a in all of the primes that are in M_1 and not in any of the primes that are in M_2, and b in all of the primes in M_2 and in none of the primes in M_1. Then $ab = 0$ and $a + b$ is not a zerodivisor in R. If we kill any minimal prime of S, either a or b becomes 0, and, in either case, a is in the ideal $(a + b)S$. Hence, a is in its tight closure and therefore in the ideal in S. Then $a \in (a + b)S \cap R = (a + b)R$, and so we can find $e \in R$ such that $a = e(a + b)$. Modulo every prime in M_1, we must have $e \equiv 0$, and modulo every prime in M_2 we must have $e \equiv 1$. It follows that $e \equiv e^2$ mod every minimal prime, and, hence, that e is a nontrivial idempotent in R. It is immediate that R is a product $Re \times Rf$ with $f = 1 - e$, and $Re \hookrightarrow Se$ and $Rf \hookrightarrow Sf$ inherit the hypothesis. Hence, by induction on the number of factors of R, both Re and Rf are weakly F-regular: consequently, so is R.

Thus, we may reduce to the case where R is a domain. If R° maps into S°, which is automatic if S is a domain, then whenever $cr^q \in I^{[q]}$ for all $q \gg 0$ in R, we have that $cr^q \in I^{[q]}S = (IS)^{[q]}$ for all $q \gg 0$ in S, and then $r \in (IS)^*$ in S, i.e., $r \in IS$, since S is weakly F-regular. But then $r \in IS \cap R = I$, and so every ideal I of R is tightly closed.

Now suppose that $S = S_1 \times \cdots \times S_n$ where $n \geq 2$. We proceed by induction on n. Every S_i is an R-algebra. If $R \to S_i$ is injective for every i, then R° maps into $S^\circ = S_1^\circ \times \cdots \times S_n^\circ$. If not, we may assume by renumbering that $R \to S_n$ has a nonzero kernel P. Let $T = S_1 \times \cdots \times S_{n-1}$. We shall show that $R \to T$ still has the property that $IT \cap R = I$ for all $I \subseteq R$, and then the result follows by induction on n. Suppose not, and choose $I \subseteq R$ and $u \in R - I$ such that $u \in IT \cap R$. Let a be a nonzero element of P. Then $au \in aIT \cap R$, but $au \notin aI$ in R. Since au maps to 0 in S_n and $aIS = (0)$ in S_n, we have that $au \in aI(T \times S_n) = aIS$ as well, and so $au \in aIS \cap R - aI$, a contradiction. $\square$

Further comments on 2. Note that it is *not* true that the hypothesis that $(*)$ every ideal of R is contracted from S implies that R° maps into S°. Let $R = K[x]$, $S = K[x] \times K$, where K is a field, and consider the homomorphism $R \to S$ such that $f \mapsto \big(f, \, f(0)\big)$. The product projection $\pi_1 : S \to R$ on the first coordinate is an algebra retraction of S to R, which implies that $(*)$ holds. But $x \in R^\circ$ maps to $(x, \, 0) \notin S^\circ$.

Likewise, $(*)$ does not imply that there is a choice of minimal primes $\mathfrak{p}$ in R and $\mathfrak{q}$ in S such that $\mathfrak{q}$ lies over $\mathfrak{p}$ and the induced map $R/\mathfrak{p} \to S/\mathfrak{q}$ still has property $(*)$. For example, suppose that $R = K[x^2, \, x^3] \subseteq K[x]$, where K is a field of characteristic other than 2, and x is an indeterminate over K. Let y be a new indeterminate, and let $S = R[y]/(y^2 - x^2)$.

Then S is R-free on the basis consisting of the images of 1 and y, and so every ideal of R is contracted from S. R is a domain, while S has two minimal primes, which are the contractions of $y-x$ and $y+x$, respectively, from $K[x,y]$. The quotient by either minimal prime of S is $K[x]$, and $(*)$ fails for $R \subseteq K[x]$, since x^3 is in the expansion of x^2R.

3. If $P \in \mathrm{Ass}\,(M)$ then $R/P \hookrightarrow M$. Applying $\mathcal{F}^e$, which is faithfully flat, we have $R/P^{[q]} \hookrightarrow \mathcal{F}^e(M)$. Since $\mathrm{Rad}\,(P^{[q]}) = P$, P is a minimal prime of $P^{[q]}$, and so $R/P \hookrightarrow R/P^{[q]} \hookrightarrow \mathcal{F}^e(M)$. Hence, $P \in \mathrm{Ass}\,\bigl(\mathcal{F}^e(M)\bigr)$. Now suppose that $P \notin \mathrm{Ass}\,(M)$. Whether $P \in \mathrm{Ass}\,(M)$ or $P \in \mathrm{Ass}\,\bigl(\mathcal{F}^e(M)\bigr)$ is unaffected by localization at P. (Note that if $T = R_P$, $\mathcal{F}^e_T(M_P) \cong F^e_R(M)_P$.) Therefore, we may assume that $(R,\,P,\,K)$ is local, and that $P \notin \mathrm{Ass}\,(M)$. Then there exists $x \in P$ that is not a zerodivisor on M. It follows that x^q is a nonzerodivisor on $\mathcal{F}^e(M)$, and so $P \notin \mathrm{Ass}\,\bigl(\mathcal{F}^e(M)\bigr)$, as required. $\square$

Further comments on 3. It is not true in general that if M is a finitely generated module over a Noetherian ring R, then M has a filtration by prime cyclic modules R/P such that $P \in \mathrm{Ass}\,(M)$. E.g., let R be any local domain whose maximal ideal m is not principal, and consider m as an R-module. The only associated prime is 0. Any prime cyclic filtration of m will involve one copy of R, but there will also be copies of R/P for $P \neq (0)$. However, it is true that M has a filtration such that each factor is a torsion-free module over R/P for some $P \in \mathrm{Ass}\,(M)$. Each finitely generated torsion-free module over R/P can be embedded in a finitely generated free module over R/P. These two facts, which we leave as exercises, lead to a different proof that $\mathrm{Ass}\,\bigl(\mathcal{F}^e(M)\bigr) inc \mathrm{Ass}\,(M)$. It suffices to show this for each torsion-free factor, and this reduces to the case of a free R/P-module and then to the case of R/P itself. Then one can conclude using the argument given in class that every $P^{[q]}$ is P-primary. $\square$

4. For every generator u_i of J we can choose $c_i \in R^\circ$ such that $cu_i^q \in I^{[q]}$ for all $q \gg 0$. Let $c \in R^\circ$ be the product of the c_i. Then $c \in R^\circ$ is such that $cJ^{[q]} \subseteq I^{[q]}$ for all $q \gg 0$. Now $0 \le \ell(R/I^{[q]}) - \ell(R/J^{[q]})$ (since $I^{[q]} \subseteq J^{[q]}$), and this is the same as $\ell(J^{[q]}/I^{[q]})$. Since J has k generators, $J^{[q]}$ has at most k generators, and the same holds for $N_q = J^{[q]}/I^{[q]}$. Since c and $I^{[q]}$ both kill N_q, we can map $R/(I^{[q]} + cR)^{\oplus k}$ onto N_q, which bounds its length by $k\ell\bigl(R/(I^{[q]} + cR)\bigr) = k\ell(\overline{R}/\mathfrak{A}^{[q]}) \le k\ell(\overline{R}/\mathfrak{A}^{qh})$. Since $\overline{R}$ has dimension $d-1$ and $\mathfrak{A}$ is primary to its maximal ideal, this length is bounded by $C_1(qh)^{d-1}$, using the ordinary Hilbert function. This yields the uppoer bound $kC_1h^{d-1}q^{d-1}$, so that we may take $C = kC_1h^{d-1}$. $\square$

5. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the minimal primes of R, and let $c_i \in R - \mathfrak{p}_i$ represent a test element in $R/\mathfrak{p}_i$. We may choose d_i not in $\mathfrak{p}_i$ but in all other minimal primes of R. Let $c = c_1d_1 + \cdots + c_nd_n$. Then $c \in R^\circ$, and if $u \in N^*_M$, this is true modulo every $\mathfrak{p}_i$, and so $c_iu \in N + \mathfrak{p}_iM$ for all i. Then $c_id_iu \in N$, since d_i kills $\mathfrak{p}_i$, and adding shows that $cu \in N$, as required. (The argument is valid both for test elements and for big test elements.) $\square$

6. This result is proved in the Lecture Notes of October 8.

Math 711, Fall 2007 **Problem Set #2 Solutions**

1. $\subseteq$ is clear. To prove $\supseteq$, if c is a test element and $u \in \bigcap_n (I + m^n)^*$ then for all q and n, $cu^q \in (I + m^n)^{[q]} = I^{[q]} + (m^n)^{[q]} \in I^q + m^n$. Fix q. Then $cu^q \in \bigcap_n (I^{[q]} + m^n) = I^q$. Hence, $u \in I^*$. $\square$

2. $u \in I^*$ iff $cu^q \in I^{[q]}$ for all q iff $cu^q \in I^q\widehat{R}$ for all q (since $\widehat{R}$ is faithfully flat over R, $J\widehat{R} \cap R = J$ for all $J \subseteq R$) iff $cu^q \in (I\widehat{R})^{[q]}$ for all q iff $u \in (I\widehat{R})^*$. It is not necessary that I be m-primary. More generally, if $R \subseteq S$, $c \in R$ is a test element for both rings, and $JS \cap R = J$ for all $J \subseteq R$, then $u \in I^*_R$ iff $u \in (IS)^*_S$. $\square$

3. Since R and S are domains, $R^\circ \subseteq S^\circ$ and $I^* \subseteq (IS)^* = IS$. Hence $I^* \subseteq IS \cap R$. The fact that $IS \cap R \subseteq I^*$ was proved in class (see the Theorem on the first page of the Lectcure Notes from October 12).

4. Frobenius closure of ideals commutes with localization: if W is a multiplicative system in R and $(u/w)^q \in (W^{-1}R)^{[q]}$, where $u \in R$ and $w \in W$, then for some $w_1 \in W$ we have $w_1u^q \in I^{[q]}$, and then $(w_1u)^q \in I^{[q]}$ as well. But then $w_1u \in I^{\mathrm{F}}$, and so $u \in I^{\mathrm{F}}$, which shows that $u/w \in I^{\mathrm{F}}W^{-1}R$ as well. Now suppose that $u \in I^*$ but the $cu \notin I^{\mathrm{F}}$. We want to obtain a contradiction. The latter condition can be preserved by localizing at a maximal ideal m in the support of the image of cu in R/I^{F}. We then have that $u/1 \in (IR_m)^*$ in R_m, but that $u/1 \notin (IR_m)^{\mathrm{F}}$. Choose $q \geq N_m$. We also have that $u^q/1 \in \big((IR_m)^{[q]}\big)^*$, and so $c^qu^q/1 \in (IR_m)^{[q]}$, since c^q is a multiple of c^{N_m}. But this says that $(cu/1)^q \in (IR_m)^{[q]}$, which shows that $cu/1 \in (IR_m)^{\mathrm{F}}$, a contradiction. $\square$

5. Let c_S be a test element for S. Then c_S satisfies an equation of integral dependence on R whose constant term is not 0 (or factor out a power of x). Hence, c_S has a multiple c in R°. Now suppose that $u \in H^*_G$, where H is a submodule of the module G over R. Fix an R-linear map $\theta : S \to R$ whose value on 1 is nonzero: call the value d. θ induces an R-linear map $\eta : S \otimes G \to G$ such that $s \otimes g \mapsto \theta(s)g$: hence, if $g \in G$, $\eta(1 \otimes g) = dg$. We have $1 \otimes u \in \langle S \otimes_R H\rangle^*_{S\otimes_R G}$ and so $1 \otimes cu \in \langle S \otimes_R H\rangle$, i.e., $cu = \sum_{j=1}^h s_j \otimes h_j$, $s_j \in S$, $h_j \in H$. Apply η to obtain $cdu = \sum_{j=1}^n \theta(s_j)h_j \in H$. Thus, cd is a test element for R. $\square$

6. Let $x \in m$. It suffices to show that if $N \subseteq M$ are finitely generated modules and $u \in N^*_M$, then $xu \subseteq N$, for then $m \subseteq \tau(R)$ (if $\tau(R) = R$, R is weakly F-regular). If not, chose N' with $N \subseteq N' \subseteq M$ such that N' is maximal with respect to not containing xu. Then M/N' is a finite length essential extension of Rxu, which is killed by m. We may replace u and $N \subseteq M$ by $u + N'$ and $0 \subseteq M/N'$ as a counterexample. For large t, $I_t = (x_1^t, \ldots, x_d^t)R$ kills M, and since R/I_t is (R/I_t)-injective, M embeds in R/I_t. xu must map to a socle generator, which we may take to be the image, z, of $(x_1 \cdots x_d)^{t-1}y$. By hypothesis, $(I_t, z)R$ is tightly closed, so that Kz is tightly closed in R/I_t. But since $u \in 0^*_M$ its image $v \in 0^*_{R/I_t} \subseteq (Kz)^*_{R/I_t} = Kz$. Since $v \in Kz$, $xv = 0$. Since $M \subseteq R/I_t$, we also have $xu = 0$, a contadiction. $\square$

Math 711, Fall 2007 **Problem Set #3 Solutions**

1. Since the test ideal $\tau(R)$ has height two, it cannot be contained in the union of P and the minimal primes of R. Hence, we can choose a test element $c \in R^\circ$ that is not in P. If $u \in N^*M$, we have that $cu^q \in N_M^{[q]}$ for all $q \gg 0$. This is preserved when we apply $S \otimes_R \_$, and the image of c is not 0. $\square$

2. (a) Every element of I^* maps into $(IW^{-1}R)^*$, from which $I^*W^{-1}R \subseteq (IW^{-1}R)^*$. To show $\supseteq$, , let $r/w \in (IW^{-1}R)^*$. Then $r \in (IW^{-1}R)^*$ as well, so that for all $q \gg 0$, $(c/1)(r^q/1) \in (IW^{-1}R)^{[q]} = I^{[q]}W^{-1}R$. By the Proposition on p. 2 of the Lecture Notes from September 17, $W^{-1}R^\circ$ maps onto $(W^{-1}R)^\circ$, and so we may assume that $c \in R^\circ$. Then for all $q \gg 0$ there exists $w_q \in W$ such that $w_q cr^q \in I^{[q]}$. Since w is not in any associated prime of $I^{[q]}$, it is a nonzerodivisor on $I^{[q]}$. Then $cr^q \in I^{[q]}$, and $r \in I^*$. $\square$

(b) For every q, $x_1^q, \dots, x_n^q$ is a regular sequence in the Cohen-Macaulay ring R, and so $R/I^{[q]}$ is Cohen-Macaulay, which implies that all associated primes of $I^{[q]}$ are minimal primes of $I^{[q]}$ and, hence, of I. By part (a), we can localize at W, the complement of the union of the minimal primes of I, and $IW^{-1}R$ will be tightly closed, while $PW^{-1}R$ is a maximal idea of $W^{-1}R$. Thus, I remains tightly closed when we localize at $PW^{-1}R$, by the Lemma on p. 2 of the Lecture Notes from September 17. We have a reduced Cohen-Macaulay local ring in which a system of parameters generates a tightly closed ideal, and the ring is F-rational by the Theorem on p. 9 of the Lecture Notes from October 8. $\square$

(c) R is F-rational and so it is certainly Cohen-Macaulay and reduced. Choose part of a system of parameters for R that is also a system of parameters for R_P. The ideal these elements generate in R is tightly closed, and, hence, so is the ideal they generate in R_P. $\square$

3. Let P be maximal in $\mathrm{Ass}\,(M)$ and let $N = \mathrm{Ann}_M P$. Then $N \neq 0$, and it will suffice to show that $(*)$ $\mathrm{Ass}\,(M) = \mathrm{Ass}\,(N) \cup \mathrm{Ass}\,(M/N)$. In fact, $\mathrm{Ass}\,(N) \subseteq \mathrm{Ass}\,(M)$ and any prime in $\mathrm{Ass}\,(N)$ must contain P. It follows that $\mathrm{Ass}\,(N) = \{P\}$, since P is maximal in $\mathrm{Ass}\,(M)$, and that N is a torsion-free module over R/P. If $(*)$ holds, then by Noetherian induction on M, M/N will have a filtration as required whose inverse image in M, together with N, will give the required filtration of M. To prove $(*)$ note that we always have $\subseteq$ and that $\mathrm{Ass}\,(N) \subseteq \mathrm{Ass}\,(M)$. We need only show that $\mathrm{Ass}\,(M/N) \subseteq \mathrm{Ass}\,(M)$. Suppose $Q \in \mathrm{Ass}\,(M/N)$. If P is not contained in Q, then $N_Q = 0$, and so $M_Q = (M/N)_Q$. Thus, $QR_Q \in \mathrm{Ass}\,(M_Q)$ over R_Q, and so $Q \in \mathrm{Ass}\,(M)$, as required. Now suppose that $P \subset Q$ strictly, and that Q is the annihilator of $u \in M - N$. Since $u \notin N$, we can choose $r \in P$ such that $ru \neq 0$. But then $Qru = rQu \subseteq rN = 0$, and so Q or a larger prime is in $\mathrm{Ass}\,(M)$, contradicting the maximality of P. $\square$

(b) If $P \in \mathrm{Ass}_R(M)$, then $R/P \hookrightarrow M$, and so $S/PS = S \otimes_R R/P$ injects into $S \otimes_R M$. Thus, $\mathrm{Ass}_S(S/PS) \subseteq \mathrm{Ass}\,_S(S \otimes_R M)$ for every $P \in \mathrm{Ass}_R(M)$. This proves $\supseteq$. For the other direction, suppose that we have a finite filtration of M such that every factor N_i is a torsion-free module over R/P_i for some $P_i \in \mathrm{Ass}_R(M)$. Then we have a filtration of $S \otimes_R M$ by the modules $S \otimes N_i$. It suffices to show that if N_i is nonzero torsion-free over R/P_i, then $\mathrm{Ass}_S(S \otimes_R N_i) \subseteq \mathrm{Ass}_S(S/P_iS)$. But if N_i is torsion-free over R/P_i, it embeds in a free module $(R/P_i)^{\oplus h}$ by the Lemma on the first page of the Lecture Notes from October 12. Therefore, $S \otimes_R N_i$ embeds in $S \otimes_R (R/P)^{\oplus h}$, which is a direct sum of copies of S/PS. Hence, $\mathrm{Ass}\,_S(S \otimes_R N_i) \subseteq \mathrm{Ass}_S(S/P_iS)$. $\square$

4. Evidently $\tau(R) \subseteq I :_R I^*$ for every ideal I. In the local case, if I_t is a sequence of m-primary irreducible ideals cofinal with the powers of m, then $\tau(R) = \bigcap_t (I_t :_R I_t^*)$. To see this, suppose c is in the intersection but not in $\tau(R)$. Then there exist finitely generated modules $N \subseteq M$ such that $u \in N^*$ but $cu \notin N$. Replace N by N' maximal such that $N \subseteq N' \subseteq M$ and $cu \notin N'$. Then replace, u, M, N' by v, $M/N', 0$, where v is the image of u in M/N'. Every nonzero submodule of M contains $Rcv = Kcv$, and so M is a finite length essential extension of K and is killed by some I_t: then $M \hookrightarrow R/I_t$ with cv corresponding to the socle element. Then v corresponds to an element r of I_t^*/I_t with $cr \notin I_t$, a contradiction, since $cI_t^* \subseteq I_t$ by hypothesis. If $x_1, \ldots, x_n$ is generated by test elements in the Gorenstein ring (R, m, K), let $I_t = (x_1^t, \ldots, x_n^t)$. We only need that $I :_R I^* = I_t :_R I_t^*$ for all t. Let $u \in I_t^*$. Then $x_iu \in I_t$ for all i, and $u \in I_t :_R I = I_t + y^{t-1}R$, where $y = x_1 \cdots x_n$. But if $u = f + y^{t-1}r$, then $r \in I_t^* :_R y^{t-1} = J$: we'll show that $J \subseteq I^*$. Since $y^{t-1}r \in I_t^*$, for some $d \in R^\circ$ and all $q \gg 0$, $dy^{q(t-1)}r^q \in (I_t)^{[q]} = I_q \Rightarrow dr^q \in I_{tq} :_R y^{tq-q} = I^{[q]}$. Thus, $r \in I^*$, and $I_t^* = I_t + y^{t-1}I^*$. But then $cI_t^* \subseteq I_t$ iff $cy^{t-1}I^* \subseteq I_t$, and this holds iff $cI^* \subseteq I_t :_R y^{t-1} = I$. Thus, $I_t^* :_R I_t = I^* :_R I$, as required. $\square$

5. (a) With R F-finite or complete, it follows from part (6) of the splitting crriterion at the top of p. 3 of the Lecture Notes from October 24 that the map is split iff $uS \notin (x_1, \ldots, x_n)S$, where S is R viewed as an R-algebra via $F : R \to R$. But this means precisely that $u^p \notin (x_1^p, \ldots, x_n^p)R$.

(b) Use x, y as a system of parameters. The socle mod (x, y) is represented by z^2. Note that R is free over $A = K[[x, y]]$ on the basis 1, z, z^2, and so every element can be uniquely represented as $a_0 + a_1z + a_2z^2$ with the $a_i \in A$. The ring is F-split if and only if $z^{2p} \notin (x^p, y^p)$. Let $p = 3k + r$, where $r = 1$ or 2 and so $2p = 6k + 2r$. Then $z^{2p} = z^{6k}z^{2r} = \pm(x^3 + y^3)^{2k}z^2$ if $r = 1$ and $\pm(x^3 + y^3)^{2k+1}z$ if $r = 2$. This is in (x^p, y^p) iff all terns of $(x^3 + y^3)^{2k}$ (resp., $(x^3 + y^3)^{2k+1}$) are: the binomial coefficients do not vanish, since $2k + 1 < p$. In case $r = 1$ there is a term involving $x^{3k}y^{3k}$ which is not in (x^p, y^p). In the second case, every term involves an exponent on x^3 or on y^3 that is at least $k + 1$, and $3k + 3 > p$. Hence, the ring is F-split if $p \equiv 1 \bmod 3$ and is not F-split if $p \equiv 2 \bmod 3$.

6. (a) When N is already a module over $W^{-1}R = S$, $S \otimes_R N \cong N$ as S-modules. Hence, $\mathcal{F}_S^e(M) \cong \mathcal{F}_S^e(S \otimes_R M) \cong S \otimes_{\mathbb{R}} \mathcal{F}_R^e(M)$ (by property (11) on p. 3 of the Lecture Notes from September 12), and this is simply $\mathcal{F}_R^e(M)$ because every $w \in W$ already acts invertibly on this module, since w^q does.

(b) By the equivalent condition (c) in the Proposition on p. 3 of the Lecture Notes from October 22, it suffices to show that for every prime ideal Q of $W^{-1}R$, 0 is tightly closed in the injective hull of $W^{-1}R/Q$. We know that Q has the form $PW^{-1}R$ for some prime ideal

P of R disjoint from W. Thus it suffices to check that 0 is tightly closed in $E = E(R/P)$ thought of as an $W^{-1}R$ module. Suppose to the contrary that $u \neq 0$ is in the tight closure of 0. By the Proposition on p. 2 of the Lecture Notes from September 17, we may assume the element used in establishing that u is in the tight closure is the image of $c \in R^{\circ}$. Then cu^q is 0 in $\mathcal{F}_S^e(E)$ for all $q \gg 0$. Since $\mathcal{F}_S^e(E) \cong \mathcal{F}_R^e(E)$, this shows that u is in the tight closure of 0 in E working over R, a contradiction. $\square$

Math 711, Fall 2007 **Problem Set #4 Solutions**

1. Let ${}^eR$ indicate R and viewed as an R-algebra via F_R^e and similarly for ${}^eS$. We have that $\mathcal{F}_R^e(M) \otimes_R \mathcal{F}_S^e(N) = ({}^eR \otimes_R M) \otimes_{{}^eR} ({}^eS \otimes_S N) \cong (M \otimes_R {}^eR) \otimes_{{}^eR} ({}^eS \otimes_S N)$ (by the associativity of $\otimes$) $\cong M \otimes_R ({}^eS \otimes_S N) \cong ({}^eS \otimes_S N) \otimes_R M \cong {}^eS \otimes_S (N \otimes_R M)$ (by the associativity of $\otimes$) $\cong {}^eS \otimes_S (M \otimes_R N) = \mathcal{F}_S^e(M \otimes_R N)$. Then, as we trace through the identifications, $u^q \otimes v^q \mapsto (1 \otimes u) \otimes (1 \otimes v) \mapsto (u \otimes 1) \otimes (1 \otimes v) \mapsto u \otimes (1 \otimes v) \mapsto u \otimes (v \otimes 1) \mapsto (u \otimes v) \otimes 1 \mapsto 1 \otimes (u \otimes v)$, as required. □

2. If x is a nonzerodivisor on R, it is also on the smallest ideal $\neq 0$ in the specified filtration (or on R/I, if $I = 0$), which is $\cong (R/I)^t$, $t > 0$. Thus, x is a nonzerodivisor on R/I. If x is a nonzerodivisor on R/I, it is also on each I_{t-1}/I_t, since these are (R/I)-free. By the Proposition on p. 1, October 8, and its proof, x is a nonzerodivisor on R, and the filtration is preserved when we kill x. This proves (a). Since I is nilpotent, $\dim(R/I) = \dim(R)$ $\Rightarrow$ the image of a system of parameters for R is a system of parameters for R/I. The statement about the Cohen-Macaulay property in (b) now follows at once from part (a), and the fact that as we successively kill elements of a system of parameters, we are in the same situation that we had initially, but with the dimension one smaller. □

3. (a) Localize at an element in all minimal primes except P so that P is the only minimal prime. Any finitely generated (R/P)-module has a localization at one element not in P that is free. We may apply this successively to each factor in a filtration as discussed in the statement of the problem. Now, when we localize at any prime containing P, we are in the situation of Problem 2, and part (b) gives the required result. □

(b) We apply conditions (1) and (2°) of the criterion at the top of p. 3 of the Lecture Notes from November 5. We know that if $Q \subseteq P$ and R_P is Cohen-Macaulay then R_Q is Cohen-Macaulay. Now suppose that R_P is Cohen-Macaulay and we want an open neighborhood U of P in $\mathcal{V}(P)$ such that R_Q is Cohen-Macaulay for $Q \in U$. Choose a maximal regular sequence in PR_P consisting of images of elements $x_1, \ldots, x_h$ in R. After localizing at one element of R_P, these form a regular sequence in R, and we may kill them without affecting the issue. Thus, we may assume that P is a minimal prime of R. After localizing at one more element of $R - P$, we have from part (a) that P is the only minimal prime of R and that R_Q is Cohen-Macaulay iff $(R/P)_Q$ is Cohen-Macaulay. Thus, we need only consider the case where $R = R/P$ is a domain. Suppose that $R = S/\mathfrak{p}$ where $\mathfrak{p}$ is is a prime ideal of the Cohen-Macaulay ring S. After localizing at one element of $S - \mathfrak{p}$, $\mathfrak{p}$ will contain a maximal regular sequence that is also a maximal regular sequence in $S_\mathfrak{p}$. We may kill it without affecting the issue. We now have that $\mathfrak{p}$ is a minimal prime of the Cohen-Macaulay ring S. By another application of part (a), we may localize at a single element of $S - \mathfrak{p}$ so that $\mathfrak{p}$ is the only minimal prime of S and S_Q is Cohen-Macaulay iff $(S/\mathfrak{p})_Q$ is Cohen-Macaulay. But then $S/\mathfrak{p}$ is Cohen-Macaulay. □

4. Since S is a torsion-free finitely generated R-module it is embeddable in a finitely generated free R-module R^h. The image of 1 in R^h will have at least one nonzero coordinate,

and the composite of $S \hookrightarrow R^h$ and projection on that cooridinate will give an R-linear map $\theta : S \to R$ such that $\theta(1) = c \in R^\circ$. Now suppose that $u \in \langle S \otimes_R N\rangle$ in $S \otimes_R M$. Then there exists $d \in S^\circ$ such that $du^q \in \langle S \otimes_R N\rangle^{[q]} = \langle S \otimes_R N^{[q]}\rangle$ for all $q \gg 0$. We may replace d by a nonzero multiple R°, and so we may assume that that $d \in R^\circ$. Now apply $\theta \otimes \mathbf{1}_{\mathcal{F}^e(M)}$ to obtain that $c(du^q) \in N^{[q]}$ for all $q \gg 0$, as required. $\square$

5. Write R as a finite-module over a DVR A: it is A-free. Let $M^\natural = \mathrm{Hom}_A(M, A)$. The rank of M over R is its rank over A divided by the rank of R over A, and the same holds for $M^\natural$. Then $M^\natural$ and M have the same rank over R. It suffices to show that the type of M is the number of generators of $M^\natural$ over R. Let x be a regular parameter for A. Let $N = M/xM$. Then $M^\natural/xM^\natural \cong \mathrm{Hom}_K(N, A/xA) = \mathrm{Hom}_K(N, K)$. Let $u_1, \dots, u_h$ generate the maximal ideal of R/xR. Let $\_^*$ indicate duals into K. We have an exact sequence $0 \to V \to N \to N^h$ where $\dim_K(V)$ is the type of M/xM and of M and the map has matrix $(u_1 \ \dots \ u_h)$. Applying $\mathrm{Hom}_K(\_, K)$ gives an exact sequence which shows that $V^* \cong N^*/(u_1, \dots, u_h)N^* \cong M^\natural/mM^\natural$. $\square$

6. Again apply (1) and (2°): we know (1). Since the Cohen-Macaulay locus is open, we may assume that the ring is Cohen-Macaulay. Suppose the type of R_P is t. We may also localize at $c \in R - P$ so that R/P is Cohen-Macaulay. As in 3., we may assume P is the only minimal prime of R. If $R = S/J$, with S Gorenstein, then $R/P = S/Q$ for a prime ideal Q of S. After localizing $c \in S - Q$, we may kill a maximal regular sequence for S_Q that is is in J. After localizaing at $c' \in S - Q$ we may assume that S is Gorenstein with unique minimal prime Q, and that $R = S/J$ with $J \subseteq Q$. Since R_P has type t, we have an S_Q-module embedding $\iota : R/P \hookrightarrow (S/Q)^{\oplus t}$: embed the socle of R_P and then extend the map to R_P using that S_Q is injective. Since localization commutes with Hom, we have $R \hookrightarrow S^t$ inducing $\alpha\iota$, where α is a unit of S_Q. Then $0 \to R \to S^t \to C \to 0$ is exact where each S-module is killed by a power of Q. Filter R and C so that the finitely many factors are (S/Q)-modules, and localize at $c'' \in S - Q$ so that all factors are free over $S/Q = R/P$. Then all of R, C, S^t are maximal Cohen-Macaulay modules. If we localize at any prime $\mathcal{M}$ of S and kill a system of parameters $y_1, \dots, y_k$, we get an exact sequence $0 \to R_{\mathcal{M}}/(y_1, \dots, y_k)R_{\mathcal{M}} \to \big(S_{\mathcal{M}}/(y_1, \dots, y_k)S_{\mathcal{M}}\big)^{\oplus t} \to C_{\mathcal{M}}/(y_1, \dots, y_k)C_{\mathcal{M}} \to 0$, and since the socle in the middle term has dimension at most t, so does the socle in $R/(y_1, \dots, y_k)R$.

If R is excellent, localize at $c \in R - P$ so that R/P is regular. Let $M_i = \mathrm{Ann}_R P^i$ and $M = M_1$. Localize at $c' \in R - P$ so that all the M_{i+1}/M_i are (R/P)-free. Then $M \cong (R/P)^{\oplus t}$, since M is R/P-free, and its rank is t because R_P has type t. For each prime Q of R, let $B = {}^Q B$ be the quotient of R_Q by the images of elements $x_1, \dots, x_K \in R$ that form a regular system of parameters in $(R/P)_Q$. We shall write $\__B$ for $B \otimes_R \_$. $PR_B = PB$ is the maximal ideal of $R_B = B$, and is nilpotent. B/PB is a field. We show by induction on n that, after localizing at $c'' \in R - P$, then $(*)$ for $Q \in \mathrm{Spec}\,(R)$, $\mathrm{Ann}_B P^i$ is $(M_i)_B$. In particular, the socle of B is $(M_1)_B \cong (B/PB)^t$, and so the type is t, as required. By the induction hypothesis, we may assume that we have localized so that $(*)$ holds for R/M_1. We know $M_1 = (R/P)^{\oplus t}$. We have an exact sequence $(*)\quad 0 \to M_1 \to R \to R/M_1 \to 0$ which yields $(\#)\quad 0 \to \mathrm{Hom}_R(R/P, M_1) \xrightarrow{f} \mathrm{Hom}_R(R/P, R) \to \mathrm{Hom}_R(R/P, R/M_1) \xrightarrow{\partial}$

$\mathrm{Ext}^1_R(R/P,\, M_1) \to D \to 0$, where $D = \mathrm{Coker}\,(\partial)$. The map f is onto and so ∂ is injective. We want to compare the result of applying $\_{}_B$ to $(\#)$ with the result of forming the long exact sequence $(\#_B)$, , truncated at the same spot, for $\mathrm{Hom}_B\bigl(B/PB,\, \_\bigr)$ applied to the short exact sequence obtained by applying $\_{}_B$ to $(*)$. We want these two to be the same. It suffices to localize at $c''' \in R - P$ so the map ∂_B in $(\#_B)$ is still injective, and $\_{}_B$ commutes with the formation of $\mathrm{Hom}_R(R/P,\, R/M_1)$ and $\mathrm{Ext}^1(R/P,\, M)$ as well as the formation of the connecting homomorphism. For then the counterpart f_B of f in $(\#_B)$ will again be onto. This can be achieved by localizing to make sufficiently many (but finitely many) auxiliary modules have finite filtrations by free (R/P)-modules, along with the observation that for $\mathrm{Hom}_R(R/P,\, R/M_1)$, we get what we need from the induction hypothesis. Localization at Q and killing a regular system of parameters in R_Q then preserve exactness. Let $G_2 \to G_1 \to G_0 \to R/P \to 0$ be part of a finite free R-resolution for R/P. Then we also have exact sequences $0 \to Z_1 \to \mathrm{Hom}_R(G_1,\, M_1) \to \mathrm{Hom}_R(G_2,\, M_1) \to E \to 0$, $0 \to Z_0 \to \mathrm{Hom}_R(G_0,\, M_1) \to B_1 \to 0$, and $0 \to B_1 \to Z_1 \to \mathrm{Ext}^1_R(R/P,\, M_1) \to 0$, If we localize so that every module occurring has a finite filtration by free R/P-modules, then $x_1, \ldots, x_k$ is a regular sequence on every module after localization at Q, and the exactness is preserved when we apply $\_{}_B$. Moreover, $\_{}_B$ commutes with Hom from a free R-module. The fact needed about the connecting homomorphism is now easy to check. $\square$

Math 711, Fall 2007 **Problem Set #5 Solutions**

1. (a) The extension is module-finite since the equation is monic in Z, and generically étale since adjoining a cube root gives a separable field extension in characteristic $\neq 3$. The matrix has as entries the traces of the elements $z^{i-1+j-1}$, $1 \leq i, j \leq 3$. The trace of 1 is 3, and the trace of multiplication by z or z^2 is 0 (the matrices have all zeros on the diagonal). Since $z^3 = -(x^3+y^3)$ and $z^4 = -(x^3+y^3)z$, the matrix of traces is $\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & -3(x^3+y^3) \\ 0 & -3(x^3+y^3) & 0 \end{pmatrix}$, whose determinant is $-27(x^3+y^3)^2 = -27z^6$.

(b) The partial derivatives are $3X^2$, $3Y^2$, and $3Z^2$, and 3 is invertible in K. $\square$

2. R is Gorenstein, and not weakly F-regular, since $z^2 \in (x, y)^*$. (The solution for 5(b) in Problem Set #3 gives $x(z^2)^q \in (x^q, y^q)$ for all q.) Hence, no parameter ideal is tightly closed in R. Since z^2 is a socle generator mod (x, y), $(xy)z^2$ is mod (x^2, y^2). Mod $J = (x^2, y^2, xyz^2)$ the ring is K-spanned by 1, x, y, z, xy, xz, yz, z^2, xz^2, yz^2 and xyz. It suffices to show that $J = I^*$: since $I \neq I^*$, $xyz^2 \in I^*$. If not, there exists $v \in I^*$ representing a socle element of $R/J - \{0\}$. The socle in R/J is spanned by the images of xz^2, yz^2, and xyz. Hence, it suffices if when $a, b, c \in K$, not all 0, then for some q, $x^2(axz^2 + byz^2 + cxyz)^q \notin (x^{2q}, y^{2q})$. The left hand side is $A + B + C$ where $A = a^q x^{q+2}(x^3+y^3)^k z^\rho$, $B = b^q x^2 y^q (x^3+y^3)^k z^\rho$, and $C = c^q x^{q+2} y^q (x^3+y^3)^h z^{\rho'}$, where $2q = 3k + \rho$, $q = 3h + \rho'$, with $1 \leq \rho, \rho' \leq 2$. R is $K[x, y]$-free on the basis $1, z, z^2$. Since $\rho \equiv 3\rho' \mod 3$, terms from C cannot cancel those from A or B. Exponents on x in terms from A are $\equiv q+2 \mod 3$; those from B are $\equiv 2 \mod 3$: these cannot cancel either.

Thus, if $az^2x + bz^2y + cxyz \in I^*$, each term with nonzero coefficient $\in I^*$. Thus, it suffices to show that each of $z^2x, z^2y, zxy \notin I^*$. Say $zxy \in I^*$. Then colon-capturing (cf. the Theorem, bottom of p. 2, November 12) gives $z \in (x^2, y^2)^* : xy \subseteq \bigl((x^2, y^2) : xy\bigr)^* = (x, y)^*$. But $x^2 z^q = x^2(x^3+y^3)^h z a^\rho$, and if $q = p$, $x^2(x^3+y^3)^h$ has a term $x^2 x^{3\lfloor h/2 \rfloor} y^{3(h - \lfloor h/2 \rfloor)}$. Since $3\lfloor h/2 \rfloor \leq 3h/2 \leq p/2 < p$ and $3(h - \lfloor h/2 \rfloor) \leq 3\bigl(h - (h-1/2)\bigr) \leq 3h + 3/2 < p+1 < 2p$, and $\binom{k}{\lfloor h/2 \rfloor} \neq 0$ with $k < p$, $z \notin (x^2, y^2)$.

If $xz^2 \in (x^2, y^2)^*$, then $z^2 \in (x^2, y^2)^* : x \subseteq \bigl((x^2, y^2) : x\bigr)^* = (x^2, y)^*$. We will show this is false. (By symmetry, this handles $v = yz^2$.) Then $x^2 z^{2q} \in (x^{2q}, y^q)$ for all q $\Rightarrow x^2(x^3+y^3)^k z^{\rho'} \in (x^{2q}, y^q)$ and so $x^2(x^3+y^3)^k \in (x^{2q}, y^q)$. But $\binom{k}{1} x^2 (x^3)^{k-1} y^3 \notin (x^{2q}, y^q)$: since p does not divide $k = (2q - \rho')/3$ the coefficient is nonzero, while the degree in x is $2 + 3k - 3 = 3k - 1 < 2q$ and the degree in y is $3 < q$ for all $q \gg 0$.

It follows that the test ideal in R_m where $m = (x, y, z)R$ is $(x^2, y^2)R_m : JR_m = mR_m$, i.e., the annihilator of 0^*_E in the injective hull of R_m/mR_m is m. This is also true for $E_R(R/m) \cong E$. The localization at other maximal ideals is regular, and the annihilator of $0^*_{E'} = 0$ in the injective hull E' of R/m' for any other maximal ideal m' of R. It follows from the Theorem at the top of p. 5, notes from Novemberr 30, that $\tau(R) = m$. $\square$

3. Suppose $u \in R$ (we may assume this after clearing denominators) has the property that its image in $W^{-1}R$ is in $(IW^{-1}R)^* - (I^*)W^{-1}R$. Choose a prime ideal of $W^{-1}R$ that contains $(I^*)W^{-1}R :_{W^{-1}R} u \supseteq IW^{-1}R$. Localizing at this prime gives a counterexample in which $W = R - P$ for some prime P with $I \subseteq P$. But then I is generated by part of a system of parameters for R_P, and we may replace tight closure by plus closure throughout. Since plus closure commutes with localization, the result follows.

4. We need to prove that every ideal I generated by parameters in R is tightly closed. But if $u \in R$ and $u \in I^* = I^+$, there is a module-finite extension S of R such that $u \in IS \cap R$. Since $R \hookrightarrow S$ splits by hypothesis, $IS \cap R = I$. $\square$

5. Since R is complete, it suffices to prove that ideals I of R are contracted from S. Suppose $u \in IS \cap R$. Since R is weakly F-regular, it suffices to show that $u \in I^*$. Hence, it suffices to show that S is a solid R-algebra, i.e., that $H^d_m(S) \neq 0$, or $H^d_{mS}(S) \neq 0$. Since height $(mS) = d$, we can pick a minimal prime $\mathcal{M}$ of mS of height d. Then $\mathcal{M}S_{\mathcal{M}} = \mathrm{Rad}\,(mS_{\mathcal{M}})$, and so $H^d_{mS}(S)_{\mathcal{M}} = H^d_{mS}(S_{\mathcal{M}}) = H^d_{\mathcal{M}S_{\mathcal{M}}}(S_{\mathcal{M}}) \neq 0$, since $\dim\,(S_{\mathcal{M}}) = d$. $\square$

6. Assume $(*_q)\quad cG^q = u_{q1}G_1^q + \cdots u_{qh}G_h^q$ for $q \gg q_1$ where $G, G_1, \ldots, G_h$ all have the same degree and $c \neq 0$. The same holds when we pass to a homogenous component $c_k \neq 0$ of c and the degree k components of the u_i. Thus, we may assume that c and all $u_{qh} \in [R]_k$. Take h minimum. If all of the $u_{qi} \in Kc$, divide by c and take qth roots to show $G \in I$. Hence, for every q, at least one $u_{qi} \notin cK$. Choose i such that $u_{qi} \notin Kc$ for $q \in \mathcal{Q}$ with $|\mathcal{Q}| = \infty$. By renumbering, say $i = h$, so that $u_{qh} \notin Kc$ for $q \in \mathcal{Q}$. It suffices if there exist q_0 and $c' \in R^\circ$, such that for $q \subseteq \mathcal{Q}$, there exists an R^{q_0}-lineaar map $\theta_q : R \to R$ such that $\theta_q(c) = c'$ and $\theta_q(u_{hq}) = 0$. For then applying θ_q for $q \geq \max\{q_0, q_1\}$ with $q \in \mathcal{Q}$ to $(*_q)$ shows that $c'G^q \in (G_1, \ldots, G_{h-1})^{[q]}$ for infinitely many q, and we may replace h by $h-1$.

Let $\mathcal{K} = \mathrm{frac}\,(R)$ and $K' = \bigcap_q \mathcal{K}^q$. Then $K' = K$: to see this, choose a separating transcendence basis for $\mathcal{K}$ and enlarge $\mathcal{K}$ to be Galois over a pure transcendental extension $\mathcal{F} = K(y_1, \ldots, y_d)$. Given $w \in K' - K$, all elementary symmetric functions of its conjugates over $\mathcal{F}$ are also in K', and so one of them $z \in \mathcal{F} \cap K' - K$. Write $z = (f/g)^q$ with $f, g \in K[\underline{y}]$ in lowest terms and not all exponents divisible by p. Then z has a pqth root in $\mathcal{K}$, and so f/g has a pth root in $\mathcal{K}$ not in $\mathcal{F}$, contradicting that $\mathcal{K}/\mathcal{F}$ is Galois.

Let $v_1, \ldots, v_N$ be a K-basis for $[R]_K$. Then $\dim_{\mathcal{K}^q} \mathrm{span}_{\mathcal{K}^q}\{v_1, \ldots, v_n\}$ cannot decrease with q. Pick q_0 for which it is maximum, and renumber so that $v_1, \ldots, v_t$ give a basis for the span over $\mathcal{K}^{q_0}$. If $t < N$, write v_{t+1} as a $\mathcal{K}^{q_0}$-linear combination of $v_1, \ldots, v_t$. Then we must have that some coefficient is not in K, and we can choose $q' > q_0$ so that this coefficient is not in $\mathcal{K}^{q'}$. Then $v_1, \ldots, v_{t+1}$ are independent over $\mathcal{K}^{q'}$: a new relation would give a relation on $v_1, \ldots, v_t$. Thus, $v_1, \ldots, v_N$ are independent over $\mathcal{K}^{q_0}$. Extend $v_1, \ldots, v_N$ to $v_1, \ldots, v_B \in R$, a $\mathcal{K}^{q_0}$-basis for $\mathcal{K}$ over $\mathcal{K}^{q_0}$. Then we can choose $d \in R^{q_0} - \{0\}$ such that $dR \subseteq M = \sum_{j=1}^B R^{q_0}v_j$. We can now define θ_q as follows. Choose a K-linear map $T : V \to R$ that sends c to c, and kills u_h: this is possible since c and u_h are linearly independent over K. Extend this map to $M = \sum_{j=1}^B R^{q_0}v_j \to R$: let the values on $v_1, \ldots, v_N$ be given by T, and choose the values on the other v_j arbitrarily. This gives $\eta_q : M \to R$ that is R^{q_0}-linear such that $\theta_q(c) = c$ and $\eta_q(u_{qh}) = 0$. Finally, define θ_q on R by $\theta_q(r) = \eta_q(dr)$. Then $\theta_q(c) = \eta_q(dc) = d\eta_q(c) = dc$, and $\theta_a(u_{hq}) = \eta_q(du_{hq}) = d\eta_q u_{hq}) = 0$. Take $c' = dc$. $\square$