FOUNDATIONS OF TIGHT CLOSURE THEORY

Mel Hochster

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA

E-mail address: hochster@umich.edu

FOUNDATIONS OF TIGHT CLOSURE THEORY

Prof. Mel Hochster, instructor
hochster@umich.edu

These are lecture notes for Math 615, Winter 2022. The individual lectures are organized into sections.

Contents

Preface

These notes give an introduction to tight closure theory based on lectures at the University of Michigan given in Math 711 in Fall, 2007, which were revised for Math 615 in Winter 2022. It is primarily the positive characteristic theory that 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. The structure of the individual lectures has been preserved.

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 sets of supplementary problems 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 over a period of years through grants DMS-0400633, DMS-0901145, DMS-1401384, and DMS-1902116.

1. Lecture 1

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.

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.

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* $(R,\, \mathfrak{m},\, K)$ 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 $(R,\, \mathfrak{m},\, K)$ 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, $0 \leq i \leq n-1$, 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 $(R,\, \mathfrak{m},\, K)$, 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 $x_1,\, \ldots, x_n \in R$ is a possibly improper regular sequence on M and and S is any flat R-algebra, then the images of $x_1,\, \ldots, x_n$ 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 $x_1,\, \ldots, x_n$ is a regular sequence on M and S is flat over R, it remains a regular sequence provided that $S \otimes_R \big(M/(x_1,\, \ldots, x_n)M\big) \neq 0$, which is always the case when S is faithfully flat over R.

1.1. Nakayama's Lemma, including the homogeneous case. Recall that in Nakayama's Lemma one has a *finitely generated module* M over a quasilocal ring $(R, \mathfrak{m}, K)$. The lemma states that if $M = mM$ then $M = 0$. (In fact, if $u_1, \ldots, u_h$ 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 $h, k \in H$, $R_hM_k \subseteq M_{h+k}$. 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.

Theorem 1.1. *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_tv_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_tv_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. $\square$

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 $(R, \mathfrak{m}, K)$, 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 $(R, \mathfrak{m}, K)$ may also be characterized as the least integer n such that there exists a sequence $x_1, \ldots, x_n \in m$ such that $m = \mathrm{Rad}\big((x_1, \ldots, x_n)R\big)$ (equivalently, such that $\overline{R} = R/(x_1, \ldots, x_n)R$ 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 $(R, \mathfrak{m}, K)$ 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 $x_1, \ldots, x_k$ have been chosen so that $x_1, \ldots, x_k$ is part of a system of parameters (equivalently, such that $\dim\big(R/(x_1, \ldots, x_k)R\big) = \dim(R) - k)$), if $k < \dim(R)$ the minimal primes of $(x_1, \ldots, x_k)R$ cannot cover m. It follows that we can choose x_{k+1} not in any such minimal prime, and then $x_1, \ldots, x_{k+1}$ 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 $(x_1, \ldots, x_k)R$ such that $\dim(R/Q) = \dim\big(R/(x_1, \ldots, x_k)R\big)$ (which is $\dim(R) - k$).

Discussion 1.2. Cohen-Macaulay rings 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*, local complete intersection 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.

1.2. 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:

Theorem 1.3. *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 homogeneous 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. $\square$

Corollary 1.4. *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,

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

and so equality holds throughout, as required. □

Proposition 1.5. *(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 homogeneous 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 1.6. *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

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

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) $\Rightarrow$ (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) $\Rightarrow$ (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 1.7. **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) $(R, \mathfrak{m}, K)$ is local and $f_1, \ldots, f_n$ and $g_1, \ldots, g_n$ are two systems of parameters. (1)
(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, $1 \le i \le n$). 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 $(R, \mathfrak{m}, K)$ 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 1.8. *Let $(R, \mathfrak{m}, K)$ 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 1.9. *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 1.10. *et 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, $0 \le k \le n-1$. 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 1.9 we also have:

THEOREM 1.11. *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 $(R, \mathfrak{m}, K)$ 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 $x_1, \dots, x_n$ is a system of parameters, R turns out to be module-finite over the formal power series ring $K[[x_1, \dots, x_n]]$ 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.

1.3. 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 $(R, \mathfrak{m}, K)$ 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 $(R, \mathfrak{m}, K)$ is local and normal, then it is a domain. 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.

1.4. 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 1.12. *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 $\{I_n S\}_n$ is stable from some point on, say $I_t S = I_N S$ for all $t \geq N$. We may then apply (a) to obtain that $I_t = I_t S \cap R = I_N S \cap R = I_N$ 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 $F_1, \ldots, F_n$ of positive degree. Then $R = A[F_1, \ldots, F_n]$: otherwise, choose a form G of least degree that is in R and not in $A[F_1, \ldots, F_n]$. Then $G \in J$, and so we can write G as a sum of terms $H_j F_j$ 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 $\operatorname{frac}(S)$ 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 $r = a/b \in R$. □

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

EXAMPLE 1.13. 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, $K[x, y, z]/(x, y) \cong K[z]/(z^3)$. □

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.)

1.6. 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 $n \in \mathbb{N}$).

DISCUSSION 1.14. **Consequences of tight closure theory.** 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 in positive prime characteristic is an open question.

(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 $(R, \mathfrak{m}, K)$ 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 was first shown when the ring R contains a field [**Ho94a, HH95**] . 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. Cf. [**Heit02, Ho02**]. Recently, the result has been proved in general: see [**And20, ?**].

Big Cohen-Macaulay algebras can be used to prove results like those mentioned in (1), (4), and (6) for tight closure. In fact the existence of a tight closure theory with sufficiently good properties in mixed characteristic is closed to being 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. There are specific results in this direction in [**Die10, R.G.18, Jia21b**]

2. Lecture 2

2.1. 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) from Lecture 1.

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.

2.2. Analytic spread. In order to give a proof of the result of Rees described above, we introduce the notion of analytic spread. Let $(R, \mathfrak{m}, K)$ 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 $\mathfrak{a}(I)$. 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 $h = \mathfrak{a}(I)$, 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.

2.3. 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, $(R, \mathfrak{m}, K)$ is a normal local domain of dimension 2 and P is a height one prime such that no symbolic power of P is principal. 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. $\square$

2.4. 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 eth 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 qth powers of elements of I. If one has generators for I, their qth 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.)

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 2.1. *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. The maps f $R^q \subseteq R$, $R \xrightarrow{F^e} R$, and $R \subseteq R^{1/q}$ are isomorphic in the domain case.

2.5. 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 situation as in the domain case.

That it, as in the domain case one has a commutative diagram:

$$\begin{array}{ccc} R^q & \xrightarrow{\iota} & R \\ \big\downarrow & & \big\downarrow \mathrm{id} \\ R & \xrightarrow{F^e} & R \\ \big\downarrow & & F^{-e}\big\downarrow \\ R & \xrightarrow{\mathrm{id}} & R^{1/q} \end{array}$$

where the horizontal maps are injections and the vertical maps are all isomorphisms. The map ι is the inclusion map and $F^{-e}(r) = r^{1/q}$.

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 $q \leq q'$, and we define

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

Discussion 2.2. 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 $q \to \infty$.

2.6. 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 characteristic p, 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. $(R, \mathfrak{m}, K)$ 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 $I :_R uR$.

2.7. 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.

2.8. Properties of tight closure. 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 $1 \le j \le h$.

(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.

(6) **(Colon-capturing)** If $(R, \mathfrak{m}, K)$ is a complete local domain (more generally, if $(R, \mathfrak{m}, K)$ is a reduced, excellent, and equidimensional), the elements $x_1, \ldots, x_k, x_{k+1}$ are part of a system of parameters for R, and $I_k = (x_1, \ldots, x_k)R$, 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 does not commute with localization. But property (7) shows that it has an important form of compatibility with localization.

(8) If $(R, \mathfrak{m}, K)$ 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 $(R, \mathfrak{m}, K)$ 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.

2.9. 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 $\operatorname{frac}(R)$ is contained in the algebraic closure L of $\operatorname{frac}(S)$, and L is also an algebraic closure for R, since the elements of S are integral over R and, hence, algebraic over $\operatorname{frac}(R)$. 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, the map $S \hookrightarrow T$ extends to an injection. $S^+ \hookrightarrow T^+$.

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

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

where both vertical maps are inclusions.

2.10. Other characterizations of tight closure. For many purposes it suffices to characterize tight closure in the case of a complete local domain. Let $(R, \mathfrak{m}, K)$ be a complete local domain of characteristic p. 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 2.4. *Let $(R, \mathfrak{m}, K)$ be a complete local domain of characteristic p, $u \in R$, and $I \subseteq R$. Choose a complete DVR (V, m_V, L) containing $(R, \mathfrak{m}, K)$ 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 [**HH91b**].

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^*.

2.11. 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 $u \in S$. A detailed treatment may be found in [**Ho94a**].

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 often very difficult to determine whether M is solid or not.

For those familiar with local cohomology, we note that if $(R, \mathfrak{m}, K)$ 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 2.5. *Let $(R, \mathfrak{m}, K)$ 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 2.6. *Let* $(R, \mathfrak{m}, K)$ *be a complete local domain of characteristic* p. *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 refrring to the Frobenius endomorphism, and thereby suggest closure operations not necessarily in characteristic p 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. An example due to Paul Roberts [**Rob94**] shows that if K has characteristic 0 and $R = K[[x, y, z]]$, then in R one has that $x^2y^2z^2$ is in the solid closure of (x^3, y^3, z^3). Specifically, the algebra $K[[x, y, z]][u, v, w]/(x^2y^2z^2 - ux^3 - vy^3 - wz^3)$ is solid! This is proved not by exhibiting the nonzero map back to R but by proving that a specific element in the local cohomology is not 0. The argument uses classical identities involving detteereminants of matrices of binomial coefficients.

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, and the existence of big Cohen-Macaulay algebras in mixed characteristic is now known: see, for example [**And20**].

3. Lecture 3

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 [**Mo83**]. We use $\ell(M)$ for the length of a finite length module M.

3.1. Hilbert-Kunz multiplicities. Let $(R, \mathfrak{m}, K)$ 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 3.1 (P. Monsky). *Let* $(R, \mathfrak{m}, K)$ *be a local ring of characteristic* p *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

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

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 of the existence of the limit γ is, in a sense, not constructive. He achieves this by proving that $\{\dfrac{\ell(M/\mathfrak{A}^{[q]}M)}{q^d}\}_q$ is a Cauchy sequence. The limit is only known to be a real number, not a rational number.

Example 3.2. Here is one instance of the non-polynomial behavior of Hilbert-Kunz functions. See [**HaMo83**]. Let

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

with maximal ideal m. Then

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

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

Theorem 3.3. *Let $(R, \mathfrak{m}, K)$ be a complete local ring of characteristic p 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 $(R, \mathfrak{m}, K)$ 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.

3.2. The rings R^+. 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 [**HH92**].

THEOREM 3.4. *Let $(R, \mathfrak{m}, K)$ be a complete (excellent also suffices) local domain of characteristic p. 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 3.5. *Let $(R, \mathfrak{m}, K)$ be a complete local domain of characteristic p. 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 $(R, \mathfrak{m}, K)$ 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. see Example **??**. 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^+.

3.3. Using trace to get a retraction. One key point is the following:

THEOREM 3.6. *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 1.12

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 $1 \le i, j \le n$ 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 $d < j \le n$ 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

$$T = V s_1 + \cdots + V s_n,$$

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 $s_1, \dots, s_d$ 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 $s_1, \dots, s_d \in S$ 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 3.7. *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 $f_1, \dots, f_h \in I$ and $s_1, \dots, s_h \in S$ such that

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

Let $S_1 = R[s_1, \dots, s_h]$. 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 1.12, 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.

3.4. Absolute integral closure, plus closure, and related ideas. Note that the result on homomorphisms of absolute integral closures of rings given in the Proposition 2.3 then yields:

Theorem 3.8. *Let $R \to S$ be a local homomorphism of complete local domains of characteristic p. 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 [**Sm94**] (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 3.9. *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) of 2.8 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 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, tight closure does not commute with localization [**?**].

Recently, the Theorem that R^+ is a big Cohen-Macaulay algebra when $(R, \mathfrak{m}, K)$ is an excellent local domain of characteristic p has been strengthened by C. Huneke and G. Lyubeznik. See [**HuLy07**]. 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.

Next, we want to mention the following result of Ray Heitmann [**Heit02**], referred to earlier. Ideas related to this result have led to vast recent progress, in which the existence of big Cohen-Macaulay algebras have been shown to exist in general by arguments utiizing almost mathematics, perfectoid geometry (cf. [**HeitMa18, And20**]) and in some cases very sophisticated cohomological techniques: see [**Bha21**].

Theorem 3.10 (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 $N \in \mathbb{N}$, $p^{1/N}r \in (x, y)R^+$.*

The condition satisfied by r in this Theorem bears a striking resemblance to one of our characterizations of tight closure: see condition (#) in Discussion 2.2. In a way, it is very different: in tight closure theory, the element c is anything but p, which is 0. [**Heit05**] 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 [**Ho02**].

For some of the most recent advances in this area we refer the reader to [**And20, Bha21, Jia21b**]. As indicated in [**Jia21b**] and the earlier papers [**Die10**] and [**R.G.18**], the construction of big Cohen-Macaulay algebras and the existence of operations similar to tight closure go hand in hand.

4. Lecture 4

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.

4.1. 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 $\mathrm{id}_S \otimes_R h$ 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 $\big(r_{ij}\big)$ to the cokernel of the matrix $\big(f(r_{ij})\big)$.
(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.

4.2. The Frobenius functors. Let R be a ring of characteristic p. 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) cF^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 (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 characteristic p, 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 characteristic p. 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.

4.3. 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 4.1. *Let R be a Noetherian ring of prime characteristic $p > 0$. . 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, $1 \le i \le n$, 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 $N_M^{[q]}$ 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 $\square$

Let R and S be Noetherian rings of characteristic p. 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 4.2. *Let $R \to S$ be a homomorphism of Noetherian rings of characteristic p 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. $\square$

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

Theorem 4.3. *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, $1 \leq i \leq n$, $u_i \in (N_i)^*_{M_i}$ 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, $1 \leq i \leq n$.*

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 $q \gg 0$, $c_iu^q \in N^{[q]} + P_iF^e(M)$, 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 $q \gg 0$,

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

since every $d_iP_i \subseteq J$.

Then $c = \sum_{i=1}^n d_ic_i$ 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 $q \geq q_0$. Choose q_1 such that $J^{[q_1]} = 0$. Then $c^{q_1}u^{qq_1} \in N^{[qq_1]}$ for all $q \geq q_0$, which implies that $c^qu^q \in N^{[q]}$ for all $q \geq q_1q_0$. □

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

Corollary 4.4. *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 $R_{red} = R/J$.*

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 4.5. *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 4.6. *Let R be a Noetherian ring of prime characteristic $p > 0$. . Let $N \subseteq M$ be R-modules. Consider the condition:*

(#) 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 $u_1, \dots, u_n$ 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 $q_0 = \max\{q_1, \dots, q_n\}$. 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 $r_1u_1 + \dots + r_nu_n + u$ 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 $v \in N^*$. $\square$

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

COROLLARY 4.7. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let $N \subseteq M$ be finitely generated R-modules. Then $(N^*_M)^*_M = N^*_M$.* $\square$

5. Lecture 5

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

PROPOSITION 5.1. *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. $\square$

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.

5.1. Criteria for flatness. 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 characteristic p.

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

THEOREM 5.2. *Let $(R, \mathfrak{m}, K)$ 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 $P \in \mathrm{Spec}\,(R)$ 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.

DISCUSSION 5.3. We have the following additional comments on the Theorem. Suppose that M is a module over a local ring $(R, \mathfrak{m}, K)$ 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 5.4. *Let $\theta : (R, \mathfrak{m}, K) \to (S, \mathfrak{n}, L)$ be a homomorphism of local rings that is* local, *i.e., $\theta(\mathfrak{m}) \subseteq \mathfrak{n}$. 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

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

The image $f(u)$ of u in $Q \otimes_R \big(N/(m^t M \cap N)\big)$ 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

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

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. $\square$

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 5.5. *Let $(R, \mathfrak{m}, K) \to (S, \mathfrak{n}, L)$ 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^tS 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. $\square$

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 5.6. *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 $R = K[y, x_1, x_2, x_3, \ldots]$ be a polynomial ring in infinitely many variables over K. Let $I = (x_1 y, x_2 y^2, \ldots, x_n y^n, \ldots)$ and let $J = (x_1, x_2, \ldots, x_n, \ldots)$. 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 5.7. *Let R be a regular Noetherian ring of characteristic p. 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

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

□

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

Theorem 5.8. *Let R be a regular Noetherian ring of characteristic p. 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 $(R, \mathfrak{m}, K)$. 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 $c \in R^\circ$. □

6. Lecture 6

6.1. Weaky F-regular rings. 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 characteristic p 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 6.1. *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 6.2 (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. $\square$

Proposition 6.3. *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 $g \in I$. $\square$

Lemma 6.4. *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 6.5. *Let R be a Noetherian ring of prime characteristic $p > 0$. Then the following conditions are equivalent:*

(a) R is weakly F-regular.
(b) $R_\mathfrak{m}$ is weakly F-regular for every maximal ideal $\mathfrak{m}$ 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 Lemma 6.1 $R/\mathfrak{A}$ is killed by a power of a maximal ideal $\mathfrak{m}$, so that $\mathfrak{A}$ is $\mathfrak{m}$-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 $R_\mathfrak{m}$ are tightly closed, and the equivalence with (c) follows from Lemma 6.4. □

We next make the following elementary observations about tight closure.

PROPOSITION 6.6. *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. $\square$

6.2. The Briançon-Skoda theorem. We next give a tight closure version of the Briançon-Skoda theorem. This result was proved by Briançon and Skoda [**BrSk74**] for finitely generated $\mathbb{C}$-algebras and analytic regular local rings using a criterion of Skoda [**Sk72**] for when an analytic function is in an ideal in terms of the finiteness of a certain integral. Lipman and Teissier [**LT81**] gave an algebraic proof for certain cases, and Lipman and Sathaye [**LS81**] proved the result in general for regular rings, even in mixed caracteristic. 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 characteristic p.

THEOREM 6.7 (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 6.8. *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 6.9. *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 Spec (R) is connected. We first want to show that R is a domain in this case. If not, there are minimal primes $P_1, \ldots, P_n$, $n \geq 2$, 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

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

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 characteristic p. 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 [**ELS01**], using the theory of multiplier ideals. The proof we give here may be found in [**HH02**].

THEOREM 6.10. *Let P be a prime ideal of height h in a regular ring R of characteristic p. Then for every integer $n \geq 1$, $P^{(hn)} \subseteq P^n$.*

The version stated above remains true with the hypotheses weakened in various ways. For example P onlty needs to be a radical ideal, and there are many other refinements. See, for example, [**HH02**].

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.

Using the methods of perfectoid geometry, the result for radical ideaals was extended to the case of mixed characteristic in [**MaSch18**] under mild hypotheses on the regular ring. Stronger results valid for all regular rings have been obtained quite recently in [**Mur22**].

There are further comments about what can be proved in the sequel: see Discussion 6.12 at the end of this subsection. 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 6.11. *Let P be a prime ideal of height h in a regular ring R of characteristic p.*

(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. □

Discussion 6.12. 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 [**HH02**]

7. Lecture 7

7.1. 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 7.1. 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 7.2. *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 7.3. *If $N \subseteq M$ are R-modules, S is faithfully flat over R, and $v \in M \setminus N$, 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 $(*)\quad Rv \to S \otimes_R Rv$ 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 7.4. *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 (big) 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. □

Definition 7.5 (**Test ideals.**). Let R be a Noetherian ring of prime characteristic $p > 0$, and assume that R is reduced. We define the $\tau(R)$ 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 7.6. *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 7.7. *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. □

DISCUSSION 7.8. Earlier, in 2.7 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 [**Mat70**, Chapter 13].

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

7.2. 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-algebras

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

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 $(R, \mathfrak{m}, K)$ 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 $R \to S$.

7.3. 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 7.9. *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:

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

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

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

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 7.10. *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 7.11. *Let $(R, \mathfrak{m}, K) \to (S, Q, L)$ 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 7.12. *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. □

Corollary 7.13. *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. □

Theorem 7.14. *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 $x_1, \dots, x_n$ so as to minimize $[L : L']$ where $L' = K(x_1, \dots, x_n)^{\mathrm{sep}}$. Suppose that $y \in L$ is not separable over $K(x_1, \dots, x_n)$. Choose a minimal polynomial $F(z)$ for y over $K(x_1, \dots, x_n)$. 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 $H(x_1, \dots, x_n, z) \in K[x_1, \dots, x_n][z]$ such that the coefficients in $K[x_1, \dots, x_n]$ are relatively prime, and such that the polynomial is irreducible over $K(x_1, \dots, x_n)[z]$. By Gauss's Lemma, this polynomial is irreducible in $K[x_1, \dots, x_n, z]$. 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 $K(x_1, \dots, x_{n-1}, y)$, and we may use the transcendence basis $x_1, \dots, x_{n-1}, y$ for L. Note that $x_n, y \in K(x_1, \dots, x_{n-1}, y)^{\mathrm{sep}} = L''$, which is therefore strictly larger than $L' = K(x_1, \dots, x_n)^{\mathrm{sep}}$. Hence, $[L : L''] < [L : L']$, a contradiction. □

We can now prove:

Theorem 7.15. *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 **??**

Evidently, (1) ⇒ (2). But (2) ⇒ (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 Corollary refsepreg

Now consider the case where R is essentially of finite type over κ. Evidently, (3) ⇒ (5) ⇒ (4) ⇒ (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) ⇒ (3).

Let κ^∞ denote the perfect closure $\displaystyle\bigcup_q \kappa^{1/q}$ 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 $u_1, \dots, u_n$ be a minimal set of generators of the maximal ideal of $B = \kappa^\infty \otimes_\kappa R_m$, and choose κ' sufficiently large that $u_1, \dots, u_n$ are elements of $A = \kappa' \otimes_R R_m$. Let $J = (u_1, \dots, u_n)A$. 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 7.13 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. $\square$

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 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 [**Swan98**].

7.4. 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 [**Nag**, pp. 204–5, Appendix], 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 7.16. *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 7.17. *Let $(R, \mathfrak{m}, K)$ 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. $\square$

Corollary 7.18. *If* $(R,\,\mathfrak{m},\,K)$ *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 7.19. *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 $x_1,\,\dots,x_h$, by Corollary 1.8 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 $R/(x_1,\,\dots,x_h)$: 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 $\dim(R)-h = \dim\big(R/(x_1,\,\dots,x_h)\big)$. 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. □

7.5. Excellent rings revisited. 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 7.20. *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 7.21. *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 [**Mat70**], as mentioned earlier.

Note that one does not expect the completion of an excellent local doman to be a domain. For example, consider the domain $\mathrm{S} = \mathbb{C}[x,\,y]/(y^2 - x^2 - x^3)$, which has dimension one. 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 7.22. **A DVR that is not excellent.** Let K be a perfect field of characteristic p, 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 pth 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,

$$f = t_1x + t_2x^2 + \cdots + t_nx^n + \cdots \in \widehat{V} - V.$$

Note that the pth 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.

8. Lecture 8

8.1. F-finite rings. Let R be a Noetherian ring of characteristic p. 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 8.1. *Let R be a Noetherian ring of characteristic p.*

(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 $(R, \mathfrak{m}, K)$ 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 $A = R^pu_1 + \cdots + R^pu_n$. 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 $S = R_{\mathrm{red}}$. 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 $(R, \mathfrak{m}, K)$ 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 [**Ku76**].

Theorem 8.2 (Kunz). *Every F-finite ring is excellent.*

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

Theorem 8.3. *[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,

$$\{P \in \mathrm{Spec}\,(R) : R_P \text{ is regular}\}$$

is open. Since the complement is closed, there is an ideal I such that

$$\mathcal{V}(I) = \{P \in \mathrm{Spec}\,(R) : R_P \text{ is not regular}\}.$$

We refer to this set of primes as the *singular locus* of $\mathrm{Spec}\,(R)$ 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 8.4. *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 8.5. **F-split rings.** Let R be a ring of characteristic p. 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 8.6. *Let R be a reduced ring of characteristic p. 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:

$$\begin{tikzcd} R^{1/q} \arrow[r, "\theta_e"] & R^{1/q'} \\ R^{1/p} \arrow[u, "\cong"] \arrow[r, "\theta"] & R \arrow[u, "\cong"] \end{tikzcd}$$

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. $\square$

8.2. 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 (Theorem 8.3) stated earlier.

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 $1 \le t \le r \le s$ 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 8.7. *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 8.8. **Strong F-regularity.** Let R be a Noetherian ring of characteristic p, 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 8.9. 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. Also note that if there exists an element $s \in S$ such that the map $\alpha : R \to M$ with $1 \mapsto su$ splits, then the map $\beta : R \to M$ with $1 \mapsto u$ splits. If θ splits α, the map θ' define by $\theta'(m) = \theta(sm)$ splits β.

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

PROPOSITION 8.10. *A strongly F-regular ring R is F-split. In fact, if R is reduced and F-finite and there exists an element $c \in R^\circ$ and a choice of $q = p^e$ such that the map $R \to R^{1/q}$ with $1 \mapsto c^{1/q}$ splits, then R is F-split.*

We also note:

PROPOSITION 8.11. *Suppose that R is a reduced Noetherian ring of characteristic p, 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

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

commutes. Then θ' is $R^{1/p}$-linear and $\theta'(c^{1/pq}) = 1 \in R^{1/p}$. By Remark 8.9, $R \to R^{1/q}$ 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. □

The following fact is now remarkably easy to prove.

Theorem 8.12. *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 8.13. *A strongly F-regular ring is weakly F-regular and, in particular, normal.* □

8.3. 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 8.14 (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*

$$\theta_M : S \otimes_R Hom_R(M, N) \to Hom_S(S \otimes_R M, S \otimes_R N)$$

sending $s \otimes f$ to $s(\mathrm{id}_S \otimes f)$ 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 8.15. *If W is a multiplicative system in R and M is finitely presented, we have that $W^{-1}Hom_R(M, N) \cong Hom_{W^{-1}R}(W^{-1}M, W^{-1}N)$. Moreover, if (R, m) is a local ring and both M, N are finitely generated, we may identify $Hom_{\widehat{R}}(\widehat{M}, \widehat{N})$ with the m-adic completion of $Hom_R(M, N)$ (since m-adic completion is the same as tensoring over R with $\widehat{R}$ (as covariant functors) on finitely generated R-modules).* $\square$

9. Lecture 9

9.1. Properties of Tor. We give a very brief treatment of the Tor functors. If M is any R-module we may form a left resolution of M by projective or even free modules: this means we have a left complex $P_\bullet$

$$\xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \cdots \to \cdots \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0$$

such that the $\mathrm{Coker}\,(d_1) \cong M$ and the complex is exact at P_i for $i \geq 1$. Then for any R-module N, $\mathrm{Tor}_i^R(M, N) := H_i(P_\bullet \otimes_R N)$, which turns out to be independent of the choice of $P_\bullet$ up to canonical isomorphsim. One may also use a projective resolution $Q_\bullet$ of N to obtain the same modules. Then:

THEOREM 9.1. *Let R be any commutative ring and M and N denote R-modules. Then:*

(a) $\mathrm{Tor}_i^R(M,M)$ *is a covariant functor of M and N.*
(b) $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R N$ *as functors in M, N.*
(c) $Tor_i^R(M,N)$ *vanishes for $i \geq 1$ if M or N is flat (hence, if either is free or projective).*
(d) If $0 \to M' \to M \to M'' \to 0$ is exact there is long exact sequence

$$\cdots \to Tor_i^R(M',\, N) \to Tor_i^R(M,\, N) \to Tor_i^R(M'',\, N) \to Tor_{i-1}^R(M',\, N)$$
$$\to \cdots \to \mathrm{Tor}_1^R(M',\, N) \to \mathrm{Tor}_1^R(M,\, N) \to \mathrm{Tor}_1^R(M'',\, N)$$
$$\to M' \otimes_R N \to M \otimes_R N \to M'' \otimes_R N \to 0.$$

(e) $\mathrm{Tor}_i^R(M,N) \cong \mathrm{Tor}_i^R(N,M)$ *as functors of two variables.*
(f) The endomorphism induced on $\mathrm{Tor}_i^R(M,N)$ *by multiplication by $r \in R$ acting on either M or N is multiplication by r acting on* $\mathrm{Tor}_i^R(M.N)$.
(g) $\mathrm{Ann}_R M + \mathrm{Ann}_R N$ *kills* $\mathrm{Tor}_i^R(M,N)$.
(h) If S is a flat R-algebra, $S \otimes_R \mathrm{Tor}_i^R(M,N) \cong \mathrm{Tor}_i^S(S \otimes_R M, S \otimes_R N)$.
(i) The calculation of $\mathrm{Tor}_I^R(M,N)$, *commutes with arbitrary direct sums and direct limits in either M or N.*
(j) If R, M and N are Noetherian, then every $\mathrm{Tor}_i^R(M,N)$ *is Noetherian.*

9.2. Regular sequences and Tor. We next want to note some elementary connections between properties of regular sequences and the vanishing of Tor.

THEOREM 9.2. *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:

$$0 \to \mathrm{Tor}_1^R(I_{k+1},\, M) \to M/I_k M \xrightarrow{x_{k+1}\cdot} M/I_k M$$

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 $M/I_k M$, and this is 0 because $x_1, \ldots, x_n$ is a possibly improper regular sequence on M. $\square$

The following result was stated earlier, as Theorem 5.2, and 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 9.3. *Let $(R, \mathfrak{m}, K)$ 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 Discussion 5.3, 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 Corollary 1.8, 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 associated 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 Theorem 9.2. 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. $\square$

9.3. When does a short exact sequence split? Throughout this section,

$$0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} Q \to 0$$

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 $\eta\alpha = \mathrm{id}_N$. 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 $\beta\theta = \mathrm{id}_Q$. 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 9.4. *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. Consider the sequence

$$(*) \quad 0 \longrightarrow Hom_R(Q,\, N) \xrightarrow{\alpha_*} Hom_R(Q,\, M) \xrightarrow{\beta_*} Hom_R(Q,\, Q) \to 0$$

which is exact except possibly at $Hom_R(Q,\, Q)$, 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 id_Q is in the image of β_*.

Proof. Because Hom commutes with finite direct sum, we have that (1) ⇒ (2), while (2) ⇒ (3) ⇔ (4) ⇒ (5) is clear. It remains to show that (5) ⇒ (1). Suppose $\theta : Q \to M$ is such that $\beta_*(\theta) = \mathrm{id}_Q$. Since β_* is induced by composition with β, we have that $\beta\theta = \mathrm{id}_Q$. □

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

$$\mathcal{D}(I) = \mathrm{Spec}\,(R) - \mathcal{V}(I).$$

In particular,

$$\mathcal{D}(fR) = \{P \in \mathrm{Spec}\,(R) : f \notin P\},$$

and we also write $\mathcal{D}(f)$ or $\mathcal{D}_f$ for $\mathcal{D}(fR)$.

Theorem 9.5. *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 $P \in \mathrm{Spec}\,(R)$ 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 $\mathrm{Spec}\,(R)$.

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 id_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. $\square$

9.4. Supplementary Problems I.

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 characteristic p. 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 $(R, \mathfrak{m}, K)$ be a local ring of characteristic p 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 characteristic p. 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 $(R, \mathfrak{m}, K)$ 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 $t \geq 1$.

10. Lecture 10

10.1. Behavior of strongly F-regular rings.

Theorem 10.1. *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) $\Rightarrow$ (3) $\Rightarrow$ (2) $\Rightarrow$ (1).

To show that (1) $\Rightarrow$ (3), suppose that R is strongly F-regular and let W be a multiplicative system. By the Proposition 6.3, 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) $\Rightarrow$ (2) is obvious.

It remains to show that (2) $\Rightarrow$ (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. $\square$

Corollary 10.2. *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. $\square$

Corollary 10.3. *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. $\square$

Proposition 10.4. *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 ith 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. $\square$

We also have:

Proposition 10.5. *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 9.5, the map $R \to R^{1/q}$ such that $1 \mapsto c^{1/q}$ spits over R, as required. □

THEOREM 10.6. *An F-finite regular ring is strongly F-regular.*

PROOF. We may assume that $(R, \mathfrak{m}, K)$ 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. 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 10.7. q **th 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 10.8. *Let R be a reduced F-finite ring of characteristic p, 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 Remark splitrmk 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

$$\alpha^{1/qq_c} : R^{1/qq_c q_d} \to R^{1/qq_c}$$

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. $\square$

10.2. Strong F-regularity and big test elements. We want to use the theory of strongly F-regular F-finite rings to prove the existence of big test elements.

We first prove two preliminary results:

LEMMA 10.9. *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 10.10. *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 $\eta_1 = c^2\mathrm{id}_R$, 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

$$\eta_{pq}(u) = \theta\big(c^{(p-2)/p}\eta_q(u)\big).$$

Consequently, we have, as required, that

$$\eta_{pq}(1) = \theta\big(c^{(p-2)/p}\eta_q(1)\big) = \theta(c^{(p-2)/p}c^{2/p}) = \theta(c) = c\theta(1) = c^2. \qquad \square$$

$\square$

We can now prove the following:

THEOREM 10.11. *[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 Lemma 10.9 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 this theorem, c^{3N} is then a big test element, and so it suffices to prove the second statement.

Suppose that c satisfies the hypothesis of the second statement. By part (a) of the Proposition 7.4, it suffices to show that if $N \subseteq M$ are arbitrary modules and $u \in N_M^*$, then $c^3u \in N$. 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 $c^3v \in H$. 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.,

$$(\#) \quad dv^{q_d q} = \sum_{i=1}^{n} r_i h_i^{q_d q}$$

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

$$\gamma' : G' = R^{1/qq_d} \otimes_R G \to R \otimes_R G \cong G$$

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. □

Discussion 10.12. As noted earlier in Theorem 8.3 and Corollary 8.4, 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 [**Ku69**]. 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. □

LEMMA 10.13. *Let R be any Noetherian ring (there is no characteristic restriction) and let M be a finitely generated R-module. Then the set* $\{P \in \operatorname{Spec}(R) : M_P \text{ is } R_P - \text{free}\}$ *is Zariski open and is nonempty if R is a domain with fraction field $\mathcal{K}$, in which case there exists $c \in R^\circ$ such that M_c is free.*

PROOF. We can map a finitely generated free module $G \twoheadrightarrow M$, and so we have a short exact sequence $0 \to N \to G \to M \to 0$. The set of primes P such that this is split after localization at P is the same as the set of primes P such that M_P is R_P-free, and we may apply Theorem 9.5(e). If R is a domain, (0) is in the set. Call the defining ideal of the non-free locus I, i.e., the non-free locus is $V(I)$. Then I is a nonzero ideal, or else $(0) \subseteq V(I)$. Choose $c \in I \setminus \{0\}$. $\square$

COROLLARY 10.14. *If R is a nonzero reduce F-finite ring, the regular locus is dense and open.*

PROOF. It suffices to prove this for each connected component, and so we may assume that R is a domain. But then the regular locus is the free locus of $R^{1/p}$. $\square$

In any case, we have proved:

COROLLARY 10.15. *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.*

11. Lecture 11

11.1. The Radu-André theorem and completely stable big test elements. Our next objective is to show that the big test elements produced by Theorem 10.11 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. This will take a considerable effort.

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 [**?, An93**]:

THEOREM 11.1. *Theorem (Radu-André) Let $R \to S$ be a geometrically regular map of F-finite rings of characteristic p. 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 11.2. *Let $R \to S$ be a geometrically regular map of F-finite rings of characteristic p. 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 11.3. *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 $1 \in A$. $\square$

In the proof of the Radu-André Theorem we will need the result just below. A more general theorem may be found in [**Mat70**, 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 11.4 (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 5.4 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

$$\mathrm{Tor}_1^A\big((A/I)^{\oplus h},\, M\big) \longrightarrow \mathrm{Tor}_1^A(Q,\, M) \longrightarrow Z \otimes_A M \xrightarrow{\ \alpha\ } (A/I)^{\oplus h} \otimes_A M$$

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 11.5. *Let $f : A \to B$ be a homomorphism of Noetherian rings of characteristic p 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

$$g\big(\mathcal{V}(bB)\big) = \mathcal{V}(b^q A) \subseteq \mathrm{Spec}\,(A). \qquad \square$$

$\square$

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 11.6 (Radu-André). *Let R and S be F-finite rings of characteristic p 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 $(R, \mathfrak{m}, K)$ 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 see that it can be identified with

$$K^{(e)} \otimes_K (S/mS) \cong (S/mS)[K^{1/q}] \subseteq (S/mS)^{1/q},$$

(note that F^e is injective) and $(S/mS)[K^{1/q}]$ 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 Theorem 1.11 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 11.7. *If $R \to S$ is a flat map of F-finite rings of characteristic p 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 10.8, it will suffice to show that there is an S-linear map $S^{1/q} \to S$ such that $c^{1/q} \mapsto 1$. Let $\theta' = \theta \otimes_R \mathrm{id}_S : R^{1/q} \otimes_R S \to S$, so that θ' is an S-linear map such that $\theta'(c^{1/q} \otimes 1) = 1$. By Corollary 11.2, 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 11.8. *Let R be a reduced F-finite ring of characteristic p 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 Theorem 10.8, 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 $\_ \otimes_R \mathrm{id}_S$ 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 Lemma 10.9 $\square$

12. Lecture 12

12.1. 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

$$\begin{array}{ccc} A_n & \xrightarrow{d_n} & A_{n-1} \\ {\scriptstyle \phi_n}\uparrow & & {\scriptstyle \phi_{n-1}}\uparrow \\ B_n & \xrightarrow{\delta_n} & B_{n-1} \end{array}$$

commute. The *mapping cone* $\mathcal{C}^{\phi_\bullet}_\bullet$ of $\phi_\bullet$ is defined so that $\mathcal{C}^{\phi_\bullet}_n := A_n \oplus B_{n-1}$ 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 $\mathcal{C}^{\phi_\bullet}_\bullet$.

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 12.1. *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 $B_0/\delta_1(B_1) \to A_0/d_1(A_1)$) is injective. Then the mapping cone is an acyclic left complex, and its augmentation is $A_0/\big(d_1(A_1) + \phi_0(B_0)\big)$.* □

12.2. The Koszul complex. The Koszul complex $\mathcal{K}_\bullet(x_1, \dots, x_n;\, R)$ of a sequence of elements $x_1, \dots, x_n \in R$ 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 $\mathcal{K}_\bullet(x_1, \dots, x_n;\, R)$ recursively as follows. If $n > 1$, multiplication by x_n (in every degree) gives a map of complexes

$$\mathcal{K}_\bullet(x_1, \dots, x_{n-1};\, R) \xrightarrow{x_n\cdot} \mathcal{K}_\bullet(x_1, \dots, x_{n-1}),$$

and we let $\mathcal{K}_\bullet(x_1, \dots, x_n;\, R)$ be the mapping cone of this map.

We may prove by induction that $\mathcal{K}_n(x_1, \dots, x_n;\, R)$ 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 $\mathcal{K}_j(x_1, \dots, x_n;\, R)$ 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 $\mathcal{K}_\bullet(x_1, \ldots, x_{n-1}; R)$, by using the free generator $u_{\sigma \cup \{n\}}$ to correspond to u_σ. In this way, it is clear that $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, R)$ is free, and we have indexed its generators in degree j precisely by the j element subsets of $\{1, 2, \ldots, n\}$. It is straightforward to check that the differential is as described above.

12.3. Koszul homology. We define the i th *Koszul homology module*

$$H_i(x_1, \ldots, x_n;\, M)$$

of M with respect to $x_1, \ldots, x_n$ as the i th homology module $H_i\big(\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M)$ of the Koszul complex.

We note the following properties of Koszul homology.

PROPOSITION 12.2. *Let R be a ring and $\underline{x} = x_1, \ldots, x_n \in R$. 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* $H_i(x_1, \ldots, x_n;\, M)$.
(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 $x_1, \ldots, x_n$ is a possibly improper regular sequence on M, then $H_i(\underline{x};\, M) = 0$, $i \ge 1$.

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 $(v_1, \ldots, v_n) \mapsto x_1 v + \cdots + x_n v_n$. 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 12.1. 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. □

Corollary 12.3. *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 $\mathrm{Tor}_n(R/I,\, R/I) = 0$. □

We can define the *Koszul complex* of $x_1, \ldots, x_n \in R$ on an R-module M, which we denote $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M)$, in two ways. One is simply as the complex $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, R) \otimes_R M$. The second is to let $\mathcal{K}_\bullet(x_1; M)$ be the complex

$$0 \to Ru_1 \otimes_R M \to M \to 0,$$

and then to let $\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M)$ be the mapping cone of multiplication by x_n mapping the complex $\mathcal{K}_\bullet(x_1, \ldots, x_{n-1};\, M)$ 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.

12.4. Alternative description of the Koszul complex using exterior algebra. We can also describe the Koszul complex as follows. Let $\underline{x} := x_1, \ldots, x_n \in R$. Let $\mathcal{K}_1 := \mathcal{K}_1(\underline{x}; R)$ be the free module $Ru_1 + \cdots + Ru_n$ on n generators. Then we may identify $\mathcal{K}_i(\underline{x}; R)$ with $\bigwedge^i(\mathcal{K}_1)$ by letting $u_{j_1,\ldots,j_i}$ correspond to $u_{j_1} \wedge \cdots \wedge u_{j_i}$ when $1 \le j_1 < j_2 < \cdots < j_i \le n$. Thus, the entire Koszul complex is the graded associative skew-commutative algebra $\bigwedge(\mathcal{K}_1)$. The skew-commutativity means that if v has degree i and w has degree j, then $u \wedge v = (-1)^{ij} v \wedge u$. It then turns out that the formula

$$d(u_{j_1} \wedge \cdots \wedge u_{j_i}) = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u_{i_1} \wedge \cdots \wedge u_{j_{t-1}} \wedge u_{j_{t+1}} \wedge \cdots \wedge u_{j_i}$$

is correct whenever $j_1, \ldots, j_i$ are integers between 1 and n inclusive, regardless of whether they are in order or whether there are repetitions. In fact, d is an R-derivation on the exterior algebra in the sense that it is R-linear, and if v has degree i, then

$$d(v \wedge w) = dv \wedge w + (-1)^i v \wedge dw.$$

In fact, d is the unique way of extending the map $\mathcal{K}_1 \to R$ such that $u_j \mapsto x_j$ to such a derivation on the exterior algebra.

Here is an application of this point of view. Let $\underline{x} = x_1, \ldots, x_n$ and $\underline{y} = y_1, \ldots, y_n$ be two sets of generators for the same ideal. Let X and Y be $1 \times n$ row vectors with these as entries, and suppose that A is $n \times n$ matrix such that $XA = Y$. One can choose such a matrix to be invertible if the y_i are a permutation of the x_i or obtained from them by operations like multiplying a generator by a unit or adding multiples of one generator to another. Then A induces a map of Koszul complexes which is an isomorphism if A is invertible. To see this, note that A is the matrix of map $\mathcal{K}_1(\underline{y};\, R) \to \mathcal{K}_1(\underline{x};\, R)$ such that this diagram commutes:

$$\begin{array}{ccccc}
\mathcal{K}_1(\underline{y}; R)R & \xrightarrow{Y} & R & \longrightarrow & 0 \\
{\scriptstyle A}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{id}} & & \\
\mathcal{K}_1(\underline{y}; R)R & \xrightarrow{X} & R & \longrightarrow & 0
\end{array}$$

The map extends to a map of the entire Koszul complexes using $\bigwedge^i A : \mathcal{K}_i(\underline{y};\, R) : \mathcal{K}_i(\underline{x};\, R)$ when $\mathcal{K}_i$ is defined using exterior algebra. The map is an isomorphism when A is invertible. By tensoring with an R-module M we also have that A gives a map $\mathcal{K}_\bullet(\underline{y};\, M) \to \mathcal{K}_\bullet(\underline{x};\, M)$ which is an isomorphism when A is invertible.

Hence, A also induces maps of Koszul homology $H_i(\underline{y}; M) \to H_i(\underline{x}; M)$ when which are isomorphisms when A is invertible. Thus, permuting the elements $\underline{x}$ does not change the Koszul homology.

When R is local and $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ generate the same ideal, there is always an invertible matrix A such that $XA = Y$. Hence, in the local case, $H_i(\underline{x}; M)$ does not depend on which generators one chooses for the ideal $(\underline{x})$ *if one does not change the number of generators.*

12.5. Independence of Koszul homology from the choice of 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 calculating $H_j(\underline{x};\, M)$, we can recover the S-module structure on the Koszul homology 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 $H_i(\underline{x};\, M)$.

12.6. 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 12.4. *With notation as in the preceding paragraph,*

$$H_i(\underline{x}_1, \ldots, \underline{x}_; M) \cong \operatorname{Tor}_j^B\big(B/(\underline{X})B,\, M\big).$$

Corollary 12.5. *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

$$(*) \quad H_i(\underline{x};\, M) \cong \operatorname{Tor}_i^B(B/(\underline{X})B,\, M).$$

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 $\operatorname{Tor}_i^B(B/(\underline{X})B,\, M)$. It follows that every $x_i = X_i - (X_i - x_i)$ kills it as well, and the result now follows from $(*)$. $\square$

12.7. An application to the study of regular local rings. Let M be a finitely generated R-module over a local ring $(R,\, \mathfrak{m},\, K)$. 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 $Z_i = \operatorname{Ker}(\alpha_i)$, 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.

Discussion 12.6. **Syzygies**

When M is any R-module and we map a projective module P_0 onto M, the kernel is referrred to as a *(first) module of syzygies* of M, and denoted $\operatorname{syz}^1 M$. We make the convention $\operatorname{syz}^0 M = M$. These modules are not unique. We then define, recursively, and $i+1$st module of syzygies $\operatorname{syz}^{i+1}(M)$ any $\operatorname{syz}^1\big(\operatorname{syz}^i(M)\big)$. Giving a projective. resolution of M and giving successive modules of syzygies of M are essentially equivalent processes. When $(R, \mathfrak{m}, K)$ is local and M is finitely generated, finitely generated projectives are free, and we may calculate may calculate minimal modules of syzygies. A minimal choice of $\mathrm{syz}^1 M$ is obtained by mapping a free module onto M so that a free basis for the free module maps to a minimal set of generators of M. The ranks of the free modules in a minimal free resolution are called the *Betti numbers* b_i of M. Note that b_i is the same as the least number of generators of a minimal i th module of syzygies of M.

We then have the following:

PROPOSITION 12.7. *Let $(R, \mathfrak{m}, K)$ be local, let M be a finitely generated R-modules, and let*

$$\cdots \longrightarrow R^{b_i} \xrightarrow{\alpha_i} \cdots \longrightarrow R^{b_0} \longrightarrow M \longrightarrow 0$$

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

$$\cdots \xrightarrow{0} K^{b_i} \xrightarrow{0} \cdots \xrightarrow{0} K^{b_0} \xrightarrow{0} 0\cdot$$

Since all the maps are zero, the result stated is immediate. □

THEOREM 12.8 (Auslander-Buchsbaum). *Let $(R, \mathfrak{m}, K)$ 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 $(R, \mathfrak{m}, K)$ 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 in some cases but was proved when 2 is invertible in the ring in [**Wa17**]. We refer the reader interested in learning more about this problem to the following selected references: [**BE77, Chan97, Char91, Du00, EiHu92, EvGr85, Hart79, HRi05, HuUl87, Sant80**] and [**Wa17**].

13. Lecture 13

13.1. 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 13.1. *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. □

Corollary 13.2. *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 13.3. *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 13.4. *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 Proposition 13.3, 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

$$H_i(\underline{x}^-;\, M)\xrightarrow{(-1)^i x_n\cdot} H_i(\underline{x}^-;\, M)\to H_i(\underline{x};\, M)\to$$

$$H_{i-1}(\underline{x}^-;\, M)\xrightarrow{(-1)^{i-1}x_n\cdot} H_{i-1}(\underline{x}^-;\, M)\to\cdots$$

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. □

13.2. Injective modules. In studying tight closure, it turns out to be important to understand how it behaves in certain injective modules. We therefore will spend some effort on understanding injective modules.

If $0 \to M \to N \to Q \to 0$ is an exact sequence of R-modules, we know that for any R-module N the sequence

$$0 \to \mathrm{Hom}_R(Q,\, N) \to \mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_R(M,\, N)$$

is exact. An R-module E is called *injective* if, equivalently, (1) $\mathrm{Hom}_R(\_\,,\, E)$ is an exact functor or (2) for any injection $M \hookrightarrow N$, the map $\mathrm{Hom}_R(N,\, E) \to \mathrm{Hom}_R(M,\, E)$ is surjective. In other words, every R-linear map from a submodule M of N to E can be extended to a map of all of N to E.

PROPOSITION 13.5. *An R-module E is injective if and only if for every I ideal I of R and R-linear map $\phi : I \to E$, ϕ extends to a map $R \to E$.*

PROOF. "Only if" is clear, since the condition stated is a particular case of the definition of injective module when $N = R$ and $M = I$. We need to see that the condition is sufficient for injectivity. Let $M \subseteq N$ and $f : M \to E$ be given. We want to extend f to all of N. Define a partial ordering of maps of submodules M' of N to E as follows: $g \le g'$ means that the domain of g is contained in the domain of g' and that g is a restriction of g' (thus, g and g' agree on the smaller domain, where they are both defined). The set of maps that are $\ge f$ (i.e., extensions of f to a submodule $M' \subseteq N$ with $M \subseteq M'$) has the property that every chain has an upper bound: given a chain of maps, the domains form a chain of submodules, and we can define a map from the union to E by letting is value on an element of the union be the value of any map in the chain that is defined on that element: they all agree. It is easy to see that this gives an R-linear map that is an upper bound for the chain of maps. By Zorn's lemma, there is a maximal extension. Let $f' : M' \to N$ be this maximal extension. If $M' = N$, we are done. Suppose not. We shall obtain a contradiction by extending f' further.

If $M' \neq N$, choose $x \in N - M'$. It will suffice to extend f' to $M' + Rx$. Let $I = \{i \in R : ix \in M'\}$, which is an ideal of R. Let $\phi : I \to E$ be defined by $\phi(i) = f'(ix)$ for all $i \in I$. This makes sense since every $ix \in M'$. By hypothesis, we can choose an R-linear map $\psi : R \to E$ such that $\psi(i) = \phi(i)$ for all $i \in I$. We have a map $\gamma : M \oplus R \to E$ defined by the rule $\gamma(u \oplus r) = f'(u) + \psi(r)$. We also have a surjection $M \oplus R \to M + Rx$ that sends $u \oplus r \mapsto u + rx$. We claim that γ kills the kernel of this surjection, and therefore induces a map $M' + Rx \to E$ that extends f'. To see this, note that if $u \oplus r \mapsto 0$ the $u = -rx$, and then $\gamma(u \oplus r) = f'(u) + \psi(r)$. Since $-u = rx$, $r \in I$, and so $\psi(r) = \phi(rx) = f'(-u) = -f'(u)$, and the result follows. $\square$

Recall that a module E over a domain R is *divisible* if, equivalently,

(1) $rE = E$ for all $r \in R - \{0\}$ or (2) for all $e \in E$ and $r \in R - \{0\}$ there exists $e' \in E$ such that $re' = e$.

COROLLARY 13.6. *Over a domain R, every injective module is divisible. Over a principal ideal domain R, a module is injective if and only if it is divisible.*

PROOF. Consider the problem of extending a map of a principal ideal $aR \to E$ to all of R. If $a = 0$ the map is 0 and the 0 map can be used as the required extension. If $a \neq 0$, then since $aR \cong R$ is free on the generator a, the map to be extended might take any value $e \in E$ on a. To extend the map, we must specify the value e' of the extended map on 1 in such a way that the extended maps takes a to e: the condition that e' must satisfy is precisely that $ae' = e$. Thus, E is divisible if and only if every map of a principal ideal of R to E extends to a map of R to E. The result is now obvious, considering that in a principal ideal domain every ideal is principal. □

It is obvious that a homomorphic imag e of a divisible module is divisible. In particular, $W = \mathbb{Q}/\mathbb{Z}$ is divisible $\mathbb{Z}$-module and therefore injective as a $\mathbb{Z}$-module. We shall use the fact that W is injective to construct many injective modules over many other rings. We need several preliminary results.

First note that if C is any ring and V is any C-module, we have a map

$$M \to \mathrm{Hom}_C(\mathrm{Hom}_C(M, V), V)$$

for every R-module M. If $u \in M$, this maps sends u to

$$\theta_u \in \mathrm{Hom}_C\big(\mathrm{Hom}_C(M, V), V\big),$$

define by the rule that $\theta_u(f) = f(u)$ for all $f \in \mathrm{Hom}_C(M, V)$.

Now let $\_^\vee$ denote the contravariant exact functor $\mathrm{Hom}_{\mathbb{Z}}(\_, W)$, where $W = \mathbb{Q}/\mathbb{Z}$ as above. As noted in the preceding paragraph, for every $\mathbb{Z}$-module A we have a map $A \to A^{\vee\vee}$, the double dual into W.

LEMMA 13.7. *With notation in the preceding paragraph, for every $\mathbb{Z}$-module A, A the homomorphism $\theta_A = \theta : A \to A^{\vee\vee}$ is injective.*

If A happens to be an R-module then the map $A \to A^{\vee\vee}$ is R-linear, and for every R-linear map $f : A_1 \to A_2$ we have a commutative diagram of R-linear maps

$$\begin{array}{ccc} A_1^{\vee\vee} & \xrightarrow{f^{\vee\vee}} & A_2^{\vee\vee} \\ {\scriptstyle\theta_{A_1}}\uparrow & & \uparrow{\scriptstyle\theta_{A_2}} \\ A_1 & \xrightarrow[f]{} & A_2 \end{array}$$

PROOF. Given a nonzero element $a \in A$, we must show that there exists $f \in \mathrm{Hom}_{\mathbb{Z}}(A, W)$ such that the image of f under θ_a, is not 0, i.e., such that $f(a) \neq 0$. The $\mathbb{Z}$-submodule D of A generated by a is either $\mathbb{Z}$ or else a nonzero finite cyclic module, which will be isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n > 1$. In either case, there will exist a surjection $D \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ for some $n > 1$, and $\mathbb{Z}/n\mathbb{Z}$ embeds in W: it is isomorphic to the span of the class of $1/n$ in $\mathbb{Q}/\mathbb{Z}$. Thus, we have a nonzero map $D \to W$, namely $D \twoheadrightarrow \mathbb{Z}/n\mathbb{Z} \hookrightarrow W$. Since $D \subseteq A$ and W is injective as a $\mathbb{Z}$-module, this map extends to a map of $f : A \to W$. Evidently, $f(a) \neq 0$.

The verifications of the remaining statements are straightforward and are left to the reader. □

LEMMA 13.8. *Let R be a C-algebra, let G be a flat R-module, and let W be an injective C-module. Then $Hom_C(G, W)$ is an injective R-module.*

PROOF. Because of the natural isomorphism

$$\mathrm{Hom}_R(M, \mathrm{Hom}_C(G, W)) \cong \mathrm{Hom}_C(M \otimes_R G, W)$$

we may view the functor

$$\mathrm{Hom}_R(\_,\, \mathrm{Hom}_C(G, W))$$

as the composition of two functors: $\_ \otimes_R F$ followed by $\mathrm{Hom}_C(\_, W)$. Since G is R-flat, the first is exact, while since W is C-injective, the second is exact. Therefore, the composition is exact. $\square$

We can now put things together:

THEOREM 13.9. *Over every commutative ring R, every R-module embeds in an injective R-module. In fact, this embedding can be achieved canonically, that is, without making any arbitrary choices.*

PROOF. Let M be any R-module. In this construction, $\mathbb{Z}$ will play the role of C above. We can map a free R-module F onto $\mathrm{Hom}_{\mathbb{Z}}(M, W)$, were $W = \mathbb{Q}/\mathbb{Z}$ is injective over $\mathbb{Z}$. We can do this canonically, as in the construction of Tor, by taking one free generator of F for every element of $\mathrm{Hom}_{\mathbb{Z}}(M, W)$. By Lemma 13.8 $F^\vee = \mathrm{Hom}_Z(F, W)$ is R-injective. Since we have a surjection $F \twoheadrightarrow M^\vee$, we may apply $\mathrm{Hom}_{\mathbb{Z}}(\_, W)$ to get an injection $M^{\vee\vee} \hookrightarrow F^\vee$. But we have injection $M \hookrightarrow M^{\vee\vee}$, and so the composite $M \hookrightarrow M^{\vee\vee} \hookrightarrow F^\vee$ embeds M in an injective R-module canonically. $\square$

While the embedding does not involve the axiom of choice, the proof that it is an embedding and the proof that $F^\vee$ is injective do: both use that W is injective. The argument for that used that divisible $\mathbb{Z}$-modules are injective, and the proof of that depended on the Proposition refIext, whose demonstration used Zorn's lemma. Note that if $E \subseteq M$ are R-modules and E is injective, then the identity map $E \to E$

extends to a map from all of M to E that is the identity on E. This means that $E \subseteq M$ splits, and so $M \cong E \oplus_R (M/E)$. This is dual to the fact a surjection $M \twoheadrightarrow P$, with P projective, splits.

14. Lecture 14

14.1. Essential extensions and injective hulls.

DEFINITION 14.1. If R is a ring, a homomorphism of R-modules $h : M \to N$ is called an *essential extension* if it is injective and the following equivalent conditions hold:

(a) Every nonzero submodule of N has nonzero intersection with $h(M)$.
(b) Every nonzero element of N has a nonzero multiple in $h(M)$.
(c) If $\phi : N \to Q$ is a homomorphism and ϕh is injective then ϕ is injective.

PROOF. (a) and (b) are equivalent because a nonzero submodule of N will always have a nonzero cyclic submodule (take the submodule generated by any nonzero element). If (a) holds and $\mathrm{Ker}\,\phi$ is not zero it will meet $h(M)$ in a nonzero module. On the other hand if (c) holds and $W \subseteq N$ is any submodule, let $\phi : N \to N/W$. If W is not zero, this map is not injective, and so ϕh is not injective, which means that W meets $h(M)$. $\square$

PROPOSITION 14.2. *Let M, N, and Q be R-modules.*

(a) If $M \subseteq N \subseteq Q$ then $M \subseteq Q$ is essential if and only if $M \subseteq N$ and $N \subseteq Q$ are both essential.

(b) *If $M \subseteq N$ and $\{N_i\}_i$ is a family of submodules of N each containing M such that $\bigcup_i N_i = N$, then $M \subseteq N$ is essential if and only if $M \subseteq N_i$ is essential for every i.*
(c) *The identity map on M is an essential extension.*
(d) *If $M \subseteq N$ then there exists a maximal submodule N' of N such that $M \subseteq N'$ is essential.*

PROOF. (a), (b) and (c) are easy exercises. (d) is immediate from Zorn's lemma, since the union of a chain of submodules of N containing M each of which is an essential extension of M is again an essential extension of M. $\square$

EXAMPLE 14.3. Let R be an integral domain. The fraction field of R is an essential extension of R, as R-modules.

EXAMPLE 14.4. Let (R, m, K) be a local ring and let N be an R-module such that every element of N is killed by a power of m. Thus, every finitely generated submodule of N has finite length. Let $\mathrm{Soc}\, N$, the socle of N, be $\mathrm{Ann}_N m$, the largest submodule of N which may be viewed as a vector space over K. The $\mathrm{Soc}\, N \subseteq N$ is an essential extension. To see this, let $x \in N$ be given nonzero element and let t be the largest integer such that $m^t x \neq (0)$. Then we can choose $y \in m^t$ such that $yx \neq 0$. Since $m^{t+1}x = 0$, $my \subseteq mm^t x = 0$, and so $y \in \mathrm{Soc} M$. (Exercise: show that if $S \subseteq N$ is any submodule such that $S \subseteq N$ is an essential extension, then $\mathrm{Soc} N \subseteq S$.)

We leave it as an informal exercise to show that if $M_i \subseteq N_i$ is essential, $i = 1, 2$, then $M_1 \oplus M_2 \subseteq N_1 \oplus N_2$ is essential, and that the same holds for arbitrary (possibly infinite) direct sums.

In the situation of Proposition 14.2, we shall say that N' is a *maximal essential extension* of M within N. If $M \subseteq N$ is an essential extension and N has no proper essential extension we shall say that N is a *maximal essential extension* of M. It is not clear that maximal essential extensions in the absolute sense exist. However, they do exist: we shall deduce this from the fact that every module can be embedded in an injective module.

PROPOSITION 14.5. *Let R be a ring.*

(a) *An R-module is injective if and only if it has no proper essential extension.*
(b) *If M is an R-module and $M \subseteq E$ with E injective, then a maximal essential extension of M within E is an injective module and, hence, a direct summand of E. Moreover, it is a maximal essential extension of M in an absolute sense, since it has no proper essential extension.*
(c) *If $M \subseteq E$ and $M \subseteq E'$ are two maximal essential extensions of M, then there is a (non-canonical) isomorphism of E with E' that is the identity map on M.*

PROOF. (a) It is clear that an injective R-module E cannot have a proper essential extension: if $E \subseteq N$ then $N \cong E \oplus E'$, and nonzero elements of E' cannot have a nonzero multiple in E. It follows that $E' = 0$. On the other hand, suppose that M has no proper essential extension and embed M in an injective module E. By Zorn's lemma we can choose $N \subseteq E$ maximal with respect to the property that $N \cap M = 0$. Then $M \subseteq E/N$ is essential, for if N'/N were a nonzero submodule of E/N that did not meet M then $N' \subseteq E$ would be strictly larger than N and would meet M in 0. Thus, $M \to E/N$ is an isomorphism, which implies that $E = M + N$. Since $M \cap N = 0$, we have that $E = M \oplus N$, and so M is injective.

(b) Let E' be a maximal essential extension of M within the injective module E. We claim that E' has no proper essential extension whatsoever, for if $E' \subseteq Q$ were such an extension the inclusion $E' \subseteq E$ would extend to a map $Q \to E$, because E is injective. Moreover, the map $Q \to E$ would have to be injective, because its restriction to E' is injective and $E' \subseteq Q$ is essential. This would yield a proper essential extension of E' within E, a contradiction. By part (a), E' is injective, and the rest is obvious.

(c) Since E' is injective the map $M \subseteq E'$ extends to a map $\phi : E \to E'$. Since $M \subseteq E$ is essential, ϕ is injective. Since $E \cong \phi(E) \subseteq E'$, $\phi(E)$ is injective and so $E' = \phi(E) \oplus E''$. Since $M \subseteq E'$ is essential and $M \subseteq \phi(E)$, E'' must be zero. □ □

If $M \to E$ is a maximal essential extension of M over R we shall also refer to E is an *injective hull* or an *injective envelope* for M and write $E = E_R(M)$ of $E = E(M)$. Note that every R-module M has an injective hull, unique up to non-canonical isomorphism. Note also that if $M \subseteq E$, where E is any injective, then M has a maximal essential extension E_0 within E that is actually a maximal essential extension of M. Thus, $M \subseteq E$ will factor $M \subseteq E(M) \subseteq E$, and then $E(M)$ will split off from E, so that we can think of E as $E(M) \oplus E'$, where E' is some other injective.

As an informal exercise, show that there is an isomorphism $E(M_1 \oplus M_2) \cong E(M_1) \oplus E(M_2)$. (The corresponding statement for infinite direct sums is false in general, because a direct sum of injective modules need not be injective. However, it is true if the ring is Noetherian.)

14.2. Cosyzygies. If M is a module, we refer to the cokernel of an embedding $M \hookrightarrow E$, where E is injective, as a *first module of cosyzygies* of M. Given $0 \to M \to E^0 \to C^1 \to 0$ exact, where E^0 is injective, we can repeat the process: embed $C^1 \hookrightarrow E^1$ and then we get a cokernel C^2, a second module of cosyzygies of M. Recursively, we can define a $j+1$st module of cosyzygies to be a first module of cosyzygies of a jth module of cosyzygies. We have the analogue of Schanuel's lemma on syzygies: given two nth modules of cosyzygies, C_n and C_n', there are injectives E and E' such that $C_n \oplus E \cong C_n \oplus E'$. The main point is to see this for first modules of syzygies. But if we have

$$0 \to M \xrightarrow{\iota} E \xrightarrow{\pi} C \to 0$$

and

$$0 \to M \xrightarrow{\iota'} E' \xrightarrow{\pi'} C' \to 0$$

then we also have

$$0 \to M \xrightarrow{\iota \oplus \iota'} E \oplus E' \to C'' \to 0.$$

The image of M does not meet $E \oplus 0 \cong E$, and so E injects into C''. The quotient is easily seen to be isomorphic with $E'/\mathrm{Im}\,(M) \cong C'$, i.e., there is an exact sequence

$$0 \to E \to C'' \to C' \to 0,$$

and so $C'' \cong E \oplus C'$. Similarly, $C'' \cong E' \oplus C$, and so $C \oplus E' \cong C' \oplus E$.

Constructing a sequence of modules of cosyzygies of M is equivalent to giving a right injective resolution of M, i.e., a right complex $E^\bullet$, say

$$0 \to E^0 \to E^1 \to E^2 \to \cdots \to E^n \to \cdots,$$

such that all of the E^n are injective, $n \geq 0$, and which is exact except possibly at the 0 spot, while $M \cong H^0(E^\bullet)$, which is $\operatorname{Ker}(E^0 \to E^1)$. An n th module of cosyzygies for M is recovered from the injective resolution for every $n \geq 1$ as $\operatorname{Im}(E_{n-1} \to E_n)$, or as $\operatorname{Ker}(E_n \to E_{n+1})$.

14.3. Projective dimension and injective dimension. We can define the *projective dimension* (respectively, *injective dimension* $\operatorname{pd}_R M$ (respectively, $\operatorname{id}_R M$) of an R-module M as follows. If $M = 0$ it is -1. Otherwise, it is finite if and only if M has a finite left projective (respectively, right injective) resolution, and it is the length of the shortest such resolution. Then $\operatorname{pd}_R M \leq n$ (respectively, $\operatorname{id}_R M \leq n$), where $n \geq 0$, if and only if M has a projective (respectively, injective) resolution of length at most n. If M has no finite projectvive (respectively, injective) resolution we define $\operatorname{pd}_R M$ (respectively, $\operatorname{id}_R M$) to be $+\infty$. We note that the following are equivalent conditions on a nonzero module M and nonnegative integer n :

(1) M has a projective (respectively, injective) resolution of length at most n.
(2) Some n th module of syzygies (respectively, cosyzygies) of M is injective.
(3) Every n th module of syzygies (respectively, cosyzygies) of M is injective.

We know that over a regular local ring R, every finitely generated module has projective dimension at most $\dim(R)$.

14.4. Minimal injective resolutions.

Discussion 14.6. Given an R-module M we can form an injective resolution as follows: let $E_0 = E(M)$, let $E_1 = E(E_0/\operatorname{Im} M)$, let $E_2 = E(E_1/\operatorname{Im} E_0)$, and, in general, if

$$0 \to E_0 \to E_1 \to \cdots \to E_i$$

has been constructed (with $M = \operatorname{Ker}(E_0 \to E_1)$), let $E_{i+1} = E(E_i/\operatorname{Im} E_{i-1})$. Note that we have $E_i \twoheadrightarrow E_i/(\operatorname{Im} E_{i-1}) \subseteq E_{i+1} = E(E_i/\operatorname{Im} E_{i-1})$ so that we get a composite map $E_i \to E_{i+1}$ whose kernel is $\operatorname{Im} E_{i-1}$. It is evident that this yields an injective resolution of M.

We shall say that a given injective resolution

$$0 \to E_0 \to \cdots \to E_i \to \cdots$$

(with $M = \operatorname{Ker}(E_o \to E_1)$) is a *minimal injective resolution* of M if $M \to E_0$ is an injective hull for M and if for every $i \geq 0$, $\operatorname{Im}(E_i \to E_{i+1}) \subseteq E_{i+1}$ is an injective hull for $\operatorname{Im}(E_i \to E_{i+1})$. The discussion just above shows that minimal injective resolutions exist. It is quite easy to see that any two minimal injective resolutions for M are isomorphic as complexes.

15. Lecture 15

15.1. 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 $\operatorname{Ext}^j_R(N, M)$ 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

$$\operatorname{Ext}^j_R(N, M) = H^j\big(\operatorname{Hom}_R(G_\bullet, M)\big).$$

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 15.1. *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 15.2. *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.) □

16. Lecture 16

16.1. 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 $u_{j_1,\, \ldots, j_i}$ 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 $k_1,\, \ldots, k_{n-i}$ be the elements of the set

$$\{1,\, 2,\, \ldots,\, n\} - \{j_1,\, \ldots, j_i\}$$

arranged in increasing order, and let $u_{j_1,\, \ldots, j_i}$ correspond to $u_{k_1,\, \ldots, k_{n-i}}$ which we shall also denote as $v_{j_1,\, \ldots, j_i}$.

When a free R-module G has free basis $b_1,\, \ldots, b_t$, this determines what is called a *dual basis* $b'_1,\, \ldots,\, b'_t$ 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 $v'_{j_1,\, \ldots, j_i}$. However, when we compute the value of the differential d^*_{n-i+1} on $v'_{j_1,\, \ldots, j_i}$, while the coefficient of $v'_{h_1,\, \ldots, h_{i-1}}$ 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 $v'_{h_1,\, \ldots, h_{i-1}}$ is

$$d^*_{n-i+1}(v'_{j_1,\, \ldots, j_i})(v_{h_1,\, \ldots, h_{i-1}}) = v'_{j_1,\, \ldots, j_i}\big(d_{n-i+1}(v_{h_1,\, \ldots, h_{i-1}})\big),$$

which is the coefficient of $v_{j_1,\, \ldots, j_i}$ in $d_{n-i+1}(v_{h_1,\, \ldots, h_{i-1}})$.

Note that the complement of $\{j_1,\, \ldots, j_i\}$ in $\{1,\, 2,\, \ldots,\, n\}$ is the same as the complement of $\{h_1,\, \ldots, h_{i-1}\}$ in $\{1,\, 2,\, \ldots,\, n\}$, 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 $\{h_1, \ldots, h_{i-1}\}$ 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 $j_1, \ldots, j_i$ 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 $\{1, 2, \ldots, n\}$. 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. □

This duality enables us to compute Ext using Koszul homology, and, hence, Tor in certain instances:

THEOREM 16.1. *Let $\underline{x} = x_1, \ldots, x_n$ be a possibly improper regular sequence in a ring R and let M be any R-module. Then*

$$\mathrm{Ext}^i_R(R/(\underline{x})R;\, M) \cong H^i(\underline{x};\, M) \cong H_{n-i}(\underline{x};\, M) \cong \mathrm{Tor}^R_{n-i}(R/(\underline{x})R,\, M).$$

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 $R/(\underline{x})R$. □

We also note:

PROPOSITION 16.2. *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 $X_i \mapsto x_i$, $1 \le i \le n$. For example, we may take $B = R[X_1, \ldots, X_n]$ and map to R using the R-algebra map that sends $X_i \mapsto x_i$, $1 \le i \le n$. 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 16.1. □

16.2. Cohen-Macaulay rings revisited. A Noetherian local ring $(R, \mathfrak{m}, K)$ is Cohen-Macaulay (respectively, a finitely generated module M over R is small Cohen-Macaulay or maximal Cohen-Macaulay) if the following three equivalent conditions hold:

(CM1) Some system of parameters for R is a regular sequence on R.
(CM2) Every system of parameters for R is a regular sequence on R.
(CM3) The depth of R (respectively, M) on $\mathfrak{m}$ is equal to the Krull dimension of R.

More generally, if R is Noetherian but not necessarily local the following conditions are equivalent, and define the notion of Cohen-Macaulay for rings that are not necessarily local:

(CM4) Every local ring of R at a maximal ideal is Cohen-Macaulay.

(CM5) Every local ring of R at a prime ideal is Cohen-Macaulay.

(CM6) For every proper ideal I of R, the height of I is equal to the depth of R on I (which is the length of any maximal regular sequence in I).

We also note the following properties:

(CM7) If R is Cohen-Macaulay, then so is the polynomial ring $R[x_1, \ldots, x_n]$.

(CM8) If R is Cohen-Macaulay, then so is the formal power series ring ring $R[[x_1, \ldots, x_n]]$.

(CM9) Regular rings are Cohen-Macaulay.

(CM10) If a local ring R is Cohen-Macaulay, then the associated primes of (0) are minimal, and the quotient by any minimal prime has the same Krull dimension as R.

(CM11) A local ring is Cohen-Macaulay if and only if its completion is Cohen-Macaulay.

(CM12) If R is module-finite over a subring A that is regular, then R is Cohen-Macaulay if and only if R is projective as an A-module. If A is local or a polynomial ring over a field, R is Cohen-Macaulay if and only if it is free as an A-module.

(CM13) If R Cohen-Macaulay, then R is universally catenary (i.e., in any algebra S essentially of finite type over R, if $P \subseteq Q$ are primes of S, all saturated chains of primes joining P to Q have the same length).

(CM14) If R is Cohen-Macaulay and either local or finitely generated and $\mathbb{N}$-graded over a field, for every minimal prime of P of R, the Krull dimension of R/P is the same as the Krull dimension of R.

(CM15) If R is Cohen-Macaulay and $f_1, \ldots, f_h$ are elements of R generating an ideal I of height h, then every associated prime of I is minimal, and has height h. Moreover, R/I is again Cohen-Macaulay. In particular, these statements hold when R is regular.

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: xy, xz, $1-x$ gives a counterexample. These three elements are not aa regular sequencek, although they are in the order $1-x, xy, xz$. Thus, in general, regular sequences cannot be permuted.

However:

Proposition 16.3. *Let $(R, \mathfrak{m})$ be a local ring with $f_1, \ldots, f_n \in \mathfrak{m}$ or suppose that R is an $\mathbb{N}$-graded Noetherian ring and that $f_1, \ldots, f_n$ are homogeneous elements of positiver degree. If $f_1, \ldots, f_n$ is a regular sequence on the finitely generated module M (which is $\mathbb{Z}$-graded in the homogeneous case) , then so is every permutation of $f_1, \ldots, f_n$.*

Proof. . Since transpositions of consecutive elements of the set of integers from 1 to n generate all permutations, it suffices to show that we still have aa regular sequence when we interchange f_i, f_{i+1}. By working modulo $(f_1, \ldots, f_{i-1})M$, we reduce to the case where $n = 1$. We change notation and let $f := f_1$, $g := f_2$. Assume f, g is a regular sequence, We claim that g is not a zerodivisor on M. To see this, let $N := \mathrm{Ann}_M g$. Note that if $u \in N$, $gu = 0 \in fN$. Hence, $u = fv$. Thus, $g(fv) = 0$, and since f is not a zerodivisor on M, $gv = 0$. Thus, $v \in N$, which shows that $N = fN$. By Nakayama's lemma (or its homogeneous form), $N = 0$. Finally, suppose f is a zerodivisor mod gM, say $fu = gw$. Then $gw \in fM$ implies

$w \in fM$, say $w = fz$. Then $gw = gfz = fu$ and $f(u - gz) = 0$. Since f is not a zerodivisor on M, $u = gz \in gM$, as required. □

Note that every zero-dimensional Noetherian ring is Cohen-Macaulay, as is every one-dimensional reduced ring (this includes one-dimensional domains). Once one localizes at a height one prime, a parameter is not in any associated prime of (0), since these are all minimal primes in the reduced case, and so a parameter is not a zerodivisor.

However, $K[[x,y]]/(x^2)$ is Cohen-Macaulay even though it is not reduced. Being reduced is sufficient for the Cohen-Macaulay property in the reduced case, but not necessary.

Note that $K[[x,y]/(x^2, xy)$ is not Cohen-Macaulay, since the image of x kills the maximal ideal. This one-dimensional ring has depth 0 on its maximal ideal.

17. Lecture 17

17.1. More examples connected with the Cohen-Macaulay property. We recall the following characterization of normal Noetherian domains:

Theorem 17.1. *A Noetherian domain R is normal if and only if both of the following two conditions hold:*

(1) Every associated prime of a nonzero nonunit element $f \in R$ has height one.
(2) If P is a height one prime ideal of R, then R_P is a Noetherian discrete valuation domain.

One can also show that if a Noetherian domain R is normal, then $R = \bigcap\{R_P : P \in \operatorname{Spec}(R)$ and height $(P) = 1\}$.

The relevance to the theory of Cohen-Macaulay rings is this:

Corollary 17.2. *If I is a proper ideal of height at least two in a normal Noetherian domain R, then the depth of R on I is at least two. Hence, a normal ring of dimension at most two is Cohen-Macaulay.*

Proof. Choose any nonzero element $f \in I$. The associated primes of f, say $P_1, \ldots, P_k$, are all height one. Hence, I is not contained in $\bigcup_{i=1}^k P_i$, or else it would be contained in one of the P_i and could not have height two. Choose $g \in I$ not in any P_i. Then g is a nonzerodivisor in R/fR, and so f, g is a regular sequence in I. The final statement is now clear. □

The ring $K[x^2, x^3, y]$ is Cohen-Macaaulay (one may also complete and use double brackets): $K[x^2, x^3]$ is a one-dimensional domain, and so Cohen-Macaulay, and adjoining an indeterminant preserves the Cohen-Macaulay property. Thus, normality is not necessary for a ring to be Cohen-Macaulay in dimension 2, even though it is sufficient. Another instructive example is to take any Artin local ring, and adjoin variables, either to form polynomial rings or formal power series rings. The rings obtained are all Cohen-Macaulay, can have any specified dimension, even though they have nonzero nilpotents. E.g., $K[x,y,z]/(x^2)$ or $K[[x,y,z]]/(x^2)$ is two-dimensional, is not reduced, and has nonzeronilpotents.

The ring $R := K[x^2, x^3, xy, y]$, its localization at $(x^2, x^3, xy, y)R$, and the completion of this localization are not Cohen-Macaulay. In the local ring, x^2, y is a system of parameters but not a regular sequence since $x^3y = (xy)(x^2) \in x^2R$ but $x^3 \notin x^2R$.

This is also true for $R := K[x^4, x^3y, xy^3, y^4]$, its localization at $(x^4, x^3y, xy^3, y)^3R$, and the completion of this localization: these rings are not Cohen-Macaulay. In the local ring, x^4, y^4 is a system of parameters but not a regular sequence, since $(x^3y)^2y^4 = (xy^3)^2(x^4) \in x^2R$ but $(x^3y)^2 \notin x^4R$.

The Segre product of the homgeneous coordinate ring $R := K[X, Y, Z]/(X^3 + Y^3 + Z^3]$ of an elliptic curve, where K is a field of characteristic not 3, and a polynomial ring $K[s, t]$ in two variables is normal of dimension 3 but not Cohen-Macaulay: see Example 1.13. Segre product

17.2. 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 17.3. *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 □

PROPOSITION 17.4. *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 $x_1, \ldots, x_n$ is a possibly regular sequence on M_1 and N. Then x_1 is a nonzerodivisor on M, for if $x_1 u = 0$, 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 $x_2, \ldots, x_n$ is a possibly improper regular sequence on M/x_1M, and hence that $x_1, \ldots, x_n$ 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 $x_1, \ldots, x_n$ 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 $h = 2$. □

THEOREM 17.5. *Let $x_1, \ldots, x_n \in R$ and let M be an R-module. Let $t_1, \ldots, t_n$ be integers ≥ 1. Then $x_1, \ldots, x_n$ is a regular sequence (respectively, a possibly improper regular sequence) on M iff $x_1^{t_1}, \ldots, x_n^{t_n}$ 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 $x_1, \ldots, x_n$ is a regular sequence on M. By induction on n, it will suffice to show that $x_1^{t_1}, x_2, \ldots, x_n$ is a regular sequence on M: we may pass to $x_2, \ldots, x_n$ 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 $x_2, \ldots, x_n$ 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 $x_1, \ldots, x_{j-1}, x_j^t, x_{j+1}, \ldots, x_n$ is a regular sequence on M, then $x_1, \ldots, x_n$ is: we may change the exponents to 1 one at a time. The issue may be considered mod $(x_1, \ldots, x_{j-1})M$. Therefore, it suffices to consider the case $j = 1$, and we need only show that if $x_1^t, x_2, \ldots, x_n$ is a regular sequence on M then so is $x_1, \ldots, x_n$. It is clear that if x_1^t is a nonzerodivisor then so is x_1.

By induction on n we may assume that $x_1, \ldots, x_{n-1}$ is a regular sequence on M. We need to show that if $x_nu \in (x_1, \ldots, x_{n-1})M$, then $u \in (x_1, x_2, \ldots, x_{n-1})M$. If we multiply by x_1^{t-1}, we find that

$$x_n(x_1^{t-1}u) \in (x_1^t, x_2, \ldots, x_{n-1})M,$$

and so

$$x_1^{t-1}u = x_1^tv_1 + x_2v_2 + \cdots + x_{n-1}v_{n-1},$$

i.e.,

$$x_1^{t-1}(u - x_1v_1) - x_2v_2 - \cdots - x_{n-1}v_{n-1} = 0.$$

By the induction hypothesis, $x_1, \ldots, x_{n-1}$ is a regular sequence on M, and by the first part, $x_1^{t-1}, x_2, \ldots, x_{n-1}$ is a regular sequence on M. By the Lemma 17.3, we have that

$$u - x_1v_1 \in (x_1^{t-1}, x_2, \ldots, x_{n-1})M,$$

and so $u \in (x_1, \ldots, x_{n-1})M$, as required. $\square$

THEOREM 17.6. *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 $\sum_{j \neq i} x_j^{a_j+1} u_j - x_i^{a_j}(yu - x_i u_i) = 0$. Since powers of the x_j are again regular, Lemma 17.3 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. $\square$

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 17.7. *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*

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

in such a way that the action of $[x_i] \in I/I^2 = [gr_I(R)]_1$ on $gr_I(M)$ 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 $gr_I(R) \cong (R/I)[X_1, \ldots, X_n]$ 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, $u \in IM$, contradicting that $u \in M - IM$. $\square$

17.3. Cohen-Macaulay rings and lifting while preserving height.

Proposition 17.8. *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 $\mathrm{depth}_I R = 0$. Now suppose that $\mathrm{height}\,(I) > 0$. Each prime in $\mathrm{Ass}\,(R)$ 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 $\mathrm{Ass}\,(R)$. 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 17.9. *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, $1 \le i \le d$, $y_i \in x_i + (x_{i+1}, \ldots, x_d)R$, and for all i, $1 \le i \le d$, $y_1, \ldots, y_i$ 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. $\square$

PROPOSITION 17.10. *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, $1 \le i \le d$. Then there are elements $\delta_1, \ldots, \delta_d \in \mathfrak{p}$ such that if $y_i = x_i + \delta_i$, $1 \le i \le d$, then $(y_1, \ldots, y_i)R$ has height i, $1 \le i \le d$.*

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 $(Q/\mathfrak{p}) \ge t + 1$, a contradiction. □

The following result will be useful in proving the colon-capturing property for tight closure.

LEMMA 17.11. *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 17.9, we may assume without loss of generality that $x_1, \ldots, x_i$ generate an ideal of height i in R, $1 \le i \le k$. We also know this for $i = k + 1$. Choose z_i arbitrarily such that z_i maps to x_i, $1 \le i \le k + 1$. 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 Proposition 17.10 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, $1 \le i \le k + 1$. Since $S/(y_1, \ldots, y_h)S$ is again Cohen-Macaulay, it follows from Proposition 17.9 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. □

18. Lecture 18

18.1. Colon-capturing. We can now prove a result on the colon-capturing property of tight closure.

THEOREM 18.1 (colon-capturing). *Let R be a reduced Noetherian ring of characteristic p 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 $(x_1, \ldots, x_t)R$, $0 \le t \le k + 1$. 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:*

(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 exponent 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

$$rx_{k+1} = r_1x_1 + \cdots + r_kx_k$$

in R. Then we can lift $r, r_1, \ldots, r_k$ to elements $s, s_1, \ldots, s_k \in S$ such that

$$sz_{k+1} = s_1z_1 + \cdots + s_kz_k + v,$$

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 $d^2cr^q \in I_k^{[q]}$ for all $q \gg 0$. But then $r \in I_k^*$, as required. $\square$

Corollary 18.2. *Let R be a Noetherian ring of characteristic p 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. $\square$

18.2. Maps of quotients by regular sequences. Let $\underline{x} = x_1, \dots, x_n$ and $\underline{y} = y_1, \dots, y_n$ be two regular sequences in R such that $J = (y_1, \dots, y_n)R \subseteq (x_1, \dots, x_n)R = I$. 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 18.3. *Let $x_1, \dots, x_n$ and $y_1, \dots, y_n$ be two regular sequences on a Noetherian module M over a Noetherian ring R. Suppose that*

$$J = (y_1, \dots, y_n)R \subseteq (x_1, \dots, x_n)R = I.$$

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

$$(y_1 \, \dots \, y_n) = (x_1 \, \dots \, x_n)A.$$

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 $DI \subseteq J$.

We now complete the proof in the case where $\underline{x}$, $\underline{y}$ are regular sequences in R. The surjection $R/J \twoheadrightarrow R/I$ lifts to a map of projective resolutions of these modules: we can use any projective resolutions, but under our extra hypothesis, we can 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:

$$\begin{tikzcd}
\mathcal{K}_1(\underline{x};\, R) \arrow[r, "(x_1 \dots x_n)"] & R \arrow[r] & R/(x_1, \dots, x_n) \arrow[r] & 0 \\
\mathcal{K}_1(\underline{y};\, R) \arrow[r, "(y_1 \dots y_n)"] \arrow[u, "A"] & R \arrow[r] \arrow[u, "\mathrm{id}_R"] & R/(y_1, \dots, y_n) \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

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 a special case of the Theorem 16.1 in the case where $i = n$. The results are the same as $H_0(\underline{x}; M) \cong M/(\underline{x})M$ and $H_0(\underline{y}; M) \cong M/(\underline{y})M$.

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,

$$\mathrm{Ext}_R^{n-1}(I/J; M) \to \mathrm{Ext}_R^n(R/I;\, M) \to \mathrm{Ext}_R^n(R/J; M).$$

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

It remains to prove the general case, when we do not know *a priori* that $\underline{x}$, $\underline{y}$ are regular sequences. The idea is to map a ring B to R containing elements $\underline{X} := X_1, \ldots, X_n$, $\underline{Y} := Y_1, \ldots, Y_n$. and n^2 elements U_{ij}, $1 \le i,\, j \le n$ such that

(1) $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ are regular sequences in B.
(2) $(Y_1 \;\ldots\; Y_n) = (X_1 \;\ldots\; X_n)(U_{ij})$, so that $(Y_1, \ldots, Y_n)B \subseteq X_1, \ldots, X_n)B$.
(3) Under the map $B \to R$, $\underline{X}$, $\underline{Y}$ and (U_{ij}) map to $\underline{x}$, $\underline{y}$, and A, respectively.

There are many possible choices for the ring B, but we shall take B to be the polynomial ring $\mathbb{Z}[X_1, \ldots, X_n, U_{11}, \ldots, U_{nn}]$, where $U := (U_{ij})$ is an $n \times n$ matrix U of indeterminates, and define the Y_j as the entries of $(X_1 \;\ldots\; X_n)U$. We then map B to R so that every $X_j \mapsto x_j$ and every $U_{ij} \mapsto a_{i,j}$. It remains to show that the Y_j form a regular sequence in B. To see this, consider the $n^2 - n$ elements U_{ij} for $i \neq j$ the elements $U_{ii} - X_i$, and the Y_i. By the permutability of regular sequences in the positive homogeneous $\mathbb{N}$-graded case, it suffices to show that these are a regular sequence. This is clear for the first $n^2 - n$ elements, and the next n elements (these n are indeterminates, up to linear automorphisms of the forms of degree 1). But modulo these n^2 elements, we obtain the ring $\mathbb{Z}[X_1, \ldots, X_n]$, and the Y_i map to the X_i^2. □

Remark 18.4. 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 $\mathrm{Ext}_R^n(R/I,\, R)$ 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 $\mathrm{Ext}_R^n(R/J,\, R)$ with R/J.

Remark 18.5. 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 $\mathrm{Ext}_R^i(N,\, M) = 0$ for $i < d$. If $d \ge 1$, 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

$$0 \longrightarrow M \xrightarrow{x_1\cdot} M \longrightarrow M/x_1M \longrightarrow 0.$$

18.3. The type of a Cohen-Macaulay module over a local ring. Let $(R,\, \mathfrak{m},\, K)$ 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:

Theorem 18.6. *Let $(R,\, \mathfrak{m},\, K)$ 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, $1 \le i \le d$,

$$\operatorname{Ext}^d_R(K,\, M) \cong \operatorname{Ext}^{d-i}_R\big(K,\, M/(x_1,\, \ldots, x_i)M\big).$$

In particular, for every maximal regular sequence on M, the socle in $M/(x_1,\, \ldots, x_d)M$ is isomorphic to $\operatorname{Ext}^d_R(K,\, M)$, 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

$$\operatorname{Ext}^d_R(K,\, M) \cong \operatorname{Ext}^{d-i}_R\big(K,\, M/(x_1,\, \ldots, x_i)M\big)$$

reduces at once to the case where $i = 1$. To see this, apply the long exact sequence for Ext arising from the application of $\operatorname{Hom}_R(K,\, \_)$ to the short exact sequence

$$0 \to M \to M \to M/x_1M \to 0.$$

Note that $\operatorname{Ext}^j(K,\, M) = 0$ for $j < d$, since the depth of M on $\operatorname{Ann}_R K = m$ is d, and that $\operatorname{Ext}^j(K,\, M/x_1M) = 0$ for $j < d-1$, similarly. Hence, we obtain, in part,

$$0 \longrightarrow \operatorname{Ext}^{d-1}_R(K,\, M/x_1M) \longrightarrow \operatorname{Ext}^d_R(K,\, M) \xrightarrow{x_1\cdot} \operatorname{Ext}^d_R(K,\, M).$$

Since $x_1 \in m$ kills K, the map on the right is 0, which gives the required isomorphism. $\square$

Proposition 18.7. *Let $M \neq 0$ be a Cohen-Macaulay module over a local ring R. Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be two systems of parameters on M with $(y_1, \ldots, y_n)R \subseteq (x_1, \ldots, x_n)R$ and let $A = \big(a_{ij}\big)$ be a matrix of elements of R such that $(y_1 \ \ldots \ y_n) = (x_1 \ \ldots \ x_n)A$. Let $D = \det(A)$. Then the map $M/(x_1,\, \ldots, x_n)M \to M/(y_1,\, \ldots, y_n)M$ induced by multiplication by D on the numerators carries the socle of $M/(x_1,\, \ldots, x_n)M$ isomorphically onto the socle of $M/(y_1,\, \ldots, y_n)M$. In particular, if $y_i = x_i^t$, $1 \le i \le n$, then the map induced by multiplication by $x_1^{t-1} \cdots x_n^{t-1}$ carries the socle of the quotient module $M/(x_1,\, \ldots, x_n)M$ isomorphically onto the socle of $M/(x_1^t,\, \ldots, x_n^t)M$.*

Proof. By the Theorem 18.3 multiplication by D gives an injection

$$M/(x_1,\, \ldots, x_n)M \hookrightarrow M/(y_1,\, \ldots, y_n)M$$

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 $x_1^{t-1},\, \ldots, x_n^{t-1}$. $\square$

18.4. F-rational rings.

Definition 18.8. F-rational rings. We shall say that a local ring $(R,\, \mathfrak{m},\, K)$ 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 18.9. *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 6.9. In particular, R is equidimensional, and by part (a) of the Theorem 18.1, we have that for every k, $0 \leq k \leq n-1$,

$$(x_1, \dots, x_k) :_R x_{k+1} \subseteq (x_1, \dots, x_k)^* = (x_1, \dots, x_k),$$

so that R is Cohen-Macaulay. $\square$

Theorem 18.10. *Let $(R, \mathfrak{m}, K)$ be a reduced local ring of characteristic p. If R is Cohen-Macaulay and the ideal $I = (x_1, \dots, x_n)$ 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 $I_t = (x_1^t, \dots, x_n^t)R$. 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 18.7, 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

$$cz^q \in \big((x_1^q)^t, \dots, (x_n^q)^t\big) :_R (x_1^q)^{t-1} \cdots (x_n^q)^{t-1}.$$

By the Theorem 17.6 applied to the regular sequence $x_1^q, \dots, x_n^q$, the right hand side is $(x_1^q, \dots, x_n^q) = I^{[q]}$, 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 $y_1, \dots, y_n$. For $t \gg 0$, $(x_1^t, \dots, x_n^t)R \subseteq (y_1, \dots, y_n)R$. Then there is an injection $R/y_1, \dots, y_n)R \hookrightarrow R/(x_1^t, \dots, x_n^t)R$ by the Theorem increg. Since 0 is tightly closed in the latter, it is tightly closed in $R/(y_1, \dots, y_n)R$, and so $(y_1, \dots, y_n)R$ is tightly closed in R. $\square$

We shall see soon that under mild conditions, if $(R, \mathfrak{m}, K)$ is a local ring of characteristic p 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.

19. Lecture 19

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 result will enable us to prove the result that we want.

THEOREM 19.1. *Let $(R, \mathfrak{m}, K)$ be a reduced local ring of characteristic p, 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 tightly 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 18.1, 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 fromTheorem 18.1 $\square$

We therefore have:

THEOREM 19.2. *Let $(R, \mathfrak{m}, K)$ 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.*

THEOREM 19.3. *Let R be an F-rational local ring. Then for every prime ideal P of R, R_P is F-rational.*

PROOF. Let P have height d. Since R is Cohen-Macaulay, there is a maxima regular sequence $\underline{x} = x_1, \ldots, x_d$ in P. Let $I = (\underline{x})R$. We know that $I = I^*$. It will suffice to show that IR_P is tightly closed in R_P, since R_P is Cohen-Macaulay and the image of $\underline{x}$ is a system of parameters in R_P. Let W be the complement of the union of the minimal primes $P_1, \ldots, P_k$ of I. These are the same as the associated primes of I, so W consists of nonzerodivisors on I. Note that P is one of these primes. We now show that $IW^{-1}R$ is tightly closed in $W^{-1}R$. (We know that R is a domain, so that we may think of R as contained in $W^{-1}R$.) If not $IW^{-1}R$ is not tightly closed in $W^{-1}R$, after multiplying by units that are image of elements of W, we may assume that we have an element $f \in R \setminus I$ that is in the tight closure of $W^{-1}I$, so that for some nonzero $c \in R$ we have $cf^q \in W^{-1}I^{[q]}$ for all $q \gg 0$, and this means that for all $q \gg 0$, we have $w_q \in W$ such that $w_q cf^q \in I^{[q]}$. Since $I^{[q]}$ is generated by parameters and it has the same associated primes as I. Therefore, w is not a zerodivisor on $I^{[q]}$, and so $cf^q \in I^{[q]}$ for all $q \gg 0$. Hence $f \in I^* = I$, a contradiction. nd Since P is now maximal in $W^{-1}R$ and $IW^{-1}R$ is primary to P, we have that IR_P is tightly closed in R_P, by Lemma 6.4. $\square$

It is therefore natural to define a Noetherian ring R of characteristic p to be *F-rational* if its localization at every maximal ideal (equivalently, at every prime ideal) is F-rational.

19.1. Supplementary Problems II.

In all problems, R, S are Noetherian rings of characteristic p.

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 $(R, \mathfrak{m}, K)$. 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 characteristic p, 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 $(R, \mathfrak{m}, K)$ 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 $\big(x_1^t, \ldots, x_d^t, (x_1 \cdots x_d)^{t-1} y\big)R$ is tightly closed. Prove that either R is weakly F-regular, or else that $\tau(R) = m$.

20. Lecture 20

20.1. Capturing the contracted expansion from an integral extension. 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 20.1. *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 $b_1, \ldots, b_h$ 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 $u_1, \ldots, u_n$ generate M. Then each u_n is a linear combination of $b_1, \ldots, b_h$ 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 $1 \le i \le n$. 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 $f(u) = (d_1, \ldots, d_h)$ 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 $\theta = \pi \circ f$. □

We also note:

Theorem 20.2. *If R is a Noetherian domain of characteristic p and $R \subseteq S$, where S is a solid R-algebra, then $IS \cap R \subseteq I^*$. More generally, if G is any free R-module and we think of G as a submodule of $S \otimes_R G$, so that we may write $GS = S \otimes_R G$. Then for every submodule $H \subseteq G$, $HS \cap G \subseteq H^*_G$.*

Proof. We prove the more general result for $H \subseteq G$. Suppose $\alpha : S \to R$ and $\alpha(t) = c \neq 0$. Let $\beta : S \to R$ by $\beta(s) = \alpha(st)$. Then $\beta(1) = c$. Note that β induces an R-linear map $\gamma : S \otimes G \to G$ by applying β to the coefficient of every element in a free basis for G. Note that for $h \in H$, $s \in S$, $\gamma(sh) = \beta(s)h$.

If $g \in HS$, say $g = \sum_{j=1}^n h_j s_j$, where $G \in G$ and the $h_j \in H$, then for all q we have $g^q \cdots 1 = \sum_{j=1}^n s_j^q h_j^q$. Apply γ to obtain $cg^q = \beta(1)g^q = \gamma(g^q) = \gamma(sum_{j=1}^n h_j^q s_j^q) = sum_{j=1}^n \beta(s_j^q) h_j^q \in H^{[q]}$ and so $g \in H^*_G$. □

Theorem 20.3. *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 $IS \cap R \subseteq I^*$. Likewise, if $H \in G$ where G is free over R, $HS \cap G \subseteq H^*_G$.*

Proof. Let $g \in HS \cap G$. It suffices to show that the image of g is in H^*_G 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 g in $H \otimes_R R/\mathfrak{p}$ is in $H(S/\mathfrak{q})$. We have therefore reduced to the case where R and S are domains.

Since $g \in HS$, there exist $h_1, \ldots, h_n$ in H such that

$$g = s_1 h_1 + \cdots + s_n h_n,$$

where the $s_j \in S$. Hence, we may replace S by $R[s_1, \ldots, s_n] \subseteq S$, and so assume that S is module-finite over R. By the Lemma 20.1 S is solid as an R-algebra, and the result now follows from Theorem 20.2. □

20.2. Gorenstein rings.

Definition 20.4. Gorenstein local rings A local ring $(R, \mathfrak{m}, K)$ 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 $(R, \mathfrak{m}, K)$ 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/fR 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 are aiming to prove that for Gorenstein rings, F-rational, weakly F-regular, and F-regular are equivalent condition. This is extremely useful. In the case of a Gorenstein local ring R with system of parameters $\underline{x} = x_1, \ldots, x_d$, if u generates the socle in $R/(\underline{x})$, then R is F-regular if and only if u is not in the tight closure of $(\underline{x})$!

20.3. Artin Gorenstein rings. Arbitrary products of injectives are injective over any ring, and so finite direct sums of injective modules are injective. Over a Noetherian ring, an arbitrary direct sum of injectives is injective: this is not true in general. One can argue as follows. It suffices to show that a map of an ideal I into the direct sum extends to the whole ring. Since I is finitely generated, the map factors through a finite direct sum, and the map then extends working entirely with this finite direct sum.

As a corollary, every injective module E over a Noetherian ring is a direct sum of injective hulls $E_R(R/P)$ of prime cyclic modules. To prove this, consider a maximal family modules of the form $E(R/P)$ in E such that each is disjoint from the sum of all of the oethers (which exists by Zorn's lemma). Let $E_0 \subseteq E$ be the sum of all these. We shall show that $E_0 = E$. If not, the inclusion splits, and $E = E_0 \oplus E_1$ with $E_1 \neq 0$. Choose an element $u \in E_1$ that is not 0. Let $P \in \mathrm{Ass}\,(Ru)$. Then u has a nonzero multiple ru with $ruR \cong R/P$. The injection $R/P \to E_1$ extends to $E_R(R/P)$. This gives an injection $E(R/P) \hookrightarrow E_1 \subseteq E$. But then we may enlarge the family we started with by inclusing this copy of $E(R/P)$. $\square$

We shall need the following very important result.

Theorem 20.5. *If an Artin local ring is Gorenstein, it is injective as a module over itself.*

In the case where the Artin local ring $(R, \mathfrak{m}, K)$ contains a field we can argue as follows. By the structure theory of complete local rings, R contains a copy of K and may be thought of as as a K-algebra. Let $E := \mathrm{Hom}_K(R, K)$, which has an R-module structure because R does, $\mathrm{Hom}_R(M, E) \cong \mathrm{Hom}_K(M \otimes_R, K)$ by the adjointness of tensor and Hom, and one obtains that $\mathrm{Hom}_R(\_\,, E)$ and $\mathrm{Hom}_K(\_\,, K)$ are isomorphic functors from R-modules to R-modules. Since $\mathrm{Hom}_K(\_\,, K)$ is an exact functor, so is $\mathrm{Hom}_R(\_\,, E)$. Thus, E is an injective R-module, and it has the same length (in this case, dfimension as aa K-vector space) as R. We can map the socle in R, a copy of K, isomorphically to a copy of K in the socle of E. This give a map $K \hookrightarrow E$ that extends, since E is injective, to all of R. Morever, since $K \to R$ is essential, this map is an injection of $R \to E$. Since R and E have the same length, we have that $R \cong E$. Since R is an essential extension of K, R is the injective hull of K over R.

For the general case, see, for example, [**?**, Theorems (3.1.17) and (3.2.10)].

In consequence, we are able to prove the following most useful result. Notice that it reduces to 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 20.6. *Let $(R, \mathfrak{m}, K)$ be a reduced Gorenstein local ring of characteristic p. 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) 1 R is weakly F-regular.
(2) 2 R is F-rational
(3) 3 $(x_1, \ldots, x_n)R$ is tightly closed.
(4) 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 Theorem 18.10. 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 Lemma 6.1, 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. $\square$

21. Lecture 21

21.1. 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 21.1. *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 21.2. *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 proof of Theorem 21.1 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 Theorem 11.8, 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 characteristic p.

21.2. 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 q th 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

$$1,\, \lambda_{j+1},\, \lambda_{j+1}^2,\, \ldots,\, \lambda_{j+1}^{p-1}$$

is a basis for $L_{j+1} = K^p[\lambda_1, \ldots, \lambda_{j+1}]$ over $L_j = K[\lambda_1, \ldots, \lambda_j]$ 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 p-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 $\lambda_1, \ldots, \lambda_h$ of the p-base and for all q, $[K^q[\lambda_1, \ldots, \lambda_h] : K^q] = q^h$ 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 21.3. *With K a field of characteristic p 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.*

21.3. 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 21.4. *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.

We next want to prove Theorem 21.4. Recall that $A = K[[x_1, \dots, x_n]]$ and that Γ is cofinite in a fixed p-base Λ for K.

First note that it is clear that $K[[x_1, \dots, x_n]] \to K_e[[x_1, \dots, x_n]]$ 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 Theorem 5.2. 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

$$(A^\Gamma)^q \in (K_e)^q[[x_1^q, \dots, x_n^q]] \in K[[x_1, \dots, x_n]] = A.$$

Thus, every $A_e = K_e[[x_1, \dots, x_n]]$ 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 $mA_e = (x_1, \dots, x_n)A_e$. 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, $mA^\Gamma = (x_1, \dots, x_n)A^\Gamma$ 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 $K^\Gamma[[x_1, \dots, x_n]] = B$, 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 21.5. *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 $f_1, \dots, f_n \in I$ and $b_1, \dots, b_n \in B$. We can choose i so large that $u, f_1, \dots, f_n \in A_i$, and let $J = (f_1, \dots, f_n)A_i$. 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 $g_1, \dots, g_n \in I$ generates IB. Let $I_0 = (g_1, \dots, g_n)A$. 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 $(x_1, \dots, x_n)A^\Gamma$, we have that A^Γ is regular. To complete the proof of Theorem 21.4, it remains only to prove:

Theorem 21.6. *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 $K_e[[x_1, \dots, x_n]]$. Let $\theta_1, \dots, \theta_h$ 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 $\theta_1^{1/p}, \dots, \theta_h^{1/p}$ of degree at most $p-1$ in each element, and let $\mathcal{N}$ be the set of monomials in $x_1^{1/p}, \dots, x_d^{1/p}$ 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,

$$(A_e)^{1/p} = K_e^{1/p}[[x_1^{1/p}, \dots, x_d^{1/p}]].$$

This is spanned over $K_e^{1/p}[[x_1, \dots, x_d]]$ 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 $K_e^{1/p}[[x_1, \dots, x_n]]$ is spanned by $\mathcal{N}$ over $K_{e+1}[[x_1, \dots, x_n]] = A_{e+1}$. Hence, $A_e^{1/p}$ is spanned by $\mathcal{T} = \mathcal{M}\mathcal{N}$ over A_{e+1}, as claimed. $\square$

Note that $A^\Gamma \subseteq K^\Gamma[[x_1, \dots, x_n]]$, 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

$$\sum_{e=0}^{\infty} c_e x^e \in K^\Gamma[[x]] - K[[x]]^\Gamma.$$

21.4. 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 $R = A = K[[x_1, \dots, x_n]]$, we may enlarge the residue class field K of A to L by considering instead $L[[x_1, \dots, x_n]]$. 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

$$L\widehat{\otimes}_K R = \varprojlim_t \frac{L \otimes_K R}{m^t(L \otimes_K R)} \cong \varprojlim_t \bigl(L \otimes_K \frac{R}{m^t}\bigr).$$

In case $R = K[[\underline{x}]]$, where $\underline{x} = x_1, \dots, x_n$ are formal power series indeterminates, this yields

$$\varprojlim_t L \otimes_K \bigl(\frac{K[[\underline{x}]]}{(\underline{x})^t}\bigr) \cong \varprojlim_t L \otimes_K \bigl(\frac{K[\underline{x}]}{(\underline{x})^t}\bigr) \cong \varprojlim_t \frac{L[\underline{x}]}{(\underline{x})^t} \cong L[[\underline{x}]],$$

which gives the result we wanted.

Now suppose that we have a local map $(R, \mathfrak{m}, K) \to (S, \mathfrak{n}, K)$ 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 $\varprojlim_t L \otimes_K R/\mathfrak{n}^t R$, 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 $s_t \in \mathfrak{n}^t S_L = m^t S_L$ for all $t \in \mathbb{N}$. Since $m^t R_L$ maps onto $\mathfrak{n}^t S_L$, we can left this series to

$$r_0 + r_1 + \cdots + r_t + \cdots$$

where for every $t \in \mathbb{N}$, $r_t \in m^t R_L$ 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 $K[[x_1, \ldots, x_n]]$, it follows that $L\widehat{\otimes}_K R$ is a homomorphic image of a ring of the form $L[[x_1, \ldots, x_n]]$, 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 faithfully 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.

21.5. 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 21.7. *Let B be a complete local ring of characteristic p with coefficient 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 21.8. *Let M be an R-module, let $P_1, \ldots, P_h$ 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 induction 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

$$0 \longrightarrow S \otimes_R (P \cap Q) \longrightarrow S \otimes_R M \xrightarrow{\mathrm{id}_S \otimes f} \big(S \otimes_R (M/P)\big) \oplus \big(S \otimes_R (M/Q)\big).$$

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 $\mathrm{id}_S \otimes f$ 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. We first show 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 Lemma 21.8. 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 Theorem 21.7, it will suffice to prove the following:

Theorem 21.9. *Let K be a field of characteristic p with p-base Λ. Let $A = K[[x_1, \dots, x_n]]$, 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 Theorem 21.7. Beyond that, we shall need to prove some auxiliary results first.

To see why the preceding Theorem implies part (a) of Theorem 21.7, 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 21.9 above implies part (a) of the Theorem 21.7.

21.6. Intersecting the fields K^Γ. In order to prove the Theorem above, we need several preliminary results. One of them is quite easy:

Lemma 21.10. *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, $\lambda_1, \dots, \lambda_t$ 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 $u \notin K^\Gamma$. $\square$

22. Lecture 22

22.1. Results on intersecting fields. We shall also need the following result, as well as part (b) of the Theorem stated after it.

THEOREM 22.1. *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.*

PROOF. We prove 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. $\square$

THEOREM 22.2. *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) $\displaystyle\bigcap_i \mathrm{frac}\,(\mathcal{K}_i[x_1, \ldots, x_n]) = \mathrm{frac}\,(\mathcal{K}[x_1, \ldots, x_n])$.

(b) $\displaystyle\bigcap_i \mathrm{frac}\,(\mathcal{K}_i[[x_1, \ldots, x_n]]) = \mathrm{frac}\,(\mathcal{K}[[x_1, \ldots, x_n]])$.

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 $\mathrm{frac}\,(\mathcal{K}_i[x_1, \ldots, x_n])$, 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 $f/g \in \mathrm{frac}\,(\mathcal{K}[x_1, \ldots, x_n])$, as required.

We shall have to work a great deal harder to prove part (b). We first introduce some terminology. A 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

$$C \to \mathrm{Hom}_B\big(\mathrm{Hom}(C, B), B\big)$$

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 indeterminate $\mathcal{F}((x)) = \mathcal{F}[[x]][x^{-1}]$ 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 22.3. *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*

$$\big(\mathrm{frac}\,(C[[x]])\big) \cap \mathcal{F}((x)) = \mathrm{frac}\,(B[[x]]).$$

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 $u = f(w)/f(v) \in \operatorname{frac}(B[[x]])$, as required. $\square$

We can now prove part (b) of the Theorem 22.2.

Proof. 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

$$\operatorname{frac}(\mathcal{K}_j([[x]]) = \mathcal{K}_j[[x]][x^{-1}].$$

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

$$(*) \qquad \bigcap_j \mathcal{K}_j((x_1, \ldots, x_n)) \subseteq \mathcal{K}_{j_0}((x_1, \ldots, x_n)) \cap \mathcal{K}((x_1, \ldots, x_{n-1}))((x_n)).$$

We now want to apply Lemma 22.3. Let $B = \mathcal{K}[[x_1, \ldots, x_{n-1}]]$ and $C = \mathcal{K}_{j_0}[[x_1, \ldots, x_{n-1}]]$. 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. Lemma 22.3 applied with $x = x_n$ then asserts precisely that

$$(**)\quad \mathcal{K}_{j_0}((x_1, \ldots, x_n)) \cap \mathcal{K}((x_1, \ldots, x_{n-1}))((x_n)) =$$
$$\mathrm{frac}\,(C[[x]]) \cap \big(\mathrm{frac}\,(B)\big)((x_n)) = \mathrm{frac}\,(B[[x_n]]) = \mathcal{K}((x_1, \ldots, x_n)).$$

From $(*)$ and $(**)$, we have that

$$\bigcap_i \mathcal{K}_i((x_1, \ldots, x_n)) \subseteq \mathcal{K}((x_1, \ldots, x_n)).$$

The opposite inclusion is obvious. □

Corollary 22.4. *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 $K[[x_1, \ldots, x_n]]$. Then*

$$\bigcap_{\Gamma \textit{ cofinite in } \Lambda} \mathrm{frac}\,(A^\Gamma) = \mathrm{frac}\,(A).$$

Proof. Since the completion of A^Γ is $K^\Gamma[[x_1, \ldots, x_n]]$, we have that

$$(*)\qquad \bigcap_{\Gamma \text{ cofinite in } \Lambda} \mathrm{frac}\,(A^\Gamma) \subseteq \bigcap_{\Gamma \text{ cofinite in } \Lambda} \mathrm{frac}\,(K^\Gamma[[x_1, \ldots, x_n]]).$$

Since

$$\bigcap_{\Gamma \text{ cofinite in } \Lambda} K^\Gamma = K$$

by Lemma 21.10 and part (b) of Theorem 22.2 we have that the right hand term in $(*)$ is $\mathrm{frac}\,(K[[x_1, \ldots, x_n]])$. This proves one of the inclusions needed, while the opposite inclusion is obvious. □

22.2. Structure of field extensions. We also want to observe the following:

Lemma 22.5. *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 Theorem 21.9.

Proof. 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 Corollary 22.4 and Theorem 22.1, 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 Corollary 7.13 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, $\Omega' \cong \mathcal{F}[X]/\big(h(X)\big)$, where h is a separable polynomial. Then

$$\mathcal{G} \otimes_{\mathcal{F}} \Omega' \cong \mathcal{G}[X]/\big(h(X)\big),$$

and since h is a separable polynomial, this ring is reduced. $\square$

We have now completed the proof of Theorem 21.4

23. Lecture 23

23.1. Preserving the singular locus with the Γ construction. By the *singular locus* $\mathrm{Sing}(R)$ 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 $\mathrm{Sing}(R)$ 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 23.1. *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 $\mathrm{Spec}\,(R^\Gamma)\mathrm{Spec}\,(R) = X$, given by contraction of primes. The unique prime ideal of R^Γ lying over P in R is $\mathrm{Rad}\,(PR^\Gamma)$. See Proposition 11.5. 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 7.10. 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 (c) of Theorem 21.7, 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, $Q_0 R_P^{\Gamma_0} = PR_P^{\Gamma_0}$ 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. $\square$

23.2. Proof of the existence of completely stable big test elements. We are now in a position to fill in the details of the proof of Theorem 21.1 on the existence of completely stable big test elements. The proof was sketched earlier to motivate our development of the gamma construction.

We need two preliminary results.

Lemma 23.2. *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 Lemma 22.5, 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. $\square$

Lemma 23.3. *Let B be a semilocal ring with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$. Let $J = \bigcap_{i=1} \mathfrak{m}_i$ be the Jacobson radical of B. Let A_i be the completion of B_{m_i} with respect to $\mathfrak{m}_i$, which is the same as the completion of B with respect to $\mathfrak{m}_i$. Then $\widehat{B}^J \cong \prod_{i=1}^k A_i$.*

Proof. Note that the completion of $B_{\mathfrak{m}_i}$ with respect to $\mathfrak{m}_i$ is the same as the completion of B with respect to $\mathfrak{m}_i$ because $B/\mathfrak{m}_i^n$ is already local (it has only one prime ideal) and so $B/\mathfrak{m}_i^n \cong B_{\mathfrak{m}_i}/(\mathfrak{m}_i B^n_{\mathfrak{m}_i)}$. Also since the $\mathfrak{m}_i$ as well as their n th powers are pairwise comaximal,

$$(\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_k)^n = (\prod_{i=1}^k \mathfrak{m}_i)^k = \prod_{i=1}^k \mathfrak{m}_i^k,$$

by the Chinese remainder theorem, which also yields

$$\varprojlim_n B/J^n \cong \varprojlim_n B/(\prod_{i=1}^k \mathfrak{m}_i^n) \cong \varprojlim_n \big(\prod_{i=1}^k (B/\mathfrak{m}_i^n)\big) \cong \prod_{i=1}^k (\varprojlim_n B/\mathfrak{m}_i^n) \cong \prod_{i=1}^k A_i.$$

$\square$

24. Lecture 24

24.1. Proof of Theorem 21.1. . We now restate Theorem 21.1: we then give the proof.

Theorem 24.1. *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 Lemma 23.2, $\widehat{B} \otimes_B R$ 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 Corollary , $(\widehat{B} \otimes_B R)_c$ 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 Proposition testchar.

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 Theorem 11.8. $\square$

24.2. Gorenstein rings and strong F-regularity revisited. 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 and Gorenstein, weak F-regularity implies strong F-regularity.

We first note the following fact:

Proposition 24.2. *Let R be a Noetherian ring of prime characteristic $p > 0$. Then the following conditions are equivalent:*

(a) If $N \subseteq M$ are arbitrary 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 Lemma 6.1 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 24.3. *Let $(R, \mathfrak{m}, K)$ be a Gorenstein local ring of characteristic p. Then the conditions of Proposition 24.2 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.

25. Lecture 25

25.1. Injective hulls of the residue class fields of Artin local rings. The following result is true for every Artin local ring $(A, \mathfrak{m}, K)$. However, we only give the proof when A contains a field, which is the only case we need. In this case, A contains a copy of K (not necessarily unique) so that we may assume we have $K \subseteq A$ such that K maps isomorphically onto $A/\mathfrak{m} \cong K$. We showed earlier that in this case $E := E_A(K) \cong \mathrm{Hom}_K(A, K)$ and that the functors $\mathrm{Hom}_R(\_\,, E)$ and $\mathrm{Hom}_K(\_\,, K)$ are isomorphic: see Subsection 20.3.

THEOREM 25.1. *Let $(A, \mathfrak{m}, K)$ be an Artin local ring. Then:*

(a) $E_A(K)$ has the same length as A.
(b) A is injective as an A-module iff A has type 1 iff A is an essential exteen-sion of K.
(c) $Hom_A(\_\,, E)$ preserves length when applied to a finite length A-module.
(d) For every finite length R-module M, the map $M \to Hom_R\big(Hom_R(M, E), E\big)$ is an isomorphism.
(e) The map $A \to Hom_A(E, E)$ given by sending a to multiplication by a is an isomorphism.

PROOF. (a), (b), (c), and (d) follow at once from the identificaation of the functors $\mathrm{Hom}_R(\_\,, E)$ and $\mathrm{Hom}_K(\_\,, K)$, and (e) follows from (d) when $M = A$. Parts (a) and (b) were noted earlier. $\square$

25.2. Calculation of the injective hull of a Gorenstein local ring.

THEOREM 25.2. *Let $(R, \mathfrak{m}, K)$ be a Gorenstein local ring with system of parameters $x_1, \dots, x_n$. For every integer $t \geq 1$, let $I_t = (x_1^t, \dots, x_n^t)R$. 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 $R/(x_1, \dots, x_n)R$, 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 18.3 applied to $x_1, \dots, x_n$ and $x_1^t, \dots, x_n^t$, with the matrix $A = \mathrm{diag}(x_1^{t-1}, \dots, x_n^{t-1})$. See also the last statement of Proposition 18.7, which will prove the final statement of this 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 clearly 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 $b_{t+1}y = a_tb_ty = (a_ty)b_t$, and θ_t is induced by multiplication by a_ty 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. $\square$

25.3. The injective hull of the residue class field of a local ring.

Proposition 25.3. *Let R be a Noetherian ring, let P be a prime ideal, and let $\kappa = \kappa_P$ denote $R_P/PR_P \cong \operatorname{frac}(R/P)$.*

(a) $E = E_R(R/P)$ is indecomposable (not a direct sum of two nonzero modules).

(b) $E_R(R/P)$ is an $R_P$module and is isomorphic with $E_{R_P}(\kappa)$

Proof. (a) If $E = E_1 \oplus E_2$ where both are nonzero, then $E_1 \cap R/P$ and $E_2 \cap R/P$ are both nonempty. But any two nonzero ideals in a domain have nonzero intersectioon, which implies that $E_1 \cap E_2$ is nonzero, a contradiction.

(b) Let $f \in R \setminus P$. Multiplication by f yields a map $E_R(R/P) \xrightarrow{f\cdot} E_R(R/P)$. Since this map is injective on R/P, it is injective on E, i.e., $f\cdot$ yields an in injection of E into E. Since the image is an injective module, it splits from E. By part (a), this implies that the image is all of E, so that $f\cdot : E \to E$ is an automorphism. Thus, multiplication by any $f \in R - P$ yields an automorphism of E, whose inverse can serve as the action of $1/f$ on E. $\square$

Proposition 25.4. *Let $(R, \mathfrak{m}, K)$ be local. Then $E_R(K) \cong E_{\widehat{R}}(K)$.*

Proof. The category of modules such that every element is killed by a power of the maximal ideal is the same over R and over $\widehat{R}$. All essential extensions of K over either ring are in this category, and are essential over either ring. So the maximal essential extensions are the same. $\square$

Proposition 25.5. *Let $(R, \mathfrak{m}, K)$ be local, and let $I \subseteq \mathfrak{m}$ be an ideal. Then $E_{R/I}(K) \cong \operatorname{Ann}_{E_R(K)} I \cong \mathit{Hom}_R\big(R/I,\, E_R(K)\big)$.*

Proof. $E' := E_{R/I}$ is an essential extension of K over R/I and, hence, over R. It is therefore contained in a maximal essential extension E. But then $\operatorname{Ann}_E I \supseteq E'$ is an essential extension of K over R/I contaain E', and so must equal E'. $\square$

Discussion 25.6. We can understand the injective hull of any R/P, P prime, as follows. We have that $E_R(R/P) \cong E_{R_P}(\kappa_P)$. This reduces the problem to understanding the injective hull of residue class field of a local ring. We may then complete, and write the ring as $T := K[[x_1, \ldots, x_n]]/I$ Hence, it is the annihilator of I in $E_K(T)$. But T is Gorenstein, and we can write the injective hull as

$$\varinjlim_t K[[x_1, \ldots, x_n]]/(x_1^t, \ldots, x_n^t) \cong \varinjlim_t K[x_1, \ldots, x_n]/(x_1^t, \ldots, x_n^t) \cong$$

$$\varinjlim_t \big(K[x_1]/(x_1^t) \otimes_R \cdots \otimes_R K[x_n]/(x_n^t)\big) \cong \bigotimes_{i=1}^n \big(\varinjlim_t K[x_i]/(x_i^t)\big).$$

We may identify

$$\varinjlim_t K[x_i](x_i^t) \cong K[x_i, x_i^{-1}]/K[x_i]$$

via the homomorphism such that the image of 1 in $K[x_i]/(x_i^t]$ maps to the image of $x_i^{-t} \in K[x_i, x_i^{-1}]/K[x_i]$. Let $y_j = \prod_{i\neq j} x_i$, $1 \le j \le n$, so that for each j, $x_j y_j = x_1 \cdots x_n$. Then:

$$E_{K[[x_1,\,\ldots,x_n]]}(K) \cong \bigotimes_{i=1}^n \big(K[x_i, x_i^{-1}]/K[x_i]\big)$$

$$\cong K[x_1,\,\ldots,x_n]_{x_1\cdots x_n}/\sum_{j=1}^n K[x_1,\,\ldots,x_n]_{y_j}$$

which, as a K-vector space, has as a basis the images of the strictly negative monomials $x_1^{-a_1} \cdots x_n^{-a_n}$ with all of the $a_i \ge 1$. The image of $x_1^{-1} \cdots x_n^{-1}$ generates the socle. Multiplication by a nonnegative monomial μ times a strictly negative monomial μ is the obvious one, in which one adds exponents, except that if any exponent becomes nonnegative the result is interpreted as 0.

25.4. The action of Frobenius on $E_R(K)$ for $(R, \mathfrak{m}, K)$ local Gorenstein. Let $(R,\,\mathfrak{m},\,K)$ be a Gorenstein local ring of characteristic p, 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 $t \ge 1$, 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 idenifty $\mathcal{F}^e(E)$ with E. Under this identification, if $v = \langle r;\, x_1^t,\,\ldots,x_n^t\rangle$, then $v^q = \langle r^q;\, x_1^{qt},\,\ldots,x_n^{qt}\rangle$.

26. Lecture 26

We can now prove the assertions in the first paragraph of Theorem 24.3. We begin with the argument to show that 0 is tightly closed in $E_R(K)$ for a weakly F-regular Gorenstein local ring

Proof. Let $(R, \mathfrak{m}, K)$ be a Gorenstein local ring of characteristic p. 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 and weakly F-regular, 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.

26.1. Splitting criteria and approximately Gorenstein local rings. Many of the results of this section do not depend on the characteristic.

Theorem 26.1. *Let $(R, \mathfrak{m}, K)$ 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 suppose that R is not necessarily complete, but that M is finitely generated. By part (b) of Theorem splitcrit 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 26.2 (splitting criterion for Gorenstein rings). *Let $(R, \mathfrak{m}, K)$ be a Gorenstein local ring, and let $x_1, \ldots, x_n$ be a system of parameters for R. Let $u \in R$ represent a socle generator in R/I, where $I = (x_1, \ldots, x_n)$, 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 Theorem 26.1 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 Theorem 25.2 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 Theorem 17.6 $\square$

Remark 26.3. 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 $(R, \mathfrak{m}, K)$ 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.

Remark 26.4. Note that the following conditions on an m-primary ideal I in a local ring $(R, \mathfrak{m}, K)$ are equivalent:

(1) R/I is a 0–dimensional Gorenstein.
(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 modulo 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 images 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 26.5. *Let $(R, \mathfrak{m}, K)$ 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 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 following.

THEOREM 26.6. *Let $(R, \mathfrak{m}, K)$ 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 26.7. *Let $(R, \mathfrak{m}, K)$ 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 $t \geq 1$, $u_t w \notin I_t M$.

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. $\square$

26.2. 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 Remark 26.4.

(1) 1 The socle in M/N is one-dimensional as K-vector space.
(2) 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 $N \subseteq m^t M$. Thus, a local ring R is approximately Gorenstein if and only if R itself has small cofinite irreducibles.

Note the the question of whether $(R, \mathfrak{m}, K)$ 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 $M/m^t M \cong \widehat{M}/m^t\widehat{M}$ 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:

Theorem 26.8. *Proposition Let $(R, \mathfrak{m}, K)$ 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}. □

Before giving the main result of this section, we note the following fact, due to Chevalley, that will be needed in the argument.

Theorem 26.9 (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 $t \gg 0$. □

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 26.10. *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 $Ru_1, \ldots, Ru_s$, 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 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 $P_1, \ldots, P_s$ such that, for every i, $\dim R/P_i = 1$, such that $P_1, \ldots, P_s$ 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 $m^t M$ 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 $i \le h$ 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. $\square$

27. Lecture 27

27.1. The Auslander-Buchsbaum theorem on depth and projective dimension. For the following basic result, we refer the reader to p. 67 of the Lecture Notes from Math 615, Winter 2015.

Theorem 27.1 (Auslander-Buchsbaum). *Let $(R, \mathfrak{m}, K)$ be local and $M \neq 0$ a finitely generated R-module that has finite projective dimension, denoted $\mathrm{pd}_R M$. Then*

$$\mathrm{pd}_R M = \mathit{depth}_{\mathfrak{m}} R - \mathit{depth}_{\mathfrak{m}} M.$$

Corollary 27.2. *Under the hypothesis of Theorem 27.1, $\mathrm{pd} M \leq \mathit{depth}_{\mathfrak{m}} R$. In particular, if $\mathit{depth}_{\mathfrak{m}} R = 0$, then M is free.*

If R is regular local of Krull dimension n, we have $\mathrm{depth}_{\mathfrak{m}} R = n$, and every finitely generated module has finite projective dimension. Hence:

Corollary 27.3. *Suppose that $(R, \mathfrak{m}, K)$ is regular local of Krull dimension n and M is a finitely generated nonzero module. Let I be the annihilator of M. Then $\mathrm{pd}_R M = n - \mathit{depth}_R M$, and M is Cohen-Macaulay if and only if $\mathrm{pd}_R M = n - \dim(M) = n - \dim(R/I) = \mathrm{height}\,(I)$.*

Corollary 27.4. *If R is regular local then $M \neq 0$ is free if and only if $\mathit{depth}_{\mathfrak{m}} M = n$.*

Remark 27.5. In working with these results, it is useful to know that a Cohen-Macaulay module over a local ring has *pure dimension*, i.e., every nonzero submodule has the same Krull dimension as M. This is equivalent to the statement that if $P \in \mathrm{Ass}\,(M)$, then $\dim(R/P) = \dim(M)$. This follows from the more general fact that if $x_1, \ldots, x_s$ is aa regular sequence on M, then every submodule of M has dimension at least s. (Use induction on s. If $s = 1$, this is clear, since a zero-dimensional module cannot have positive depth. In general, let $N \subseteq M$ and let x be a nonzerodivisor on M. Let $N' = \bigcup_t N :_M x^t$. This is the same as $N : x^t$ for all $t \gg 0$ since M has ACC. N' has the same dimension as N, since it contains N but is isomorphic to $x^t N' \subseteq N$ for all $t \gg 0$. Then x is not a zerodivisor on M/N', and it follows that $N'/xN' \subseteq M/xM$. The result now follows from the induction hypothesis.)

27.2. Supplementary Problems III.

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 $(R, \mathfrak{m}, K)$ 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 $(R, \mathfrak{m}, K)$ be a Gorenstein local ring of characteristic p, 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 $(R, \mathfrak{m}, K)$ be a Gorenstein local ring of characteristic p 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 characteristic p, 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.]

27.3. Proof of equivalence of conditions for strong F-regularity for F-finite rings. It still remains to prove the final assertion Theorem 24.3: 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 27.6. *Let* $(R, \mathfrak{m}, K)$ *be a local ring of characteristic* p.

(a) 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) 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,

$$\mathcal{F}^e_{\widehat{R}}(M) \cong \mathcal{F}^e_{\widehat{R}}(\widehat{R} \otimes_R M) \cong \widehat{R} \otimes_R \mathcal{F}^e_R(M) \cong \mathcal{F}^e_R(M).$$

□

THEOREM 27.7. *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 $q = q_1q_2$. 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, $(du^{q_1}))^{q_2q_3} \in (N^{[q_1]})^{[q_2q_3]}$. 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 $u \in N^*_M$. □

THEOREM 27.8. *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. □

We next want to establish a result that will enable us to prove the final assertion of Theorem 24.3.

THEOREM 27.9. *Let* $(R, \mathfrak{m}, K)$ *be a complete local ring of characteristic* p*. If* R *is reduced and* $c \in R^\circ$*, let* $\theta_{e,c} : R \to R^{1/q}$ *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 e such that the $\theta_{e,c}$ splits.*
(4) *R is reduced, and for some $c \in R^\circ$ 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 $c \in R^\circ$ such that R_c is regular, there exists e such that $\theta_{e,c}$ splits.*
(6) *R is reduced, and for some $c \in R^\circ$ that is a big test element, there exists e such that $\theta_{e,c}$ splits.*

Proof. Note that all of the conditions imply that R is reduced.

We already know that conditions (1) and (2) are equivalent, and that (3) $\Rightarrow$ (2), while (3) $\Rightarrow$ (4) $\Rightarrow$ (5) (the latter because of $c \in R^\circ$ and R_c is regular, c has a power that is a test element). Moreover, if there is a splitting for $\theta_{e,c}$ and c^k is a big test element, we also have that $c^{p^{e_1}}$, where and $p^{e_1} \geq k$, is a test element. Since $(c^{p^{e_1}})^{1/p^{e+e_1}} = c^{1/p^e}$, we have that $\theta_{e+e_1, c^{p^{e_1}}} = \theta_{e,c}$ splits. Hence, (6) $\Rightarrow$ (4), while (4) $\Rightarrow$ (6) is obvious, so that (4), (5), and (6) are equivalent. It will therefore follow that all six conditions are equivalent if prove that (2) is equivalent to both (3) and (6).

The argument is as follows. Let v generate the socle, a copy of $K = R/\mathfrak{m}$, in E. Every nonzerro submodule of E contains v. Thus, 0 is tightly closed in E iff v is not in 0^*_E. The latter is equivalent to the condition that for all c in R^0 (respectively, for a single big test element c) there exists e such that

$$(\dagger) \quad cv^{p^e} \neq 0 \in \mathcal{F}^e(E).$$

We think of the map $F^e : R \to R^{1/p^e}$ as isomorphic to $R \hookrightarrow R^{1/p^e}$. The $(\dagger)$ is equivalent to the condition that $c^{1/p^e}(1 \otimes v) \neq 0$ in $R^{1/p^e} \otimes_R E$. This in turn is equivalent to the condition thati if one tensors $\theta_{e,c} : R \to R^{/p^e} \otimes_R E$, the image of v is not 0. But since $K \cong Rv \hookrightarrow E$ is essential, this in turn is equivalent to the condition that $E \to R^{1/p^e} \otimes_R E$ is injective. This is turn is equivalent to the condtion that the dual map $\mathrm{Hom}_R(R^{1/p} \otimes_R E, E) \to \mathrm{Hom}_R(E, E)$ is surjective. By the adjointes of tensor and Hom and the isomorphism $R \cong \mathrm{Hom}_R(E, E)$ when R is complete, this becomes the condition that $\mathrm{Hom}_R(R^p, R) \to R$ is surjective. The this is equivalent to giving an Rlinear map $\alpha : R^{1/p^e} \to R$ such that $\alpha \circ \theta_{e,c}$ is the identity map on R. Hence, for every c and for every e, $(\dagger)$ holds if and only if

$$(\ddagger)\theta_{e,c} : R \to R^{1/p^e}$$

is split. It follows that 0 is tightly closed in E if and only if for all $c \in R^\circ$ there exists e such that $\theta_{e,c}$ splits (respectively, for one big test element $c \in R^\circ$ there exists e such that $\theta_{e,c}$ splits.) This say precisely that (2) is equivalent to both (3) and (6). $\square$

Remark 27.10. It is not really necessary to assume that R is reduced in the last three conditions. 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 $\theta_{e,c}$ 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 e 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:

THEOREM 27.11. *Let $(R, \mathfrak{m}, K)$ be an F-finite reduced 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 27.12. *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 $(R, \mathfrak{m}, K)$ 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 Theorem 24.3.

COROLLARY 27.13. *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, $(R, \mathfrak{m}, K)$ 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 27.14. 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.

27.4. Examples of strongly F-regular rings. We note the following examples, with references to the literature. "Polynomial ring" means polynoomial ring over a field of characteristic $p > 0$. Let $1 \le t \le r \le s$ and $a_1, \dots, a_n$ be positive integers. Then all of the rings listed below are strongly F-regular. . Note that examples (2) - (6) are finitely generated $\mathbb{N}$-graded rings (in (6), the grading is obtained by weighting the variables) over a field. The rings in (4) are direct summands of polynomial rings ([**Ho72**]). The result in (6) can be proved using the criteria in [**HH94b**, §7].

(1) Regular rings
(2) Generic determinantal rings: quotients of a polynomial ring over a field by the ideal generated by size t minors of a an $r \times s$ matrix formed from the indeterminates ([**HH94b**, §7])
(3) Toric rings: integrally closed rings generated by monomials in a polynomial ring (including Veronese subrings of and iterated Segre products of polynomial rings)
(4) Homogeneous coordinates rings of Grassmann varieties: these are generated by the $r \times r$ minors of an $r \times s$ matrix of indeterminates (and so are subrings of polynomial rings) ([**HH94b**, §7])
(5) Generic Pfaffian rings: quotients of a polynomial ring by the ideal generated by the Pfaffians of a given size of an alternating matrix of indeterminates (if $t = 2h$ is even, the symmetrically placed size t minors have determinants that are perfect squares: these minors are the squares of the Pffaffians) ([**Ba01**])
(6) For all sufficiently large primes p, the hypersurface defined by $x_1^{a_1} + \cdots + x_n^{a_n}$ over a field K of characteristic p when $\sum_i \frac{1}{a_i} > 1$ (the condition asserts that in a certain precise sense, the a_i are small compared to n)
(7) Direct summands of any of the above.

28. Lecture 28

28.1. Local cohomology: a first look.

Definition 28.1. Let R be a Noetherian ring and let M be an arbitrary module. Suppose that $I \subseteq R$ is an ideal. Notice that if $I \supseteq J$ the surjection $R/J \to R/I$ induces map $\mathrm{Ext}^i(R/I, M) \to \mathrm{Ext}^i(R/J, M)$. Thus, if $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_t \supseteq \cdots$ is a decreasing sequence of ideals then we get a direct limit system

$$\cdots \to \mathrm{Ext}^i_R(R/I_t, M) \to \mathrm{Ext}^i_R(R/I_{t+1}, M) \to \cdots$$

and we may form the direct limit of these Ext 's. We define $H^i_I(M) = \varinjlim_t \mathrm{Ext}^i(R/I^t, M)$, and call this module the i th *local cohomology module of M with support in I*.

Discussion 28.2. Suppose that we replace the sequence $\{I_t\}_t$ by an infinite subsequence. The direct limit is obviously unaffected. Likewise, if $\{J_t\}_t$ is another decreasing sequence of ideals which is cofinal with I_t (i.e., for all t, there exists u such that $J_u \subseteq T_t$ and v such that $I_v \subseteq J_t$), then the direct limit computed using the J's is the same. We can form a sequence $I_{a(1)} \supseteq J_{b(1)} \supseteq I_{a(2)} \supseteq J_{b(2)} \supseteq \cdots \supseteq I_{a(t)} \supseteq J_{b(t)} \supseteq \cdots$ which yield the same result, on the one hand, as $\{I_{a(t)}\}_t$ and, hence, as $\{I_t\}_t$. Similarly, it yields the same result as $\{J_t\}_t$.

In particular, if $I = (x_1, \cdots, x_n)R$, then the sequence $I_t = (x_1^t, \cdots, x_n^t)R$ is cofinal with the powers of I, and so may be used to compute the local cohomology.

We also have:

THEOREM 28.3. *If I, J are ideals of the Noetherian ring R with the same radical, then $H^i_I(M) \cong H^i_J(M)$ canonically for all i and for all R-modules M.*

PROOF. Each of the ideals I, J has a power contained in the other, and it follows that the sequences $\{I^t\}_t, \{J^t\}_t$ are cofinal with one another. □

DISCUSSION 28.4. If $X \subseteq \operatorname{Spec} R$ is closed, then $X = V(I)$ where I is determined up to radicals: we may write $H^i_X(M)$ for $H^i_I(M)$ and refer to *local cohomology with support in X*.

DISCUSSION 28.5. $\operatorname{Ext}^i_R(R/I^t, M)$ is a covariant additive functor of M, and Ext has a long exact sequence. All this is preserved when we take a direct limit. Thus, each $H^i_I()$ is a covariant additive functor, and given a short exact sequence of modules

$$0 \to A \to B \to C \to 0$$

there is a long exact sequence

$$0 \to H^0_I(A) \to H^0_I(B) \to H^0_I(C) \to H^1_I(A) \to H^1_I(B) \to H^1_I(C) \to$$
$$\cdots \to H^{i-1}_I(A) \to H^i_I(A) \to H^i_I(B) \to H^i_I(C) \to H^{i+1}_I(A) \to \cdots$$

which is functorial in the given short exact sequence. Moreover, if M is injective, $H^i_I(M) = 0$ for all $i \geq 1$. It is also worth noting that if $x \in R$ then the map $M \xrightarrow{x} M$ induces the map $H^i_I(M) \xrightarrow{x} H^i_I(M)$ on local cohomology.

Note, however, that even when M is finitely generated, the modules $H^i_I(M)$ need note be finitely generated, except under special hypotheses. However, we shall see that when I is a maximal ideal of R, they do have DCC.

DISCUSSION 28.6. H^0_I. Note that $\operatorname{Hom}_R(R/I, M)$ may be identified with $\operatorname{Ann}_M I$ and that the map $\operatorname{Hom}_R(R/I, M) \to \operatorname{Hom}_R(R/J, M)$ when $I \supseteq J$ may then be identified with the obvious inclusion $\operatorname{Ann}_M I \subseteq \operatorname{Ann}_M J$. This means that $H^0_I(M)$ may be identified with the functor which assigns to M its submodule $\cup_t \operatorname{Ann}_M I^t$, the submodule of M consisting of all elements that are killed by a power of I.

DISCUSSION 28.7. A minor variation on the definition of the local cohomology functors is as follows: First define $H^0_I(M) = \{x \in M : x \text{ is killed by some power of } I\}$. The define $H^i_I(M)$ as the ith right derived functor of H^0_I. Thus, to compute H^i_I one would choose an injective resolution of M, say $0 \to E_0 \to \cdots \to E_i \to \cdots$, where $M = \operatorname{Ker}(E_0 \to E_1)$, and then take the cohomology of $0 \to H^0_I(E_0) \to \cdots \to H^0_I(E_i) \to \cdots$. In the original definition one first takes the cohomology of the complex $\mathcal{C}^\bullet_t$:

$$0 \to \operatorname{Hom}_R(R/I^t, E_0) \to \cdots \to \operatorname{Hom}_R(R/I^t, E_i) \to \cdots$$

and then takes the direct limit of the cohomology. In the second definition, up to isomorphism, one takes the direct limit of the complexes $\mathcal{C}^\bullet_t$ and then takes cohomology. Since calculation of homology or cohomology commutes with taking direct limits, these two definitions are simply minor variations on one another.

PROPOSITION 28.8. *Let R be a Noetherian ring, $I \subseteq R$ and let M be any R-module. Then every element of $H^i_I(M)$ is killed by a power of I.*

PROOF. Every element is in the image of some $\operatorname{Ext}^i_R(R/I^t, M)$ for some t, and I^t kills that Ext. □ □

We now prove that local cohomology can be used to test depth.

THEOREM 28.9. *Let I be an ideal of a Noetherian ring R and let M be a finitely generated R-module. Then $H^i_I(M) = 0$ for all i if and only if $IM = M$. If $IM \neq M$ then the least value d of i such that $H^i_I(M) \neq 0$ is the depth of M on I, i.e., the length of any maximal M-sequence contained in I.*

PROOF. If $IM = M$ then $I^tM = M$ for all t, and then $I^t + \operatorname{Ann} M = R$ for all t. Since $I^t + \operatorname{Ann} M$ kills $\operatorname{Ext}^i_R(R/I^t, M)$, it follows that every one of these Ext's is zero, and so all the local cohomology modules vanish.

Now suppose that $IM \neq M$ and let $x_1, \ldots, x_d$ be a maximal M-sequence in I. We shall show by induction on d that $H^i_I(M) = 0$ if $i < d$ while $H^d_I(M) \neq 0$. If $d = 0$ this is clear, since then some element of $M - \{0\}$ will be killed by I and will be nonzero in $H^0_I(M)$. If $d > 0$ the short exact sequence $0 \to M \xrightarrow{x} M \to M/xM \to 0$ with $x = x_1$ yields a long exact sequence for local cohomology:

$$\cdots \to H^{i-1}_I(M/xM) \to H^i_I(M) \xrightarrow{x} H^i_I(M) \to H^i_I(M/xM) \cdots .$$

For $i < d$ the induction hypothesis shows that x is a nonzerodivisor on $H^i_I(M)$, which must vanish, since every element is killed by a power of $x \in I$. When $i = d$ the sequence also shows that $H^{d-1}_I(M/xM)$, which we know from the induction hypothesis is nonzero, injects into $H^d_I(M)$ (we already have $H^{d-1}_I(M) = 0$). $\square$

Our next objective is to give quite a different method of calculating local cohomology: equivalently, we may use either a direct limit of Koszul cohomology or a certain kind of Čechcohomology. In order to present this point of view, we first discuss the tensor product of two or more complexes, and then define Koszul homology and cohomology. We subsequently explain how to set up a direct limit system and, after a while, prove that we can obtain local cohomology in this way.

One of the virtues of having this point of view is that it will enable us to prove a very powerful theorem about change of rings. One of the virtues of local cohomology is that it is "more invariant," in some sense, than other theories that measure some of the same qualities. Its disadvantage is that it usually produces modules that are not finitely generated.

28.2. Tensor products of complexes and Koszul homology.

DISCUSSION 28.10. We shall discuss Koszul cohomology, using the notion of the tensor product of two complexes to define it. Let $K_\bullet$ and $L_\bullet$ be complexes of R-modules with differentials d, d', respectively. Then we let $M_\bullet = K_\bullet \otimes_R L_\bullet$ denote the complex such that:

(1) $M_h = \bigoplus_{i+j=h} K_i \otimes L_j$ and
(2) $d(a_i \otimes b_j) = da_i \otimes b_j + (-1)^i a_i \otimes d'b_j$ when $a_i \in K_i$ and $b_j \in L_j$

It is easy to check that this does, in fact, give a complex. If there are n complexes then we may define the tensor product

$$K^{(1)}_\bullet \otimes_R \ldots \otimes_R K^{(n)}_\bullet$$

recursively as

$$\left(K^{(1)}_\bullet \otimes_R \cdots \otimes_R K^{(n-1)}_\bullet\right) \otimes_R K^{(n)}_\bullet,$$

or we may take it to be the complex $M_\bullet$ such that

$$M_h = \bigoplus_{i(1)+\cdots+i(n)=h} K^{(1)}_{i(1)} \otimes_R \cdots \otimes_R K^{(n)}_{i(n)}$$

and such that if $a^j_{i(j)} \in K^{(j)}_{i(j)}$ for each j, then

$$d\left(a^1_{i(1)} \otimes \cdots \otimes a^n_{i(n)}\right) = \sum_{t=1}^{n} (-1)^{i(1)+\cdots+i(t-1)} a^1_{i(1)} \otimes \cdots \otimes d^t a_{i(t)} \otimes \cdots \otimes a^n_{i(n)},$$

where d^t denotes the differential on $K^{(t)}_\bullet$.

Given a sequence of n elements of a ring R, say $\underline{x} = x_1, \dots, x_n$, we may define the (homological) Koszul complex $K_\bullet(\underline{x}; R)$ as follows: If $n = 1$ and $x_1 = y$, it is the complex $0 \to K_1 \xrightarrow{y} K_0 \to 0$ where $K_1 = K_0 = R$ and the middle map is multiplication by y. Then, in general, $K_\bullet(\underline{x}; R) = K_\bullet(x_1; R) \otimes_R \cdots \otimes_R K_\bullet(x_n; R)$.

For the cohomological version we proceed slightly differently: We let $K^\bullet(y; R)$ (with one element, y, in the sequence) be the complex

$$0 \to K^0 \xrightarrow{y} K^1 \to 0$$

in which $K^0 = K^1 = R$ and the middle map is multiplication by y. We then let

$$K^\bullet(\underline{x}; R) = K^\bullet(x_1; R) \otimes_R \cdots \otimes_R K^\bullet(x_n; R).$$

We may then define $K_\bullet(\underline{x};\, M) = K_\bullet(\underline{x}; R) \otimes_R M$ and $K^\bullet(\underline{x};\, M) = K^\bullet(x; R) \otimes_R M$, which is isomorphic with $\mathrm{Hom}_R(K_\bullet(\underline{x}; R), M)$. We are mainly interested in the cohomological version here.

Discussion 28.11. Let M be an R-module and let $x \in R$ be any element. We may form a direct limit system

$$M \xrightarrow{x} M \xrightarrow{x} M \xrightarrow{x} \cdots M \xrightarrow{x} \cdots .$$

Let N be the set of all elements in N killed by some power of x, i.e., $N = \mathrm{Ker}\,(M \to M_x)$. Let $M' = M/N$. The copy of N (notice, by the way, that $N = H^0_{xR}(M)$) inside each copy of M is killed in the direct limit. Thus, the system above has the same direct limit as

$$M' \xrightarrow{x} M' \xrightarrow{x} M' \xrightarrow{x} \cdots M' \xrightarrow{x} \cdots .$$

This system is isomorphic with an increasing union, as indicated in the commutative diagram below:

$$\begin{array}{ccccccccccc}
M' & \hookrightarrow & M' \cdot \frac{1}{x} & \hookrightarrow & M' \cdot \frac{1}{x^2} & \hookrightarrow & \cdots & \hookrightarrow & M' \cdot \frac{1}{x^t} & \hookrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \\
M' & \xrightarrow{x} & M' & \xrightarrow{x} & M' & \xrightarrow{x} & \cdots & \xrightarrow{x} & M' & \xrightarrow{x} & \cdots
\end{array}$$

where $M' \cdot \frac{1}{x^t}$ denotes $\{m'/x^t : m' \in M'\} \subseteq M'_x$, and the map $M' \to M' \cdot \frac{1}{x^t}$ is the R-isomorphism sending m' to m'/x^t for every $m' \in M'$. Since the union of the modules in the top row is $M'_x \cong M_x$, it follows that the direct limit of the system in the bottom row is also M_x, and so the direct limit of the original system $M \xrightarrow{x} M \xrightarrow{x} M \xrightarrow{x} \cdots M \xrightarrow{x} \cdots$ is M_x as well (where the map from the tth copy of M into M_x sends m to m/x^t). The case where $M = R$ is of particular interest.

Discussion 28.12. If $\underline{x} = x_1, \ldots, x_n$ is a sequence of elements of R, we let $\underline{x}^t$ denote the sequence $x_1^t, \ldots, x_n^t$. We next want to describe how to form a direct limit system, indexed by t, from the Koszul complexes $K_\bullet(\underline{x}^t; M)$, where M is an R-module.

We begin with the case where $n = 1$, $x_1 = x$, and $M = R$. Then the map from $K^\bullet(x^t; R) \to K^\bullet(x^{t+1}; R)$ is as indicated by the vertical arrows in the diagram below:

$$\begin{array}{ccccccc} & & K^0 & & K^1 & & \\ 0 & \longrightarrow & R & \xrightarrow{x^t} & R & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle \mathrm{id}_R} & & \Big\downarrow{\scriptstyle x} & & \\ 0 & \longrightarrow & R & \xrightarrow{x^{t+1}} & R & \longrightarrow & 0 \end{array}$$

When we have maps of complexes $K_1^\bullet \xrightarrow{f} L_1^\bullet$, $K_2^\bullet \xrightarrow{g} L_2^\bullet$ there is an induced map $K_1^\bullet \otimes K_2^\bullet \to L_1^\bullet \otimes L_2^\bullet$ (such that the element $x \otimes y$ is sent to $f(x) \otimes g(y)$), and a similar observation applies to the tensor product of several complexes. Thus, the maps $K^\bullet(x_i^t; R) \to K^\bullet(x_i^{t+1}; R)$ that we constructed above may be tensored together over R to produce a map $K^\bullet(\underline{x}^t; R) \to K^\bullet(\underline{x}^{t+1}; R)$, and we may tensor over R with an R-module M to obtain a map $K^\bullet(\underline{x}^t;\, M) \to K^\bullet(\underline{x}^{t+1};\, M)$.

This leads to two equivalent cohomology theories. On the one hand, we may use the induced maps $H^\bullet(\underline{x}^t; M) \to H^\bullet(\underline{x}^{t+1} M)$ and take the direct limit.

On the other hand, we may form the complex $\varinjlim_t K^\bullet(\underline{x}^t; M)$, which we shall denote $K^\bullet(\underline{x}^\infty; M)$, and then take its cohomology, which we shall denote $H^\bullet(\underline{x}^\infty; M)$. This gives the same result as taking the direct limit of Koszul cohomology, since the calculation of cohomology commutes with direct limits.

Our main result along these lines, whose proof we defer for a while, is this:

Theorem 28.13. *Let R be a Noetherian ring and let $x_1, \ldots, x_n$ be elements of R. Let $I = (x_1, \ldots, x_n)R$. Then $H_I^j(M) \cong H^\bullet(\underline{x}^\infty; M)$ canonically as functors of M.*

The idea of our proof is this: we establish the result when $j = 0$ by an easy calculation, we note that both $H_I^\bullet(\_)$ and $H^\bullet(\underline{x}^\infty;\, \_)$ give rise to functorial long exact sequences given short exact sequences of modules, and also that both vanish in higher degree when the module M is injective. The result will then follow from very general considerations concerning cohomological functors. Before giving the details of the argument, we want to analyze further the complexes $K^\bullet(\underline{x}^\infty; M)$.

When the x's form a regular sequence there is quite a different explanation of why this complex ought to give the local cohomology. In that case $K^\bullet(\underline{x}^t; R)$ is a projective resolution of $R/(\underline{x}^t)R$. Applying $\mathrm{Hom}_R(\_,\, M)$ yields the same result as forming $K^\bullet(\underline{x}^t; R) \otimes_R M = K^\bullet(\underline{x}^t; M)$, and so $H^\bullet(\underline{x}^t;\, M)$ is $\mathrm{Ext}_R^\bullet(R/(\underline{x}^t),\, M)$ in this case, and the direct limit system of complexes $K^\bullet(\underline{x}^t; M)$ is the correct one for calculating the direct limit of these Ext's. What is somewhat remarkable is that the direct limit of Koszul cohomology gives the local cohomology whether the x_i form a regular sequence or not.

28.3. Description of the direct limit of cohomological Koszul complexes. We first consider the case where there is only one x and $M = R$. We refer to the diagrams $(\#_t)$ above that were used to define the direct limit system. The direct limit of the K^0's, each of which is a copy of R, and where each map is the identity map on R, is R. Thus, $K^0(x^\infty;\, R) = R$. The direct limit of the K^1's is

$$\varinjlim_t \,(R \xrightarrow{x} R \xrightarrow{x} R \xrightarrow{x} \cdots R \xrightarrow{x} \cdots) \cong R_x.$$

Moreover, the limit of the maps is the standard map $R \to R_x$ (which sends 1_R to 1_{R_x} and is injective when x is not a zerodivisor in R). Since $\otimes_R$ commutes with direct limits, it is easy to see that $K^\bullet(\underline{x}^\infty;\, R) \cong \underset{R}{\to}\bigotimes_{i=1}^{n} (0 \to R \to R_{x_i} \to 0)$. The term in degree 0 is simply the tensor product of n copies of R, and may be identified with R. The term in degree 1 is the direct sum of n terms, each of which is tensor product of $i-1$ copies of R, R_{x_i}, and then $n-i$ copies of R. Thus, the term in degree 1 is $R_{x_1} \oplus \cdots \oplus R_{x_n}$. The term in degree j, $0 \le j \le n$, is the sum of $\binom{n}{j}$ terms, one for each j element subset $S = \{i(1), \ldots, i(j)\}$ of the integers from 1 to n, where the term corresponding to $\{i(1), \ldots, i(j)\}$ consists of the tensor product of n terms, such that the hth term is a copy of R if $h \notin S$ and is a copy of $R_{x_{i(\nu)}}$ if $h = i(\nu) \in S$. Since $R_x \otimes_R R_y \cong R_{xy}$ (with the obvious generalization to tensor products of several such terms), we may use the following description: For each set $S \subseteq \{1, \ldots, n\}$, let $x(S) = \prod_{i\in S} x_i$ (note that $x(\emptyset) = 1$). Then $K^j(\underline{x}^\infty; R) \cong \bigoplus_{S\subseteq\{1,\,\ldots,\,n\},\,|S|=j} R_{x(S)}$.

When there are just two elements x, y the direct limit complex looks like:

$$0 \to R \to R_x \oplus R_y \to R_{xy} \to 0$$

while in the case where there are three elements x, y, z the direct limit complex looks like:

$$0 \to R \to R_x \oplus R_y \oplus R_z \to R_{yz} \oplus R_{xz} \oplus R_{xy} \to R_{xyz} \to 0.$$

Moreover, the map from each term to the next is easy to describe: it suffices to explain how $R_{x(S)}$ maps to $\bigoplus_{|T|=|S|+1} R_{x(T)}$: we then take the direct sum of all these maps. If we think of the sum $\bigoplus_{|T|=|S|+1} R_{x(T)}$ as a product, we see that this map will be given by component maps $R_{x(S)} \to R_{x(T)}$, where T has one more element in it than S does. The map is zero unless $S \subseteq T$. If $S \subseteq T$ then $R_{x(T)}$ is, up to isomorphism, the localization of $R_{x(S)}$ at the single element corresponding to the index that is in T and not in S. The map $R_{x(S)} \to R_{x(T)}$ is, except for sign, the obvious map of the ring $R_{x(S)}$ into its localization at the additional element. The only issue is what sign to attach, and the definition for tensor products of complexes tells us that is done with the same pattern as in the cohomological Koszul complex. To be completely explicit, the sign attached is $(-1)^a$, where a is the number of elements of S that precede the element of T that is not in S.

It is worth noting that the first map $R \to R_{x_1} \oplus \cdots \oplus R_{x_n}$ simply sends the element $r \in R$ to $r/1 \oplus \cdots \oplus r/1$, where the ith copy of $r/1$ is to be interpreted as an element of R_{x_i}.

We next want to discuss $K^\bullet(\underline{x}^\infty; M)$. The key point is that every $K^\bullet(\underline{x}^t; M) \cong K^\bullet(\underline{x}^t; R) \otimes_R M$, and it readily follows that $K^\bullet(\underline{x}^\infty; M) \cong K^\bullet(\underline{x}^\infty; R) \otimes_R M$. Thus, $K^j(\underline{x}^\infty; M) \cong \oplus_{|S|=j} M_{x(S)}$ and the maps are constructed from the ones in the case where $M = R$ by applying $\_ \otimes_R M$: thus, they are direct sums of maps whose components are maps induced by "localizing further," but with suitable signs attached. For example, in case the sequence of elements is x, y, z, the direct limit complex is

$$0 \to M \to M_x \oplus M_y \oplus M_z \to M_{yz} \oplus M_{xz} \oplus M_{xy} \to M_{xyz} \to 0.$$

We should also note that, in complete generality, the first map in the complex

$$M \to M_{x_1} \oplus \cdots \oplus M_{x_n}$$

simply sends m to $m/1 \oplus \ldots \oplus m/1$, where the i th copy of $m/1$ is to be interpreted as an element of M_{x_i}

We shall write $H^j(\underline{x}^\infty; M)$ for $H^j(K^\bullet(\underline{x}^\infty; M))$. We note the following facts

PROPOSITION 28.14. *Let $\underline{x} = x_1, \ldots, x_n$ be a sequence of elements in any ring R. Let $I = (x_1, \ldots, x_n)R$. Let M, M', M'', M_λ, etc., be arbitrary R-modules.*

(a) *a $K^\bullet(\underline{x}^\infty; R)$ is a complex of flat R-modules.*
(b) *b $H^0(\underline{x}^\infty; M)$ is the submodule of M consisting of all elements killed by a power of I. Thus, if R is Noetherian, it coincides with $H^0_I(M)$.*
(c) *c Given a short exact sequence $0 \to M' \to M \to M'' \to 0$ of R-modules there is a functorial long exact sequence of cohomology*

$$\begin{aligned} 0 \to H^0(\underline{x}^\infty; M') &\to H^0(\underline{x}^\infty; M) \to H^0(\underline{x}^\infty; M'') \\ &\to H^1(\underline{x}^\infty; M') \to H^1(\underline{x}^\infty; M) \to H^1(\underline{x}^\infty; M'') \to \ldots \\ &\to H^i(\underline{x}^\infty; M') \to H^i(\underline{x}^\infty; M) \to H^i(\underline{x}^\infty; M'') \to \ldots \\ &\to H^n(\underline{x}^\infty; M') \to H^n(\underline{x}^\infty; M) \to H^n(\underline{x}^\infty; M'') \to 0. \end{aligned}$$

(d) *If $\{M_\lambda\}_\lambda$ is any direct limit system of R-modules then*

$$H^j(\underline{x}; \varinjlim_\lambda M_\lambda) \cong \varinjlim_\lambda H^j(\underline{x}^\infty; M_\lambda).$$

In particular, $H^j(\underline{x}^\infty; \_)$ commutes with arbitrary direct sums.
(e) *For every value of j, every element of $H^j(\underline{x}^\infty; M)$ is killed by Ann M.*
(f) *Let $R \to S$ be a homomorphism, let $x_1, \ldots, x_n \in R$, and let $\underline{y} = y_1, \ldots, y_n$ denote their images in S. Let M be an S-module viewed as an R-module by restriction of scalars. Then $H^j(\underline{x}^\infty; M) \cong H^j(\underline{y}^\infty; M)$ as S-modules. (The first is an S-module because multiplication by any element of S gives an R-endomorphism of M which induces an R-endomorphism of the module $H^j(\underline{x}^\infty; M)$.)*

PROOF. (a) is obvious, since each module in the complex is a direct sum of localizations of R. Now $H^0(\underline{x}^\infty; M)$ is the kernel of the map $M \to M_{x_1} \oplus \cdots \oplus M_{x_n}$ sending m to $m/1 \oplus \cdots \oplus m/1$, and m will be in the kernel if and only if it is killed by a power of x_i for each i : this is equivalent to the assertion that m is killed by a power of I, since I is finitely generated by the x_i. The short exact sequence $0 \to M' \to M \to M'' \to 0$ may be tensored with the flat complex $K^\bullet(\underline{x}^\infty; R)$. Because of that flatness, we get a short exact sequence of complexes:

$$0 \to K^\bullet(\underline{x}^\infty; M') \to K^\bullet(\underline{x}^\infty; M) \to K^\bullet(\underline{x}^\infty; M'') \to 0$$

which, by the snake lemma, yields the long exact sequence of cohomology we want. (d) is clear from the fact that both $\otimes$ and calculation of (co)homology commute with formation of direct limits. (e) is immediate from the fact $H^j(\underline{x}^\infty; M)$ is a direct limit of Koszul cohomology $H^j(\underline{x}^\infty; M)$ (and this is the same as Koszul homology numbered backwards).

Finally, (f) follows from the fact that the action of any x_i or any product x of the x_i on M is the same as the action of the corresponding y_i or product y of y_i. This means that we may identify each M_x with the corresponding M_y, and so the complex $K^\bullet(\underline{x}^\infty; M)$ may be identified with the complex $K^\bullet(\underline{y}^\infty; M)$. The cohomology is then evidently the same. □ □

We next observe:

LEMMA 28.15. *Let $\underline{x} = x_1, \ldots, x_n$ be a sequence of elements of the ring R and let M be an R-module of finite length. Then $H^j(\underline{x}^\infty; M) = 0$ for all $j \geq 1$.*

PROOF. Since M has finite length, it has a finite filtration in which all the factors have the form $R/m = K$, where m is a maximal ideal of R. By induction on the length of the filtration and the long exact sequence provided by (7.6c), it suffices to handle the case where $M = K$. But then, by (f), we may replace R by $S = R/\mathrm{Ann}M = R/m = K$. I.e., we may assume that $R = K$ is a field and that $M = K$. Here, the x_i are replaced by their images in K. If any x_i is nonzero, the x_i generate the unit ideal and the result follows from the fact that every element of every H^j is killed by a power of the unit ideal of K. If every x_i is 0 the result follows from the fact that the complex is zero in all positive degrees, since in each summand one is localizing at 0 and, for any module N over any ring, $N_x = 0$ when $x = 0$. □ □

THEOREM 28.16. *Let R be a Noetherian ring and let E be an injective module. Let $x_1, \ldots, x_n \in R$. Then $H^j(\underline{x}^\infty; E) = 0$ for all $j \geq 1$*

PROOF. Since E is a direct sum of modules $E = E(R/P)$, where P is prime, we assume by (7.6d) that $E = E(R/P) = E_{R_P}(R_P/RR_P)$. By (7.6f) we may replace R by R_P. Thus, we may assume that (R, P, K) is local. Then every element of E is killed by a power of P. Since E is the directed union of its finitely generated submodules, each of which has finite length, the result follows at once from (7.7) and (7.6d). □ □

We are now ready to go back and give the proof of (7.4).

DISCUSSION 28.17. We now give the proof of Theorem 7.4. Fix a Noetherian ring R and a sequence of elements $\underline{x} = x_1, \ldots, x_n$ in R. Let $I = (x_1, \ldots, x_n)R$. We already know that the sequences of functors $H^i_I(\_)$ and $H^i(\underline{x}^\infty; \_)$ from R-modules to R-modules behave similarly in three respects:
(1) $H^0_I(\_)$ and $H^0(\underline{x}^\infty; \_)$ are canonically isomorphic functors: in both cases their values on M may be identified with the submodule of M consisting of all elements that are killed by a power of I.
(2) Both $H^i_I(\_)$ and $H^i(\underline{x}^\infty; \_)$ vanish on injective R-modules for $i \geq 1$.
(3) Both the sequence of functors $H^i_I(\_)$ and the sequence of functors $H^i(\underline{x}^\infty; \_)$ have functorial long exact sequences induced by a given short exact sequence of modules.

These three properties are sufficient to enable us to give a canonical isomorphism between these two cohomology theories. The argument is very general: it makes no use of any properties of these functors other than (1), (2), (3) above. Both for typographical convenience and to illustrate the degree of generality of the proof, we change notation and write, simply, H^i for H^i_I and $\underline{H}^i$ for $H^i(\underline{x}^\infty; \_)$.

Now, given any R-module M we can embed M in an injective module E and so construct a short exact sequence $0 \to M \to E \to C \to 0$. This gives rise to two long exact sequences, one for H and one for $\underline{H}$. Since both vanish on injectives, we obtain exactness of the top and bottom rows in the diagram below, while the vertical arrows are provided by the identification of H^0 and $\underline{H}^0$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \underline{H}^0(M) & \longrightarrow & \underline{H}^0(E) & \longrightarrow & \underline{H}^0(C) & \longrightarrow & \underline{H}^1(M) & \longrightarrow & 0 \\
 & & \uparrow\cong & & \uparrow\cong & & \uparrow\cong & & & & \\
0 & \longrightarrow & H^0(M) & \longrightarrow & H^0(E) & \longrightarrow & H^0(C) & \longrightarrow & H^1(M) & \longrightarrow & 0
\end{array}$$

Thus, we get an induced isomorphism $H^1(M) \cong \underline{H}^1(M)$, since cokernels of isomorphic maps are isomorphic. This identification is independent of the choice of the embedding of M into E. To see this, it suffices to compare what happens when E is an injective hull of M with what happens with an embedding into some other injective. The second embedding may then be taken into $E \oplus E'$ (where $M \subseteq E$), and E' is injective. C is then replaced by $C \oplus E'$. We leave the details to the reader. It is also not hard to check that the identification of H^1 with $\underline{H}^1$ is an isomorphism of functors. The long exact sequences that yield the rows of (#) also give isomorphisms of $H^{i+1}(M) \cong H^i(C)$ for $i \geq 1$, and similarly for $\underline{H}$. Thus, once we have established the isomorphisms $H^i \cong \underline{H}^i$ for some $i \geq 1$, we may use the isomorphisms coming from the long exact sequences to get $H^{i+1}(M) \cong H^i(C) \cong \underline{H}^i(C) \cong \underline{H}^{i+1}(M)$. Again, one can check easily that the isomorphism $H^{i+1}(M) \cong \underline{H}^{i+1}(M)$ that one obtains in this way is independent of the choice of the embedding $0 \to M \to E$. It is also not difficult to check that it is an isomorphism of functors.

Finally, one can also check that our identification of $H^\bullet$ with $\underline{H}^\bullet$ is compatible with the connecting homomorphisms in long exact sequences, so that, in each instance, one gets an isomorphism of long exact sequences. The details are not difficult, and we omit them here.

This completes our discussion of the proof of Theorem 7.4. $\square$

When we speak of *the number of generators of an ideal I up to radicals* we mean the least integer n such that $\operatorname{Rad} I$ is also the radical of an ideal generated by n elements. By taking powers, we may always arrange for the n elements to be in I. We note:/medskip

Corollary 28.18. *Let I be an ideal of a Noetherian ring R. If I is generated by n elements up to radicals, then $H^i_I(M) = 0$ for $i > n$.*

Proof. Suppose that $\operatorname{Rad} I = \operatorname{Rad} J$, where $J = (x_1, \ldots, x_n)R$. Then $H^i_I(M) = H^i_J(M) = H^i(\underline{x}^\infty; M)$, and the last is obviously zero when $i > n$, since the complex $K^\bullet(\underline{x}^\infty; M)$ is zero in degree bigger than n. $\square$

Corollary 28.19. *Let $R \to S$ be a homomorphism of Noetherian rings, let $I \subseteq R$ be an ideal and let M be an S-module. Then $H^i_I(M) \cong H^i_{IS}(M)$ as S-modules.*

Proof. Let $I = (x_1, \dots, x_n)R$ and let $y_1, \dots, y_n$ be the images of the x's in S. Then $H^i_I(M)$ may be identified with $H^i(\underline{x}^\infty; M)$, and since $IS = (y_1, \dots, y_n)S$, $H^i_{IS}(M)$ may be identified with $H^i(\underline{y}^\infty; M)$, and $H^i(\underline{x}^\infty; M) \cong H^i(\underline{y}^\infty; M)$, as noted earlier, because each x_j acts on M in the same way that y_j does. $\square$ $\square$

Moreover, since we already know the corresponding fact for $H^i(\underline{x}^\infty; \_)$ we have:

Corollary 28.20. *Let R be Noetherian, $I \subseteq R$, and let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a direct limit system of R-modules. Then $H^i_I(\varinjlim_\lambda M_\lambda) \cong \varinjlim_\lambda H^i_I(M_\lambda)$.* $\square$

We leave the following as an exercise.

Proposition 28.21. *Let S be a flat Noetherian R-algebra, where R is Noetherian, and let I be an ideal of R and M an R-module. Then $S \otimes_R H^i_I(M) \cong H^i_I(S \otimes_R M) \cong H^i_{IS}(S \otimes_R M)$. In particular, this holds when S is a localization of R or when S is the m-adic completion of the local ring (R, m, K).*

Note: Further revisions of these notes are in progress. In the meantime, see §§1.–19. of the *Local Cohomology* notes on the course Web site, §7. of the paper *Tight closure of parameter ideals and splitting in module-finite extensions*, and the expository manuscript *Tight closure and strongly F-regular rings*: the links are just below the link for the revised lecture notes.

Bibliography

[Ab08] I. M. Aberbach, The existence of the F-signature for rings with large Q-Gorenstein locus. J. Algebra 319(7), 2994?3005 (2008).

[AbEn06] I. M. Aberbach and F. Enescu, *When does the F-signature exist*, Ann. Fac. Sci. Toulouse Math. (6) **15** (2006) 195–201.

[AbL03] I. M. Aberbach and G. J. Leuschke, *The F-signature and strong F-regularity*, Math. Res. Lett. **10** (2003) 51–56.

[An93] M. André, *Homomorphismes réguliers en characteristique p*, C. R. Acad. Sci. Paris **316** (1993) 643–646.

[And20] Y. André, *Weak functoriality of Cohen-Macaulay algebras*, Journal of the American Mathematical Society, **33** (2020) 63?380.

[Ba01] C. Băeţică, F-rationality of algebras defined by Pfaffians. Memorial issue dedicated to Nicolae Radu. Math. Re (Bucur.) 3 (53) (2001), 139–144.

[BE73] D. Buchsbaum and D. Eisenbud, *What makes a complex exact*, J. Algebra **25** (1973) 259–268.

[BE77] 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.

[BMRS15] A. Benito, G. Muller, J. Rajchgot, and K. E. Smith, *Singularities of locally acyclic cluster algebras*, Algebra & Number Theory **9** (2015), 913–936.

[Bha21] B. Bhatt, *Cohen-Macaulayness of absolute integral closures*, preprint, arXiv:2008.08070, v. 2.

[Bou87] J.-F. Boutot, *Singularités rationelles et quotients par les groupes réductifs*, Invent. Math. **88** (1987) 65–68.

[BrSk74] J. Briançon and H. Skoda, *Sur la clôture intégrale d'un ideal de germes de fonctions holomorphes en un point de* $\mathbf{C}^n$. C. R. Acad. Sci. Paris Sér. A **278** (1974), 949–951.

[Bru91] W. Bruns, *Algebras defined by powers of determinantal ideals*, J. Algebra **142** (1991) 150–163.

[Bru96] W. Bruns, *Tight closure* Bull. Amer. Math. Soc. **33** (1996) 447–458.

[BruHer93] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge studies in advanced mathematics **39**, 1993.

[BruV88] W. Bruns and U. Vetter, *Determinantal Rings*, Springer-Verlag Lecture Notes in Math. **1327**, 1988.

[Chan97] S.-T. Chang, *Betti numbers of modules of exponent two over regular local rings*, J. of Alg. **193** (1997) 640–659.

[Char91] H. Charalambous, *Lower bounds for Betti numbers of multigraded modules*, J. of Alg. **137** (1991) 491–500.

[CHe97] A. Conca and J. Herzog, *Ladder determinantal ideals have rational singularities*, Adv. Math. **132** (1997), 120–147.

[CMSV18] A. Conca, M. Mostafazadehfard, A.K. Singh, M. Varbaro, *Hankel determinantal rings have rational singularities*, Adv. Math. **335** (2018), 111–129.

[CMSV] A. Conca, M. Mostafazadehfard, A.K. Singh, M. Varbaro, *Cyclic covers and the F-regularity of Hankel determinantal rings*, in preparation.

[DaMuSm20] R. Datta and T. Murayama with an Appendix by K. E. Smith, *Excellence, F-singularities, and solidity*, arXiv:2007.10383 [math.AC], July 20, 2020.

[DaSm] R. Datta and K. E. Smith, *Frobenius and valuation rings*, Algebra & Number Theory **10** (2016), 1057–1090 [Correction to the article: Algebra & Number Theory **11** (2017), 1003–1007.

[Die10] G.D. Dietz, *A characterization of closure operations that induce big Cohen-Macaulay modules*, Proceedings of the American Mathematical Society, **138** (2010) 3849–3862.

[Du00] D. Dugger, *Betti Numbers of Almost Complete Intersections*, Illinois J. Math. **44** (2000) 531–541.

[ELS01] L. Ein, R. Lazarsfeld, and K. E. Smith, *Uniform bounds and symbolic powers on smooth varieties* Invent. Math. **144** (2001), 241–252.

[EiHu92] 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.

[EvGr85] E.G. Evans and P. Griffith, *Syzygies*, London Math. Soc. Lecture Note Series **106** Cambridge Univ. Press, Cambridge, 1985.

[FeW89] R. Fedder and K.-i. Watanabe, *A characterization of F-regularity in terms of F-purity*, in *Commutative Algebra*, Math. Sci. Research Inst. Publ. **15** Springer-Verlag, New York-Berlin-Heidelberg (1989) 227–245.

[Gla96] D. J. Glassbrenner, *Strong F-regularity in images of regular rings*, Proc. Amer. Math. Soc. **124** (1996) 345–354.

[GlaSm95] D. J. Glassbrenner and K. E. Smith, *Singularities of ladder determinantal varieties*, J. Pure Appl. Alg. **101** (1995) 59–75.

[GraR70] H. Grauert and O. Riemenschneider, *Verschwindungsätze für analytische kohomologiegruppen auf komplexen Räuman*, Invent. Math. **11** (1970) 263–290.

[HaMo83] C. Han and P. Monsky, *Some surprising Hilbert-Kunz functions*, Math Z. **214** (1983) 119–135.

[Ha95a] N. Hara, *F-regularity and F-purity of graded rings*, J. Algebra **172** (1995) 804–818.

[Ha95b] N. Hara, *F-injectivity in negative degree and tight closure in graded complete intersection rings*, C.R. Math. Acad. Sci. Canada **17** (1995) 247–252.

[Ha98a] N. Hara, *Classification of two dimensional F-regular and F-pure singularities*, Adv. Math. **133** (1998), 33–53.

[Ha98b] N. Hara, *A characterization of rational singularities in terms of injectivity of Frobenius maps*, Amer. J. Math. **120** (1998), 981–996.

[Hart79] R. Hartshorne, *Algebraic Vector Bundles on Projective Spaces: a Problem List*, Topology, **18** (1979) 117–128.

[Heit02] R. C. Heitmann, *The direct summand conjecture in dimension three,* Annals of Math. **156** (2002) 695–712.

[Heit05] R. C. Heitmann, *Extended plus closure and colon-capturing,* J. Algebra **293** (2005) 407–426.

[HeitMa18] R. Heitmann and L. Ma *Big Cohen-Macaulay algebras and the vanishing conjecture for maps of Tor in mixed characteristic*, Algebra Number Theory **12** (2018) 1659–1674.

[Her74] Jürgen Herzog, *Ringe der Charakteristik p und Frobeniusfunktoren*, Math. Z. **140** (1974), 67–78.

[Ho72] M. Hochster, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*, Annals of Math. **96** (1972), 318–337.

[Ho73] M. Hochster, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. **51** (1973) 25–43.

[Ho77] M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977) 463–488.

[Ho94a] M. Hochster, *Solid closure*, in *Commutative Algebra: Syzygies, Multiplicities and Birational Algebra*, Contemp. Math. **159**, Amer. Math. Soc., Providence, R. I., 1994, 103–172.

[Ho94b] M. Hochster, *Tight closure in equal characteristic, big Cohen-Macaulay algebras, and solid closure* in *Commutative Algebra: Syzygies, Multiplicities and Birational Algebra*, Contemp. Math. **159** Amer Math Soc., Providence, R. I., 1994,173–196.

[Ho95] M. Hochster, Book Review of *Cohen-Macaulay rings*, by Winfried Bruns and Jürgen Herzog, Bull. A.M.S. **32** (1995) 265–275.

[Ho96] M. Hochster, *The notion of tight closure in equal characteristic zero* in *Proc. of the CBMS Conference on Tight Closure and Its Applications* (Fargo, North

Dakota, July, 1995), Appendix to the notes on the main lectures by Craig Huneke, C.B.M.S. Regional Conference Series, Amer. Math. Soc., Providence, R.I., 1996.

[Ho02] M. Hochster, *Big Cohen-Macaulay algebras in dimension three via Heitmann's theorem,* J. Algebra **254** (2002) 395–408.

[Ho07] M. Hochster, *Foundations of Tight Closure Theory*, 276 pp., lecture notes available at http://www.math.lsa.umich.edu/ hochster/711F07/711.html.

[Ho17] M. Hochster, *Homological conjectures and lim Cohen-Macaulay sequences*, in Homological and Computational Methods in Commutative Algebra, Springer INdAM Series 20, Springer, 2017, pp. 181–197.

[HoE93] M. Hochster and J. A. Eagon*Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971) 1020–1058.

[HH88] M. Hochster and C. Huneke, *Tightly closed ideals*, Bull. Amer. Math. Soc. **18** (1988) 45–48.

[HH89a] M. Hochster and C. Huneke, *Tight closure* in *Commutative Algebra*, Math. Sci. Research Inst. Publ. **15** Springer-Verlag, New York-Berlin-Heidelberg, 1989, 305–324.

[HH89b] M. Hochster and C. Huneke, *Tight closure and strong F-regularity*, Mémoires de la Société Mathématique de France, numéro **38**, 1989,119–133.

[HH90] M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math Soc. **3** (1990) 31–116.

[HH91a] M. Hochster and C. Huneke, *Absolute integral closures are big Cohen-Macaulay algebras in characteristic p*, Bull. Amer. Math. Soc. (New Series) **24** (1991) 137–143.

[HH91b] M. Hochster and C. Huneke, *Tight closure and elements of small order in integral extensions*, J. of Pure and Appl. Algebra **71** (1991) 233–247.

[HH92] M. Hochster and C. Huneke, *Infinite integral extensions and big Cohen-Macaulay algebras*, Annals of Math. **135** (1992) 53–89.

[HH93] M. Hochster and C. Huneke, *Phantom homology*, Memoirs Amer. Math. Soc., Vol. **103**, No. 490, 1993, 1–91.

[HH94a] M. Hochster and C. Huneke, *F-regularity, test elements, and smooth base change*, Trans. Amer. Math. Soc. **346** (1994) 1–62.

[HH94b] M. Hochster and C. Huneke, *Tight closure of parameter ideals and splitting in module-finite extensions*, J. of Algebraic Geometry **3** (1994) 599–670

[HH95] M. Hochster and C. Huneke, *Applications of the existence of big Cohen-Macaulay algebras*, Advances in Math. **113** (1995) 45–117.

[HH99] M. Hochster and C. Huneke, *Tight closure in equal characteristic 0*, preprint. Partially revised in 2019 and 2021.

[HH02] M. Hochster and C. Huneke, *Comparison of symbolic and ordinary powers of ideals*, Inventiones Math. **147** (2002) 349–369.

[HH07] M. Hochster and C. Huneke, *Fine behavior of symbolic powers of ideals* llinois J. Math. **51** (2007) 171–183.

[HRi05] M. Hochster and B. Richert, *Lower bounds for Betti numbers of special extensions*, J. Pure and Appl. Alg **201** (2005) 328–339.

[HR74] M. Hochster and J. L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Advances in Math. **13** (1974) 115–175.

[HR76] M. Hochster and J. L. Roberts, *The purity of the Frobenius and local cohomology*, Advances in Math. **20** (1976) 117–172.

[HY21a] M. Hochster and Y. Yao, *F-rational signature and drops in the Hilbert-Kunz multiplicity*, preprint, 2021.

[HY21b] M. Hochster and Y. Yao, *Splitting of ^eM, strong F-regularity, and the existence of small Cohen-Macaulay modules*, preprint, 2021.

[Hu96] C. Huneke, *Tight Closure and Its Applications*, Proc. of the C.B.M.S. Conference held at Fargo, North Dakota, July, 1995, C.B.M.S. Regional Conference Series, Amer. Math. Soc., Providence, R.I., 1996.

[HuL02] C. Huneke and G. J. Leuschke, *Two theorems about maximal Cohen-Macaulay modules*, Math. Ann. **324** (2002) 391–404.

[HuLy07] C. Huneke and G. Lyubeznik, *Absolute integral closure in positive characteristic,* Advances in Math. **210** (2007) 498–504.

[HuUl87] C. Huneke and B. Ulrich, *The structure of linkage*, Ann. of Math. **126** (1987) 277–334.

[Jia21a] Z. Jiang, *Test elements in equal characteristic semianalytic algebras*, preprint, arXiv:2104.12867v1 [math.AC].

[Jia21b] Z. Jiang, *Closure operations in complete local rings of mixed characteristic*, preprint, arXiv:2010.12564v2 [mah.AC].

[KaNe18] M. Katzmann and C. B. Miranda-Neto, *Strong F-regularity and generating morphisms of local cohomology modules*, preprint, arXiv:1806.04538 [math.AC].

[Ku69] E. Kunz, *Characterizations of regular local rings of characteristic p*, Amer. J. Math. **91** (1969) 772–784.

[Ku76] E. Kunz, *On Noetherian rings of characteristic p*, Amer. J. Math. **98** (1976) 999–1013.

[LS81] J. Lipman and A. Sathaye, *Jacobian ideals and a theorem of Briançdon-Skoda*, Michigan Math. J. **28** (1981) 199–222.

[LT81] 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.

[LySm99] G. Lyubeznick and K. E. Smith, *Strong and weak F-regularity are equivalent for graded rings*, Amer. J. Math. **121** (1999), 1279–1290.

[LySm01] G. Lyubeznick and K. E. Smith, *On the commutation of the test ideal with localization and completion*, Trans. Amer. Math. Soc. **353** (2001) 3149–3180.

[Mac96] B. MacCrimmon, *Strong F-regularity and boundedness questions in tight closure*, Thesis, University of Michigan, 1996.

[MaSch18] L. Ma and K. Schwede, *Perfectoid multiplier/test ideals in regular rings and bounds on symbolic powers* Invent. Math. **214** (2018) 913–955.

[Mo83] P. Monsky, *The Hilbert-Kunz function*, Math. Ann. **263** (1983) 43–49.

[Mat70] H. Matsumura, *Commutative algebra*, Benjamin, 1970.

[Mur22] T. Murayama, *Uniform bounds on symbolic powers in regular rings*, preprint, arXiv:2111.06049v2 [math.AC].

[Nag] M. Nagata, *Local rings*, Interscience, New York, 1962.

[PS73] C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale*, Publ. Math. I.H.E.S. (Paris) **42** (1973) 323–395.

[PS74] C. Peskine and L. Szpiro,*Syzygies et multiplicités*, C. R. Acad. Sci. Paris Sér. A **278** (1974) 1421–1424.

[Pop85] D. Popescu, *General Néron desingularization*, Nagoya Math. J. **100** (1985) 97–126.

[Pol18] T. Polstra, *Uniform bounds in F-finite rings and lower semi-continuity of the F-signature*, Trans. Amer. Math. Soc. **370** (2018) 3147–3169.

[Rad92] N. Radu, *Une classe d?anneaux noethériens*, Rev. Roumanie Math. Pures Appl. **37** (1992), 78–82.

[R.G.18] Rebecca R.G., *Closure operations that induce big Cohen-Macaulay algebras.*, Journal of Pure and Applied Algebra, **222** (2018) 1878–1897.

[Rob94] P. Roberts, *A calculagtion of local cohomology*, in Commutative Algebra: Syzygies, Multiplicities and Birational Algebra, Contemp. Math. **159**, Amer. Math. Soc., Providence, R. I., 1994, 351–356.

[Sant80] L. Santoni, *Horrocks' question for monomially graded modules*, Pacific J. Math. **141** (1990) 105–124.

[SchSm10] K. Schwede and K. E. Smith, *Globally F-regular and log Fano varieties*, Adv. Math. **224** (2010), 863–894.

[Si99] A. K. Singh, *F-regularity does not deform*, Amer. J. Math. **121** (1999) 919–929.

[Sk72] H. Skoda, *Applications des techniques L^2 a la théorie des idéaux d'une algèbre de fonctions holomorphes avec poids*, Ann. Sci. École Norm. Sup. (4) **5** (1972), 545–579.

[Sm94] K. E. Smith, *Tight closure of parameter ideals*, Inventiones Math. **115** (1994) 41–60.

[Sm95a] K. E. Smith, *Test ideals in local rings*, Trans. Amer. Math. Soc. **347** (1995) 3453–3472.

[Sm95b] K. E. Smith, *Tight closure and graded integral extensions*, J. Algebra **175** (1995) 568–574.

[Sm97a] K. E. Smith, *F-rational rings have rational singularities*, Amer. J. Math, **119** (1997), 159–180.

[Sm97b] K. E. Smith, *Tight closure in graded rings*, J. Math. Kyoto Univ. **37** (1997), 35–53.

[Sm00] K. E. Smith,*Globally F-regular varieties: applications to vanishing theorems for quotients of Fano varieties*, Michigan Math. J. **48** (2000) 553–572.

[Stu08] J. F. Stubbs, *Potent elements and tight closure in Artinian modules*, Thesis, University of Michigan, 2008.

[Swan98] R. G Swan, *Néron-Popescu desingularization*, Algebra and geometry (Taipei, 1995), 135–192, Lect. Algebra Geom. **2** Int. Press, Cambridge, MA, 1998.

[Tuc12] K. Tucker, *F-signature exists*, Invent Math **190** (2012) 743–765.

[Wa17] Mark E. Walker, *Total Betti numbers of modules of finite projective dimension*, Ann. of Math. (2) **186** (2017), 641–646.

[W91] K.-i. Watanabe, *F-regular and F-pure normal graded rings*, J. of Pure and Applied Algebra **71** (1991) 341–350

[W94] K.-i. Watanabe, *Infinite cyclic covers of strongly F-regular rings*, Contemp. Math. **159** (1994) 423–43.

[Wil95] L. Williams, *Uniform stability of kernels of Koszul cohomology indexed by the Frobenius endomorphism*, J. Algebra **172** (1995) 721–743.

[Yao06] Y. Yao, *Observations on the F-signature of local rings of characteristic p*, J. Algebra **299** (2006) 198–218.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Van Nostrand, Princeton, 1960.

Index