TOPICS IN COMMUTATIVE ALGEBRA: REGULAR RINGS, COHEN-MACAULAY RINGS AND MODULES, MULTIPLICITIES, AND TIGHT CLOSURE

Mel Hochster

Math 615: Lecture of January 8, 2020

In these lectures, all rings are assumed to be commutative, associative, with multiplicative identity denoted 1, which may be subscripted with the letter denoting the ring if precision is needed. Ring homomorphisms $R \to S$ are assumed to map $1_R \in R$ to $1_S \in S$. Modules M over a ring R are assumed to be *unital*, i.e., $1 \cdot u = u$ for all $u \in M$. A *local* ring is a Noetherian ring with a unique maximal ideal. The statement that $(R,\, m)$ is local means that R is a local ring with maximal ideal m. The statement that $(R,\, m,\, K)$ is local means that R is local with maximal ideal m and residue class field $K = R/m$. We use $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ for the nonnegative integers, the integers, the rational numbers, the real numbers, and the complex numbers, respectively.

We give an overview of some the material that will be covered near the beginning of this set of lectures.

We will study regular rings, Cohen-Macaulay rings and modules, Hilbert-Samuel multiplicities, some algebraic K-theory, the method of reduction to positive characteristic, some tight closure theory and the theory of liaison, also called linkage. We shall also discuss methods for proving that rings are Cohen-Macaulay. In studying these topics we shall find many subtle connections, and discuss many open questions. We will need homological tools, including Tor, Ext, and Koszul (co)homology.

We make the convention that (R, m, K) is *quasilocal* if R has unique maximal ideal m and $K = R/m$, the residue class field.

By an *improper regular sequence* $x_1, \, \ldots\, , x_n \in R$ on an R-module M we mean a sequence of elements of R such that x_1 is not a zerodivisor on M, i.e., multiplication by x_1 is an injective map from M to M, and for $2 \leq i \leq n$, x_i is not a zerodivisor on $M/(x_1, \, \ldots\, , x_{i-1})M$. An improper regular sequence is called a *regular sequence* if, in addition, $(x_1, \ldots\, , x_n)M \neq M$. The terms *Rees sequence*, *R-sequence on M,* and *M-sequence* are also used. The empty sequence is consider a regular sequence of length 0.

Thus, an improper regular sequence may or may not be a regular sequence. $1, 0, 0, \ldots\, , 0$ is an improper regular sequence on any module. $x_1, \, \ldots\, , x_n$ is a regular sequence on $M = R = K[x_1, \, \ldots\, , x_n]$ or $M = R = K[[x_1, \, \ldots\, , x_n]]$, the polynomial or formal power series ring, where K is a field (this is also true when K is any nonzero commutative ring, but not as obvious).

If $x_1, \ldots, x_n$ is an (improper) regular sequence on each M_λ for the modules in some family indexed by $\lambda \in \Lambda$, then it is an (improper) regular sequence on $\bigoplus_\lambda M_\lambda$. Hence, a regular sequence on R is also a regular sequence on every nonzero free R-module.

Let (R, m, K) be local of Krull dimension d. By the Krull height theorem, there exist $x_1, \ldots, x_d \in m$ such that m is a minimal prime of $(x_1, \ldots, x_d)R$, and this is equivalent to the statement that m is the radical of $(x_1, \ldots, x_d)R$ or that $m^N \subseteq (x_1, \ldots, x_d)R$ for $N \gg 0$. The Krull height theorem also implies that there cannot be fewer than d elements generating an ideal whose radical is m, or the Krull dimension of R would be too small. The elements $x_1, \ldots, x_d$ are call a system of parameters for R. Note that in the power series ring $K[[x, y, z]]$, where K is a field, x, y, z is a system of parameters, but there are many much more complicated systems, e.g., $x^{19}, y^{23} + xz^{37}, z^{67} + x^{12}z^5 + y^{11}z^{53}$. A prime containing these must contain x. Looking at the second parameter, it must contain y^{23} and, hence, y. Then, looking at the third parameter, it must contain z^{67} and, hence, z. There are far more complicated examples. Note that for a zero-dimensional local ring, a system of parameters is empty, so that its cardinality is 0.

The following result is very powerful, even when R is a formal power series ring over a field. (We shall see later that a local ring (R, m, K) containing a field is regular iff its m-adic completion is a formal power series ring over a field.)

Theorem. *In a local ring R, if one system of parameters is a regular sequence, then every system of parameters is a regular sequence.*

We will prove this later. This property defines the class of *Cohen-Macaulay local* rings. We shall also see:

Theorem. *Let R be a Noetherian ring. Then R_P is Cohen-Macaulay for every prime P if and only if R_m is Cohen-Macaulay for every maximal ideal m.*

The equivalent properties in the Theorem above define the class of *Cohen-Macaulay* rings R when R is Noetherian but not necessarily local.

To explain further the motivation for studying Cohen-Macaulay rings, we want to focus on the case where $R = \bigoplus_n R_n$ is a finitely generated $\mathbb{N}$-graded algebra over a field $K = R_0$. The nonzero elements of R_n are called *homogeneous of degree n* or n-forms. Note that one has $R_h R_k \subseteq R_{h+k}$. There is a homogeneous version of Noether normalization:

Theorem. *If R is as in the paragraph above and has Krull dimension d, there exist forms of positive degree $F_1, \ldots, F_d \in R$ such that $F_1, \ldots, F_d$ are algebraically independent over K and R is module-finite over $A = K[F_1, \ldots, F_d] \subseteq R$. $F_1, \ldots, F_d$ is called a* homogeneous system of parameters *for R.*

In this situation R is Cohen-Macaulay if and only it is free as an A-module! If K is infinite and R is generated by its 1-forms R_1, then $F_1, \ldots, F_d$ may be taken to 1-forms.

Examples. Let x, y be indeterminates over K. Then $K[x^2, xy, y^2] \subseteq K[x, y]$ is Cohen-Macaulay. The elements x^2, y^2 give a homogeneous system of parameters, and $1,\ xy$ is a free basis over $K[x^2, y^2]$. The ring $R = K[x^4, x^3y, xy^3, y^4]$ is not Cohen-Macaulay: x^4, $y^4]$ is a homogenous system of parameters, but R over $A = K[x^4,^4]$ is not free over are A.

In general, a subring of a polynomial ring that is generated by monomials is Cohen-Macaulay if it is normal. If it is not normal, it may or may not be Cohen-Macaulay. $K[x^2, x^3, y]$ is Cohen-Macaulay but not normal. . Consider the polynomial ring S in rs variables x_{ij} over a field K, where $1 \leq r \leq s$, where $X = \bigl(x_{ij}\bigr)$ is an $r \times s$ matrix. We may also write $S = K[X]$ to indicate that we are adjoining all entries of the matrix X to K. If $I_t(X)$ is the ideal generated by the $t \times t$ minors of X, then $R/I_t(X)$ is Cohen-Macaulay. It is not usually a UFD (think of the case $r = s = t = 2$). The subring of S generated over K by the $r \times r$ minors of X (this is the homogeneous lf ring of a Grassmann variety) is also known to be Cohen-Macaulay

Open question. Let K be a field. Since the question in which we are interested reduces to the case where K is algebraically closed, we assume that K is algebraically closed. Let X, Y be $n \times n$ matrices whose entries are $2n^2$ indeterminates. Let $R = K[X, Y]$, a polynomial ring in $2n^2$ variables. Let $I = I_1(XY - YX)$, which is an ideal generated by n^2 quadratic forms (because the trace of $XY - YX$ is zero, we can omit one of the forms on the main diagonal, and use $n^2 - 1$ generators for the same ideal). The algebraic set defined by I can be thought of as pairs of commuting $n \times n$ matrices. By a theorem of Gerstenhaber and others, this algebraic set is irreducible, i.e., it is a variety. This implies that the radical of I is prime. But it is an open question whether I itself is prime (this is known only for a few small values of n) and the question of whether R/I is Cohen-Macaulay is also open (this is also known only for a few small values of n).

Before proceeding further, we want to discuss multiplicities briefly and then consider their interpretation in the situation of the Theorem just above.

Consider a local ring $(R,\, m,\, K)$ of Krull dimension d and an m-primary ideal I. The condition on I simply means that for some N, $m^N \subseteq I \subseteq m$. The function $\ell(R/I^{n+1})$, where ℓ is length, is called the *Hilbert function* (or *Hilbert-Samuel function* of I, and agrees with a polynomial in n of degree d for all $n \gg 0$. The polynomial is called the *Hilbert(-Samuel) polynomial.* Its leading term will have the form $\frac{e_I}{d!} n^d$ where e_I is a positive integer. The integer e_I is called the *multiplicity* of I. Note, that e_I can be obtained as a limit:

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

The multiplicity of m is called the *multiplicity* of R. Under mild assumptions, a local ring of multiplicity 1 is regular. (One can also study $\ell(M/I^{n+1}M)$ for any finitely generated R-module M. This is gives the Hilbert function and Hilbert polynomial of M: one difference is that in the module case, the degree of the Hilbert polynomial is the dimension of M.)

These multiplicities can be obtained in other ways. Given a sequence of elements $\underline{x} = x_1, \ldots, x_d$ of ring R, and an R-module M, we shall define a homology theory called *Koszul homology*: the Koszul homology modules are denoted $H_i(\underline{x}; M)$. (They vanish if $i < 0$ or if $i > d$.) We won't give the definition at this point, but we do note that $H_0(\underline{x}; M) \cong M/(\underline{x})M$ and $H_d(\underline{x}; M) \cong \mathrm{Ann}_M(\underline{x})R$. Koszul homology has many uses, including the proofs of the fundamental facts about behavior of cohomology of coherent sheaves on projective space. The connection with the multiplicities defined in the preceding paragraph is this. If $x_1, \ldots, x_d$ is a system of parameters for the local ring R, which simply means that $d = \dim(R)$ and $I = (x_1, \ldots, x_d)R$ is m-primary, then the multiplicity of the ideal I is the same as $\sum_{i=0}^{d}(-1)^i \ell\bigl(H_i(\underline{x}; R)\bigr)$, the alternating sum of the lengths of the Koszul homology modules, which do turn out to have finite length in this situation.

We want to discuss these notions in the situation where R is a finitely generated $\mathbb{N}$-graded algebra over a field K with $R_0 = K$ that is generated by forms of degree 1. Such an $\mathbb{N}$-graded algebra over K is called *a standard graded K-algebra*. This terminology is used whether K is a field or not. In the field case, Let m be the homogenous maximal ideal of R, spanned as a vector space over K by all forms of positive degree. The multiplicity of R in this case is defined to multiplicity of R_m.

(Note that if m is any maximal ideal of any ring R, R/m^{n+1} has only one prime ideal, the image of m, which consists of nilpotents. Thus, R/m^{n+1} is already local, and so

$$R/m^{n+1} \cong (R/m^{n+1})_m \cong R_m/m^{n+1}R_m \cong R_m/(mR_m)^{n+1}.$$

Hence, in our standard graded case, the Hilbert function of R is the same as $n \mapsto \ell(R/m^{n+1})$ — one does not need to localize.)

If A is any integral domain with fraction field $\mathcal{F}$ and M is an A-module we define the *torsion-free rank* (or simply *rank*) of M over A to be $\dim_{\mathcal{F}}(\mathcal{F} \otimes_A M)$, which is bounded by the number of generators of M as an A-module.

Let d be the Krull dimension of R. In this situation, one can obtain the multiplicity of R in other ways. Choose a homogeneous system of parameters consisting of linear forms $F_1, \ldots, F_d$. Let $I = (F_1, \ldots, F_d)R$. Let m be the homogenous maximal ideal of R, spanned as a vector space over K by all forms of positive degree. Then R is module-finite over $A = K[F_1, \ldots, F_d]$.

Then the multiplicity of R_m is also:

(1) The torsion-free rank of R over A.

(2) For a dense open subset U of $K^d \cong \mathrm{MaxSpec}\,(A)$, it is the cardinality in $\mathrm{MaxSpec}\,(R)$ of the set-theoretic fiber over each $u \in U$.

(3) The multiplicity of IR_m.

This multiplicity is called the *degree* of the projective scheme associated with R.

Note that R is Cohen-Macaulay if and only if it is free over A, and this is equivalent to the statement that the least number of generators of R as an A-module is equal to its torsion-free rank, i.e., its multiplicity. By the homogeneous form of Nakayama's lemma, which we will soon review, this is the same as the K-vector space dimension of $R/(F_1, \ldots, F_d)R = R/m_AR$, where $m_A = (F_1, \ldots, F_d)A$ is the homogeneous maximal ideal of A. *Thus, R*

is Cohen-Macaulay if and only if its multiplicity is the length of its quotient by a linear homogeneous system of parameters.

Math 615: Lecture of January 10, 2020

One of the auxiliary notions we will utilize is that of an *associated graded* ring or module. We first recall some material about graded rings and modules.

Let H be an additive semigroup with identity 0. A ring R is *graded* by H if it has a direct sum decomposition

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

such that $1 \in R_0$ and for all $h, k \in H$, $R_h R_k \subseteq R_{h+k}$, where

$$R_h R_k = \{rs : r \in R_h,\, s \in R_k\}.$$

It follows that R_0 is a subring of R, and every R_h is an R_0-module. A *grading* of an R-module M is a direct sum decomposition $M = \bigoplus_{h \in H} M_h$ such that for all $h,\, k \in H$,

$$R_h M_k \subseteq M_{h+k},$$

where

$$R_h M_k = \{ru : r \in R_h,\, u \in M_k\}.$$

An element of R_h for any h is called *homogeneous* or a *form.* If it is nonzero, it is said to have *degree* h. The element 0 is homogeneous, but does not have a degree. In dealing with $\mathbb{N}$-gradings, some authors assign 0 the degree -1 or $-\infty$, but this is not so natural when H is an arbitary semigroup. We leave the degree of 0 undefined. In dealing with $\mathbb{N}$-gradings, the degree of a possibly inhomogeneous element is defined to be the largest degree of a nonzero homogeneous component of the element. If $n \in \mathbb{N}$, the phrase "elements of degree $\leq n$" is then understood to include the 0 element.

When an element $u \in M$ (or R) is written in the form

$$u_{h_1} \oplus \cdots \oplus u_{h_n},$$

with the h_i distinct elements of H, the u_{h_i} are called the *homogeneous components* of u. Those not shown explicitly are 0. Every nonzero element of M or R has a unique (except for the order of the terms) expression as a sum of nonzero homogeneous components of distinct degrees.

We are mainly interested in the case where $H = \mathbb{N}$, but the cases where $H = \mathbb{Z}$, $\mathbb{N}^d$ and $\mathbb{Z}^d$ arise with reasonable frequency. When $H = \mathbb{N}^d$ or $\mathbb{Z}^d$ the term *multidegree* is sometimes used instead of degree. When $n = 2$, the term *bidegree* is sometimes used.

A submodule N of a graded module M is called *homogeneous* or *graded* if whenever $u \in N$, all homogeneous components of u are in N. An equivalent condition is that N be generated by forms. A third equivalent condition is that

$$N = \bigoplus_{h \in H} N \cap M_h,$$

and so a graded submodule inherits a grading from M. In particular, we may refer to *homogeneous* ideals of R. Arbitrary sums and intersections of graded submodules are graded, and the operations may be performed componentwise. If M is a graded module and N a graded submodule there is an obvious way of grading the quotient:

$$M/N = \bigoplus_{h \in H} M_h/N_h.$$

When M is H-graded and $S \in H$ we write $M(s)$ for the graded module with the same R-module structure as M, but with $M(h)_s = M_{h+s}$. Thus, we have simply shifted the grading.

If $H \subseteq H'$ is an additive subsemigroup, a graded ring or module over H may also be coonsidered a graded module over H', by defining the components for subscripts in $H' - H$ to be zero.

Note that $\mathbb{Z}^n$ has a total order that is compatible with addition (i.e., if $u \leq v$ then for all w, $u + w \leq v + w$. E.g., one can define $(a_1, \ldots, a_n) < (b_1, \ldots, b_n)$ if for the least j with $a)_j \neq b_j$, one has $a_j < b_j$.

Theorem. *Let M be a Noetherian graded module over a Noetherian graded ring R, where the grading is by $\mathbb{N}$ or $\mathbb{Z}$ or any additive semigroup with a total order compatible with addition, such as $\mathbb{N}^n$ or $\mathbb{Z}^n$. Then every associated prime P of M is a homogeneous ideal.*

Proof. If P is an associated prime of M it is the annihilator of a nonzero element

$$u = u_{j_1} + \cdots + u_{j_t} \in M,$$

where the u_{j_ν} are nonzero homogeneous elements of degrees $j_1 < \cdots < j_t$. Choose u such that t is as small as possible. Suppose that

$$r = r_{i_1} + \cdots + r_{i_s}$$

kills u, where for every ν, r_{i_ν} has degree i_ν, and $i_1 < \cdots < i_t$. We shall show that every r_{i_ν} kills u, which proves that P is homogeneous. If not, we may subtract off all the r_{i_ν} that do kill u: the resulting element still kills u. Therefore, to get a contradiction, it suffices to show that r_{i_1} kills u. Since $ru = 0$, the unique least degree term $r_{i_1} u_{j_1} = 0$. Therefore

$$u' = r_{i_1} u = r_{i_1} u_{j_2} + \cdots + r_{i_1} u_{j_t}.$$

If this element is nonzero, its annihilator is still P, since $Ru \cong R/P$ and every nonzero element has annihilator P. Since $r_{i_1} u_{j_\nu}$ is homogeneous of degree $i_1 + j_\nu$, or else is 0, u' has fewer nonzero homogeneous components than u does, contradicting our choice of u. □

Corollary. *If I is a homogeneous ideal of a Noetherian ring R graded by $\mathbb{N}^n$ or $\mathbb{Z}^n$, every minimal prime of I is homogeneous.*

Proof. This is immediate, since the minimal primes of I are among the associated primes of R/I. □

Without any finiteness assumptions we have:

Proposition. *If R is graded by $\mathbb{N}^n$ or $\mathbb{Z}^n$ and I is a homogeneous ideal, then* $\mathrm{Rad}\,(I)$ *is homogeneous.*

Proof. Let

$$f_{i_1} + \cdots + f_{i_k} \in \mathrm{Rad}\,(I)$$

with $i_1 < \cdots < i_k$ and each f_{i_j} nonzero of degree i_j. We need to show that every $f_{i_j} \in \mathrm{Rad}\,(I)$. If any of the components are in $\mathrm{Rad}\,(I)$, we may subtract them off, giving a similar sum whose terms are the homogeneous components not in $\mathrm{Rad}\,(I)$. Therefore, it will suffice to show that $f_{i_1} \in \mathrm{Rad}\,(I)$. But

$$(f_{i_1} + \cdots + f_{i_k})^N \in I$$

for some $N > 0$. When we expand, there is a unique term formally of least degree, namely $f_{i_1}^N$, and therefore this term is in I, since I is homogeneous. But this means that $f_{i_1} \in \mathrm{Rad}\,(I)$, as required. □

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

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

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

and so equality holds throughout, as required. □

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

Proof. We have that the set H of homogeneous elements of I is contained in $\bigcup_{i=1}^k P_k$. If $k = 1$ we can conclude that $I \subseteq P_1$. We use induction on k. Without loss of generality, we may assume that H is not contained in the union of any $k-1$ if the P_j. Hence, for every i there is a 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. □

We also note:

Proposition (vector space avoidance). *Let K be an infinite field, W a vector space over K, and let V, $W_1, \ldots, W_n$, be subspaces of W. If $V \subseteq \bigcup_i W_i$, then for some i, $V \subseteq W_i$.*

Proof. If one has a counterexample with n as small as possible (we must have $n \geq 2$) for each i choose a vector $v_i \in V$ not in W_i. Then we still have a counter-example if we replace V by by the span of the v_i over K, and W_i by $W_i \cap V$. Thus, we may assume that V is finite-dimensional and $V = \bigcup_i W_i$ where each W_i is a proper subspace of V. Let L_i be a linear form the vanishes identically on W_j. Then the product of the L_j is a nonzero polynomial that vanishes identically on K^n. Since K is infinite, this is a contradiction. □

Before proving the next theorem on homogeneous systems of parameters, we want to review Nakayama's lemma.

Review of 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).

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

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

Moreover, we have:

Theorem. *Let R be a finitely generated $\mathbb{N}$-graded K-algebra with $R_0 = K$ such that* $\dim(R) = d$. *A homogeneous system of parameters $F_1, \ldots, F_d$ for R always exists. If K is infinite and R is standard, i.e., $R = K[R_1]$, then the F_i may be chosen to be linear forms. Moreover, if $F_1, \ldots, F_d$ is a sequence of homogeneous elements of positive degree, then the following statements are equivalent.*

(1) *$F_1, \ldots, F_d$ is a homogeneous system of parameters, i.e.* $\dim\big(R/(F_1, \ldots, F_d)\big) = 0$.

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

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

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

(5) *The images of $F_1, \ldots, F_d$ in R_m form a system of parameters.*

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

Proof. We first show existence. By homogeneous prime avoidance, there is a form F_1 that is not in the union of the minimal primes of R. (In the standard case, when K is infinite, use vector space avoidance with $V = R_1$ instead of prime avoidance.) Then $\dim(R/F_1) \leq 1\dim(R) - 1$. For the inductive step, choose forms of positive degree $F_2, \ldots, F_h$, $h \leq d-1$, whose images in R/F_1R are a homogeneous system of parameters for R/F_1R (and take them linear in the standard case with K infinite). Then m is nilpotent mod $F_1, \ldots, F_h$ with $h \leq d$. But h must equal d, or the height of m will not be d. □

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

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

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

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

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

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

(1) ⇔ (5). Since $R/(F_1, \ldots, F_d)$ is graded, it has the same dimension as its localization at m, which may be identified with $R_m/(F_1, \ldots, F_d)R_m$, and one has dimension 0 iff the other does.

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

Sometimes we shall use the notation $[M]_n$ for the nth graded component of the graded module M, particularly in contexts where there is also a filtration, for in that case $\{M_n\}_n$ will frequently be used to denote an infinite descending sequence of submodules of M.

Let M be an R-module and $I \subseteq R$ an ideal. The *I-adic filtration* on R is the infinite descending sequence of ideals $\{I^n\}_n$, i.e.,

$$R \supseteq I \supseteq I^2 \supseteq \cdots \supseteq I^n \supseteq \cdots .$$

Similarly, the *I-adic filtration* on the R-module M is the sequence $\{I^nM\}_n$. An infinite descending filtration

$$(*) \qquad M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots \supseteq M_n \supseteq \cdots$$

is called *I-stable* if $IM_n \subseteq M_{n+1}$ for all n and $IM_n = M_{n+1}$ for all sufficiently large integers n. The terminology *I-good* (*I-bon* by French authors) is also used. Note that this implies that there is a constant positive integer c such that $M_{n+c} = I^nM_c$ for all $n \in \mathbb{N}$.

Given a filtration $(*)$ of M and a submodule N, N acquires a filtration using the submodules $M_n \cap N = N_n$, called the *inherited filtration.*

We recall the following result due to E. Artin and D. Rees.

Theorem (Artin-Rees Lemma). *Let $N \subseteq M$ be Noetherian modules over the Noetherian ring R and let I be an ideal of R. Then there is a constant positive integer c such that for all $n \geq c$, $I^nM \cap N = I^{n-c}(I^cM \cap N)$. That is, eventually, each of the modules $N_{n+1} = I^{n+1}M \cap N$ is I times its predecessor, $N_n = I^nM \cap N$.*

In particular, there is a constant c such that $I^nM \cap N \subseteq I^{n-c}N$ for all $n \geq c$. In consequence, if a sequence of elements in N is an I-adic Cauchy sequence in M (respectively, converges to 0 in M) then it is an I-adic Cauchy sequence in N (respectively, converges to 0 in N).

Proof. We consider the module $R[t] \otimes M$, which we think of as $M[t]$. Within this module,

$$\mathcal{M} = M + IMt + I^2Mt^2 + \cdots + I^kMt^k + \cdots$$

is a finitely generated $R[It]$-module, generated by generators for M as an R-module: this is straightforward. Therefore, $\mathcal{M}$ is Noetherian over $R[It]$. But

$$\mathcal{N} = N + (IM \cap N)t + (I^2M \cap N)t^2 + \cdots ,$$

which may also be described as $N[t] \cap \mathcal{M}$, is an $R[It]$ submodule of $\mathcal{M}$, and so finitely generated over $R[It]$. Therefore for some $c \in \mathbb{N}$ we can choose a finite set of generators whose degrees in t are all at most c. By breaking the generators into summands homogeneous with respect to t, we see that we may use elements from

$$N, (IM \cap N)t, (I^2M \cap N)t^2, \dots , (I^cM \cap N)t^c$$

as generators. Now suppose that $n \geq c$ and that $u \in I^nM \cap N$. Then ut^n can be written as an $R[It]$-linear combination of of elements from

$$N, (IM \cap N)t, (I^2M \cap N)t^2, \dots , (I^cM \cap N)t^c,$$

and hence as an sum of terms of the form

$$i_h t^h v_j t^j = (i_h v_j)t^{h+j}$$

where $j \leq c$, $i_h \in I^h$, and

$$v_j \in I^jM \cap N.$$

Of course, one only needs to use those terms such that $h + j = n$. This shows that $(I^nM) \cap N$ is the sum of the modules

$$I^{n-j}(I^jM \cap N)$$

for $j \leq c$. But

$$I^{n-j}(I^jM \cap N) = I^{n-c}I^{c-j}(I^jM \cap N),$$

and

$$I^{c-j}(I^jM \cap N) \subseteq I^cM \cap N,$$

so that we only need the single term $I^{n-c}(I^cM \cap N)$. □

The Artin-Rees Lemma asserts precisely that if M is a finitely generated module over a Noetherian ring R and $N \subseteq M$ is a submodule, the filtration on N inherited from the I-adic filtration on M is I-stable. One can generalize this slightly as follows:

Theorem (Artin-Rees Lemma, second version). *Let $N \subseteq M$ be finitely generated modules over the Noetherian ring R, let I be an ideal of R, let $\{M_n\}_n$ be an I-stable filtration of M, and let $\{N_n\}_n$ be the inherited filtration on N. Then $\{N_n\}_n$ is also I-stable.*

Proof. First, $IN_n \subseteq IM_n \cap N \subseteq M_{n+1} \cap N = N_{n+1}$. Choose c such that $M_{n+c} = I^n M_c$ for all c. Then

$$N_{n+c} = I^n M_c \cap N = I^n M_c \cap N_c,$$

since $N_c \supseteq N_{n+c}$, and, by the usual Artin-Rees Lemma applied to $N_c \subseteq M_c$, this is

$$I(I^{n-1} M_c \cap N_c) = IN_{n+c-1}$$

for all sufficiently large n. $\square$

We recall that an $\mathbb{N}$-graded ring R is Noetherian iff R_0 is Noetherian and R is finitely generated over R_0. In fact:

Proposition. *Let R be a ring graded by $\mathbb{N}$. The following conditions are equivalent:*

(a) R is a Noetherian ring.

(b) R_0 is Noetherian ring and J is a finitely generated ideal.

(c) R_0 is a Noetherian ring and R is finitely generated as an R_0-algebra, and the generators may be taken to be homogeneous.

Proof. (c) $\Rightarrow$ (b) is obvious from the Hilbert basis theorem, and (a) $\Rightarrow$ (b) follows because $R_0 = R/J$ (or because R_0 is a direct summand of R) and J is finitely generated since R is Noetherian. Now suppose that J is finitely generated. Each generator is a sum of homogeneous elements of positive degree, and so it follows that J is finitely generated by homogeneous elements of positive degree, say $f_1, \ldots, f_n$. If $R \neq R_0[f_1, \ldots, f_n]$, there is a homogeneous element g of R of least degree not in $R_0[f_1, \ldots, f_n]$. Then $g \notin R_0$ and so g has positive degree, and is in J. Then we can write $g = \sum_{i=1}^n h_i f_i$, where $h_i \in R$. Each h_i is a sum of homogeneous components: let h_i' be the component of h_i of degree $\deg(g) - \deg(f_i)$. Then we also have $g = \sum_i h_i' f_i$, where $\deg(h_i') < \deg g$, and so every $h_i' \in R_0[f_1, \ldots, f_n]$. The result follows. $\square$

Thus, if R is a Noetherian $\mathbb{N}$-graded ring we may write R as the homomorphic image of $R_0[x_1, \ldots, x_n]$ for some n, where the polynomial ring is graded so that x_i has degree $d_i > 0$. In this situation R_t is the R_0-free module on the monomials $x_1^{a_1} \cdots x_n^{a_n}$ such that $\sum_{i=1}^n a_i d_i = t$. Since all the a_i are at most t, there are only finitely many such monomials, so that every R_t is a finitely generated R_0-module. Thus, since a Noetherian $\mathbb{N}$-graded ring R is a homomorphic image of such a graded polynomial ring, all homogeneous components

R_t of such a ring R are finitely generated R_0-modules. Moreover, given a finitely generated graded module M over R with homogeneous generators $u_1, \ldots, u_s$ of degrees $d_1, \ldots, d_s$,

$$M_n = \sum_{j=1}^{s} R_{n-d_j} u_j,$$

and since every R_{n-d_j} is a finitely generated R_0-module, every M_n is a finitely generated R_0-module.

The polynomial ring $R_0[x_1, \ldots, x_n]$ also has an $\mathbb{N}^n$-grading: if we let $h = (h_1, \ldots, h_n) \in \mathbb{N}^h$, then

$$[R]_h = R_0 x_1^{a_1} \cdots x_n^{a_n}$$

where $a_i d_i = h_i$, $1 \leq i \leq n$, or 0 if for some i, d_i does not divide h_i. The usual $\mathbb{N}$-grading on a polynomial ring is obtained when all the d_i are specified to be 1.

An $\mathbb{N}$-graded Noetherian A-algebra R is called *standard* if $A = R_0$ and it is generated over R_0 by R_1, in which case it is a homomorphic image of some $A[x_1, \ldots, x_n]$ with the usual grading. The kernel of the surjection $A[x_1, \ldots, x_n] \twoheadrightarrow R$ is a homogeneous ideal.

The *associated graded ring* of R with respect to I, denoted $\mathrm{gr}_I R$, is the $\mathbb{N}$-graded ring such that

$$[\mathrm{gr}_I(R)]_n = I^n/I^{n+1},$$

with multiplication defined by the rule $[i_h][i_k] = [i_h i_k]$, where $i_h \in I^h$, $i_k \in I^k$, and $[i_h]$, $[i_k]$, and $[i_h i_k]$ represent elements of I^h/I^{h+1}, I^k/I^{k+1}, and I^{h+k}/I^{h+k+1}, respectively. It is easy to see that if one alters i_h by adding an element of I^{h+1}, the class of $i_h i_k$ mod I^{h+k+1} does not change since $i_h i_k$ is altered by adding an element of I^{h+k+1}. The same remark applies if one changes i_k by adding an element of I_{k+1}. It follows that multiplication on these classes is well-defined, and it extends to the whole ring by forcing the distributive law. This ring is generated over R/I by the classes $[i] \in I/I^2$, $i \in I$, and if $i_1, \ldots, i_s$ generate I then $[i_1], \ldots, [i_s]$, thought of in I/I^2, generate $\mathrm{gr}_I R$ over R/I. Thus, $\mathrm{gr}_I R$ is a standard graded R/I-algebra, finitely generated as an R/I-algebra whenever I is finitely generated as an ideal of R. In particular, if R is a Noetherian ring, $\mathrm{gr}_I R$ is a standard Noetherian (R/I)-algebra for every ideal I.

The associated graded ring can also be obtained from the *second Rees ring*, which is defined as $R[It, 1/t] \subseteq R[t, 1/t]$. More explicitly,

$$R[It, 1/t] = \cdots + R\frac{1}{t^2} + R\frac{1}{t} + R + It + I^2t^2 + \cdots .$$

This ring is a $\mathbb{Z}$-graded R-algebra. Let $v = 1/t$. Notice that v is not a unit in $S = R[It, 1/t]$ (unless $I = R$). In fact S/vS is $\mathbb{Z}$-graded: the negative graded components vanish, and the nth nonnegative graded component is $I^n t^n / I^{n+1} t^n \cong I^n/I^{n+1}$, since $I^{n+1}t^{n+1}v = I^{n+1}t^n$. Thus, S/vS may also be thought of as $\mathbb{N}$-graded, and, in fact, $R[It, v]/(v) \cong \mathrm{gr}_I R$.

Suppose that R contains a field of K. One may think of $R[It,\, v]$ as giving rise to a family of rings parametrized by K, obtained by killing $v - \lambda$ as λ varies in K. For values of $\lambda \neq 0$, the quotient ring is R, while for $\lambda = 0$, the quotient is $\mathrm{gr}_I R$.

If $\{M_n\}_n$ is an I-stable filtration of an R-module M, then there is an *associated graded module* $\bigoplus_n M_n/M_{n+1}$, which is easily checked to be a $\mathrm{gr}_I R$-module with multiplication determined by the rule $[i_h][m_k] = [i_h m_k]$ for $i_h \in I^h R$ and $m_k \in M_k$, where $[i_h]$, $[m_k]$, and $[i_h m_k]$ are interpreted in I^h/I^{h+1}, M_k/M_{k+1}, and M_{h+k}/M_{h+k+1}, respectively. If $M_{n+c} = I^n M_c$ for $n \in \mathbb{N}$, then this associated graded module is generated by its graded components with indices $\leq c$, namely M/M_1, M_1/M_2, $\ldots$, M_c/M_{c+1}. Thus, if R and M are Noetherian it is a finitely generated $\mathbb{N}$-graded $\mathrm{gr}_I(R)$-module, and is Noetherian. If the filtration is the I-adic filtration, one writes $\mathrm{gr}_I M$ for the associated graded module.

When we refer to a *graded ring* without specifying H, it is understood that $H = \mathbb{N}$. However, when we refer to a graded module M over a graded ring R, our convention is that M is $\mathbb{Z}$-graded. If M is finitely generated, it will have finitely many homogeneous generators: if the least degree among these is $a \in \mathbb{Z}$, then all homogeneous elements of M have degree $\geq a$, so that the nth graded component M_n of M will be nonzero for only finitely many negative values of n. When M is $\mathbb{Z}$-graded it is convenient to have a notation for the same module with its grading shifted. We write $M(t)$ for M graded so that $M(t)_n = M_{t+n}$. For example, $R(t)$ is a free R-module with a homogeneous free generator in degree $-t$: note that $R(t)_{-t} = R_0$ and so contains $1 \in R$.

Let M be a finitely generated graded module over a graded algebra R over $R_0 = A$ where A is an Artin local ring. We define the *Hilbert function* $\mathrm{Hilb}_M(n)$ of M by the rule $\mathrm{Hilb}_M(n) = \ell_A(M_n)$ for all $n \in \mathbb{Z}$, and we define the *Poincaré series* $P_M(t)$ of M by the formula $P_M(t) = \sum_{n=-\infty}^{\infty} \mathrm{Hilb}_M(n)t^n \in \mathbb{Z}[[t]]$. Note that $\ell(M_n)$ is finite for all $n \in \mathbb{Z}$, because each M_n is finitely generated as an A-module, by the discussion of the first paragraph. If A has a coefficient field, lengths over A are the same as vector space dimensions over its coefficient field. Technically, it is necessary to specify A in describing length. For example, $\ell_{\mathbb{C}}(\mathbb{C}) = 1$, while $\ell_{\mathbb{R}}(\mathbb{C}) = 2$. However, it is usually clear from context over which ring lengths are being taken, and then the ring is omitted from the notation.

Note that $Z[t] \subseteq Z[[t]]$, and that elements of the set of polynomials W with constant ± 1 are invertible. We view $W^{-1}Z[t] \subseteq Z[[t]]$, and so it makes sense to say that a power series in $\mathbb{Z}[[t]]$ is in $W^{-1}\mathbb{Z}[t]$.

Example. Suppose that $R = K[x_1, \ldots , x_d]$ the standard graded polynomial ring. Here, $A = K$ and length over K is the same as vector space dimension. The length of the vector space R_n is the same as the number of monomials $x_1^{k_1} \cdots x_d^{k_d}$ of degree n in the variables $x_1, \ldots , x_d$, since these form a K-vector space basis for R_n. This is the same as the number of d-tuples of nonnegative integers whose sum is n. We can count these as follows: form a string of k_1 dots, then a slash, then a string of k_2 dots, then another slash, and so forth, finishing with a string of k_d dots. For example, $x_1^3 x_2^2 x_4^5$ would correspond to

$$\cdot\cdot\cdot/\cdot\cdot//\cdot\cdot\cdot\cdot\cdot$$

The result is a string of dots and slashes in which the total number of dots is $k_1+\cdots+k_d = n$ and the number of slashes is $d-1$. There is a bijection between such strings and the monomials that we want to count. The string has total length $k+d-1$, and is determined by the choice of the $d-1$ spots where the slashes go. Therefore, the number of monomials is $\binom{n+d-1}{d-1}$. The Hilbert function of the polynomial ring is given by the rule $\mathrm{Hilb}_R(n) = 0$ if $n < 0$ and

$$\mathrm{Hilb}_R(n) = \binom{n+d-1}{d-1}$$

if $n \geq 0$. Note that, in this case, the Hilbert function agrees with a polynomial in n of degree $d-1 = \dim(R) - 1$ for all $n \gg 0$. This gives one formula for the Poincaré series, namely

$$\sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

We give a different way of obtaining the Poincaré series. Consider the formal power series in $Z[[x_1, \dots, x_d]]$ which is the sum of all monomials in the x_i:

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1x_2 + \cdots + x_d^2 + \cdots$$

This makes sense because there are only finitely many monomials of any given degree. It is easy to check that this power series is the product of the series

$$1 + x_j + x_j^2 + \cdots + x_j^n + \cdots$$

as j varies from 1 to d: in distributing terms of the product in all possible ways, one gets every monomial in the x_j exactly once. This leads to the formula

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1x_2 + \cdots + x_d^2 + \cdots = \prod_{j=1}^{d} \frac{1}{1-x_j}.$$

There is a unique continuous homomorphism $\mathbb{Z}[[x_1, \dots, x_d]] \to \mathbb{Z}[[t]]$ that sends $x_j \to t$ for all j. Each monomial of degree n in the x_j maps to t^n. It follows that the formal power series

$$1 + x_1 + \cdots + x_d + x_1^2 + x_1x_2 + \cdots + x_d^2 + \cdots$$

maps to $P_R(t)$, but evidently it also maps to $1/(1-t)^d$. This calculation of the Poincaré series yields the identity:

$$\frac{1}{(1-t)^d} = \sum_{n=0}^{\infty} \binom{n+d-1}{d-1} t^n.$$

Theorem. *Let R be a finitely generated graded A-algebra with $R_0 = A$, an Artin ring, and suppose that the generators $f_1, \dots, f_d$ have positive degrees $k_1, \dots, k_d$, respectively. Let M be a finitely generated $\mathbb{N}$-graded R-module. Then $P_M(t)$ can be written as the ratio of polynomials in $\mathbb{Z}[t]$ with denominator*

$$(1-t^{k_1})\cdots(1-t^{k_d}).$$

If M is finitely generated and $\mathbb{Z}$-graded, one has the same result, but the numerator is a Laurent polynomial in $\mathbb{Z}[t, t^{-1}]$.

Proof. If the set of generators is empty, M is a finitely generated A-module and has only finitely many nonzero components. The Poincaré series is clearly a polynomial (respectively, a Laurent polynomial) in t. We use induction on d. We have an exact sequence of graded modules:

$$0 \to \mathrm{Ann}_M f_d \to M \xrightarrow{f_d} M \to M/f_dM \to 0.$$

In each degree, the alternating sum of the lengths is 0. This proves that

$$P_M(t) - t^{d_k} P_M(t) = P_{M/f_dM}(t) - P_{\mathrm{Ann}_M f_d}(t).$$

Since multiplication by f_d is 0 on both modules on the right, each may be thought of as a finitely generated $\mathbb{N}$- (respectively, $\mathbb{Z}$-) graded module over $A[f_1, \dots, f_{d-1}]$, which shows, using the induction hypothesis, that $(1-t^{k_d})P_M(t)$ can be written as a polynomial (respectively, Laurent polynomial) in t divided by

$$(1-t^{k_1})\cdots(1-t^{k_{d-1}}).$$

Dividing both sides by $1 - t^{k_d}$ yields the required result. □

Math 615: Lecture of January 13, 2020

Remark. Base change over a field K to a field L does not change the Krull dimension of a finitely generated K-algebra, nor of a finitely generated module over such an algebra. A finitely generated K-algebra R is a module-finite extension of a polynomial ring $K[x_1, \dots, x_d] \hookrightarrow R$, where $d = \dim(R)$. Then $L[x_1, \dots, x_d] \cong L \otimes_K K[x_1, \dots, x_d] \hookrightarrow L \otimes_K R$, ($L$ is free and therefore flat over K), and if $r_1, \dots, r_s$ span R over $K[x_1, \dots, x_d]$, then $1 \otimes r_1, \dots, 1 \otimes r_s$ span $L \otimes R$ over $L[x_1, \dots, x_d]$.

Evidently, for graded K-algebras R with $R_0 = K$ and graded K-modules M,

$$L \otimes R = \bigoplus_n L \otimes_K R_n$$

and

$$L \otimes_K M = \bigoplus_n L \otimes_K M_n$$

are graded, and their Hilbert functions do not change.

Proposition. *If R is finitely generated and graded over $R_0 = A$, Artin local, and $f \in R$ is homogeneous of degree $k > 0$, then if f is a not a zerodivisor on M, a finitely generated graded R-module, then $P_M(t) = \frac{1}{1-t^k} P_{M/fM}$.*

Proof. This is immediate from the exact sequence

$$0 \to M(-k) \xrightarrow{f} M \to M/fM \to 0$$

of graded modules and degree preserving maps: one has

$$P_M(t) - t^k P_M(t) = P_{M/fM}(t).$$

□

By induction on the number of indeterminates, this gives at once:

Proposition. *Let A be Artin local and $x_1, \ldots, x_d$ indeterminates over A whose respective degrees are $k_1, \ldots, k_d$. Let $R = A[[x_1, \ldots, x_d]]$. Then*

$$P_R(t) = \frac{\ell(A)}{\prod_{i=1}^d (1 - t^{k_i})}.$$

□

We note the following facts about integer valued functions on $\mathbb{Z}$ that are eventually polynomial. It will be convenient to assume that functions are defined for all integers even though we are only interested in their values for large integers. We write $f \sim g$ to mean that $f(n) = g(n)$ for all $n \gg 0$.

If f is a function on $\mathbb{Z}$ we define $\Delta(f)$ by the rule

$$\Delta(f)(n) = f(n) - f(n-1)$$

for all n. We define $\Sigma(f)$ by the rule $\Sigma(f)(n) = 0$ if $n < 0$ and

$$\Sigma(f)(n) = \sum_{j=0}^{n} f(j)$$

if $n \geq 0$. Suppose that $d \in \mathbb{N}$. We shall assume that $\binom{n}{d}$, is 0 if n is negative or if $d > n$. It is a polynomial in n of degree d if $n \geq 0$, namely

$$\frac{1}{d!} n(n-1) \cdots (n-d+1).$$

It is obvious that if $f \sim g$ then $\Delta(f) \sim \Delta(g)$, that $\Sigma(f) - \Sigma(g)$ is eventually constant, that $\Delta\Sigma(f) \sim f$, and that $\Sigma\Delta(f) - f$ is equivalent to a constant function. When $f \sim g$ is a nonzero polynomial we refer to the *degree* and *leading coefficient* of f, meaning the degree and leading coefficient of g.

Lemma. *A function f from $\mathbb{Z}$ to $\mathbb{Z}$ that agrees with a polynomial in n for all sufficiently large n is equivalent to a $\mathbb{Z}$-linear combination of the functions $\binom{n}{d}$, and any such $\mathbb{Z}$-linear function has this property. Hence, a polynomial g that agrees with f has, at worst, coefficients in $\mathbb{Q}$, and the leading coefficient has the form $e/d!$, where $e \in \mathbb{Z}$ and $d = \deg(g)$.*

If $f : \mathbb{Z} \to \mathbb{Z}$ then $\Delta(f)$ agrees with a polynomial of degree $d-1$, $d \geq 1$, if and only if f agrees with a polynomial of degree d, and the leading coefficient of $\Delta(f)$ is d times the leading coefficient of f. $\Delta(f) \sim 0$ iff $f \sim c$, where c is a constant integer. For $d \geq 0$, $\Sigma(f)$ $\sim$ a polynomial of degree $d+1$ iff $f \sim$ a polynomial of degree d (nonzero if $d = 0$), and the leading coefficient of $\Sigma(f)$ is the leading coefficient of f divided by $d+1$.

Proof. Every polynomial in n is uniquely a linear combination of the functions $\binom{n}{d}$, since there is exactly one of the latter for every degree $d = 0, 1, 2, \ldots$. Note that $\Delta\binom{n}{d} = \binom{n}{d} - \binom{n-1}{d} = \binom{n}{d-1}$ for all $n \gg 0$, from which the statement about that $\Delta(f)$ is polynomial when f is follows, as well as the statement relating the leading coefficients. Also, if f is eventually polynomial of degree d, then we may apply the Δ operator d times to obtain a nonzero constant function $\Delta^d f$, whose leading coefficient is $d!a$, where a is the leading coefficient of the polynomial that agrees with f, and this is an integer for large n, whence it is an integer. It follows that the leading coefficient of f has the form $e/d!$ for some $e \in \mathbb{Z} - \{0\}$. We may therefore subtract $e\binom{n}{d}$ from f to obtain a $\mathbb{Z}$-valued function that is polynomial of smaller degree than f for large n. We may continue in this way. Thus, the polynomial that agrees with f is a $\mathbb{Z}$-linear combination of the polynomials that agree with the $\binom{n}{d}$. Note also that $\Sigma\binom{n}{d} = \binom{0}{d} + \cdots + \binom{n}{d} = \binom{d}{d} + \cdots + \binom{n}{d}$ for $n \geq d$ and 0 otherwise. The value of the sum shown, when $n \geq d$, is $\binom{n+1}{d+1}$, by a straightforward induction on n. Finally, f is equivalent to a polynomial when Δf is, since $\Sigma\Delta(f) - f$ is equivalent to a constant. □

Theorem. *Let R be a standard graded A-algebra, where (A, μ, K) is Artin local, and let M be a finitely generated graded R-module. Then the Hilbert function* $\mathrm{Hilb}_M(n)$ *of the finitely generated graded module M is eventually a polynomial in n of degree* $\dim(M) - 1$ *with a positive leading coefficient, except when M has dimension 0, in which case the Hilbert function is eventually identically 0.*

Proof. The Poincaré series can be written in the form $t^k Q(1-t)/(1-t)^d$ for some $k \leq 0$: we can write a polynomial in t as a polynomial in $1-t$ instead. This is a sum of finitely many terms of the form $mt^k/(1-t)^s$. We have already seen that the coefficient on t^n in $1/(1-t)^s$ is eventually given by a polynomial in n of degree $s-1$, and multiplying by t^k has the effect of substituting $n-k$ for n in the Hilbert function. A linear combination of polynomials is still a polynomial. It remains to prove the assertion about dimensions.

Since A is Artin, we know that $\mu^s = 0$ for some positive integer s. Then M has a filtration

$$M \supseteq \mu M \supseteq \mu^2 M \supseteq \cdots \supseteq \mu^{s-1} M \supseteq \mu^S M = 0,$$

and each of the $\mu^j M$ is a graded submodule. It follows that the Hilbert function of M is the sum of the Hilbert functions of the modules $\mu^j M/\mu^{j+1} M$. Since the dimension of M

is the supremum of the dimensions of the factors, it suffices to prove the result for each $\mu^j M/\mu^{j+1}M$, which is a module over the standard graded K-algebra $R/\mu R$. We have therefore reduced to the case where $A = K$ is a field.

We may apply $L \otimes_K \_$ for some infinite field L, and so we may assume without loss of generality that K is infinite. We use induction on $d = \dim(M)$. Let m be the homogeneous maximal ideal of R, which is generated by 1-forms. If M is 0-dimensional, this is the only associated prime of M, and M has a finite filtration with factors $\cong K$ and is killed by a power of m. Thus, M is a finite-dimensional K-vector space, and M_n is 0 for all $n \gg 0$. Now assume that M has positive dimension. Let

$$N = \bigcup_t \mathrm{Ann}_M m^t.$$

The modules $\mathrm{Ann}_M m^t$ form an ascending chain, so this is the same as $\mathrm{Ann}_M m^t$ for any $t \gg 0$ and is a graded submodule of M of finite length. The Hilbert function of M is the sum of the Hilbert functions of M/N and N, and the latter is eventually 0. Therefore we may study M/N instead of N. In M/N no nonzero element is killed by a power of m (or else its representative in M is multiplied into N by a power of m — but then it would be killed by a power of m, and so it would be in N). Replace M by M/N. Then no element of $M - \{0\}$ is killed by m, and so $m \notin \mathrm{Ass}\, M$. This means that the associated primes of M cannot cover R_1, which generates m, for then one of them would contain R_1. Thus, we can choose a degree one element f in R_1 that is not a zerodivisor on M. Then $\dim(M/fM) = \dim(M) - 1$, and so $P(n) = \mathrm{Hilb}_{M/fM}(m)$ is eventually a polynomial in n of degree $d-2$ if $d \geq 2$; if $d = 1$, it is constantly 0 for $n \gg 0$. Let $Q(n) = \mathrm{Hilb}_M(n)$. Since $Q(n) - Q(n-1) = P(n)$, Q is a polynomial of degree $d-1$, (if $d = 1$, we can conclude that Q is constant). Since $Q(n)$ is positive for $n \gg 0$, the leading coefficient is positive for all $d \geq 1$. □

Remark. The trick of enlarging the field avoids the need to prove a lemma on homogeneous prime avoidance.

Let (R, m, K) be a local ring, and let M be a finitely generated R-module with m-stable filtration $\mathcal{M} = \{M_n\}_n$. We write $\mathrm{gr}_{\mathcal{M}}(M)$ for the associated graded module $\bigoplus_{n=0}^{\infty} M_n/M_{n+1}$, which is a finitely generated $\mathrm{gr}_I R$-module, and we write $\mathrm{gr}_I M$ in case $\mathcal{M}$ is the I-adic filtration. In this situation we define $H_R(n) = \ell(R/m^{n+1})$, and call this the *Hilbert function of* R, and we write $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$, the *Hilbert function* of M with respect to the m-stable filtration $\mathcal{M}$. In case $\mathcal{M}$ is the m-adic filtration on M, we write $H_M(n)$ for $\ell(M/m^{n+1}M)$.

Our next objective is the following result:

Theorem. *Let (R, m, K) be local and let M be a nonzero R-module of Krull dimension d. Then for any m-stable filtration $\mathcal{M}$ of M, $H_{\mathcal{M}}(n)$ is eventually a polynomial in n of degree d.*

First note that $\mathrm{gr}_c MM = \bigoplus_n M_n/M_{n+1}$, then for all n, $H_{\mathcal{M}}(n) = \ell(M/M_{n+1}) = \sum_{i=0}^{n} \ell(M_i/M_{i+1})$ since M/M_{n+1} has a filtration with the M_i/M_{i+1} as factors, $0 \leq i \leq n$. This says that $\Sigma\,\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}} = H_{\mathcal{M}}$. This shows that $H_{\mathcal{M}}(n)$ is eventually polynomial in n of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$. Once we complete the proof of the theorem above, it will follow that $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big) = \dim(M)$, and, in particular, $\dim\big(\mathrm{gr}_m(R)\big) = \dim(R)$ for any local ring R. Before proving the theorem we need the following observation.

Proposition. *Let (R, m, K) be local, and let $0 \to N \to M \to \overline{M} \to 0$ be an exact sequence of finitely generated R-modules. Let $\mathcal{M}$ be an M-stable filtration on M, let $\overline{\mathcal{M}}$ be the induced filtration on $\overline{M}$ whose n th term in the image of M_n, and let $\mathcal{N}$ be the inherited filtration on N, whose n th term is $M_n \cap N$. Then the sequence*

$$0 \to \mathrm{gr}_{\mathcal{N}}(N) \to \mathrm{gr}_{\mathcal{M}}(M) \to \mathrm{gr}_{\overline{\mathcal{M}}}(\overline{M}) \to 0$$

is an exact sequence of graded modules with degree-preserving maps, and so

$$H_{\mathcal{M}}(n) = H_{\mathcal{N}}(n) + H_{\overline{\mathcal{M}}}(n)$$

for all n.

Proof. For every n, the sequence

$$(*_n) \qquad 0 \to N_n \to M_n \to (M/N)_n \to 0$$

is exact by construction: $(M/N)_n$ is the image of M_n by definition, and the kernel of $M_n \to (M/N)_n$ is the same as the kernel of $M_n \to M/N$, which is $N \cap M_n = N_n$ by definition. The exactness of $(*_n)$ and $(*_{n+1})$ implies the exactness of the sequence of quotients

$$0 \to \frac{N_n}{N_{n+1}} \to \frac{M_n}{M_{n+1}} \to \frac{(M/N)_n}{(M/N)_{n+1}} \to 0$$

for all n. □

In order to prove the Theorem, we may again consider $N = \bigcup_t \mathrm{Ann}_N m^t$, which will be the same as $\mathrm{Ann}_M m^t$ for any $t \gg 0$. Any m-stable filtration on N is eventually 0, and so $H_{\mathcal{N}}(n) = \ell(N)$ for all sufficiently large n. If M is 0-dimensional we are done. If not, by the Proposition it suffices to consider M/N instead of M.

Math 615: Lecture of January 15, 2020

We have reduced the problem of proving that the degree of the Hilbert function of $M \neq 0$ is the Krull dimension of M to the case where $m \notin \mathrm{Ass}\,(M)$. Here M is a finitely generated module over the local ring (R, m, K).

Before proceeding further, we generalize the notion of Hilbert functions to a larger context. Let M be a finitely generated module over the local ring $(R,\, m,\, K)$ and let $\mathfrak{A}$ be any ideal of R that is primary to m modulo the annihilator I of M. That is, $\mathfrak{A}+I$ is m-primary, or, equivalently, $\mathfrak{A}(R/I)$ is primary to $m/I \subseteq R/I$. Note that $\dim(M) = \dim(R/I)$, by definition. Then for any $\mathfrak{A}$-stable filtration $\mathcal{M} = \{M_n\}_n$, we define $H_{\mathcal{M}}(n) = \ell(M/M_{n+1})$. We may always use the $\mathfrak{A}$-adic filtration, in which case we write $H_{\mathfrak{A},M}(n) = \ell(M/\mathfrak{A}^n M)$. The calculation of the values of this function is unaffected if we replace R by R/I: all of the modules involved are killed by I, and multiplying any of these modules by $\mathfrak{A}$ is the same as multiplying it by the expansion of $\mathfrak{A}$ to R/I. Thus, without loss of generality, we may readily assume that M is faithful and that $\mathfrak{A}$ is m-primary, by passing to R/I as indicated.

The following result will complete the proof of the Theorem from the previous lecture:

Theorem. *Let M be a finitely generated nonzero module over a local ring $(R,\, m,\, K)$. For any $\mathfrak{A}$-stable filtration $\mathcal{M}$ on M, $H_{\mathcal{M}}(n)$ is eventually a polynomial that agrees with $\Sigma\,\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}}(M)$. The degree and leading coefficient of this polynomial are independent of the choice of the $\mathfrak{A}$-stable filtration $\mathcal{M}$. The degree is the same as $\dim(M)$, and also the same as $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.*

Proof. We kill $\mathrm{Ann}_R M$, and so assume that M is faithful over R, that $\mathfrak{A}$ is m-primary, and that $\dim(M) = \dim(R)$. Since $\mathrm{gr}_{\mathcal{M}}(M)$ is a finitely generated module over $\mathrm{gr}_{\mathfrak{A}}R$, which is a standard graded algebra over the Artin local ring $R/\mathfrak{A}$, we have that $\mathrm{Hilb}_{\mathrm{gr}_{\mathcal{M}}(M)}(n)$ is a polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big) - 1$. Since

$$\ell(M_{n+1}) = \ell(M/M_1) + \ell(M_1/M_2) + \cdots + \ell(M_n/M_{n+1}),$$

it follows that $H_{\mathcal{M}}(n)$ is polynomial of degree $\dim\big(\mathrm{gr}_{\mathcal{M}}(M)\big)$.

We know compare the leading term of the polynomial coming from $\mathcal{M} = \{M_n\}_n$ with the polynomial given by the $\mathfrak{A}$-adic filtration. Since $\mathfrak{A}M_n \subseteq M_{n+1}$ for all n, $\mathfrak{A}^n M \subseteq M_n$ for all n, and $\ell(M/M_n) \leq \ell(M/\mathfrak{A}^n M)$. Let c be such that $M_{n+c} = \mathfrak{A}^n M_c$ for all $n \geq c$. Then $M_{n+c} \subseteq \mathfrak{A}^n m$, and so $\ell(M/M_{n+c}) \geq \ell(M/\mathfrak{A}^n M)$ for all n. Thus,

$$H_{\mathcal{M}}(n+c) \geq H_{\mathfrak{A},M}(n) \geq H_{\mathcal{M}}(n)$$

for all n, and so $H_{\mathfrak{A},M}$ is trapped between two polynomials with the same degree and leading coefficient. Therefore all three have the same degree and leading coefficient. This shows that the leading term of the polynomial in independent of the choice of $\mathcal{M}$.

We next show that the degree is independent of the choice of $\mathfrak{A}$. We can choose c such that $m^b \subseteq \mathfrak{A} \subseteq m$, and then $m^{nb} \subseteq \mathfrak{A}^n \subseteq m^n$ for all n, and so

$$\ell(M/m^{nb}) \geq \ell(M/\mathfrak{A}^n M) \geq \ell(M/m^n M)$$

which shows that $H_{\mathfrak{A},M}$ is eventually a polynomial trapped between $H_M(n)$ and $H_M(bn)$. The latter two are eventually polynomials of the same degree, and so $H_{\mathcal{M}}(n)$ must be as well, since we know that it is eventually polynomial.

It remains to see that the degree is $d = \dim(M) = \dim(R)$. To see that the degree is $\leq \dim(R)$, we choose $\mathfrak{A}$ to be generated by a system of parameters $x_1, \ldots, x_d \in m$. Then $\mathrm{gr}_{\mathfrak{A}}(R)$ is generated over $R/\mathfrak{A}$ by the classes of the elements x_i in $\mathfrak{A}/\mathfrak{A}^2$. Since the algebra is generated by d elements of degree 1, the denominator of the Poincaré series for $\mathrm{gr}_{\mathcal{M}}M$ is $(1-t)^d$, at worst, and this shows that the degree of the Hilbert polynomial of the associated graded module is at most $d-1$, which yields the upper bound d for the degree of $H_{\mathcal{M}}(n)$.

The last step is to show that the degree is at least d. We use induction on $\dim(M)$: the case where $d = 0$ is trivial. Since the degree is independent of both the m-primary ideal $\mathfrak{A}$ chosen and the specific $\mathfrak{A}$-stable filtration used, it suffices to consider the m-adic filtration. Moreover, we have already shown that one need only consider the case when no element of M is killed by m (for we may kill $\bigcup_t \mathrm{Ann}_M m^t$). Thus, we may assume that $m \notin \mathrm{Ass}(M)$, and by prime avoidance we may choose $f \in m$ such that f is not a zerodivisor on M. Consider the short exact sequence

$$0 \to M \xrightarrow{f} M \to M/fM \to 0.$$

Place the m-adic filtration on the central copy of M, the inherited m-adic filtration on the left hand copy of M (using that it is isomorphic with fM to think of it as a submodule of M: specifically, $M_n = m^nM :_M f$), and the image of the m-adic filtration of M on M/fM: this is the same as the m-adic filtration on M/fM. By the Proposition from last time, we find that $H_M(n) - H_{\mathcal{M}}(n) = H_{M/fM}(n)$. By what was proved above, the two polynomials on the left have the same leading term: when we subtract, we get a polynomial of lower degree. By the induction hypothesis, the polynomial on the right has degree $\dim(M/fM) = d-1$. It follows that the degree of $H_M(n)$ is at least d. □

For emphasis, we state the following consequence separately.

Corollary. *If M is a finitely generated module over the local ring (R, m), and $\mathfrak{A}$ is m-primary, M, $\mathrm{gr}_m(M)$, and $\mathrm{gr}_{\mathfrak{A}}(M)$ have the same Krull dimension.* □

Note that if (R, m, K) is local, for any m-primary ideal $\mathfrak{A}$, we have that $R/\mathfrak{A}^n \cong \widehat{R}/\mathfrak{A}^n\widehat{R}$ (recall that $\mathfrak{A}\widehat{R} \cong \widehat{\mathfrak{A}}$), and that for any finitely generated R-module M, $\widehat{M}/\mathfrak{A}^n\widehat{M} \cong M/\mathfrak{A}^nM$ for all n. The completions referred to here are all m-adic. This shows that we may identify $\mathrm{gr}_{\mathfrak{A}}(R) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{R}$, and $\mathrm{gr}_{\mathfrak{A}}(M) \cong \mathrm{gr}_{\widehat{\mathfrak{A}}}\widehat{M}$; in particular, we have these identifications when $\mathfrak{A} = m$.

We also note:

Proposition. *If (R, m, K) is local and $\mathrm{gr}_m(R)$ is a domain then R and $\widehat{R}$ are domains.*

Proof. The result for R implies the result for $\widehat{R}$, since their associated graded rings are the same. Suppose the result is false, so that $f, g \in m - \{0\}$ are such that $fg = 0$. Since $f \neq 0$, we can choose $s \in \mathbb{N}$ such that $f \in m^s - m^{s+1}$, and, similarly, we can choose $t \in \mathbb{N}$ such that $g \in m^t - m^{t+1}$. Let $[f]$ indicate the class of f in m^s/m^{s+1} and $[g]$ the class of $g \in m^t - m^{t+1}$. Then $[f]$ and $[g]$ are nonzero homogeneous elements of $\mathrm{gr}_m(R)$, and their product is $[fg] = [0]$, contradicting that $\mathrm{gr}_m(R)$ is a domain. □

Note that the completion of a local domain need not be a domain in general. The polynomial $f = y^2 - x^2(1+x)$ is irreducible in the polynomial ring $\mathbb{C}[x, y]$, since $1 + x$ is not a square (even in the fraction field), and so $x^2(1+x)$ is not a square. Thus, it generates a prime ideal which remains prime if we localize at (x, y). Let $R = \mathbb{C}[x, y]_{(x,y)}/(f)$, which is a local domain. Its completion $\widehat{R}$ is $\mathbb{C}[[x, y]]/(f)$, but now f is reducible: $1 + x$ is a perfect square in $\mathbb{C}[[x]]$, by Hensel's lemma (or use Newton's binomial theorem to give an explicit formula for the power series square root of $1 + x$). Instead of $\mathbb{C}$, we could have used any field of characteristic different from 2. In characteristic 2, $y^3 - x^3(1 + x)$ gives a similar example.

We can use associated graded rings to characterize regular local rings.

Theorem. *A local ring (R, m, K) is regular if and only if $\mathrm{gr}_m(R)$ is a polynomial ring in d variables over K, in which case $d = \dim(R)$.*

Proof. Let $x_1, \ldots, x_s$ be a minimal set of generators for m, and note that m/m^2 is the K-vector space of forms of degree 1 in $\mathrm{gr}_m(R)$. Now $d = \dim(R) = \dim\big(\mathrm{gr}_m(R)\big)$. If $\mathrm{gr}_m(R)$ is polynomial, it must be the polynomial ring in s variables, and since it has dimension both s and d we have that $s = d$, which shows that R is regular. If R is regular, we know that $\mathrm{gr}_m(R)$ is generated over K by d one forms, and has dimension d. Thus, it is a homomorphic image of the polynomial ring in d variables over K, where the variables map to the $[x_i]$. Since the dimension of $\mathrm{gr}_m(R)$ is d, there cannot be any kernel: a proper homomorphic image of a polynomial ring in d variables has Krull dimension $< d$. This shows that $\mathrm{gr}_m(R)$ is a polynomial ring in d variables. □

Since the associated graded ring of a regular local ring is a domain, we have at once:

Corollary. *A regular local ring is a domain.* □

Math 615: Lecture of January 17, 2020

Let (R, m, K) be local, let M be a nonzero finitely generated R-module with annihilator I of Krull dimension d, and let $\mathfrak{A} \subseteq R$ be an ideal such that $\mathfrak{A}(R/I)$ is primary to

$m/I \subseteq R/I$. We define the multiplicity of M with respect to $\mathfrak{A}$ to be $d!$ times the leading coefficient of the Hilbert function of M. This function is integer-valued, and the equivalent polynomial has degree d, and is therefore a $\mathbb{Z}$-linear combination of the polynomials $\binom{n}{j}$, $0 \leq j \leq d$, and $\binom{n}{d}$ must occur with positive coefficient. Therefore, the multiplicity is a positive integer. It may also be described as

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

If $\mathfrak{A} = m$, we simply refer to the *multiplicity* of M. In particular we may refer to the *multiplicity* of R itself.

We shall be particularly interested in determining multiplicities of rings with respect to parameter ideals, i.e., ideals generated by a system of parameters. In this case, the multiplicity can be recovered as an alternating sum of lengths of homology modules for a certain homology theory, Koszul homology, which can be viewed as a special case of Tor. The proof that we shall give of our result in this direction will depend on the theory of spectral sequences.

We shall also use Tor and related homological ideas to prove properties of regular rings. The only known proofs that a localization of a regular local ring at prime is again regular are by these methods, and the proof of unique factorization also depends on these ideas.

Before beginning the development of these homological methods, we want to make a few more comments about associated graded rings and multiplicities.

Note that the multiplicity of any regular local ring is 1. To check this, observe that the associated graded ring is $K[x_1, \ldots, x_d]$ where d is the dimension, and the Hilbert polynomial corresponds to $\binom{n+d-1}{d-1}$. The Hilbert function of the local ring is obtained by summing the values of $\binom{t+d-1}{d-1}$ for $t = 0, \ldots, n$. However, we note that the number of monomials in $x_1, \ldots, x_n$ of degree $\leq n$ is the same as the number of monomials of degree precisely n in $x_0, x_1, \ldots, x_d$: there is a bijection obtained by substituting $x_0 = 1$. Thus, the Hilbert function of the regular ring corresponds to $\binom{n+d}{d}$, which has leading coefficient $1/d!$, and this shows that the multiplicity is 1.

Let $R = K[[x_1, \ldots, x_d]]$ and let $f \in R$ have a lowest degree term of degree $\mu > 0$. The multiplicity of the ring R/f is μ. We shall check this by giving a technique for calculating associated graded rings of quotients.

If (R, m, K) is local and $f \in R - \{0\}$, there is always a unique integer $t \in N$ such that $f \in m^t - m^{t+1}$. Then $[f] \in m^t/m^{t+1} = [\mathrm{gr}_m(R)]_t$ is homogeneous and nonzero: we denote this element $\mathcal{L}(f)$, and call it the *leading form* of f. Note that $\mathcal{L}(f)$ is in $\mathrm{gr}_m(R)$, not in R. If $I \subseteq R$, we write $\mathcal{L}(I)$ for the ideal of $\mathrm{gr}_m(R)$ generated by all leading forms of elements of $I - \{0\}$: this is evidently a homogeneous ideal. In attempting to find generators for $\mathcal{L}(I)$, it is not in general sufficient to take the leading forms of a set of generators of I. See problems **1.** and **5.** of Problem Set #2. However, it is easy to see that this is sufficient for a nonzero principal ideal in a formal power series ring $K[[x_1, \ldots, x_d]]$ over a field K: when one multiplies by another nonzero power series, the leading form of the product is the product of the leading forms.

Proposition. *Let $(R,\, m,\, K)$ be local and let I be a nonzero ideal of R. Then*

$$\mathrm{gr}_{m/I}(R/I) \cong \mathrm{gr}_m R/\mathcal{L}(I).$$

Proof. We have that

$$[\mathrm{gr}_{m/I}(R/I)]_n = (m/I)^n/(m/I)^{n+1} \cong (m^n + I)/(m^{n+1} + I) \cong m^n/\bigl(m^n \cap (m^{n+1} + I)\bigr).$$

But if $u \in m^{n+1}$, $i \in I$, and $u + i \in m^n$, then $u \in m^n$, and so $u \in m^n \cap I$. This shows that $m^n \cap (m^{n+1} + I) = m^{n+1} + (m^n \cap I)$, and so

$$[\mathrm{gr}_{m/I}(R/I)]_n \cong m^n/(m^{n+1} + m^n \cap I) \cong (m^n/m^{n+1})/W_n,$$

where W_n is the image of $m^n \cap I$ in $m^n/m^{n+1} = [\mathrm{gr}_m(R)]_n$. But if $f \in m^n \cap I$, then if $f \in m^{n+1}$ the image of f in $[\mathrm{gr}_m(R)]_n$ is 0, while if $f \notin m^{n+1}$ then $[f] \in m^n/m^{n+1}$ is precisely a nonzero leading form in degree n of an element of I, and the result now follows. □

We now come back to the problem of calculating the associated graded ring of $R = K[[x_1, \ldots, x_d]]/(f)$ where f has nonzero leading form L of degree $\mu \geq 1$. From the remarks we have made, $\mathrm{gr}_m(R) \cong K[x_1, \ldots, x_d]/(L)$. We have a short exact sequence $0 \to T(-\mu) \xrightarrow{L} T \to T/(L) \to 0$, where $T = K[x_1, \ldots, x_d]$. Since the Hilbert function of T corresponds to $\binom{n+d-1}{d-1}$, the Hilbert function of $T/(L)$ corresponds to $\binom{n+d-1}{d-1} - \binom{n-\mu+d-1}{d-1}$. When we sum, we get $\binom{n+d}{d} - \binom{n-\mu+d}{d}$ up to a constant. It is easy to check that if $P(n)$ has leading coefficient a, then $P(n) - P(n-\mu)$ has leading coefficient μa. Thus, the leading coefficient is $\mu/d!$, and so the multiplicity is μ, as asserted earlier.

We want to make some comments on regular sequences. Recall that x is *not a zerodivisor* on M, or is a *nonzerodivisor* on M if for $u \in M$, $xu = 0$ implies that $u = 0$: in other words, the map on M given by multiplication by u is injective. We define an *improper regular sequence* $x_1, \ldots, x_d$ in R on an R-module M to be a sequence with the property that x_1 is not a zerodivisor on M and for all j, $1 < j \leq d$, x_j is a nonzerodivisor on $M/(x_1, \ldots, x_{j-1})M$. We allow the empty sequence as an improper regular sequence.

An improper regular sequence on the R-module M is called a *regular sequence* if, moreover, $(x_1, \ldots, x_d)M \neq M$. Thus, a regular sequence is an improper regular sequence. One might use the term *possibly improper* instead, but that necessitates many uses of the extra word “possibly.” A regular sequence may sometimes be referred to as a *proper* regular sequence to emphasize the condition that $(x_1, \ldots, x_d)M \neq M$: the word “proper” is redundant here. The empty sequence is a regular sequence on M provided that $M \neq 0$.

Regular sequences are also called *Rees sequences* in honor of David Rees, who was one of the first to make use of such sequences. Some authors also refer to *R-sequences* on M, but we avoid this term.

A nonzero element of a domain R always gives an improper regular sequence of length one on R, which will be a regular sequence precisely when the element is not a unit. 2 is a regular sequence in $\mathbb{Z}$, while 2, 1 is an improper regular sequence. A unit α of R followed by any sequence of elements thereafter is an improper regular sequence on M, since the unit is not a zerodivisor even if $M = 0$, while $M/\alpha M = 0$ — every element of R is a nonzerodivisor on the 0 module. This should help explain why one usually wants to restrict to proper regular sequences.

Regular sequences are not permutable in general, although we shall prove theorems in this direction later. The sequence $z - 1$, xz, yz is a regular sequence in the polynomial ring $K[x, y, z]$ in three variables over a field K, while $xz, yz, z - 1$ is not: in the quotient by (xz), yz kills the class $[x]$ of x, which is not 0.

It is a straightforward exercise to show that in a UFD, two elements that generate a proper ideal form a regular sequence of length 2 if and only if they are relatively prime, i.e., if and only if they have no prime factor in common.

In a local ring, any regular sequence is part of a system of parameters: the first element is not a zerodivisor and so not in any associated prime. In particular, it is not in any minimal prime, and killing the first element must drop the dimension of the ring by 1. The rest of the argument is a straightforward induction. We also note:

Proposition. *A local ring (R, m) is regular if and only if m is generated by a regular sequence, in which case any minimal set of generators of m is a regular sequence.*

Proof. If m is generated by a regular sequence, it is generated by a system of parameters, which shows that the dimension of R is equal to the least number of generators of m. Now suppose that R is regular, and that $x = x_1, x_2, \ldots, x_d$ is a minimal set of generators of m. We use induction on d: the case $d = 1$ is clear. Suppose $d > 1$. Note that $x \in m - m^2$. Since R is a domain, x is not a zerodivisor. In R/xR, the dimension and the least number of generators of the maximal ideal have both dropped by one, and are therefore still equal, so that R/xR is again regular. Moreover, the images of $x_2, \ldots, x_n$ are a minimal set of generators of m/xR. The result now follows from the induction hypothesis. □

A minimal set of generators of the maximal ideal of a regular local ring R is called a *regular* system of parameters. The term is not defined except in regular local rings.

We now want to begin our treatment of Tor, for which we need to talk about projective resolutions. Let R be any ring, and M be any R-module. Then it is possible to map a projective R-module P onto M. In fact one can choose a set of generators $\{u_\lambda\}_{\lambda\in\Lambda}$ for M, and then map the free module $P = \bigoplus_{\lambda\in\Lambda} Rb_\lambda$ on a correspondingly indexed set of generators $\{b_\lambda\}_{\lambda\in\Lambda}$ onto M: there is a unique R-linear map $P \twoheadrightarrow M$ that sends $b_\lambda \to u_\lambda$ for all $\lambda \in \Lambda$. Whenever we have such a surjection, the kernel M' of $P \twoheadrightarrow M$ is referred to as a *first module of syzygies* of M. We define k th modules of syzygies by recursion: a k th module of syzygies of a first module of syzygies is referred to as a $k+1$ st module of syzygies.

There is even a completely canonical way to map a free module onto M. Given M let $\mathcal{F}(M)$ denote the module of all functions from M to R that vanish on all but finitely many elements of M. This module is R-free on a basis $\{b_m\}_{m\in M}$ where b_m is the function that is 1 on m and 0 elsewhere. The map that sends $f \in \mathcal{F}(M)$ to $\sum_{m\in M} f(m)m$ is a canonical surjection: note that it maps b_m to m. The sum makes sense because all but finitely many terms are 0.

By a *projective resolution* of M we mean an infinite sequence of projective modules

$$\cdots \to P_n \to \cdots \to \; P_1 \to P_0 \to 0$$

which is exact at P_i for $i > 0$, together with an isomorphism $P_0/\mathrm{Im}\,(P_1) \cong M$. Recall the exactness at P_i means that the image of the map into P_i is the kernel of the map from P_i. Note that it is equivalent to give an exact sequence

$$\cdots \to P_n \to \cdots \to \; P_1 \to P_0 \twoheadrightarrow M \to 0$$

which is exact everywhere. A projective resolution is called *finite* if $P_n = 0$ for all sufficiently large n.

We can always construct a projective resolution of M as follows: map a projective module P_0 onto M. Let Z_1 be the kernel, a first module of syzygies of M. Map a projective module P_1 onto Z_1. It follows that $P_1 \to P_0 \to M \to 0$ is exact, and Z_2, the kernel of $P_1 \to P_0$, is a second module of syzygies of M. Proceed recursively. If $P_n \to \cdots \to P_1 \to P_0 \to M \to 0$ has been constructed so that it is exact (except at P_n), let Z_n be the kernel of $P_n \to P_{n-1}$), which will be an n th module of syzygies of M. Simply map a projective P_{n+1} onto Z_n, and use the composite map

$$P_{n+1} \twoheadrightarrow Z_n \subseteq P_n$$

to extend the resolution.

One can form a completely canonical resolution that is free, not merely projective, by taking $P_0 = \mathcal{F}(M)$ together with the canonical map $\mathcal{F}(M) \twoheadrightarrow M$ to begin, and choosing $P_{n+1} = \mathcal{F}(Z_n)$ along with the canonical map $\mathcal{F}(Z_n) \to Z_n$ at the recursive step. We refer to this as the *canonical* free resolution of M. We shall see that one can compute Tor using any projective resolution, but it is convenient for the purpose of having an unambiguous definition at the start to have a canonical choice of resolution.

If M is an R-module, we define $\mathrm{Tor}_n^R(M,\, N)$ to be the nth homology module of the complex $\cdots \to P_n \otimes_R N \to \cdots \to P_1 \otimes_R N \to P_0 \otimes_R N \to 0$, i.e., $H_n(P_\bullet \otimes_R N)$, where $P_\bullet$ is the canonical free resolution of M. The nth homology module of a complex $G_\bullet$ is Z_n/B_n where Z_n is the kernel of the map $G_n \to G_{n-1}$ and B_n is the image of the map $G_{n+1} \to G_n$.

Despite the unwieldy definition, the values of $\mathrm{Tor}^R(M,\, N)$ are highly computable. One might take the view that all of the values of Tor make a small correction for the fact that tensor is not an exact functor. The values of Tor are not always small, but one can often show that Tor vanishes, or has finite length, and the information it can provide is very useful.

Math 615: Lecture of January 22, 2020

We make some conventions that will be useful in dealing with complexes.

By a *sequence* of R-modules (and maps, although they will usually not be mentioned) we mean a family of modules $\{M_n\}_{n\in\mathbb{Z}}$ indexed by the integers, and for every $n \in \mathbb{Z}$ an R-linear map $d_n : M_n \to M_{n-1}$. The sequence is called a *complex* if $d_n \circ d_{n+1} = 0$ for all $n \in \mathbb{Z}$. This is equivalent to the condition that $\mathrm{Im}\,(d_{n+1}) \subseteq \mathrm{Ker}\,(d_n)$ for all n. We often use the notation $M_\bullet$ to denote a complex of modules. We define $H_n(M_\bullet)$ to be $\mathrm{Ker}\,(d_n)/\mathrm{Im}\,(d_{n+1})$, the nth *homology* module of $M_\bullet$. We shall make the homology modules into a new complex, somewhat artificially, by defining all the maps to be 0. Given a complex $M_\bullet$ we make the convention $M^n = M_{-n}$ for all $n \in \mathbb{Z}$. Thus, the same complex may be indicated either as

$$\cdots \to M_{n+1} \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to M_{-1} \to$$
$$\cdots \to M_{-(n-1)} \to M_{-n} \to M_{-(n+1)} \to \cdots$$

or as

$$\cdots \to M^{-(n+1)} \to M^{-n} \to M^{-(n-1)} \to \cdots \to M^{-1} \to M^0 \to M^1 \to$$
$$\cdots \to M^{n-1} \to M^n \to M^{n+1} \to \cdots$$

for which we write $M^\bullet$. With these conventions, $H^i(M^\bullet) = H_{-i}(M_\bullet)$. Thus, there really isn't any distinction between cohomology ($H^i(M^\bullet)$) and homology. A complex that is exact at every spot is called an *exact* sequence.

By a morphism of sequences $M_\bullet \to M'_\bullet$ we mean a family of R-linear maps $\phi_n : M_n \to M'_n$ such that for every $n \in \mathbb{Z}$ the diagram

$$\begin{tikzcd}
M_n \arrow[r, "d_n"] \arrow[d, "\phi_n"'] & M_{n-1} \arrow[d, "\phi_{n-1}"] \\
M'_n \arrow[r, "d'_n"'] & M'_{n-1}
\end{tikzcd}$$

commutes. There is an obvious notion of composition of morphisms of sequences: if $\phi : M_\bullet \to M'_\bullet$ and $\psi : M'_\bullet \to M''_\bullet$, let $\psi\circ\phi : M_\bullet \to M''_\bullet$ be such that $(\psi\circ\phi)_n = \psi_n\circ\phi_n$. Then sequences of R-modules and morphisms is a category (the identity map from $M_\bullet \to M_\bullet$ is, in degree n, the identity map $M_n \to M_n$).

Given a category $\mathcal{C}$, we say that $\mathcal{D}$ is a *full subcategory* of $\mathcal{C}$ if $\mathrm{Ob}\,(\mathcal{D}) \subseteq \mathrm{Ob}\,(\mathcal{C})$ and for all objects X and Y of $\mathcal{D}$, $\mathrm{Mor}_{\mathcal{D}}(X,\,Y) = \mathrm{Mor}_{\mathcal{C}}(X,\,Y)$. Composition in $\mathcal{D}$ is the same as composition in $\mathcal{C}$, when it is defined. Note that for every subclass of $\mathrm{Ob}\,(\mathcal{C})$ there is a unique full subcategory of $\mathcal{C}$ with these as its objects. For example, finite sets and functions is a full subcategory of sets and functions, abelian groups and group homomorphisms is a full subcategory of groups and group homomorphisms, and Hausdorff topological spaces and continuous maps is a full subcategory of topological spaces and maps.

The category of complexes of R-modules is defined as the full subcategory of the category of sequences of R-modules whose objects are the complexes of R-modules. We define a *left* complex $M_\bullet$ as a complex such that $M_n = 0$ for all $n < 0$, and a *right complex* as a complex such that $M_n = 0$ for all $n > 0$. Thus, a left complex has the form

$$\cdots \to M_n \to M_{n-1} \to \cdots \to M_1 \to M_0 \to 0 \to 0 \to \cdots$$

and a right complex has the form

$$\cdots \to 0 \to 0 \to M_0 \to M_{-1} \to \cdots \to M_{-(n-1)} \to M_{-n} \to \cdots$$

which we may also write, given our conventions, as

$$\cdots \to 0 \to 0 \to M^0 \to M^1 \to \cdots \to M^{n-1} \to M^n \to \cdots$$

Left complexes and right complexes are also full subcategories of sequences (and of complexes).

A complex is called *projective* (respectively, *free*) if all of the modules occurring are projective (respectively, free).

By a *short exact sequence* we mean an exact sequence of modules $M_\bullet$ such that $M_n = 0$ except possibly when $n \in \{0,\,1,\,2\}$:

$$0 \to M_2 \to M_1 \to M_0 \to 0.$$

These also forms a full subcategory of complexes. The numbering is not very important here. We shall also refer to M_2 as the *leftmost* module, M_1 as the *middle* module, and M_0 as the *rightmost* module in such a sequence.

The homology modules of a complex may be regarded as a complex by taking all the maps to be 0. The homology operator is then in fact a covariant functor from complexes to complexes: given a map $\{\phi_n\}_n$ of complexes $M_\bullet \to M'_\bullet$, with maps $\{d_n\}_n$ and $\{d'_n\}_n$ respectively, note that if $d_n(u) = 0$, then

$$d'_n\bigl(\phi_n(u)\bigr) = \phi_{n-1}\bigl(d_n(u)\bigr) = \phi_{n-1}(0) = 0,$$

so that ϕ maps $\mathrm{Ker}\,(d_n)$ into $\mathrm{Ker}\,(d'_n)$. If $u = d_{n+1}(v)$, then

$$\phi_n(u) = \phi_n\bigl(d_{n+1}(v)\bigr) = d'_{n+1}\bigl(\phi_{n+1}(v)\bigr),$$

which shows that ϕ_n maps $\mathrm{Im}\,(d_{n+1})$ into $\mathrm{Im}\,(d'_{n+1})$. This implies that ϕ_n induces a map of homology

$$H_n(M_\bullet) = \mathrm{Ker}\,(d_n)/\mathrm{Im}\,(d_{n+1}) \to \mathrm{Ker}\,(d'_n)/\mathrm{Im}\,(d'_{n+1}) = H_n(M'_\bullet).$$

This is easily checked to be a covariant functor from complexes to complexes.

In this language, we define a *projective resolution* of an R-module M to be a left projective complex $P_\bullet$ such that $H_n(P_\bullet) = 0$ for $n \geq 1$ together with an isomorphism $H_0(P_\bullet) \cong M$. Since $H_0(P_\bullet) \cong P_0/\mathrm{Im}\,(P_1)$, giving an isomorphism $H_0(P_\bullet) \cong M$ is equivalent to giving a surjection $P_0 \twoheadrightarrow M$ whose kernel is $\mathrm{Im}\,(P_1)$. Thus, giving a projective resolution of M in the sense just described is equivalent to giving a complex

$$(*) \qquad \cdots \to P_n \to \cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$$

that is exact, and such that P_n is projective for $n \geq 0$. In this context it will be convenient to write $P_{-1} = M$, but it must be remembered that P_{-1} need not be projective. The complex $(*)$ will be referred to as an *augmented projective resolution* of M.

We recall that an R-module P is projective if and if, equivalently

(1) When $M \twoheadrightarrow N$ is onto, $\mathrm{Hom}_R(P,\, M) \to \mathrm{Hom}_R(P,\, N)$ is onto.

(2) $\mathrm{Hom}_R(P,\, \_\,)$ is an exact functor.

(3) P is a direct summand of a free module.

A direct sum of modules (finite or infinite) is projective if and only if all of the summands are. It is easy to verify (1) for free modules: if P is free on the free basis $\{b_\lambda\}_{\lambda\in\Lambda}$ and $M \twoheadrightarrow N$ is onto, given a map $f : P \to N$, we lift to a map $g : P \to M$ as follows: for each free basis element b_λ of P, choose $u_\lambda \in M$ that maps to $f(b_\lambda)$, and let $g(b_\lambda) = u_\lambda$.

We next want to define what it means for two maps of complexes of R-modules to be homotopic. Let $P_\bullet$ and $N_\bullet$ be two complexes. First note that the set of maps of complexes $\mathrm{Mor}\,(P_\bullet,\; N_\bullet)$ is an R-module: we let

$$\{\phi_n\}_n + \{\psi_n\}_n = \{\phi_n + \psi_n\}_n,$$

and

$$r\{\phi_n\}_n = \{r\phi_n\}_n.$$

We define $\{\phi_n\}_n$ to be *null homotopic* or *homotopic* to 0 if there exist maps $h_n : P_n \to N_{n+1}$ (these are *not* assumed to commute with the complex maps) such that for all n,

$$\phi_n = d'_{n+1}h_n + h_{n-1}d_n.$$

The set of null homotopic maps is an R-submodule of the R-module of maps of complexes. Note that the homology functor $H_\bullet$ is R-linear on maps of complexes.

Two maps of complexes are called *homotopic* if their difference is null homotopic.

Lemma. *If two maps of complexes are homotopic, they induce the same map of homology.*

Proof. We have

$$\phi_n - \phi'_n = d'_{n+1}h_n + h_{n-1}d_n$$

for all n. Let $z \in \mathrm{Ker}\,(d_n)$. Then

$$\phi_n(z) - \phi'_n(z) = d'_{n+1}\big(h_n(z)\big) + h_{n-1}\big(d_n(z)\big).$$

The second term is 0, since $d_n(z) = 0$, and the first term is in $\mathrm{Im}\,(d'_{n+1})$. This shows that

$$[\phi_n(z)] - [\phi'_n(z)] = 0,$$

as required. □

The following Theorem is critical in developing the theory of derived functors such as Tor and Ext. In the applications a will typically be 0, but the starting point really does not matter.

Theorem. *Let $P_\bullet$ and $N_\bullet$ be complexes such that $P_n = 0$ for $n < a-1$ and $N_n = 0$ for $n < a-1$. Suppose that $N_\bullet$ is exact, and that P_n is projective for $n \geq a$. Let $M = P_{a-1}$ (which need not be projective) and $N = N_{a-1}$. Let ϕ be a given R-linear map from M to N. Then we can choose $\phi_n : P_n \to N_n$ for all $n \geq a$ such that, with $\phi_{a-1} = \phi$, $\{\phi_n\}_n$ is a map of complexes (of course, $\phi_n = 0$ is forced for $n < a-1$). Briefly, ϕ lifts to a map $\{\phi_n\}_n$ of complexes. Moreover, any two different choices $\{\phi_n\}_n$ and $\{\phi'_n\}_n$ for the lifting (but with $\phi_{a-1} = \phi'_{a-1} = \phi$) are homotopic.*

Proof of existence. We have a composite map $P_a \to M \to N$ and a surjection $N_a \twoheadrightarrow N$. Therefore, by the universal mapping property of projective modules, we can choose an R-linear map $\phi_a : P_a \to N_a$ such that $\phi \circ d_a = d'_a \circ \phi_a$. We now shorten both complexes: we replace the right end

$$N_{a+1} \to N_a \twoheadrightarrow N \to 0$$

of $N_\bullet$ by

$$N_{a+1} \to N' \to 0,$$

where N' is the image of N_{a+1} in N_a, which is also $\mathrm{Ker}\,(N_a \to N)$. We shorten the complex $P_\bullet$ by replacing the right end

$$P_{a+1} \to P_a \to M \to 0$$

by

$$P_{a+1} \to M' \to 0,$$

where M' is the kernel of $P_a \to M$. The restriction of ϕ_a to M' gives a map ϕ' of M' to N'. We are now in precisely the same situation that we started with, and we construct ϕ_{a+1} in the same manner that we constructed ϕ_a. The existence of all the ϕ_n follows by a straightforward induction. □

Math 615: Lecture of January 24, 2020

Proof of uniqueness up to homotopy. We work with the difference of the two liftings. It therefore suffices to show that a lifting of the 0 map $M \to N$ is null homotopic. Of course, we must define $h_n = 0$ if $n < a - 1$, and we define $h_{a-1} = 0$ as well: the property we need holds because $\phi = 0$. We construct the maps h_n recursively. Suppose that we have constructed h_n for $n < b$ where $b \geq a$ such that

$$\phi_n = d'_{n+1}h_n + h_{n-1}d_n$$

for all $n < b$. It will suffice to construct $h_b : P_b \to N_{b+1}$ such that

$$\phi_b = d'_{b+1}h_b + h_{b-1}d_b.$$

We claim that the image of $\phi_b - h_{b-1}d_b$ is contained in the image of N_{b+1}. By the exactness of $N_\bullet$, it suffices to show that the image of $\phi_b - h_{b-1}d_b$ is contained in the kernel of d'_b, i.e.,

$$d'_b\phi_b - d'_bh_{b-1}d_b = 0.$$

But since

$$\phi_{b-1} = d'_bh_{b-1} + +h_{b-2}d_{b-1},$$

we may substitute

$$d'_bh_{b-1} = \phi_{b-1} - h_{b-2}d_{b-1}$$

to get

$$d'_b\phi_b - (\phi_{b-1} - h_{b-2}d_{b-1})d_b.$$

since $d_{b-1}d_b = 0$, this is just

$$d'_b\phi_b - \phi_{b-1}d_b = 0$$

since $\{\phi_n\}_n$ is a map of complexes. Since

$$\alpha = \phi_b - h_{b-1}d_b$$

has image in $\mathrm{Im}\,(N_{b+1})$, we may let β be α with its target restricted to $\mathrm{Im}\,(N_{b+1})$. Since P_b is projective and d'_{b+1} maps onto the target of β, we may lift β to a map $h_b : P_b \to N_{b+1}$, so that $d'_{b+1}h_b = \beta$, which implies that

$$d'_{b+1}h_b = \phi_b - h_{b-1}d_b,$$

as required. □

Remark. Consider the case where $a = 0$. We also have maps of complexes once the augmentations $P_{-1} = M$ and $N_{-1} = N$ are dropped, and because $h_{-1} = 0$, we still have homotopic maps of complexes.

The significance of the result just proved is that we can use *any* projective resolution of M to calculate Tor — up to canonical isomorphism.

Theorem. *Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of the R-module M. Choose a lifting of id_M to a map of resolutions $\phi_\bullet : P_\bullet \to Q_\bullet$ and also to a map of resolutions $\psi_\bullet : Q_\bullet \to P_\bullet$. Then $\phi_\bullet \otimes_R \mathrm{id}_N$ and $\psi_\bullet$ induce mutually inverse isomorphisms between $H_\bullet(P_\bullet \otimes_R N)$ $H_\bullet(Q_\bullet \otimes_R N)$ that are independent of the choices of the ϕ and ψ. In this sense, any projective resolution of M may be used to compute all the modules $\mathrm{Tor}_n^R(M,\, N)$ up to canonical isomorphism.*

Proof. If we took a different choice of $\phi_\bullet$ it would be homotopic to the original. The homotopy is preserved when we apply $\_ \otimes_R N$. Therefore we get maps of homology that are independent of the choice of $\phi_\bullet$. The same remark applies to $\psi_\bullet$. The composition $\psi_\bullet \circ \phi_\bullet$ gives a map of complexes $P_\bullet \to P_\bullet$ that lifts id_M. The identity map of complexes is also such a lifting. This shows that $\psi \circ \phi$ is homotopic to the identity map on $P_\bullet$. This homotopy is preserved when we apply $\_ \otimes_R N$. This shows that the composition of the induced maps of homology is the identity map. The argument is the same when the composition is taken in the other order. □

Notice that $Tor_n^R(M,\, N) = 0$ if $n < 0$. If

$$\cdots \to P_1 \to P_0 \twoheadrightarrow M \to 0$$

is a projective resolution of M, then

$$\mathrm{Tor}_0^R(M,\, N) = H_0(\cdots \to P_1 \otimes_R N \to P_0 \otimes_R N \to 0) \cong \frac{P_0 \otimes_R N}{\mathrm{Im}\,(P_1 \otimes_R N)} \cong \frac{P_0}{\mathrm{Im}\,(P_1)} \otimes N$$

using the right exactness of tensor. Since

$$\frac{P_0}{\mathrm{Im}\,(P_1)} \cong M,$$

we have that

$$\mathrm{Tor}_0^R(M,\, N) \cong M \otimes N.$$

We now give an alternative point of view about complexes. Let $R[d] = R[\Delta]/\Delta^2$, and give Δ degree -1. The category of sequences is the same as the category of $\mathbb{Z}$-graded $R[\Delta]$-modules and degree preserving maps. The category of complexes is the same as the full subcategory of $\mathbb{Z}$-graded $R[d]$-modules and degree-preserving maps. It is very easy to see that given $M_\bullet \to M'_\bullet$, one has induced maps $\mathrm{Ann}_{M_\bullet} d \to \mathrm{Ann}_{M'_\bullet} d$ and $dM_\bullet \to dM'_\bullet$. Homology is recovered as $\mathrm{Ann}_{M_\bullet} d/dM_\bullet$, This is an $R[d]$-module on which d acts trivially, and it is now quite obvious that there are induced maps $H_\bullet(M_\bullet) \to H_\bullet(M'_\bullet)$ of homology.

From this point of view, the map h that gives a null homotopy is a degree 1 map of graded R-modules, that is, it increases degrees of homogeneous elements by 1: it need not commute with d. Then $hd + dh$ preserves degree, and does commute with d:

$$d(hd + dh) = dhd = (hd + dh)d.$$

$hd+dh$ gives the zero map on homology because if $dz = 0$, $(hd+dh)(z) = d(h(z)) \in \mathrm{Im}\,(d)$.

We next want to show that Tor is a covariant functor of two variables. Given an R-module map $M \to M'$ it lifts to a map of projective resolutions $P_\bullet$ for M and $P'_\bullet$ for M'. This gives induced maps of homology when we apply $\_ \otimes N$. If we choose a different lifting we get homotopic maps of complexes and the homotopy is preserved when we apply $\_ \otimes_R N$. The check of functoriality in M is straightforward.

Given a map $N \to N'$, we get obvious induced maps $P_\bullet \otimes N \to P_\bullet \otimes N'$ that yield the maps of Tor. Once again, the proof of functoriality is straightforward.

Math 615: Lecture of January 27, 2020

In order to develop the theory of Tor further, we want to consider double complexes. One point of view is that a double complex consists of a family of R-modules $\{M_{ij}\}_{i,j\in\mathbb{Z}}$ together with "horizontal" R-module maps $d_{ij} : M_{ij} \to M_{i,j-1}$ and "vertical" R-module maps $d'_{ij} : M_{ij} \to M_{i-1,j}$ for all $i, j \in \mathbb{Z}$, such that every $d_{ij}d_{i,j+1} = 0$ (the rows are complexes), every $d'_{i,j}d'_{i+1,j} = 0$ (the columns are complexes) and such that all of the squares

$$\begin{tikzcd}
M_{ij} \arrow[r, "d_{i,j}"] \arrow[d, "d'_{ij}"'] & M_{i,j-1} \arrow[d, "d'_{i,j-1}"] \\
M_{i-1,j} \arrow[r, "d_{i-1,j}"'] & M_{i-1,j-1}
\end{tikzcd}$$

commute: omitting subscripts, this means that $d'd = dd'$. An alternative convention that is sometimes made instead is that in a double complex, the vertical and horizontal differentials anticommute: i.e., $d'd = -dd'$. Both conventions have advantages and disadvantages: we shall call the latter type of double complex a *signed double complex*, but this terminology is not standard.

Given a double complex in our sense, one can alway create a signed double complex by altering the signs on some of the maps. To have a standard way of doing this, our convention will be that the associated signed double complex is obtained by replacing d'_{ij} by $(-1)^i d'_{ij}$, while not changing any of the d_{ij}. There are many ways to alter signs to get the squares to anticommute. It does not matter which one is used in the sense that the homology of the total complex (we shall define the total complex momentarily) is unaffected.

An alternative point of view is obtained by working with $\bigoplus_{ij} M_{ij}$, a $(\mathbb{Z} \times \mathbb{Z})$-graded R-module. Let Δ and Δ' be indeterminates over R, and let $R[d, d'] = R[\Delta, \Delta']/(\Delta^2, {\Delta'}^2)$, where Δ has degree $(0, -1)$, Δ' has degree $(-1, 0)$, and d, d' are their images. The d_{ij} define an action of d on $\bigoplus_{ij} M_{ij}$ that lowers the second index by 1, and the d'_{ij} define an action of d' on $\bigoplus_{ij} M_{ij}$ that lowers the first index by 1. Thus, a double complex is simply a $(\mathbb{Z} \times \mathbb{Z})$-graded $R[d, d']$-module.

A signed double complex may be thought of as a $(\mathbb{Z} \times \mathbb{Z})$-graded module over the noncommutative ring Λ generated over R by elements d and d' of degrees $(0, -1)$ and $(-1, 0)$, respectively, satisfying $d^2 = {d'}^2 = 0$ and $dd' = -d'd$. Λ may be identified with the exterior algebra over R of the free R-module $Rd \oplus Rd'$.

A *morphism* of double complexes is a bidegree-preserving $\mathbb{Z} \times \mathbb{Z}$-graded $R[d, d']$-module homomorphism, so that the maps commute with the actions of d and of d'. We indicate a double complex, whether signed or not, with the notation $M_{\bullet\bullet}$: the subscript is a reminder that the bidegree has two integer components. The *total complex* of a signed double complex $M_{\bullet\bullet}$, denoted $\mathcal{T}_\bullet(M_{\bullet\bullet})$, is obtained by letting $\mathcal{T}_n(M_{\bullet\bullet}) = \bigoplus_{i+j=n} M_{ij}$, with differential $d + d'$. This is indeed a complex because $(d+d')(d+d') = d^2 + d'd + dd' + {d'}^2 = 0$. The *total complex* of a double complex $M_{\bullet\bullet}$ is simply the total complex of the associated signed double complex. This means that the differential, restricted to M_{ij}, is $d_{ij} + (-1)^i d'_{ij}$.

Example. If $M_\bullet$ and $N_\bullet$ are complexes with differentials $d_\bullet$ and $d'_\bullet$, respectively, we get a double complex $M_\bullet \otimes N_\bullet$ whose i, j term is $M_j \otimes N_i$. Thus, the i th row is

$$\cdots \to M_{j+1} \otimes_R N_i \to M_j \otimes_R N_i \otimes_R M_{j-1} \otimes_R N_i \to \cdots$$

and the j th column is

$$\begin{tikzcd}
\vdots \arrow[d] \\
M_j \otimes_R N_{i+1} \arrow[d] \\
M_j \otimes_R N_i \arrow[d] \\
M_j \otimes_R N_{i-1} \arrow[d] \\
\vdots
\end{tikzcd}$$

The differentials in the i th row are the maps $d_j \otimes \mathrm{id}_{N_i}$ while those in the j th column are the maps $\mathrm{id}_{M_j} \otimes d'_i$. We shall return to the study of double complexes of this form shortly. The total complex $\mathcal{T}_\bullet(M_\bullet \otimes_R N_\bullet)$ is called the *total tensor product* of $M_\bullet$ and $N_\bullet$, and some authors omit the word "total," but we reserve the term "tensor product" for the double complex. Note that the differential of the total tensor product applied to $u_j \times v_i$ has the value $du_j \otimes v_i + (-1)^j u_j \otimes d'v_i$.

Given a double complex, one can take homology first of the rows (giving a new double complex) and then of the columns. The result is called *iterated* homology. One can also take homology first of the columns and then of the rows: this gives the iterated homology for the other order. Third, one can take homology of the total complex. These three objects are related in a complicated way. One of the most important applications of the theory of spectral sequences is to explain the relationship. We shall return to these ideas later.

For the moment, we want to prove two lemmas about double complexes that are of immense importance. They are both special cases of the theory of spectral sequences, but we ignore this for the moment.

The first is the *snake* or *serpent* lemma. One starts with a short exact sequence of complexes

$$0 \to A_\bullet \xrightarrow{\alpha} B_\bullet \xrightarrow{\beta} C_\bullet \to 0,$$

which simply means that for all n, the sequence $0 \to A_n \to B_n \to C_n \to 0$ is exact. We may form from these a double complex in which $A_\bullet$, $B_\bullet$ and $C_\bullet$ are the columns. A typical row is then $0 \to A_n \to B_n \to C_n \to 0$, and so is exact. A key point is that in this situation there is a well-defined map $\gamma_\bullet$ from $H_\bullet(C_\bullet) \to H_{\bullet-1}(A_\bullet)$ called *the connecting homomorphism*, where the subscript $_{\bullet-1}$ indicates that degrees have been shifted by -1, so that the $\gamma_n : H_n(A_\bullet) \to H_{n-1}(C_\bullet)$. We could also have used our graded module conventions and written $H_\bullet(C_\bullet)(-1)$, but we shall use the other convention for shifting the numbering of complexes.

The definition of γ is quite simple: since every map $B_n \to A_n$ is onto, given a cycle $z \in A_n$ we may choose $b \in B_n$ such that $\beta(b) = z$. Since z maps to 0 in A_{n-1}, we have that

$\beta(db) = d\big(\beta(b)\big) = dz = 0$ maps to 0 in B_{n-1}, and so db is the image of a unique element $a \in A_{n-1}$. Moreover $da = 0$, since $d\big(\alpha(a)\big) = d(db) = 0$. Our map will send $[z] \in H_n(C_\bullet)$ to $[a] \in H_{n-1}(A_\bullet)$. Note that if had made another choice of b mapping to z, it would have the form $b + \alpha(a_1)$ for some $a_1 \in A_n$. Then $d(b + \alpha(a_1)) = db + \alpha(da_1)$, and a would change to $a + d(a_1)$, which does not change its homology class. If we change the choice of representative z to $z + dc'$ for some $c' \in C_{n+1}$, we can choose $b' \in B_{n+1}$ that maps to c', and then a new choice for b is $b + db'$. But $d(b + db') = db$. This shows that we have a well-defined map $H_n(C) \to H_{n-1}(A)$. R-linearity follows from the fact that if b_1 and b_2 map to z_1 and z_2, then $rb_1 + b_2$ maps to $rz_1 + z_2$ for $r \in R$. Very briefly, the connecting homomorphism is characterized by the formula $\gamma([\beta(b)] = [\alpha^{-1}(db)]$, which makes sense since α is injective and db is in its image when $\beta(b)$ is a cycle.

Note the following picture:

$$\begin{tikzcd}
 & b \arrow[r, mapsto] \arrow[d, mapsto] & z \\
a \arrow[r, mapsto] \arrow[d, mapsto] & db & \\
0 & &
\end{tikzcd}$$

Proposition (snake or serpent lemma). *If $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ is a short exact sequence of complexes, then there is a long exact sequence of homology:*

$$\cdots \to H_{n+1}(C_\bullet) \xrightarrow{\gamma_{n+1}} H_n(A_\bullet) \xrightarrow{\alpha_{n*}} H_n(B_\bullet) \xrightarrow{\beta_{n*}} H_n(C_\bullet) \xrightarrow{\gamma_n} H_{n-1}(A_\bullet) \to \cdots$$

where α_{n*} and β_{n*} are the maps of homology induced by α_n and β_n, respectively.

Moreover, given a morphism of short exact sequences of complexes (this makes sense, thinking of them as double complexes), we get an induced morphism of long exact sequences, and the construction is functorial.

Proof. It suffices to check exactness at $H_n(C_\bullet)$, $H_n(B_\bullet)$, and $H_n(A_\bullet)$.

A cycle z in C_n is killed by γ iff for b mapping to c, db is the image of $a \in A_{n-1}$ that is a boundary, i.e., that has the form da' for some $a' \in A_{n-1}$. But then $b - a'$ is a cycle in B_n that maps to z, which shows that $[b - a']$ maps to $[z]$, as required. Conversely, if b is a cycle that maps to z, $db = 0$ and it is immediate that $[z]$ is in the kernel of γ_n.

For a cycle in $z \in B_n$, $[z]$ is killed by β_{n*} iff $\beta(z)$ is a boundary in C_n, i.e., $\beta(z) = dc'$, where $c' \in C_{n+1}$. Choose $b' \in B_{n+1}$ that maps onto c'. Then $z - db'$ maps to 0 in C_n, and so is the image of an element $a \in A_n$: moreover, da maps to $dz - d^2b' = 0 - 0$, and $A_{n-1} \hookrightarrow B_{n-1}$, so that a is cycle and $[a]$ maps to $[z]$. Conversely, the fact that the composite $H_n(A_\bullet) \to H_n(B_\bullet) \to H_n(C_\bullet)$ is 0 is immediate from the fact that $\beta\alpha = 0$.

Finally, let $z \in A_n$ be a cycle such that $[z]$ is zero in $H_n(B_\bullet)$. Then $\alpha(z)$ is a boundary, i.e., $\alpha(z) = db$ for $b \in B_{n+1}$. By the definition of γ_{n+1} we have that $\gamma_{n+1}([\beta(b)]) = [a]$. Conversely, if $\gamma_{n+1}([\beta(b)]) = [a]$ we have that $[a]$ maps to $[db] = 0$, so that $\alpha_{n*}\gamma_{n+1} = 0$.

Suppose that one has a morphism of short exact sequences from

$$0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$$

to

$$0 \to A'_\bullet \to B'_\bullet \to C'_\bullet \to 0.$$

The functoriality of the long exact sequence is immediate from the functoriality of taking homology, except for the commutativity of the squares:

$$\begin{tikzcd} H_n(C_\bullet) \arrow[r] \arrow[d] & H_{n-1}(A_\bullet) \arrow[d] \\ H_n(C'_\bullet) \arrow[r] & H_{n-1}(A'_\bullet) \end{tikzcd} .$$

This follows from the fact that if $\alpha(a) = db$ and $\beta(b) = z$, these relations continue to hold when we map $a \in A_{n-1}$, $b \in B_n$ and $z \in C_n$ to their counterparts in A'_{n-1}, B'_n, and C'_n. □

Corollary. *If $0 \to N_2 \to N_1 \to N_0 \to 0$ is a short exact sequence of R-modules and M is any R-module, then there is a long exact sequence*

$$\cdots \to \mathrm{Tor}_n^R(M, N_2) \to \mathrm{Tor}_n^R(M, N_1) \to \mathrm{Tor}_n^R(M, N_0) \to \mathrm{Tor}_{n-1}^R(M, N_2) \to \cdots \to$$

$$\mathrm{Tor}_1^R(M, N_2) \to \mathrm{Tor}_1^R(M, N_1) \to \mathrm{Tor}_1^R(M, N_0) \to M \otimes_R N_2 \to M \otimes_R N_1 \to M \otimes_R N_0 \to 0,$$

where we are identifying $\mathrm{Tor}_0^R(M, N)$ with $M \otimes_R N$.

Moreover, the long exact sequence is functorial in the the short exact sequence

$$0 \to N_2 \to N_1 \to N_0 \to 0.$$

Proof. Let $P_\bullet$ be a projective resolution of M (so that $H_0(P_\bullet) = M$), and let $N_\bullet$ be the short exact sequence formed by the N_i. Then $N_\bullet \otimes_R P_\bullet$ is a double complex that may be thought of as the short exact sequence of complexes

$$0 \to N_2 \otimes_R P_\bullet \to N_1 \otimes_R P_\bullet \to N_0 \otimes_R P_\bullet \to 0.$$

The typical row

$$0 \to N_2 \otimes_R P_n \to N_1 \otimes_R P_n \to N_0 \otimes_R P_n \to\to 0$$

is exact because P_n is projective and, therefore, R-flat. The result is now immediate from the definition of Tor and the snake lemma. $\square$

Note that if P is projective, $\mathrm{Tor}_n^R(P, N) = 0$ for $n \geq 1$. This is obvious because with $P_0 = P$, the complex

$$0 \to P_0 \to 0$$

is a projective resolution of P, and may be used to compute Tor. We shall shortly see that this property, the functorial long exact sequence, and the fact that $\mathrm{Tor}_0^R(M,\, N) \cong M \otimes_R N$ canonically as functors of two variables completely characterizes the functor $\mathrm{Tor}_\bullet^R(\_\,,\,\_)$, up to isomorphism of functors of two variables.

One may ask if there is a comparable long exact sequence for Tor if one starts with a sequence of modules $0 \to M_2 \to M_1 \to M_0 \to 0$. There is such a sequence, and there are several ways to see this. One of them is to prove that there is a canonical isomorphism of functors of two variables $\mathrm{Tor}_n^R(M,\, N) \cong \mathrm{Tor}_n^R(N,\, M)$ for all n, induced by the canonical identification $M \otimes_R N \cong N \otimes_R M$ that lets $u \otimes v$ correspond to $v \otimes u$. But the commutativity of tensor products is not the whole story. The symmetry of Tor is asserting that one can compute $\mathrm{Tor}_n^R(M, N)$ by taking a projective resolution of N, tensoring with M, and then taking homology. It is not obvious how to compare the two. What we shall do is take projective resolutions $P_\bullet$ of M and $Q_\bullet$ of N, and compare the two ways of computing Tor with the homology of $\mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)$. The following fact about double complexes is the key — before stating it, we recall that a left complex is *acyclic* if its homology vanishes in all degrees except degree 0. (The same term is applied to right complexes whose homology vanishes except in degree 0.)

Theorem. *Let $M_{\bullet\bullet}$ be a double complex whose terms all vanish if either component of the bidegree is < 0. Suppose that every row and every column is acyclic, i.e., that the homology of every row is 0 except in degree 0, and the same holds for columns. Let A_i be the augmentation module of the i th row (its 0 th homology module) and B_j be the augmentation module of the j th column (its 0 th homology module). Note that vertical differentials give a map from the i th row to the $i-1$ st row and hence induce maps $A_i \to A_{i-1}$ for all i which makes $A_\bullet$ a complex. Similar, $B_\bullet$ is a complex. Then there are isomorphisms*

$$H_\bullet(A_\bullet) \cong H_\bullet\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big) \cong H_\bullet(B_\bullet).$$

Math 615: Lecture of January 29 , 2020

Proof of the Theorem. Every element of $H_n(\mathcal{T}_\bullet(M_{\bullet\bullet})$ is represented by a cycle of

$$M_{0n} \oplus M_{1,n-1} \oplus \cdots \oplus M_{n-1,0} + \oplus M_{n,0}.$$

Denote this cycle

$$z = u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}.$$

We work in the signed double complex associated with $M_{\bullet\bullet}$, and assume that horizontal differentials d and the vertical differentials d' anticommute. We shall also write d (respectively, d') for the maps $M_{n,0} \to A_n$ (respectively, $M_{0,n} \to B_n$). A typical term in the sum above has the form u_{ij} where $i + j = n$, and both i and j lie between 0 and n inclusive. The condition that z be a cycle is that for $1 \leq i \leq n$, $du_{i-1,j+1} = -d'u_{ij}$: this is a condition on the pairs of consecutive terms whose indices sum to n. Given such an element of $\mathcal{T}_n(M_{\bullet\bullet})$, we map it to $H_n(A_\bullet)$ by sending it to $[du_{n0}]$, where $du_{n0} \in A_n$ and the brackets indicate the class of du_{n0} in $H_n(A_\bullet)$. There is a precisely similar map that sends $[z]$ to $[d'(u_{0n})] \in H_n(B_\bullet)$. There are several things that need checking:

(1) du_{n0} is a cycle of $H_n(A_\bullet)$ (the symmetric fact for $[u_{0n}]$ then follows).

(2) $[du_{n0}]$ is independent of the choice of representative of $[z]$ (the symmetric fact for $[d'u_{0n}]$ follows).

(3) The maps $H_n\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big)$ to $H_n(A_\bullet)$ and to $H_n(B_\bullet)$ obtained in this way are surjective.

(4) These maps are also injective.

(5) These maps are R-linear.

The checks that have some interest are (3) and (4), but we look at them all.

Consider the following diagram, in which the rows are exact, the rightmost squares commute (i.e., d'_* is induced by d'), while other squares, only one of which is shown, anticommute:

$$\begin{tikzcd}
 & M_{n+1,0} \arrow[r, "d"] \arrow[d, "d'"'] & A_{n+1} \arrow[r] \arrow[d, "d'_*"] & 0 \\
M_{n,1} \arrow[r, "d"] \arrow[d, "d'"'] & M_{n,0} \arrow[r, "d"] \arrow[d, "d'"'] & A_n \arrow[r] \arrow[d, "d'_*"] & 0 \\
M_{n-1,1} \arrow[r, "d"] & M_{n-1,0} \arrow[r, "d"] & A_{n-1} \arrow[r] & 0
\end{tikzcd}$$

(1) We have that $d'_*[du_{n0}] = [dd'u_{n,0}] \in A_{n-1}$, and $d'u_{n,0} = -du_{n-1,1}$, and therefore $d'_*[du_{n0}] = [-d^2u_{n-1,1}] = [0] = 0$.

(2) If we change z by adding a boundary in the total complex, $u_{n,0}$ changes by adding a term of the form $du_{n,1} + d'u_{n+1,0}$, where $u_{n,1} \in M_{n,1}$ and $u_{n+1,1} \in M_{n+1,1}$. But $du_{n,1}$ maps to 0 in A_n because $d^2 = 0$, and $d'u_{n+1,0}$ maps to $dd'u_{n+1,0} = d'_*du_{n+1,0}$, the image of $du_{n+1,0} \in A_{n+1}$ in A_n, so that $[du_{n,0}]$ does not change.

(3) Suppose that $\zeta \in A_n$ is a cycle. We can write ζ in the form $du_{n,0}$ for some $u_{n,0} \in M_{n,0}$. We want to show that we can construct elements $u_{n-j,j}$, $1 \leq j \leq n$, such that

$$u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}$$

is a cycle in $\mathcal{T}_n(M_{\bullet\bullet})$, i.e., such that we have

$$(*_j) \quad du_{n-(j+1),j+1} = -d'u_{n-j,j}$$

$0 \leq j \leq n-1$, and we proceed to make the construction by induction on j. Because $du_{n,0} = \zeta$ is a cycle, $d'_* du_{n,0} = 0$, which implies $dd'u_{n,0} = 0$. Since $-d'u_{n,0}$ is in the kernel of d, it is in the image of d, and so we can choose $u_{n-1,1} \in M_{n-1,1}$ such that $du_{n-1,1} = -d'u_{n,0}$. This is $(*_0)$. Now suppose that the $u_{n-h,h}$ have been constructed such that $(*_{h-1})$ holds, $1 \leq h \leq j$, where $j \geq 1$. In particular, we have $(*_{j-1})$, i.e.,

$$du_{n-j,j} = -d'u_{n-j+1,j-1}.$$

We want to choose $u_{n-j+1,j+1}$ such that

$$du_{n-(j+1),j+1} = -d'u_{n-j,j}$$

so that it suffices to see that $-d'u_{n-j,j}$ is in the image of d, and, therefore, it suffices to see that it is in the kernel of d. but

$$-dd'u_{n-j,j} = d'du_{n-j,j} = d'(-d'u_{n-j+1,j-1}) = 0,$$

as required, since $(d')^2 = 0$. This shows that one can construct a cycle that maps to ζ. If we let $w_{n-j-1,j} = d'u_{n-j,j}$, we have this picture:

$$\begin{tikzcd}
 & & & & & u_{n,0} \arrow[r, mapsto] \arrow[d, mapsto] & z \\
 & & & & u_{n-1,1} \arrow[r, mapsto] \arrow[d, mapsto] & \pm w_{n-1,0} & \\
 & & & & \pm w_{n-2,1} & & \\
 & \iddots & \iddots & \iddots & & & \\
 & u_{n-j,j} \arrow[r, mapsto] \arrow[d, mapsto] & \pm w_{n-j,j-1} & & & & \\
u_{n-j-1,j+1} \arrow[r, mapsto] \arrow[d, mapsto] & \pm w_{n-j-1,j} & & & & & \\
\pm w_{n-j-2,j+1} & & & & & &
\end{tikzcd}$$

(4) Now suppose that we have a cycle in $\mathcal{T}_n(M_{\bullet\bullet})$, call it

$$z = u_{0n} \oplus u_{1,n-1} \oplus \cdots \oplus u_{n-1,1} + \oplus u_{n,0}$$

that maps to 0 in $H_n(A_\bullet)$, which means that $du_{n,0} \in A_n$ is the image of some $a_{n+1} = du_{n+1,0} \in A_{n+1}$ under the map induced by d'. This implies that $d(u_{n,0} - d'u_{n+1,0}) = du_{n,0} - d'_* du_{n+1,0} = 0$ in A_n, and therefore has the form $du_{n,1}$ for some $u_{n,1} \in M_{n,1}$. We now use recursion on j to construct

$$u_{n-1,2} \in M_{n-1,2},\ \ldots\ ,\ u_{n-j,j+1} \in M_{n-j,j+1},\ \ldots\ ,\ u_{0,n+1} \in M_{0,n+1}$$

such that for all j, $0 \leq j \leq n$,

$$(*_j) \quad du_{n-j,j+1} + d'u_{n-j+1,j} = u_{n-j,j}.$$

This will show that z is the image of

$$u_{0,n+1} \oplus u_{1,n} \oplus \cdots \oplus u_{n,1} \oplus u_{n+1,0},$$

as required. We have already done the case where $j = 0$. Suppose for a fixed j with $1 \leq j \leq n$ we have constructed these elements $u_{n+1-h,\,h}$, $0 \leq h \leq j$, such that $(*_h)$ holds for $0 \leq h \leq j-1$. In particular, for $h = j-1$, we have

$$(*_{j-1}) \quad du_{n-j+1,j} + d'u_{n-(j-1)+1,j-1} = u_{n-j+1,j-1},$$

and applying d' to both sides we get:

$$(**) \quad d'du_{n+1-j,j} = d'u_{n+1-j,j-1}$$

We want to construct $u_{n-j,j+1}$ such that $(*_j)$ holds, i.e., such that

$$du_{n-j,j+1} = u_{n-j,j} - d'u_{n+1-j,j}.$$

To show that the element on the right is in the image of d, it suffices to prove that it is in the kernel of d, i.e., that

$$du_{n-j,j} = dd'u_{n+1-j,j}.$$

But $du_{n-j,j} = -d'u_{n-j+1,j-1}$ because z is a cycle and by $(**)$,

$$-d'u_{n+1-j,j-1} = -d'du_{n+1-j,j} = dd'u_{n+1-j,j},$$

as required.

(5) R-linearity is immediate from the definitions of the maps, once we know that they are well-defined, since, at the cycle level, the map $H_n\big(\mathcal{T}_\bullet(M_{\bullet\bullet})\big) \to H_n(A_\bullet)$ is induced by restricting the product projection $\prod\limits_{i+j=n} M_{ij} \to M_{n0}$ (identifying $\bigoplus\limits_{i+j=n} M_{ij} \cong \prod\limits_{i+j=n} M_{ij}$). □

We immediately obtain the isomorphism $\mathrm{Tor}_n^R(M,\, N) \cong \mathrm{Tor}_n^R(N,\, M)$ for all n. Let $P_\bullet$ and $Q_\bullet$ be projective resolutions of M and N, respectively. Then $\mathrm{Tor}_n^R(M,\, N) \cong$

$H_n(P_\bullet \otimes_R N) \cong H_n\big(\mathcal{T}_\bullet(P_\bullet \otimes_R Q_\bullet)\big) \cong H_n(M \otimes_R Q_\bullet) \cong H_n(Q_\bullet \otimes_R M) \cong \mathrm{Tor}_n^R(N, M)$. The first and last isomorphisms follow from the definition of Tor, coupled with the fact that any projective resolution may be used to compute it, the second and third isomorphisms follow from the Theorem just proved, and the next to last isomorphism is a consequence of the commutativity of tensor product.

This means that given a short exact sequence of modules $0 \to M_2 \xrightarrow{a} M_1 \xrightarrow{b} M_0 \to 0$ there is also a long exact sequence for Tor:

$$\cdots \to \mathrm{Tor}_n^R(M_2,\, N) \to \mathrm{Tor}_n^R(M_1,\, N) \to \mathrm{Tor}_n^R(M_0,\, N) \to \mathrm{Tor}_{n-1}^R(M_2,\, N) \to \cdots .$$

This sequence can be derived directly without proving the commutativity of Tor, by constructing an exact sequence of projective resolutions of the modules M_j instead. The idea is to fix resolutions of M_2 and M_0, and use them to build a resolution of M_1. Suppose that we are given projective resolutions $P_\bullet^{(j)}$ of M_j, for $j = 2,\, 0$, and call the differentials $d^{(j)}$, $j = 0,\, 2$. From these we can construct a projective resolution $P_\bullet^{(1)}$ of M_1 such that for all n, $P_n^{(1)} = P_n^{(2)} \oplus P_n^{(0)}$. To begin, the map $d^{(0)} : P_0^{(0)} \to M_0$ lifts to a map $f_0 : P^{(0)} \to M_1$ by the universal mapping property of projective modules, because $b : M_1 \twoheadrightarrow M_0$ is onto. One gets a surjection $d^{(1)} : P^{(2)} \oplus P^{(0)} \twoheadrightarrow M_1$ using $d^{(1)} = a \circ d^{(2)} \oplus f_0$. If one lets Z_2, Z_1, and Z_0 be the kernels of the $d^{(j)}$ one has a commutative diagram:

$$\begin{tikzcd}
 & P_1^{(2)} \arrow[d] & & P_1^{(0)} \arrow[d] & \\
0 \arrow[r] & Z_2 \arrow[r] \arrow[d] & Z_1 \arrow[r] \arrow[d] & Z_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0^{(2)} \arrow[r] \arrow[d, "d^{(2)}"'] & P_0^{(2)} \oplus P_0^{(0)} \arrow[r] \arrow[d] & P_0^{(0)} \arrow[r] \arrow[d, "d^{(0)}"] & 0 \\
0 \arrow[r] & M_2 \arrow[r, "a"'] \arrow[d] & M_1 \arrow[r, "b"'] \arrow[d] & M_0 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 . &
\end{tikzcd}$$

where the sequence of kernels $0 \to Z_2 \to Z_1 \to Z_0 \to 0$ is easily checked to be exact, and the problem of constructing the degree 1 part of the resolution of M_1 is now precisely the same problem that we had in constructing the degree 0 part.

Once one has the map $P_1^{(1)} = P_1^{(2)} \oplus P_1^{(0)} \twoheadrightarrow Z_1$, the map

$$P_1^{(1)} = P_1^{(2)} \oplus P_1^{(0)} \to P_0^{(2)} \oplus P_0^{(0)} = P_0^{(1)}$$

is constructed as the composition of the map $P_1^{(2)} \oplus P_1^{(0)} \twoheadrightarrow Z_1$ with the inclusion of Z_1 in $P_0^{(2)} \oplus P_0^{(0)}$. By a straightforward induction, one can continue in this way to build an entire projective resolution $P_\bullet^{(1)}$ of M_1, and a short exact sequence of complexes

$$0 \to P_\bullet^{(2)} \to P_\bullet^{(1)} \to P_\bullet^{(0)} \to 0$$

such that for all n,

$$P_n^{(1)} = P_n^{(2)} \oplus P_n^{(0)},$$

and the induced sequence of maps on the augmentations M_j is the short exact sequence $0 \to M_2 \xrightarrow{a} M_1 \xrightarrow{b} M_0 \to 0$ that we started with.

We next note that if $r \in R$ and M, N are R-modules, then the map

$$\mathrm{Tor}_n^R(M,\, N) \to \mathrm{Tor}_n^R(M,\, N)$$

induced by multiplication by r on N is given by multiplication by r on $\mathrm{Tor}_n^R(M,\, N)$. This may be seen as follows. Choose a projective resolution $P_\bullet$ of M. When we tensor with $N \xrightarrow{r} N$, we get the map of complexes $P_\bullet \otimes_R N \xrightarrow{r} P_\bullet \otimes_R N$ induced by multiplication by r, and this induces the map of homology. The same fact holds when we use $M \xrightarrow{r} M$ to induce a map

$$\mathrm{Tor}_n^R(M,\, N) \to \mathrm{Tor}_n^R(M,\, N),$$

by the symmetry of Tor. (Alternatively, use multiplication by r on every P_n to left $M \xrightarrow{r} M$ to a map $P_\bullet \xrightarrow{r} P_\bullet$ of the projective resolution of M to itself. Then apply $\_ \otimes_R N$ and take homology.)

If $r \in \mathrm{Ann}_R N$, then multiplication $N \xrightarrow{r} N$, is the zero map, and hence induces the 0 map

$$\mathrm{Tor}_n^R(M,\, N) \to \mathrm{Tor}_n^R(M,\, N),$$

which is also the map given by multiplication by r. In consequence, we have that $\mathrm{Ann}_R N$ kills every $\mathrm{Tor}_n^R(M,\, N)$. The same holds for $\mathrm{Ann}_R M$, and so $\mathrm{Ann}_R M + \mathrm{Ann}_R N$ kills every $\mathrm{Tor}_n^R(M,\, N)$.

The following fact, while very simple, is of great utility:

Proposition. *If $x \in R$ is not a zerodivisor and M is any R-module, then $\mathrm{Tor}_n^R(M,\, R/xR)$ (which is also $\mathrm{Tor}_n^R(R/xR,\, M)$) is M/xM if $n = 0$, is $\mathrm{Ann}_M x$ if $n = 1$, and is 0 if $n \neq 0,\, 1$.*

Proof. We may use the projective resolution $0 \to R \xrightarrow{x} R \to 0$, whose augmentation is R/xR, to compute Tor. Here, the left hand copy of R is in degree 1 and the right hand copy in degree 0. When we apply $M \otimes_R \_$, we find that the values of Tor are given by the homology of the complex $0 \to M \xrightarrow{x} M \to 0$. $\square$

We next want to introduce Koszul complexes. In doing so, we first want to discuss iterated total tensor products of complexes. Given k complexes $M_\bullet^{(1)}, \dots, M_\bullet^{(k)}$, with differential $d^{(j)}$ on $M^{(j)}$, we may define a total tensor product, which we denote

$$\mathcal{T}_\bullet(M_\bullet^{(1)} \otimes_R \cdots \otimes_R M_\bullet^{(k)}),$$

recursively by the rule that for $k = 1$ it is simply the original complex, for $k = 2$ it is the total tensor product of two complexes already defined, while for $k > 2$ it is

$$\mathcal{T}_\bullet\bigl((\mathcal{T}_\bullet(M_\bullet^{(1)} \otimes_R \cdots \otimes_R M_\bullet^{(k-1)}) \otimes_R M_\bullet^{(k)}\bigr).$$

It is easy to work out that up to obvious isomorphism this is the complex $T_\bullet$ such that

$$T_n = \bigoplus_{j_1+\cdots j_k=n} M_{j_1} \otimes_R \cdots \otimes_R M_{j_k}.$$

The differential on T_n is determined by the formula

$$d(u_{j_1} \otimes \cdots \otimes u_{j_k}) = \sum_{\nu=1}^{k} (-1)^{j_1+\cdots+j_{\nu-1}} u_{j_1} \otimes \cdots \otimes u_{j_{\nu-1}} \otimes d^{(j_\nu)} u_{j_\nu} \otimes u_{j_{\nu+1}} \otimes \cdots \otimes u_{j_k}.$$

We now define the Koszul complex of a sequence of elements $x_1, \dots, x_k$ of the ring R, which we denote $\mathcal{K}_\bullet(x_1, \dots, x_k;\, R)$, as follows. If $k = 1$, $\mathcal{K}_\bullet(x_1; R)$ is the complex $0 \to R \xrightarrow{x_1} R \to 0$, where the left hand copy of R is in degree 1 and the right hand copy in degree 0. Recursively, for $k > 1$,

$$\mathcal{K}_\bullet(x_1, \dots, x_k; R) = \mathcal{T}_\bullet\bigl(\mathcal{K}_\bullet(x_1, \dots, x_{k-1};\, R) \otimes_R \mathcal{K}_\bullet(x_k;\, R)\bigr)$$

Said differently,

$$\mathcal{K}_\bullet(x_1, \dots, x_k; R) = \mathcal{T}_\bullet\bigl(\mathcal{K}_\bullet(x_1;\, R) \otimes_R \cdots \otimes_R \mathcal{K}_\bullet(x_k;\, R)\bigr).$$

We shall look very hard at these complexes. Very soon, we will prove that if $x_1, \dots, x_k$ is an improper regular sequence in R, then $\mathcal{K}_\bullet(x_1, \dots, x_k;\, R)$ is a free resolution of $R/(x_1, \dots, x_k)$. This fact can be used, in conjunction with tricks, to compute or gain information about Tor in a remarkable number of instances.

Math 615: Lecture of January 31, 2020

We first prove that Koszul complexes give free resolutions for improper regular sequences such that every element is a nonzerodivisor. The hypothesis that every element is a nonzerodivisor is not needed: we will get rid of it shortly. But the case we prove is the most important.

Theorem. *Let $x_1, \ldots, x_k$ be an improper regular sequence in R such that every x_j is a nonzerodivisor in R. Then the Koszul complex $\mathcal{K}_\bullet(x_1, \ldots, x_k;\, R)$ is acyclic, and gives a free resolution of $R/(x_1, \ldots, x_k)R$.*

Proof. The case where $k = 1$ is obvious. We proceed by induction on k. Thus, we may assume that $k > 1$, and then we know that $\mathcal{K}_\bullet(x_1, \ldots, x_{k-1};\, R)$ and $\mathcal{K}_\bullet(x_k;\, R)$ give free resolutions of $R/(x_1, \ldots, x_{k-1})R$ and R/x_kR respectively. We may use the homology of the total tensor product to compute the values of

$$\mathrm{Tor}_n^R(R/(x_1, \ldots, x_{k-1})R,\, R/x_kR).$$

This is

$$\mathcal{T}_n\bigl(\mathcal{K}_\bullet(x_1, \ldots, x_{k-1};\, R) \otimes_R \mathcal{K}_\bullet(x_k;\, R)\bigr),$$

which *is* $\mathcal{K}_\bullet(x_1, \ldots, x_k;\, R)$. By the Proposition from the previous lecture, when x is a nonzerodivisor in R, $\mathrm{Tor}_n^R(M, R/xR)$ vanishes when $n \neq 0, 1$, and

$$\mathrm{Tor}_1^R(M,\, R/xR) \cong \mathrm{Ann}_M x.$$

In our current situation, x_k is not a zerodivisor on $R/(x_1, \ldots, x_{k-1})R$ by the definition of a regular sequence, and so all of the

$$\mathrm{Tor}_n^R(R/(x_1, \ldots, x_{k-1})R,\, R/x_kR)$$

vanish except possibly when $n = 0$, where one has

$$R/(x_1, \ldots, x_{k-1})R \otimes_R R/x_kR \cong R/(x_1, \ldots, x_k)R,$$

since $R/I \otimes_R R/J \cong R/(I + J)$ quite generally. This shows that $\mathcal{K}_\bullet(x_1, \ldots, x_k;\, R)$ is a free resolution of $R/(x_1, \ldots, x_k)R$, as claimed. $\square$

Koszul complexes of this sort are, by no small measure, the best understood free resolutions. We shall look at them closely. Later, we will use our understanding of Koszul complexes to prove the following theorem, which as established by M. Auslander in the equicharacteristic case and by S. Lichtenbaum in general.

Theorem (rigidity of Tor over regular rings). *Let M and N be finitely generated modules over a Noetherian ring R whose local rings are regular. Suppose that $\mathrm{Tor}_i^R(M,\, N) = 0$. Then $\mathrm{Tor}_j^R(M,\, N) = 0$ for all $j \geq i$.*

It will be quite a while before we can prove this.

We want to give a more explicit description of the Koszul complex. Experience has shown that it is useful in considering the complexes

$$0 \to R \xrightarrow{x_j} R \to 0$$

to give separate names to the generators of the free modules, instead of calling them all 1. We therefore write

$$0 \to Ru_j \xrightarrow{x_j} Rv_j \to 0$$

for $\mathcal{K}_\bullet(x_j;\, R)$, although $u_j = v_j = 1$. The differential is described by the rule $du_j = x_j v_j$, although we might also write $du_j = x_j$. To describe the total tensor product of k such complexes, we note that from our general description of total tensor products, $\mathcal{K}_i(x_1,\, \dots\, , x_k;\, R)$ will consist of the direct sum of all k-fold tensor products consisting of one term chosen from each complex, and such that the sum of the degrees from which these terms come is i. Notice that there will by 2^k terms if we look at all degrees. There will be one term in degree i for every choice of terms such that exactly i of them are the degree one copy of R from the complex. There are $\binom{k}{i}$ such terms; if we choose the degree one factors to be from

$$\mathcal{K}(x_{j_1};\, R),\, \dots\, , \mathcal{K}(x_{j_i};\, R)$$

with $1 \le j_1 < \cdots < j_i \le k$, we write $u_{j_1, \dots, j_i}$ for the obvious generator: it is a tensor product of k terms, each of which is either u_t or v_t. Specifically, the generator can be described as $w_1 \otimes \cdots w_k$, where if $t = j_i$ for some i then $w_t = u_{j_i}$, while $w_t = v_t$ otherwise. Note that the degree in which $u_{j_1, \dots, j_i}$ occurs is i, the number of elements in the string of subscripts. With this notation, we can write down the differential explicitly as follows:

$$du_{j_1, \dots, j_i} = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u_{j_1, \dots, j_{t-1}, j_{t+1}, \dots, j_i}.$$

The matrices of the maps with respect to the bases we are using will have entries each of which is $\pm x_s$ or 0.

This is simpler than it may seem at first sight. Consider the case where $k = 2$. The Koszul complex looks like this:

$$0 \to Ru_{12} \xrightarrow{\alpha_2} Ru_1 \oplus Ru_2 \xrightarrow{\alpha_1} R \to 0.$$

u_1 maps to x_1 and u_2 maps to x_2, while u_{12} maps to $x_1 u_2 - x_2 u_1 = -x_2 u_1 + x_1 u_2$. Thus, then matrices of the maps are $\alpha_1 = \begin{pmatrix} x_1 & x_2 \end{pmatrix}$ and

$$\alpha_2 = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}.$$

The map α_1 sends $r_1 u_1 + r_2 u_2$ to $r_1 x_1 + r_2 x_2$. Its kernel is the set of relations on x_1 and x_2. The “obvious” relations are given by the multiples of $(-x_2,\, x_1)$, and when the Koszul complex is acyclic (e.g., when the $x_1,\, x_2$ is a regular sequence), the “obvious” relations are the only relations.

When $k = 3$ the Koszul complex is

$$0 \to Ru_{123} \xrightarrow{\alpha_3} Ru_{23} \oplus Ru_{13} \oplus R_{12} \xrightarrow{\alpha_2} Ru_1 \oplus Ru_2 \oplus R_3 \xrightarrow{\alpha_1} R \to 0.$$

The images of u_1, u_2, and u_3 are x_1, x_2, and x_3, respectively. The images of u_{23}, u_{13}, and u_{12} are $-x_3u_2 + x_2u_3$, $-x_3u_1 + x_1u_3$, and $-x_2u_1 + x_1u_2$, respectively. The image of u_{123} is $x_1u_{23} + x_2u_{1,3} + x_3u_{12}$. If we use the obvious bases except that we replace u_{13} by $-u_{13}$, then the matrices of the maps are $\alpha_1 = \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}$,

$$\alpha_2 = \begin{pmatrix} 0 & x_3 & -x_2 \\ -x_3 & 0 & x_1 \\ x_2 & -x_1 & 0 \end{pmatrix},$$

and

$$\alpha_3 = \begin{pmatrix} x_1 \\ -x_2 \\ x_3 \end{pmatrix}.$$

The columns of each α_{i+1} give relations on the columns of α_i, $i = 1, 2$. When the Koszul complex is acyclic, these generate all the relations.

Note that over a Noetherian ring R, whenever M and N are finitely generated, so are all the modules $\mathrm{Tor}_n^R(M,\, N)$. To see this, note that we can choose a free resolution of M by finitely generated free modules. The resolution may go on forever, but each new kernel (or module of syzygies) is a submodule of a finitely generated free module, hence, Noetherian, and one can map a finitely generated free module onto it. Applying $\_ \otimes_R N$ produces a complex of Noetherian modules, and it follows at once that all of its homology modules are Noetherian.

Things are even better when we take free resolutions of finitely generated modules over a local ring $(R,\, m,\, K)$. We start with a free module M. We may choose a minimal set of generators for M: these are elements whose images in $K \otimes_R M \cong M/mM$ are K-vector space basis. This gives $F_0 \twoheadrightarrow M$ where F_0 is free. The kernel Z_1 is a finitely generated R-module. Again, we may choose a minimal set of generators of Z_1 and map a free module F_1 onto Z_1 using these generators. We can continue in this way, and so obtain a free resolution

$$\cdots \xrightarrow{\alpha_{n+1}} F_n \xrightarrow{\alpha_n} F_{n-1} \xrightarrow{\alpha_{n-1}} \cdots \xrightarrow{\alpha_2} F_1 \xrightarrow{\alpha_1} F_0 \xrightarrow{\alpha_0} M \to 0$$

such that the image of the free basis for F_i is a minimal set of generators for $Z_i = \alpha_i(F_i)$ for all $i \geq 0$. In this notation, $Z_0 = M$ itself. Such a free resolution is called a *minimal* free resolution of M. If $F_i = R^{\oplus b_i}$, the integer b_i is called the i th Betti number of M: we shall see momentarily that it is independent of the choice of the minimal resolution of M.

Note that the columns of the matrix α_i generate the relations on the generators for Z_i given by the image of the the free basis for F_i. These generators will be minimal if and only if none of them is a linear combination of the others, which is equivalent to the condition that no coefficient on a relation among them be a unit. (If any coefficient is a unit, one can solve for that generator in terms of the others.) Therefore, a resolution with matrices α_i is a minimal free resolution if and only if every entry of every matrix is in the maximal ideal m of R.

Theorem. *let $(R,\, m,\, K)$ be a local ring, and let M be a finitely generated module. Let $F_\bullet$ be a minimal free resolution of M, and suppose that $F_i \cong R^{b_i}$. Then $\mathrm{Tor}_i(M,\, K) \cong K^{b_i}$. Thus, the i th Betti number of M is the same as $\dim_K \mathrm{Tor}_i^R(M,\, K)$.*

M has a finite resolution by free modules if and only if $\mathrm{Tor}_i^R(M,\, K) = 0$ for some $i \geq 1$, and then a minimal free resolution is finite and is at least as short as any other free resolution of M.

Proof. When we use a minimal resolution $F_\bullet$ to compute Tor, we form the complex of K-vector spaces $F_\bullet \otimes_R K$. At the i th spot we have

$$F_i \otimes_R K \cong R^{\oplus b_i} \otimes_R K \cong K^{\oplus b_i}.$$

Because all the matrices have entries in m, when we map to K all the matrices become 0. Thus, all the maps in $F_\bullet \otimes K$ are 0, and the complex is its own homology, i.e.,

$$H_i(F_\bullet \otimes K) \cong F_i \otimes_R K \cong K^{b_i},$$

as claimed.

If M has a finite free resolution of length h, it may be used to compute Tor. It follows that $\mathrm{Tor}_i^R(M,\, K) = 0$ for $i > h$. On the other hand, suppose that $\mathrm{Tor}_i^R(M,\, K) = 0$. This means that in a minimal free resolution of M, $b_i = 0$, i.e., the i th module is 0. But then the minimal free resolution continues with modules all of which are 0. □

Putting this together with our knowledge of the Koszul complex, we obtain the following result with amazing ease:

Theorem. *Let (R, m, K) be a regular local ring of dimension d, and let $x_1, \, \ldots \, , x_d$ be a minimal set of generators of m. Then $\mathcal{K}_\bullet(x_1, \, \ldots \, , x_d;\, R)$ is a minimal free resolution of K over R. In consequence, $\mathrm{Tor}_i^R(K,\, K) \cong K^{\binom{d}{i}}$, $0 \leq i \leq d$, and is 0 otherwise.*

Moreover, every finitely generated R-module M has a finite free resolution over R of length at most d.

Proof. We know that $x_1, \, \ldots \, , x_d$ is a regular sequence in R consisting of nonzerodivisors (since R is a domain). Thus, $\mathcal{K}_\bullet(x_1, \, \ldots \, , x_d;\, R)$ is a free resolution of $R/(x_1, \, \ldots \, , x_d) \cong K$. Since every entry of every matrix is either $\pm x_j$ for some j or 0, this is a minimal free resolution of K. The calculation of $\mathrm{Tor}_i^R(K,\, K)$ is immediate.

Now let M be any finitely generated R-module. Since K has a free resolution of length d, $\mathrm{Tor}_i^R(K,\, M) = 0$ for $i > d$. But this is the same as $\mathrm{Tor}_i^R(M,\, K)$, and therefore the minimal resolution of M has length at most d. □

Notice that the symmetry of Tor plays a key role in the proof that M has a finite free resolution: in some sense, the symmetry is a rather trivial fact, but it is often the case that the information it provides is not easily obtained by other methods.

The final statement is a version of the Hilbert syzygy theorem. Hilbert did the case of finitely generated graded modules over the polynomial ring in d variables over the complex numbers. Note that the fact that one has a finite free resolution is equivalent to the assertion that when one takes iterated modules of syzygies, one eventually gets one that is free.

Horrocks raised the following question. Given a module $M \neq 0$ of finite length over a regular local ring (R, m, K) of dimension d, is it true that the i th Betti number of M is at least $\binom{d}{i}$, $0 \leq i \leq d$? The question was given in a list by Hartshorne. Buchsbaum and Eisenbud conjectured that this is true. The problem, although simple to state, is open.

We shall relate the homology of Koszul complexes to the notion of multiplicity of an m-primary ideal discussed earlier. Recall that if $\mathfrak{A}$ is m-primary in a local ring (R, m, K) of Krull dimension d, then the Hilbert function $\ell(R/\mathfrak{A}^{n+1})$ agrees with a polynomial of degree d in n for large n, whose leading term has the form $\dfrac{e_{\mathfrak{A}}}{d!}n^d$, where $e_{\mathfrak{A}}$ is a positive integer called the *multiplicity of* $\mathfrak{A}$. We shall prove that if $x_1, \ldots, x_d$ is a system of parameters of the local ring R and $\mathfrak{A} = (x_1, \ldots, x_d)R$, then

$$e_{\mathfrak{A}} = \sum_{i=0}^{d}(-1)^i\ell\bigl(H_i\bigl(\mathcal{K}_\bullet(x_1, \ldots, x_d;\, R)\bigr)\bigr).$$

It does turn out that the modules $H_i\bigl(\mathcal{K}_\bullet(x_1, \ldots, x_d;\, R)\bigr)$ have finite length, so that the right hand side makes sense. We will prove this formula, which is due to Serre, using spectral sequences. It will be a while before we are able to accomplish this.

Open questions in this area are abundant. Here is one that sounds very simple. First recall that the multiplicity e_m of the maximal ideal m of R is also called the *multiplicity* of R. Let

$$(R, m, K) \to (S, n, L)$$

be a local homomorphism of local rings such that S is flat over R. Is the multiplicity of R bounded by the multiplicity of S? I.e., is $e_m \leq e_n$? This was conjectured by C. Lech, and is open even when S is a finitely generated free R-module.

Math 615: Lecture of February 3, 2020

If $x_1, \ldots, x_n \in R$ and M is an R-module, we define the *Koszul complex of* M *with respect to* $x_1, \ldots, x_n$, denoted $\mathcal{K}_\bullet(x_1, \ldots, x_n; M)$, as

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

At the i th spot we have $R^{\binom{n}{i}} \otimes_R M$. When $n = 2$ we have

$$0 \to M \xrightarrow{d_2} M \oplus M \xrightarrow{d_1} M \to 0$$

where

$$d_2(u) = -x_2u \oplus x_1u$$

and

$$d_1(v \oplus w) = x_1v + x_2w.$$

We shall often abbreviate $\underline{x}$ for $x_1, \dots, x_n$, and write $\mathcal{K}_\bullet(\underline{x};\, M)$ instead. The *Koszul homology modules* $H_\bullet(\underline{x};\, M)$ are then defined as

$$H_\bullet\bigl(\mathcal{K}_\bullet(\underline{x}; M)\bigr).$$

We note the following facts:

(1) A an R-linear map $f : M \to N$ induces, in a covariantly functorial way, a map of Koszul complexes $\mathcal{K}_\bullet(\underline{x};\, M) \to \mathcal{K}_\bullet(\underline{x};\, N)$ and, hence, a map of Koszul homology $H_\bullet(\underline{x};\, M) \to H_\bullet(\underline{x}; N)$. If $M = N$ and the map is multiplication by $r \in R$, the induced map on Koszul complexes and on their homology is also given by multiplication by the ring element r.

(2) By the right exactness of tensor product,

$$H_0(\underline{x};\, M) \cong \bigl(R/(x_1, \dots, x_n)R\bigr) \otimes_R M \cong M/(x_1, \dots, x_n).M$$

The last map

$$\mathcal{K}_n(\underline{x};\, M) \cong M \to M^{\oplus n} \cong \mathcal{K}_{n-1}(\underline{x};\, M)$$

has the form

$$u \mapsto (\pm x_1u, \dots, \pm x_nu)$$

for some choice of signs (which depends on the choices of free basis). However, for any choice, the kernel is clearly $\mathrm{Ann}_M(x_1, \dots, x_n)R$, i.e.,

$$H_n(\underline{x};\, M) \cong \mathrm{Ann}_M(x_1, \dots, x_n)R.$$

(3) Given a short exact sequence of modules

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

there is a functorial short exact sequence of complexes

$$0 \to \mathcal{K}_\bullet(\underline{x};\, M_2) \to \mathcal{K}_\bullet(\underline{x};\, M_1) \to \mathcal{K}_\bullet(\underline{x};\, M_0) \to 0$$

induced by forming the tensor product of the given short exact sequence with $\mathcal{K}_\bullet(\underline{x}; R)$ (which we think of as a column). The rows are all exact because each is obtained by tensoring

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

with a free R-module. By the snake lemma there is a functorial long exact sequence of Koszul homology:

$$0 \to H_n(\underline{x};\, M_2) \to H_n(\underline{x};\, M_1) \to H_n(\underline{x};\, M_0) \to \cdots$$

$$\to H_i(\underline{x};\, M_2) \to H_i(\underline{x};\, M_1) \to H_i(\underline{x};\, M_0) \to H_{i-1}(\underline{x};\, M_2) \to \cdots$$

$$\to H_0(\underline{x};\, M_2) \to H_0(\underline{x};\, M_1) \to H_0(\underline{x};\, M_0) \to 0.$$

(4) Let $h : R \to S$ be a ring homomorphism and let $x_1, \dots, x_n \in R$. Let M be an S-module. Then M becomes R-module by restriction of scalars, i.e., we let $r \in R$ act by the rule $r \cdot u = h(r)u$. The Koszul complexes

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

and

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

are isomorphic in a very strong sense. As R-modules, the terms are identical. The maps are also identical: each map is completely determined by the manner in which the x_i (respectively, the $h(x_i)$) act on M, and multiplication by x_i is, by definition, the same endomorphism of M as multiplication by $h(x_i)$. The only issue is whether one is "remembering" or "forgetting" that M is an S-module as well as an R-module. Thus, there is a sense in which $H_\bullet(x_1, \dots, x_n;\, M)$ and $H_\bullet(h(x_1), \dots, h(x_n);\, M)$ are equal, not just isomorphic. Even if one "forgets" for a while that M is an S-module, the S-module structure on $H_\bullet(x_1, \dots, x_n; M)$ can be recovered. If $s \in S$, multiplication by s gives an R-linear map $M \to M$, and so induces a map $H_\bullet(x_1, \dots, x_n;\, M) \to H_\bullet(x_1, \dots, x_n;\, M)$, and this recovers the S-module structure on $H_\bullet(x_1, \dots, x_n;\, M)$.

5) We want to see that Koszul homology may be regarded as an instance of Tor. Let $x_1, \dots, x_n \in R$ and M be an R-module. Let A be any ring that maps to R. We may always choose $A = \mathbb{Z}$ or $A = R$. If R happens to contain a field K we may want to choose $A = K$. In any case, think of R as an A-algebra. Let $X_1, \dots, X_n$ be indeterminates over A, and let $B = A[X_1, \dots, X_n]$, the polynomial ring in n variables over A. Extend $A \to R$ to a ring homomorphism $B \to R$ by mapping $X_i \mapsto x_i$, $1 \le i \le n$. We can do this by virtue of the universal mapping property of polynomial rings. Then multiplication by X_i on M is the same as multiplication by x_i, $1 \le i \le n$. In B, $X_1, \dots, X_n$ is a regular sequence, and every X_i is a nonzerodivisor (this typically is not true at all for the x_i in R). Then $\mathcal{K}_\bullet(X_1, \dots, X_n;\, B)$ is a free resolution of $B/(X_1, \dots, X_n)B \cong A$, but keep in mind that when we view A as a B-module here, all of the X_i act trivially. Then $\mathrm{Tor}_i^B(A,\, M)$ is the i th homology module of

$$\mathcal{K}_\bullet(X_1, \dots, X_n;\, B) \otimes_B M = \mathcal{K}_\bullet(X_1, \dots, X_n; M) = \mathcal{K}_\bullet(\underline{x};\, M),$$

which leads to an identification

$$\mathrm{Tor}_i^B(A,\, M) \cong H_i(\underline{x};\, M).$$

The long exact sequence for Koszul homology is simply an instance of the long exact sequence for Tor if one takes this point of view. The R-module structure of $\mathrm{Tor}_i^B(A,\, M)$ can be recovered: multiplication by an element $r \in R$ is a B-linear map $M \to M$, and so induces a map

$$\mathrm{Tor}_i^B(A,\, M) \to \mathrm{Tor}_i^B(A,\, M)$$

which gives the action of multiplication by r on $\mathrm{Tor}_i^B(A,\, M)$.

6) It is obvious that $\mathrm{Ann}_R M$ kills all the Koszul homology modules $H_i(\underline{x};\, M)$, since it kills M and therefore every module in the complex $\mathcal{K}_\bullet(\underline{x};\, M)$. Less obvious is the fact that $(x_1,\, \ldots\, , x_n)R$ kills every $H_i(\underline{x}; M)$. We may see this as follows. With notation as in 5), we may view $H_i(\underline{x};\, M) \cong \mathrm{Tor}_i^B(A,\, M)$, and since every X_i kills A, multiplication by X_i kills $\mathrm{Tor}_i^B(A,\, M)$. This implies that multiplication by X_i on M induces the zero map $\mathrm{Tor}_i^B(A,\, M) \to \mathrm{Tor}_i^B(A,\, M)$. But that means that multiplication by x_i acting on M induces the zero map $\mathrm{Tor}_i^B(A,\, M) \to \mathrm{Tor}_i^B(A,\, M)$, and this implies that x_i kills $\mathrm{Tor}_i^B(A,\, M) \cong H_i(\underline{x};\, M)$, as required. In particular, if $x_1,\, \ldots\, , x_n$ generate the unit ideal, then all of the Koszul homology modules $H_i(\underline{x};\, M) = 0$.

We have seen that Koszul homology can be viewed as an instance of Tor. It is worth pointing out that it is often profitable to interpret Tor as some kind of Koszul homology if one can: Koszul homology is typically better understood than other instances of Tor.

Suppose that we have a short exact sequence

$$0 \to M_1 \to P \to M \to 0,$$

i.e., that M_1 is a first module of syzygies of M. Let N be any R-module. The long exact sequence for Tor yields a four term exact sequence

$$0 \to \mathrm{Tor}_1^R(M\, N) \to M_1 \otimes_R N \to P \otimes_R N \to M \otimes_R N \to 0,$$

because $\mathrm{Tor}_i^R(P,\, N) = 0$ for $i \geq 1$. In particular, $\mathrm{Tor}_1^R(P,\, N) = 0$. This characterizes $\mathrm{Tor}_1^R(M,\, N)$ as $\mathrm{Ker}\,(M_1 \otimes_R N \to P \otimes_R N)$. Because the higher values of $\mathrm{Tor}_i^R(P,\, N)$ are 0, the long exact sequence also yields isomorphisms

$$\mathrm{Tor}_{i+1}^R(M\, N) \cong \mathrm{Tor}_i(M_1,\, N)$$

for $i \geq 1$. More generally, if M_j is any j th module of syzygies of M, which means that there is an exact sequence

$$0 \to M_j \to P_{j-1} \to \cdots P_1 \to P_0 \to M \to 0$$

such that the P_t are projective, $0 \leq h \leq j$ (but we also define M to be a zeroth module of syzygies of M), then, by a trivial induction

$$\mathrm{Tor}_{i+j}^R(M,\, N) \cong \mathrm{Tor}_i^R(M_j,\, N)$$

for $i \geq 1$ and $j \geq 0$. In particular,

$$\mathrm{Tor}_{j+1}^R(M,\, N) \cong \mathrm{Tor}_1^R(M_j,\, N).$$

If we also have an exact sequence

$$0 \to M_{j+1} \to P_j \to M_j \to 0,$$

with P_j projective then

$$\mathrm{Tor}_{j+1}^R(M,\, N) \cong \mathrm{Ker}\,(M_{j+1} \otimes_R N \to P_j \otimes_R N).$$

This reduces the calculation of Tor to the calculation of modules of syzygies and the kernels of maps of tensor products. It also proves the assertion made earlier that Tor is completely determined by the three conditions (1) Tor_0^R agrees with $\otimes_R$, (2) higher Tor vanishes if the first given module is projective, and (3) there is a functorial long exact sequence.

Modules of syzygies are not uniquely determined. But they are determined up to taking direct sums with projective modules, as shown by the following result.

Theorem (Schanuel's Lemma). *Let*

$$0 \to M_1 \to P \xrightarrow{\alpha} M \to 0$$

and

$$0 \to M_1' \to P' \xrightarrow{\alpha'} M \to 0$$

be exact sequences, where P and P' are projective. Then

$$M_1 \oplus P' \cong M_1' \oplus P.$$

Proof. We have a surjection $\beta : P \oplus P' \twoheadrightarrow M$ that sends $u \oplus u'$ to $\alpha(u) + \alpha'(u')$. Let N be the kernel. It will suffice to show that $N \cong M_1' \oplus P$. The isomorphism $N \cong M_1 \oplus P'$ then follows by symmetry. Consider the map $\pi : N \to P$ that sends $u \oplus u' \in N$ to $u \in P$. Given $u \in P$, we can choose $u' \in P'$ such that $\alpha'(u') = -\alpha(u)$, since α' is surjective. It follows that π is surjective. $u \oplus u' \in \mathrm{Ker}\,(\pi)$ iff $u = 0$ and $u' \in \mathrm{Ker}\,(\alpha') = M_1'$. Thus, $\mathrm{Ker}\,(\pi) \cong M_1'$, and we have a short exact sequence

$$(*) \quad 0 \to M_1' \to N \to P \to 0.$$

Since P is projective, and since $N \to P \to 0$ is surjective, the identity map $P \to P$ lifts to a map $\gamma : P \to N$ such that $\pi \circ \gamma$ is the identity map on P. This means that the short exact sequence $(*)$ is split, and so $N \cong M_1' \oplus P$, as required. $\square$

It follows by a straightforward induction that for any two k th modules of syzygies M_k and M'_k of M, there are projectives P and P' such that

$$M_k \oplus P' \cong M'_k \oplus P.$$

Note that if R and M are Noetherian, we may take all the projectives used to be finitely generated, and then all the modules of syzygies will be finitely generated. Given two finitely generated k th modules of syzygies M_k and M'_k of M obtained in this way, we can find finitely generated projectives P and P' such that

$$M_k \oplus P' \cong M'_k \oplus P.$$

If R is local, the situation is simplified by the fact that finitely generated projective modules are free. (This is also true for infinitely generated projective modules, by a theorem of Kaplansky, but we have not proved it.)

Let R be a nonzero ring. A module M is said to have *finite projective dimension* if it has a finite projective resolution. The *projective dimension* of the 0 module is defined to be -1. The *projective dimension* of a nonzero projective module is defined to be 0. Recursively, the *projective dimension* of a module M is defined to be n if it has a projective resolution

$$0 \to P_n \to \cdots \to P_1 \to P_0 \to 0$$

(where $M \cong P_0/\mathrm{Im}\,(P_1)$) and it does not have projective dimension $n-1$. That is, a nonzero module M has projective dimension n if and only if a shortest projective resolution of M has length n. Modules that do not have a finite projective resolution are said to have *infinite projective dimension*, or projective dimension $+\infty$. The projective dimension of M is denoted $\mathrm{pd}_R M$ or simply $\mathrm{pd}\, M$.

From what we have said, if M is not 0, $\mathrm{pd}\, M \le n$ iff some (equivalently, every) n th module of syzygies of M is projective. It is straightforward to see that if M is not projective and M_1 is a first module of syzygies of M, then $\mathrm{pd}\, M_1 = \mathrm{pd}\, M - 1$, where we define $+\infty - 1 = +\infty$.

From the results proved in the previous lecture, it is clear that a finitely generated nonzero module M over a local ring has finite projective dimension if and only if its minimal resolution is finite, which happens if and only if some $\mathrm{Tor}_i^R(M,\, K) = 0$, $i \ge 1$, in which case $\mathrm{pd}_R M < i$. What happens is that either no $\mathrm{Tor}_i^R(M,\, K)$ vanishes for $i \ge 0$, which is the case where M has infinite projective dimension, or that these vector spaces are nonzero up to the projective dimension of M, and then are all 0. In particular:

Corollary. *Let M be a finitely generated nonzero module over a local ring $(R,\, m,\, K)$. Then M has finite projective dimension if and only if some $\mathrm{Tor}_i^R(M,\, K) = 0$, $i \ge 1$, and the projective dimension is the largest value of i such that $\mathrm{Tor}_i^R(M,\, K) \ne 0$.* □

Our next goal is to prove:

Theorem (Auslander-Buchsbaum-Serre). *Let $(R,\, m,\, K)$ be a local ring of Krull dimension d. Then the following conditions are equivalent:*

(1) *K has finite projective dimension over R.*

(2) *Some $\mathrm{Tor}_i^R(K,K)$ vanishes for $i \geq 1$.*

(3) $\mathrm{pd}_R K = d$.

(4) *Every finitely generated R-module has finite projective dimension.*

(5) *R is a regular local ring.*

We have already shown that (5) implies both (3) and (4), both of which clearly imply (1), and that (1) and (2) are equivalent. What remains to be done is to show that (1) implies (4). Once we have proved this, we can show easily that if we localize a regular local ring at any prime, we get a regular local ring. I do not know how to prove this without using the equivalence of (1) and (5). It was an open question for a long time, until homological methods were introduced into commutative algebra.

Math 615: Lecture of February 5, 2020

To illustrate the usefulness of Tor, we first consider the following example using only elementary methods. We then analyze the situation using Tor.

Example: an elementary calculation of behavior of tensor products. Let $R = K[x,\, y]$ or $K[[x,y]]$ be a polynomial ring or formal power series ring in two variables, and let $m = (x,y)R$. We shall show that the element $\epsilon = x \otimes y - y \otimes x$ in $m \otimes_R m$ is not 0 but is killed by m, and show that it spans the kernel of the surjection $m \otimes_R m \twoheadrightarrow m^2$ induced by the bilinear map $m \times m \to m^2$ sending (u,v) to uv. No nonzero K-linear combination of x and y is in m^2, so that m/m^2 is a K-vector space with basis consisting of the images $\overline{x}$ and $\overline{y}$ of x and y. Therefore $m/m^2 \otimes_k m/m^2$ has a basis consisting of $\overline{x} \otimes \overline{x}$, $\overline{x} \otimes \overline{y}$, $\overline{y} \otimes \overline{x}$, and $\overline{y} \otimes \overline{y}$, and so $\overline{x} \otimes \overline{y} - \overline{y} \otimes \overline{x} \neq 0$. Since $\epsilon = x \otimes y - y \otimes x$ maps to this element under the obvious surjection $m \otimes m \twoheadrightarrow m/m^2 \otimes_K m/m^2$, ϵ is not 0. But x kills ϵ since $x(x \otimes y - y \otimes x) = (x^2) \otimes y - (xy) \otimes x = x \otimes (xy) - x \otimes (xy) = 0$. By symmetry, y must also kill ϵ, and therefore m does.

Next note that if we map the free module $R^2 \twoheadrightarrow m$ by $(r,\, s) \mapsto rx + sy$, then the kernel is spanned by $(-y,\, x)$: $rx + sy = 0$ implies that $x \,|\, sy$, and since x is prime and x does not divide y, we can write $s = ax$ for some $a \in R$. But the $rx + axy = 0$, and it follows that $r = -ay$, so that $(rm,\, s) = a(-y,\, x)$. This enables us to identify m with $(Rt \oplus Ru)/R(-yt + xu)$ where t and u are free generators mapping to x and y respectively. We shall think of the second copy of m as $(Rv \oplus Rw)/R(-yv + xw)$, where v maps to x and w maps to y. Then $M \otimes_R M \cong (Rt \otimes v \oplus Rt \otimes w \oplus Ru \otimes v \oplus Ru \otimes w)/N$ where N is spanned by the four elements $-yt \otimes v + xu \otimes v$, $-yt \otimes w + xu \otimes w$, $-yt \otimes v + xt \otimes w - yu \otimes v + xu \otimes w$. If we let $t \otimes v, t \otimes w, u \otimes v$, and $u \otimes w$ correspond, in that order, to the standard generators of R^4, what we have is the quotient of R^4 by the span of the four vectors $(-y, 0, x, 0)$, $(0, -y, 0, x)$, $(-y, x, 0, 0)$, and $(0, 0, -y, x)$. Killing $t \otimes y - u \otimes v$ (which corresponds to $(0, 1, -1, 0)$) has the effect of killing $x \otimes y - y \otimes x$ in $m \otimes m$. Therefore, $m \otimes m/R\epsilon$ may be identified with a quotient of the free module on three generators (they correspond to $t \otimes v$, $t \otimes w$, and $u \otimes w$). We identify this with R^3, and the submodule V that we need to kill is then spanned by $(-y, x, 0)$ and $(0, -y, x)$. Now $m \otimes m/R\epsilon \cong R^3/V$ maps to m^2 in such a way that the respective generators map to x^2, xy, and y^2. Therefore, we are done if we show that $\{(a, b, c) \in R^3 : ax^2 + bxy + cy^2 = 0\}$ (the relations on x^2, xy, y^2) is spanned by $(-y, x, 0)$ and $(0, -y, x)$. But if $ax^2 + bxy + cy^2 = 0$, we have $y \,|\, ax^2 \Rightarrow y \,|\, a$. Suppose that $a = a'y$. Adding $a'(-y, x, 0)$ we get a relation $(0, b_1, c_1)$ on x^2, xy, y^2, and this means that $b_1xy + c_1y^2 = 0$, and so $b_1x + c_1y = 0$. As before, we see that (b_1, c_1) is a multiple of $(-y, x)$, and so $(0, b_1, c_1)$ is a multiple of $(0, -y, x)$. □

We next want to see how the long exact sequence for Tor can be applied here. We have a short exact sequence

$$0 \to m \to R \to K \to 0.$$

Applying $\_ \otimes_R m$ we get:

$$0 \to \mathrm{Tor}_1^R(K,\, m) \to m \otimes_R m \to m \to m/m^2 \to 0,$$

where the map $m \otimes_R m \to m$ is easily checked to send $u \otimes v$ to uv and so has image m^2. Since m is a first module of syzygies of K,

$$\mathrm{Tor}_1^R(K,\, m) \cong \mathrm{Tor}_2^R(K,\, K),$$

which we have already seen is K. Thus, understanding Tor tells us that $\mathrm{Ker}\,(m \otimes_R m \twoheadrightarrow m^2)$ will be a copy of $K = R/m$.

Note that if I and J are any two ideals of R, applying $\_ \otimes_R R/J$ to

$$0 \to I \to R \to R/I \to 0$$

produces

$$0 \to \mathrm{Tor}_1^R(R/I,\, R/J) \to I/IJ \to R/J \to R/(I + J) \to 0$$

showing that

$$\mathrm{Tor}_1^R(R/I,\, R/J) \cong \mathrm{Ker}\,(I/IJ \to R/J),$$

where $[i]$ mod IJ maps to $[i]$ mod J. The kernel is evidently $(I/\cap J)/IJ$, so that

$$\mathrm{Tor}_1^R(R/I,\, R/J) = (I \cap J)/IJ.$$

The condition that $\mathrm{Tor}_1^R(R/I,\, R/J) = 0$ may be thought of as saying that I and J are "relatively prime." It always holds when I and J are comaximal (since the Tor is killed by $I + J = R$), and it holds for nonzero principal ideals $I = fR$ and $J = gR$ in a UFD R if and only if f and g have no common prime factor.

We want to make one more observation about modules of syzygies. Suppose that an R-module M has generators $u_1, \dots, u_n$ and that one maps a free module $R^n \twoheadrightarrow M$ by sending $(r_1, \dots, r_n)$ to $\sum_{j=1}^n r_j u_j$. The kernel is a first module of syzygies of M, but it also the module of all relations on the generators $u_1, \dots, u_n$ of M, and is called the *module of relations* on $u_1, \dots, u_n$. Thus, when the projective used is free, we may think of the first module of syzygies as a module of relations.

Proposition. *Let (R, m, K) a local ring.*

Given a finite exact sequence of finitely generated R-modules such that every term but one has finite projective dimension, then every term has finite projective dimension.

In particular, given a short exact sequence

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

of finitely generated R-modules, if any two have finite projective dimension over R, so does the third. Moreover:

(a) $\operatorname{pd} M_1 \le \max\{\operatorname{pd} M_0, \operatorname{pd} M_2\}$.

(b) *If* $\operatorname{pd} M_1 < \operatorname{pd} M_0$ *are finite, then* $\operatorname{pd} M_2 = \operatorname{pd} M_0 - 1$. *If* $\operatorname{pd} M_1 \ge \operatorname{pd} M_0$, *then* $\operatorname{pd} M_2 \le \operatorname{pd} M_1$.

(c) $\operatorname{pd} M_0 \le \max\{\operatorname{pd} M_1, \operatorname{pd} M_2 + 1\}$.

Proof. Consider the long exact sequence for Tor:

$$\cdots \to \operatorname{Tor}^R_{n+1}(M_1, K) \to \operatorname{Tor}^R_{n+1}(M_0, K) \to \operatorname{Tor}_n(M_2, K)$$
$$\to \operatorname{Tor}^R_n(M_1, K) \to \operatorname{Tor}^R_n(M_0, K) \to \cdots$$

If two of the M_i have finite projective dimension, then two of any three consecutive terms are eventually 0, and this forces the third term to be 0 as well.

The statements in (a), (b), and (c) bounding some $\operatorname{pd} M_j$ above for a certain $j \in \{0, 1, 2\}$ all follow by looking at trios of consecutive terms of the long exact sequence such that the middle term is $\operatorname{Tor}^R_n(M_j, K)$. For n larger than the specified upper bound for $\operatorname{pd}_R M_j$, the Tor on either side vanishes. The equality in (b) for the case where $\operatorname{pd} M_1 < \operatorname{pd} M_0$ follows because with $n = \operatorname{pd} M_0 - 1$, $\operatorname{Tor}^R_{n+1}(M_0, K)$ injects into $\operatorname{Tor}^R_n(M_2, K)$.

The statement about finite exact sequences of arbitrary length now follows by induction on the length. If the length is smaller than three we can still think of it as 3 by using terms that are 0. The case of length three has already been handled. For sequences of length 4 or more, say

$$0 \to M_k \to M_{k-1} \to \cdots \to M_1 \to M_0 \to 0,$$

either M_k and M_{k-1} have finite projective dimension, or M_1 and M_0 do. In the former case we break the sequence up into two sequences

$$0 \to M_k \to M_{k-1} \to B \to 0$$

and

$$(*) \quad 0 \to B \to M_{k-2} \to \cdots \to M_1 \to M_0 \to 0.$$

The short exact sequence shows that $\operatorname{pd} B$ is finite, and then we may apply the induction hypothesis to $(*)$. If M_1 and M_0 have finite projective dimension we use exact sequences

$$0 \to Z \to M_1 \to M_0 \to 0$$

and

$$0 \to M_k \to M_{k-1} \to \cdots \to M_2 \to Z \to 0$$

instead. □

Lemma. *If M has finite projective dimension over (R, m, K) local, and $m \in \operatorname{Ass}(R)$, then M is free.*

Proof. If not, choose a minimal free resolution of M of length $n \geq 1$ and suppose that the left hand end is

$$0 \to R^b \xrightarrow{A} R^a \to \cdots$$

where A is an $a \times b$ matrix with entries in m. The key point is that the matrix A cannot give an injective map, because if $u \in m - \{0\}$ is such that $\operatorname{Ann}_R u = m$, then A kills a column vector whose only nonzero entry is u. □

Lemma. *If M has finite projective dimension over R, and x is not a zerodivisor on R and not a zerodivisor on M, then M/xM has finite projective dimension over both R and over R/xR.*

Proof. Let $P_\bullet$ be a finite projective resolution of M over R. Then $P_\bullet \otimes_R R/xR$ is a finite complex of projective R/xR-modules whose homology is $\operatorname{Tor}_n^R(M,\, R/xR)$, which is 0 for $n \geq 1$ when x is not a zerodivisor on R or M. This gives an (R/xR)-projective resolution of M over R/xR. The short exact sequence

$$0 \to P \xrightarrow{x} P \to P/xP \to 0$$

shows that each P/xP has projective dimension at most 1 over R, and then M/xM has finite projective dimension over R by the Proposition above. □

Lemma. *Let (R, m, K) be local, let I_n denote the $n \times n$ identity matrix over R, let x be an element of $m - m^2$, and let A, B be $n \times n$ matrices over R such that $xI_n = AB$. Suppose that every entry of A is in m. Then B is invertible.*

Proof. We use induction on n. If $n = 1$, we have that $(x) = (a)(b) = (ab)$, where $a \in m$. Since $x \notin m^2$, we must have that b is a unit. Now suppose that $n > 1$. If every entry of B is in m, the fact that $xI_n = AB$ implies that $x \in m^2$ again. Thus, some entry of B is a unit. We permute rows and columns of B to place this unit in the upper left hand corner. We multiply the first row of B by its inverse to get a 1 in the upper left hand corner. We next subtract multiples of the first column from the other columns, so that the first row becomes a 1 followed by a string of zeros. We then subtract multiples of the first row from the other rows, so that the first column becomes 1 with a column of zeros below it. Each of these operations has the effect of multiplying on the left or on the right by an invertible $n \times n$ matrix. Thus, we can choose invertible $n \times n$ matrices U and V over R such that $B' = UBV$ has the block form

$$B' = \begin{pmatrix} 1 & 0 \\ 0 & B_0 \end{pmatrix},$$

where the submatrices 1, 0 in in the first row are 1×1 and $1 \times (n-1)$, respectively, while the submatrices 0, B_0 in the second row are $(n-1) \times 1$ and $(n-1) \times (n-1)$, respectively.

Now, with

$$A' = V^{-1}AU^{-1},$$

we have

$$A'B' = V^{-1}AU^{-1}UBV = V^{-1}(AB)V = V^{-1}(xI_n)V = x(V^{-1}I_nV) = xI_n,$$

so that our hypothesis is preserved: A' still has all entries in m, and the invertibility of B has not been changed. Suppose that

$$A' = \begin{pmatrix} a & \rho \\ \gamma & A_0 \end{pmatrix}$$

where $a \in R$ (technically a is a 1×1 matrix over R), ρ is $1 \times (n-1)$, γ is $(n-1) \times 1$, and A_0 is $(n-1) \times (n-1)$. Then

$$xI_n = A'B' = \begin{pmatrix} a(1) + \rho(0) & a(0) + \rho B_0 \\ \gamma(1) + A_0(0) & \gamma(0) + A_0 B_0 \end{pmatrix} = \begin{pmatrix} a & \rho B_0 \\ \gamma & A_0 B_0 \end{pmatrix}$$

from which we can conclude that $xI_{n-1} = A_0 B_0$. By the induction hypothesis, B_0 is invertible, and so B' is invertible, and the invertibility of B follows as well. □

The following is critical in proving that if K has finite projective dimension over (R, m, K) then R is regular.

Theorem. *If M is finitely generated and has finite projective dimension over R, and $x \in m - m^2$ kills M and is not a zerodivisor in R, then M has finite projective dimension over R/xR.*

Proof. We may assume M is not 0. M cannot be free over R, since $xM = 0$. Thus, we may assume $\mathrm{pd}_R M \geq 1$. We want to reduce to the case where $\mathrm{pd}_R M = 1$. If $\mathrm{pd}_R M > 1$, we can think of M as a module over R/xR and map $(R/xR)^{\oplus h} \twoheadrightarrow M$ for some h. The kernel M_1 is a first module of syzygies of M over R/xR. By part (b) of the Proposition, $\mathrm{pd}_R M_1 = \mathrm{pd}_R M - 1$. Clearly, if M_1 has finite projective dimension over R/xR, so does M. By induction on $\mathrm{pd}_R M$ we have therefore reduced to the case where $\mathrm{pd}_R M = 1$. To finish the proof, we shall show that if $x \in m - m^2$ is not a zerodivisor in R, $xM = 0$, and $\mathrm{pd}_R M = 1$, then M is free over R/xR.

Consider a minimal free resolution of M over R, which will have the form

$$0 \to R^n \xrightarrow{A} R^k \to M \to 0$$

where A is an $k \times n$ matrix with entries in m. If we localize at x, we have $M_x = 0$, and so

$$0 \to R_x^n \to R_x^k \to 0$$

is exact. Thus, $k = n$, and A is $n \times n$. Let e_j denote the j th column of the identity matrix I_n. Since $xM = 0$, every xe_j is in the image of A, and so we can write $xe_j = Ab_j$ for a certain $n \times 1$ column matrix b_j over R. Let B denote the $n \times n$ matrix over R whose columns are $b_1, \ldots, b_n$. Then $xI_n = AB$. By the preceding Lemma, B is invertible, and so A and $AB = xI_n$ have the same cokernel, up to isomorphism. But the cokernel of xI_n is $(R/xR)^{\oplus n} \cong M = \mathrm{Coker}\,(A)$, as required. □

We can now prove the result that we are aiming for, which completes the proof of the Theorem stated at the end of the previous lecture.

Theorem. *Let (R, m, K) be a local ring such that $\mathrm{pd}_R K$ is finite. Then R is regular.*

Proof. If $m \in \mathrm{Ass}\,(R)$, then we find that K is free. But $K \cong R^n$ implies that $n = 1$ and R is a field, as required. We use induction on $\dim(R)$. The case where $\dim(R) = 0$ follows, since in that case $m \in \mathrm{Ass}\,(R)$.

Now suppose that $\dim(R) \geq 1$ and $m \notin \mathrm{Ass}\,(R)$. Then m is not contained in m^2 nor any of the primes in $\mathrm{Ass}\,(R)$, and so we can choose $x \in m$ not in m^2 nor in any associated prime. This means that x is not a zerodivisor in R. By the preceding Theorem, the fact that K has finite projective dimension over R implies that it has finite projective dimension over R/xR. By the induction hypothesis, R/xR is regular. Since $x \notin m^2$ and x is not a zerodivisor, both the least number of generators of the maximal ideal and the Krull dimension drop by one when we pass from R to R/xR. Since R/xR is regular, so is R. □

Math 615: Lecture of February 7, 2020

We can give some immediate corollaries of our homological characterization of regular local rings. First note:

Proposition. *Let R be a ring and M an R-module.*

(a) *If $\mathrm{pd}_R M = n$ and S is flat over R, then $\mathrm{pd}_S S \otimes_R M \le n$. In particular, this holds when S is a localization of R.*

(b) *If $(R, m) \to (S, Q)$ is local homomorphism of local rings (i.e., m maps into Q), S is R-flat, M is finitely generated, and $\mathrm{pd}_R M = n$ (whether finite or infinite) then $\mathrm{pd}_S S \otimes_R M = n$.*

Proof. For part (a) take a projective resolution $P_\bullet$ of M. Then $S \otimes_R P_\bullet$ gives a projective resolution of the same length for $S \otimes_R M$: because S is flat, $S \otimes_R \_$ preserves exactness. For part (b), choose $P_\bullet$ to be a minimal projective resolution for M over R, whether finite or infinite. Applying $S \otimes_R \_$ gives a minimal resolution of $S \otimes_R M$: the entries of each matrix occurring in $P_\bullet$ map into Q because the homomorphism is local. The two minimal resolutions have the same length. □

Corollary. *If (R, m) is a regular local ring, then for every prime ideal Q of R, R_Q is regular.*

Proof. $\mathrm{pd}_{R_Q} R_Q/QR_Q \le \mathrm{pd}_R R/Q$ by (a) of the Proposition just above, and so is finite. □

Corollary. *If $(R, m) \to (S, Q)$ is a flat local homomorphism of local rings and S is regular, then R is regular.*

Proof. $\mathrm{pd}_R R/m = \mathrm{pd}_S S \otimes_R (R/m)$ and so is finite, by part (b) of the proposition just above. □

We define a Noetherian ring to be *regular* if all of its local rings at prime ideals are regular. By the first Corollary above, it is equivalent to require that its local rings at maximal ideals be regular.

Corollary. *Over a regular ring of Krull dimension d, $\mathrm{pd}M \le d$ for every finitely generated R-module M.*

Proof. Consider a projective resolution of M by finitely generated projective modules, say $P_\bullet$, and let $M_d = \mathrm{Ker}\,(P_{d-1} \to P_{d-2})$, so that

$$0 \to M_d \to P_{d-1} \to P_{d-2} \to \cdots \to P_1 \to P_0 \to M \to 0$$

is exact. It suffices to prove that M_d is projective. By the Theorem on page 103 the Lecture Notes for Math 614, Fall 2017, projective is equivalent to locally free (and to flat) for finitely generated modules over a Noetherian ring. Localize the sequence at some prime ideal Q of R. Then R_Q is regular of dimension at most d, and so $(M_d)_Q$ is R_Q-free, since it is a dth module of syzygies over a regular local ring of Krull dimension at most d. □

There are regular Noetherian rings of infinite Krull dimension. (Take a polynomial ring in a countably infinite set S of variables over a field K, and partition S into sets $S_1, S_2, \ldots, S_n, \ldots$ such that S_n contains n variables, say $X_{n1}, \ldots, X_{nn}$. Let P_n be the prime ideal generated by the variables in S_n. Let T be the polynomial ring in the variables in S over K, and let $W = T - \bigcup_n P_n$, a multiplicative system. Let $R = W^{-1}T$, and let $Q_n = P_nT$. It is not hard to show that the Q_n are precisely the maximal ideals of R. Moreover it turns out that $R_{Q_n} \cong L_n[X_{n1}, \ldots, X_{nn}]_{m_n}$, where L_n is the field generated over K by the variables in $S - S_n$, and m_n is the homogeneous maximal ideal of the polynomial ring $L_n[X_{n1}, \ldots, X_{nn}]$. Thus, R_{Q_n} is regular of Krull dimension n, and R has infinite Krull dimension. R is Noetherian because every nonzero element is contained in only finitely many of the Q_n. We leave it as an exercise to check that if a ring has the property that its localization at every maximal ideal is Noetherian and every nonzero element is contained in only finitely many maximal ideals, then the ring is Noetherian.)

But even over Noetherian regular rings of infinite Krull dimension, every finitely generated module has finite projective dimension.

Let $R \to S$ be a homomorphism of Noetherian rings, let I be an ideal of R, and choose generators of I, say $I = (x_1, \ldots, x_n)R$. Let M be a finitely generated S-module. In this situation, we want to define the *depth* of of M on I: we let the depth be $+\infty$ if $IM = M$, while if $IM \neq M$, we let it be the length of any maximal regular sequence in I on M. To justify this definition we need to prove that all maximal regular sequences have the same length: in the course of doing so, we shall show that the depth is at most the number of generators of I.

Note first that $IM = M$ iff $IS + \mathrm{Ann}_S M = S$. For $IM = M$ iff $ISM = M$ iff $S/IS \otimes_S M = 0$. Recall:

Proposition. *The support of a tensor product of two finitely generated modules M, N over a Noetherian ring R is the intersection of their supports. Hence, the tensor product is 0 if and only if the sum of the annihilators is the unit ideal.*

Proof. $(M \otimes_R N)_P \cong M_P \otimes_{R_P} N_P$, and by Nakayamas lemma, a finitely generate module A over (R_P, PR_P, κ) is nonzero if and only if $\kappa\otimes)_{R_P} A \neq 0$. But $\kappa \otimes_{R_P} (M_P \otimes_{R_P} N_P) \cong (\kappa \otimes_{R_P} \kappa) \otimes_{R_P} (M_P \otimes_{R_P} N_P) \cong (\kappa \otimes_{R_P} M_P) \otimes_{R_P} (\kappa \otimes_{R_P} N_P)$. Since the tensor product of two vectors spaces over a field is 0 if and only if one of them is 0, this is 0 if and only if $M_P = 0$ or $N_P = 0$, and the statement about supports follows.

Since the support of a finitely generated module is the set of primes containing its annihilator, the final statement fullows. □

Thus, in the situation where depth is taken to be $+\infty$, the Koszul homology $\mathcal{K}_\bullet(\underline{x};\, M)$ all vanishes, since it is killed by $(x_1,\, \ldots\, , x_n)$ and by $\mathrm{Ann}_S M$.

We shall prove very shortly that the length of a maximal regular sequence on M in $I = (x_1,\, \ldots\, , x_n)R$ can be recovered by looking at the number of Koszul homology modules, starting the count with $H_n(\underline{x};\, M)$, that vanish. We prove a preliminary result that does not need any finiteness hypotheses.

Lemma. *Let R be any ring, let $I = (x_1,\, \ldots\, , x_n)R$, and let M be any R-module. Suppose that $f_1,\, \ldots\, , f_d \in I$ is an improper regular sequence on M. Then $H_{n-j}(\underline{x};\, M) = 0$, $0 \leq j < d$. In particular, if $x_1,\, \ldots\, , x_n$ is an improper regular sequence on M, then $H_i(\underline{x};\, M) = 0$ for all $i \geq 1$.*

Proof. We use induction on d. Note that $H_i(\underline{x};\, M) = 0$ for $i \geq n+1$ and any M. If $d = 1$, we use the fact that $H_n(\underline{x};\, M) \cong \mathrm{Ann}_M(x_1,\, \ldots\, , x_n)$: since $f_1 \in I$ is a nonzerodivisor on M, then annihilator vanishes. Now suppose that $d > 1$ and that we know that the result for smaller integers. We have the exact sequence

$$0 \to M \xrightarrow{f_1} M \to M/f_1 M \to 0.$$

In the long exact sequence for Koszul homology, the maps given by multiplication by any element of I, including f_1, are 0. This implies that the long exact sequence can be broken up into short exact sequences:

$$(*_j) \quad 0 \to H_{j+1}(\underline{x};\, M) \to H_{j+1}(\underline{x};\, M/f_1M) \to H_j(\underline{x};\, M) \to 0.$$

But we know that $f_2,\, \ldots\, ,\, f_d$ is a regular sequence on M/f_1M, from which we deduce that $H_{j+1}(\underline{x};\, M/f_1M) = 0$ for all $j+1 > n-(d-1) = n-d+1$, by the induction hypothesis. The result we want now follows at once from the sequences $(*_j)$, since the vanishing of the middle term implies the vanishing of both end terms. □

Theorem (Koszul complex characterization of depth). *Let R, S be Noetherian rings such that S is an R-algebra, let $I = (x_1,\, \ldots\, , x_n)R$, and let M be a Noetherian S-module. If $IM \neq M$ then any regular sequence in I on M has length at most n, and if d is the length of any maximal regular sequence, then $H_{n-j}(\underline{x};\, M) = 0$ for $j < d$, while $H_{n-d}(\underline{x};\, M) \neq 0$. Thus, all maximal regular sequences on M in I have the same length.*

Moreover, $\mathrm{depth}_I M = \mathrm{depth}_{IS} M$.

Proof. We already know from the Lemma that if there is a regular sequence of length d, then $H_{n-j}(\underline{x};\, M) = 0$ for $j < d$. Since $H_0(\underline{x};\, M) = M/IM$ does not vanish here, we immediately see that the length of any regular sequence on M in I is bounded by n. It remains only to show that if $f_1, \ldots , f_d \in I$ is a maximal regular sequence, then $H_{n-d}(\underline{x}; M) \neq 0$.

We use induction on d. If $d = 0$, this means that $(x_1, \ldots, x_d)R$ consists entirely of zerodivisors on M, which means in turn that it is contained in the union of inverse images in R of the associated primes of M in S. Therefore, it is contained in one of these, and there exists $u \in M - \{0\}$ killed by $(x_1, \ldots, x_d)$. But then $u \in Ann_M(x_1, \ldots, x_n)R = H_n(\underline{x};\, M)$. Now suppose that $d > 0$ and we know the result for smaller d. Now we know that $f_2, \ldots, f_d$ is a *maximal* regular sequence on M/f_1M, so that $H_{n-d+1}(\underline{x};\, M/f_1M) \neq 0$. With notation as in the proof of the Lemma, we have for $j = n - d$ an exact sequence:

$$(*_{n-d}) \quad 0 \to H_{n-d+1}(\underline{x};\, M) \to H_{n-d+1}(\underline{x};\, M/f_1M) \to H_{n-d}(\underline{x};\, M) \to 0.$$

We know that $H_{n-d+1}(\underline{x};\, M) = 0$ from the Lemma, and so the other two terms are isomorphic, yielding that $H_{n-d}(\underline{x};\, M) \cong H_{n-d+1}(\underline{x};\, M/f_1M) \neq 0$.

The final statement follows because the Koszul complex of S with respect to the images of the x_j in S is the same as $\mathcal{K}_\bullet(\underline{x};\, M)$ over R. □

Thus, our notion of depth is well-defined. If $(R,\, m)$ is local, $\operatorname{depth} M$ means $\operatorname{depth}_m M$. Some authors ambiguously refer to $\operatorname{depth}_I R$ as $\operatorname{depth} I$, which can lead to confusion in the case where I is an ideal of a local ring, where it might mean $\operatorname{depth}_m I$ with I considered as a module rather than an ideal. We shall not use $\operatorname{depth} I$ for $\operatorname{depth}_I R$.

We are now in a position to prove that a regular domain is normal. We first recall the following characterization of normal Noetherian rings: see, for example, p. 139 of the Lecture Notes for Math 614, Fall 2017. We use the abbreviation "DVR" for a Noetherian discrete valuation domain: this is the same as a regular local ring of dimension one.

Theorem. *Let R be a Noetherian domain. Then R is normal if and only if (1) every associated prime of any nonzero principal ideal has height one, and (2) the localization of R at every height one prime is a DVR. In particular, if R is one-dimensional and local, then R is normal if and only if R is a DVR.*

Theorem. *If R is a regular domain, then R is normal.*

Proof. By the Theorem just above, it suffices to see that an associated prime of a principal ideal has height one, and that the localization at a height one prime is a DVR. To see the first statement, we can localize at such an associated prime. Then we have a regular local ring $(R,\, m)$ such that one nonzero element gives a maximal regular sequence in m on R. Take $x \in m - m^2$. Since all maximal regular sequences have the same length, x also gives a maximal regular sequence. But R/xR is a domain, and so this can only be true if $m = xR$ is maximal. Finally, a one-dimensional regular ring has a maximal ideal that is generated by one element, and so it must be a DVR. □

Math 615: Lecture of February 10, 2020

We discuss a method for determining the ideal of all leading forms of an ideal generated by polynomials with constant term zero in a formal power series ring $K[[x_1, \ldots, x_n]]$ over a field K.

Suppose that

$$f_1, \ldots, f_h \in m = (x_1, \ldots, x_n)R,$$

where $R = K[[x_1, \ldots, x_n]]$, a formal power series ring. Let $I = (f_1, \ldots, f_h)$. To find

$$\mathcal{L}(I) \subseteq \mathrm{gr}_m R \cong K[x_1, \ldots, x_n],$$

first note that if $g \neq 0, g_1, \ldots, g_n \in R$ are such that $g = \sum_{i=1}^m f_i g_i$, and $\deg \mathcal{L}(g) = d$, then $\mathcal{L}(g)$ is unchanged if we drop all terms of degree $> d$ from the g_i, although the value of g changes. Thus, we may assume that the $g_i \in K[x_1, \ldots, x_n] \subseteq R$. There is a K-homomorphism

$$\Theta : K[x_1, \ldots, x_n] \to K[t, x_1, \ldots, x_n] = B$$

with $x_i \mapsto x_i t$. Let $f^{\diamondsuit}$ denote $\Theta(f)$. Then $g^{\diamondsuit} = t^d G$, where $G|_{t=0} = \mathcal{L}(g)$. In other words, when $g^{\diamondsuit}$ is regarded as a polynomial in t, its constant term is $\mathcal{L}(g)$.

Let

$$J_s = (f_1^{\diamondsuit}, \ldots, f_n^{\diamondsuit}) :_B t^s.$$

The argument above shows that every leading form of an element of I is the constant term of some element of J_s for some s. Note that the ideals J_s ascend with s and so are eventually all equal. The converse is also true: if $t^s G \in (f_1^{\diamondsuit}, \ldots, f_h^{\diamondsuit})B$, we may substitute $t = 1$ to obtain that $G(1, x_1, \ldots, x_n) \in (f_1, \ldots, f_n)K[x_1, \ldots, x_n]$, and it follows that the constant term of G when viewed as a polynomial in t is in $\mathcal{L}(I)$.

Therefore, to get generators of $\mathcal{L}(f_1, \ldots, f_m)$, think of the generators of J_s for s sufficiently large as polynomials in t and take their constant terms.

Evidently, $tu \in J_s$ iff $t^s(tu) \in (f_1^{\diamondsuit}, \ldots, f_n^{\diamondsuit}) = J_0$, and so $J_{s+1} = J_s :_B t$. Therefore, the sequence J_s is stable as soon as $J_s = J_{s+1}$ for one value of s, for then t is not a zerodivisor on J_s. We indicate how to find J_{s+1} once J_s is known. Suppose that $a_1, \ldots, a_k \in B$ are generators in J_s. Then the elements b of J_{s+1} are those that satisfy $bt = \sum_{j=1}^k q_j a_j$ for some choice of q_j. If we have a set of generators for the relations on t, $a_1, \ldots, a_k$, the coefficients of t will generate J_{s+1}. In considering such relations, if $q_j = Q_j + tH_j$ where $Q_j \in K[x_1, \ldots, x_n]$, then we have

$$(b - \sum_{j=1}^k H_j a_j)t = \sum_{j=1}^k Q_j a_j.$$

Since $\sum_{j=1}^k H_j a_j \in J_s$, the additional generators for J_{s+1} over J_s all come from relations $b't = \sum_{j=1}^k Q_j a_j$ where the $Q_j \in K[x_1, \ldots, x_n]$. Let $a_j = A_j + tW_j$ with $A_j \in K[x_1, \ldots, x_n]$. Then the Q_j must give a relation on the A_j. Each relation on the A_j gives rise to a value of b', and we get generators for J_{s+1} if we take the generators of J_s and those values of b' coming from generators for the relations on the A_j in $K[x_1, \ldots, x_n]$.

We now consider the specific example in $K[[x,y,z]]$ where $f_1 = x^2 - y^3 + z^6$ and $f_2 = xy - z^3$.

Then $(x^2 - y^3 + z^6)^\diamondsuit = t^2 a$ for $a = x^2 - ty^3 + t^4 z^6$ and $(xy - z^3)^\diamondsuit = t^2 b$ for $b = xy - tz^3$, and so $a, b \in J_2$. Then $ya - xb = tc$ (using the obvious generator for the relations on x^2, xy) where $c = -y^4 + xz^3 + t^3 yz^6 \in J_3$. We will show that t is not a zerodivisor mod $(a, b, c) = J_3$. The constant terms of a, b, c are x^2, xy, $-y^4 + xz^3$. Clearly, in any relation $Q_1 x^2 + Q_2 xy + Q_3(-y^4 + xz^3) = 0$, we must have that $x \mid Q_3$. One such relation is $(-z^3, y^3, x)$. Given any other, we can subtract a multiple of $(-z^3, y^3, x)$ from it so as to make $Q_3 = 0$. This leaves a relation of the form $(Q_1', Q_2', 0)$, which is essentially a relation on x^2, xy, and so must be a multiple of $(y, -x, 0)$. That is, $(y, -x, 0)$ and $(-z^3, y^3, x)$ span the relations. $ya - xb$ gives nothing new, while

$$-z^3 a + y^3 b + xc = ty^3 z^3 - t^4 z^9 - ty^3 z^3 + t^3 xyz^6 = t^3 xyz^6 - t^4 z^9 = t^3 z^6 b,$$

and so $t^2 z^6 b \in J_4$. Since $b \in J_2 \subseteq J_3$, $J_4 = J_3$ and t is not a zerodivisor on $(a, b, c) = J_3$. This shows that $\mathcal{L}(I) = (x^2,\, xy,\, -y^4 + xz^3)$.

Example. When the leading form of f in $\mathrm{gr}_m R$ is L and one kills an ideal $\mathfrak{A} \subseteq m$, even if it is principal, it need not be true that the leading form of the image $\overline{f}$ in $\mathrm{gr}_{\overline{m}}(R/I)$ is the image of L. For example, suppose that $R = K[[x,y,z]]$ with $f = xy + y^{101}z^{997}$. The leading form of f is xy. But in the quotient R/xR, the leading form of the image of f is $y^{101}z^{997}$.

Our next goal is to prove a famous theorem of Auslander and Buchsbaum connecting depth and projective dimension. We first want to observe some basic facts about the behavior of depth.

Proposition. *Let $R \to S$ be a homomorphism of Noetherian rings, let M be a finitely generated S-module, and let I be an ideal of R. Let I and J be ideals of R.*

(a) *Let T be a flat Noetherian S-algebra. Then* $\mathrm{depth}_I T \otimes_S M \geq \mathrm{depth}_I M$*, with equality if T is faithfully flat. In particular, depth can only increase if T is a localization of S.*

(b) $\mathrm{depth}_I M = \inf_{Q \in \mathrm{Supp}\,_S(M/IM)} \mathrm{depth}_I M_Q = \inf_{Q \in \mathrm{Spec}\,(S)} \mathrm{depth}_I M_Q$. *(The infimum of the empty set is defined to be $+\infty$.)*

(c) *If I and J have the same radical,* $\mathrm{depth}_I M = \mathrm{depth}_J M$.

Proof. (a) Let $I = (x_1, \dots, x_n)$. Then for all j,

$$H_j(\underline{x};\, T \otimes_S M) \cong T \otimes_S H_j(\underline{x}; M),$$

since T is S-flat. Thus, the number of vanishing Koszul homology modules cannot decrease when we tensor with T. Moreover, if T is faithfully flat, neither can it increase. Note that the case of infinite depth corresponds to the case where all Koszul homology vanishes.

(b) By part (a), localizing can only increase the depth. It suffices to show that if $M \neq IM$, we can localize at a prime while preserving the depth. Let $f_1, \dots, f_d$ be a maximal regular sequence in I on M. Then $M/(f_1, \dots, f_d)M$ has depth 0, and so I is contained in the union of the inverse images of the finitely many primes in $\mathrm{Ass}\,_S\bigl(M/(f_1, \dots, f_d)M\bigr)$. Thus, it is contained in the inverse image of one of these primes: call it Q. Replace M by M_Q. We still have $QS_Q \in \mathrm{Ass}\,_S\bigl((M/(x_1, \dots, x_n)M)_Q\bigr)$, and so $f_1, \dots, f_d \in I$ is a maximal regular sequence on M_Q.

(c) It suffices to consider the case where J is the radical of I. A regular sequence in I is automatically a regular sequence in J. Given a regular sequence $f_1, \dots, f_d$ in J, each f_j has a power $f_j^{N_j} \in I$. By the final problem of Problem Set #3, $f_1^{N_1}, \dots, f_d^{N_d}$ is a regular sequence on M in I. □

The next result is very similar to the Proposition at the top of the second page of the Notes from February 5, and its proof is very similar, although Koszul homology is used instead of $\mathrm{Tor}^R_\bullet(\_\,, K)$.

Proposition. *Let $R \to S$ be a homomorphism of Noetherian rings, let*

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

be an exact sequence of finitely generated S-modules, and let I be an ideal of R. The following statements hold, even if one or more of the depths is $+\infty$ (with the conventions $+\infty \pm 1 = +\infty$ and if $u \in \mathbb{N} \cup \{+\infty\}$, $\min\{u, +\infty\} = u$).

(a) $\mathrm{depth}_I M_1 \geq \min\{\mathrm{depth}_I M_0,\, \mathrm{depth}_I M_2\}$.

(b) *If*

$$\mathrm{depth}_I M_1 > \mathrm{depth}_I M_0,$$

then

$$\mathrm{depth}_I M_2 = \mathrm{depth}_I M_0 + 1.$$

If $\mathrm{depth}_I M_1 \leq \mathrm{depth}_I M_0$, *then* $\mathrm{depth}_I M_2 \geq \mathrm{depth}_I M_1$.

(c) $\mathrm{depth}_I M_0 \geq \min\{\mathrm{depth}_I M_1, \mathrm{depth}_I M_2 - 1\}$.

Proof. Let $x_1, \dots, x_s$ denote generators of the ideal I and consider the long exact sequence for Koszul homology:

$$\cdots \to H_{n+1}(\underline{x};\, M_1) \to H_{n+1}(\underline{x};\, M_0) \to H_n(\underline{x};\, M_2)$$

$$\to H_n(\underline{x};\, M_1) \to H_n(\underline{x};\, M_0) \to \cdots$$

If M_2 has infinite depth, then $H_n(\underline{x};\, M_1) \cong H_n(\underline{x};\, M_0)$ for all n, so that M_1 and M_0 have the same depth, and all of (a), (b), (c) hold. If M_1 has infinite depth, then $H_{n+1}(\underline{x};\, M_0) \cong H_n(\underline{x};\, M_2)$ for all n and $\mathrm{depth}_I M_2 = \mathrm{depth}_I M_0 + 1$. Again, all three statements hold. If M_0 has infinite depth then $H_n(\underline{x};\, M_2) \cong H_n(\underline{x};\, M_1)$ for all n, and $\mathrm{depth}_I M_2 = \mathrm{depth}_I M_1$. Again, all three statements hold. We may assume that all three depths are finite.

Part (a) follows from the long exact sequence because of $H_n(\underline{x};\, M_2) = 0 = H_n(\underline{x};\, M_0)$ for all $n > d$, then $H_n(\underline{x};\, M_1) = 0$ for all $n > d$. All of the other statements follow similarly from the long exact sequence for Koszul homology: each of the Koszul homology modules one needs to vanish is surrounded by two Koszul homology modules that vanish from the hypothesis. For the equality in part (b), let $d = \mathrm{depth}_I M_0$. We must show as well that $H_{s-(d+1)}(\underline{x};\, M_2) \neq 0$. Let $n = s - d - 1$ in the long exact sequence, which becomes:

$$\cdots \to 0 \to H_{s-d}(\underline{x};\, M_0) \to H_{s-d-1}(\underline{x};\, M_2) \to \cdots$$

and we know that $H_{s-d}(\underline{x};\, M_0) \neq 0$. □

The following result sharpens the result of the second Lemma on the third page of the notes from February 5.

Lemma. *If (R, m, K) is local, M is a finitely generated nonzero R-module, $\mathrm{pd}_R M$ is finite, and $x \in m$ is a nonzerodivisor on R and on M, then $\mathrm{pd}_{R/xR} M/xM = \mathrm{pd}_R M$.*

Proof. Take a minimal resolution $P_\bullet$ of M over R. As in the proof of that Lemma, $R/xR \otimes_R P_\bullet$ is a resolution of M/xM over R/xR, but now we note that it is minimal, so that the projective dimension does not change. □

Theorem (M. Auslander and D. Buchsbaum). *Let $(R,\, m,\, K)$ be local and $M \neq 0$ a finitely generated R-module. If M has finite projective dimension then*

$$\mathrm{pd}_R M + \mathrm{depth}\, M = \mathrm{depth}\, R.$$

Proof. If the depth of R is 0, then M is free, by the first Lemma on the fourth page of the Notes from February 5, and the result is clear. If the $\mathrm{depth} R > 0$, and $\mathrm{depth}\, M > 0$ as well, the maximal ideal of R is not contained in the union of all associated primes of R and of M. Thus, we can choose $x \in m$ that is not in any associated prime of M or of R, and so x is a nonzerodivisor on both R and M. By the Lemma just above, $\mathrm{pd}_{R/xR} M/xM = \mathrm{pd}_R M$, and by the induction hypothesis this is

$$\mathrm{depth}\, R/xR - \mathrm{depth}\, M/xM = \mathrm{depth}\, R - 1 - (\mathrm{depth}\, M - 1) = \mathrm{depth}\, R - \mathrm{depth}\, M,$$

as required. If the depth of R is positive and the depth of M is 0, form a short exact sequence

$$0 \to M' \to R^b \to M \to 0,$$

so that M' is a first module of syzygies of M. Then M' will have depth $0+1=1$ by part (b) of the preceding Proposition, while $\operatorname{pd} M' = \operatorname{pd} M - 1$. Working with M' we have that both $\operatorname{depth} R$ and $\operatorname{depth} M'$ are positive, and so we are in a case already done. Thus,

$$\operatorname{pd} M = \operatorname{pd} M' + 1 = (\operatorname{depth} R - \operatorname{depth} M') + 1 = \operatorname{depth} R - 1 + 1 = \operatorname{depth} R,$$

as required, since $\operatorname{depth} M = 0$. □

Math 615: Lecture of February 12, 2020

We review some basic facts about the tensor and exterior algebras of a module over a commutative ring R.

The tensor product of n copies of M with itself is denoted $M^{\otimes n}$ or $T^n_R(M) = T^n(M)$. By convention, $T^0(V) = R$. Then

$$T(M) = \bigoplus_{n=0}^{\infty} T^n(M)$$

becomes an associative (usually non-commutative) $\mathbb{N}$-graded ring with identity, with R in the center: the multiplication is induced by the obvious bilinear maps

$$T^m(M) \otimes_R T^n(M) \to T^{m+n}(M)$$

(each of these maps is an isomorphism). Note that this *tensor algebra* is generated as a ring over R by $T^1(M)$, which we may identify with M. Of course, $T^n(M)$ is the degree n component. Note that if $L : M \to N$ is an R-linear map, there is an induced map $T^n(L) : T^n(M) \to T^n(N)$, and $T^n(L' \circ L) = T^n(L') \circ T^n(L)$ when the composition $L' \circ L$ is defined. Together these maps give a degree preserving ring homomorphism $T(M) \to T(N)$, which is surjective whenever L is. T is a covariant functor from R-modules to $\mathbb{N}$-graded associative R-algebras such that R is in the center. Moreover, T has the following universal property: if $f : M \to S$ is any R-linear map of the R-module M into an associative R-algebra S with R in the center, then f extends uniquely to an R-linear ring homorphism $T(M) \to S$.

An R-multilinear map $M^n \to N$ is called *alternate* or *alternating* if its value is 0 whenever two entries of an n-tuple are equal. (This implies that switching two entries negates the value. Making an even permutation of the entries will not change the value, while an odd permutation negates the value.) Let $\bigwedge^n_R(M) = \bigwedge^n(M)$ denote the quotient of $M^{\otimes n}$ by the subspace spanned by all n-tuples two of whose entries are equal. We make the convention that $\bigwedge^0 R \cong R$, and note that we may identify $M \cong \bigwedge^1 M$. Then

$$\bigwedge(M) = \bigoplus_{n=0}^{\infty} \bigwedge^n(M)$$

is an associative $\mathbb{N}$-graded algebra with R in the center, with $\bigwedge^n(M)$ as the component in degree n. $\bigwedge(M)$ is called the *exterior algebra* of M over R, and $\bigwedge^n(M)$ is called the nth *exterior power* of M over R. One can also construct $\bigwedge(M)$ by killing the two-sided ideal of $T(M)$ generated by elements of the form $u \otimes u$, $u \in M$.

The multiplication on $\bigwedge(M)$ is often denoted $\wedge$. If the elements u_j span M, then the elements $u_{j_1} \wedge \cdots \wedge u_{j_i}$ span $\bigwedge^i(M)$. If v has degree m and w has degree n, then one can easily check that $v \wedge w = (-1)^{mn} w \wedge v$. Thus, the even degree elements are all in the center, while any two odd degree elements anti-commute. If G is free with free basis $u_1, \ldots, u_n$, then the elements $u_{j_1} \wedge \cdots \wedge u_{j_i}$, $1 \le j_1 < \cdots < j_i \le n$ form a free basis for $\bigwedge^i(G)$, and $\bigwedge^i(G)$ has rank $\binom{n}{i}$. In particular, $\bigwedge^N(G) = 0$ if $N >$ rank G (or, more generally, if G is not necessarily free but is spanned by fewer than N elements).

Given a linear map $L : M \to N$, there is an induced map $\bigwedge^n(L) : \bigwedge^n(M) \to \bigwedge^n(N)$, and $\bigwedge^n(L' \circ L) = \bigwedge^n(L) \circ \bigwedge^n(L')$ when the composition $L' \circ L$ is defined. Together these maps give a ring homomorphism of $\bigwedge(M) \to \bigwedge(N)$ that preserves degrees. Thus, $\bigwedge$ is a covariant functor from R-modules to graded associative R-algebras with R in the center.

An associative $\mathbb{N}$-graded R-algebra Λ such that R maps into the center of Λ and also into Λ_0 is called *skew-commutative* (or even *commutative* by some authors!) if whenever $u, v \in \Lambda$ are homogeneous,

$$uv = (-1)^{\deg(u)\deg(v)} vu$$

in Λ. Then $\bigwedge(M)$ has the following universal property: if Λ is any skew-commutative R-algebra and $\theta : M \to \Lambda_1$ any R-linear map, θ extends uniquely to a degree-preserving R-homomorphism $\bigwedge(M) \to \Lambda$.

If G is free of rank n with basis $u_1, \ldots, u_n$ and $L : G \to G$ has matrix α, then $\bigwedge^n(L) : \bigwedge^n G \to \bigwedge^n G$ sends $u_1 \wedge \cdots \wedge u_n$ to $\det(\alpha) u_1 \wedge \cdots \wedge u_n$. To see this, note that we have that

$$\bigwedge^n(u_1 \wedge \cdots \wedge u_n) = (a_{11}u_1 + \cdots + u_{n1}v_n) \wedge \cdots \wedge (u_{n1}v_1 + \cdots + a_{nn}u_n).$$

Expanding by the generalized distributive law yields n^n terms each of which has the form $a_{i_1,1} \cdots a_{i_n,n} u_{i_1} \wedge \cdots \wedge u_{i_n}$. If two of the i_t are equal, this term is 0. If they are all distinct, the v_{i_t} constitute all the elements $u_1, \ldots, u_n$ in some order: call the corresponding permutation σ. Rearranging the v_j gives $\mathrm{sgn}\,(\sigma) a_{i_1,1} \cdots a_{i_n,n} v_1 \wedge \cdots \wedge v_n$. The sum of all of the $n!$ surviving terms is $\det(\alpha) v_1 \wedge \cdots \wedge v_n$, using one of the standard definitions of $\det(\alpha)$. The fact that the determinant of a product of two $n \times n$ matrices is the product of the determinants may be deduced from the fact that $\bigwedge^n$ preserves composition.

Note also that if $M \to N$ is surjective, then $\bigwedge^n M \to \bigwedge^n N$ is surjective for all n. It is straightforward to check that if $R \to S$ is any map of commutative rings, there is an isomorphism

$$S \otimes_R \textstyle\bigwedge_R^n M \to \bigwedge_S^n (S \otimes_R M).$$

The map $M \to S \otimes M$ sending $u \mapsto 1 \otimes u$ induces a degree-preserving map

$$\textstyle\bigwedge_R M \to \bigwedge_S^n (S \otimes_R M),$$

and hence a map

$$S \otimes_R \textstyle\bigwedge_R M \to \bigwedge_S^n (S \otimes_R M).$$

On the other hand $S \otimes \bigwedge_R M$ is $S \otimes_R M$ in degree 1, giving an S-linear map of $S \otimes_R M$ into the degree one part of $S \otimes \bigwedge_R M$, and this yields a map

$$\textstyle\bigwedge_S^n (S \otimes_R M) \to S \otimes_R \bigwedge_R M,$$

using the appropriate universal mapping properties. These maps are easily checked to be mutually inverse degree-preserving S-algebra isomorphisms, under which

$$(s_1 \otimes u_1) \wedge \cdots \wedge (s_n \otimes u_n) \in \textstyle\bigwedge_S^n (S \otimes_R M)$$

corresponds to

$$(s_1 \cdots s_n) \otimes (u_1 \wedge \cdots \wedge u_n) \in S \otimes \textstyle\bigwedge_R M.$$

In particular, localization commutes with the formation of exterior algebras and exterior powers.

We have previously introduced $\mathcal{K}_i(x_1, \ldots, x_n;\, R)$ with a free R-basis consisting of elements $u_{j_1, \ldots, j_i}$ where $1 \le j_1 < \cdots < j_i \le n$. In particular, $u_1, \ldots, u_n$ is a free basis for $\mathcal{K}_1(x_1, \ldots, x_n;\, R)$. It turns out to be convenient to think of $\mathcal{K}_i(x_1, \ldots, x_n;\, R)$ as $\bigwedge^i(G)$, where $G = \mathcal{K}_1(x_1, \ldots, x_n;\, R)$ is the free module on n generators, letting $u_{j_1, \ldots, j_i}$ correspond to $u_{j_1} \wedge \cdots \wedge u_{j_i}$. We obviously have isomorphisms of the relevant free R-modules. We still have $d(u_j) = x_j$, $1 \le j \le n$. The formula for the differential d is

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

We shall refer to an R-linear map of a graded skew-commutative R-algebra Λ into itself that lowers degrees of homogeneous elements by one and satisfies

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

when u is a form as an *R-derivation.*

Once we identify $\mathcal{K}(x_1, \ldots, x_n;\, R)$ with $\bigwedge(G)$, the differential R is a derivation. By the R-bilinearity of both sides in u and v, it suffices to verify $(\#)$ when $u = u_{j_1} \wedge \cdots u_{j_h}$

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

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

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

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

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

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

For example, if the sequence of elements is $x_1, \ldots, x_n$ and we compose the map $R^n \to R$ these elements give with the automorphism of $R^n \to R^n$ with matrix A, where A is an invertible $n \times n$ matrix (this is equivalent to taking a new free basis for R^n), we get the Koszul complex of a new sequence of elements $y_1, \ldots, y_n$, the elements of the row $Y = XA$ where $X = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix}$ and $Y = \begin{pmatrix} y_1 & \ldots & y_n \end{pmatrix}$. Since this amounts to using the same map $R^n \to R$ with a new free basis for R^n, the Koszul complex we get from Y is isomorphic to that we get from X, and its homology is the same.

Another, nearly equivalent, point of view is that the isomorphism $A : R^n \to R^n$ extends to an isomorphism $\mathcal{K}_\bullet(y_1,\, \dots\,, y_n;\, R) \cong \mathcal{K}_\bullet(x_1,\, \dots\,, x_n;\, R)$: in degree i, we have the map $\bigwedge^i(A) : \bigwedge^i(R^n) \cong \bigwedge^i(R^n)$. The commutativity of the squares is easily checked. Notice that for $i = 0,\, 1$ we have the diagram:

$$\begin{tikzcd}
R^n \arrow[r, "Y"] \arrow[d, "A"'] & R \arrow[r] \arrow[d, "\text{id}"] & 0 \arrow[d] \\
R^n \arrow[r, "X"'] & R \arrow[r] & 0
\end{tikzcd}$$

In particular, permuting the x_i, multiplying them by units, and adding a multiple of one of the x_i to another are operations that do not change the Koszul complex nor Koszul homology, up to isomorphism. In the local case, any two sets of generators of an ideal such that the two sets have the same cardinality are equivalent via the action of an invertible matrix.

To see this, note that if the set of generators is not minimal we can pick a subset that is minimal and subtract sums of multiples of these from the redundant generators to make them 0. Therefore it suffices to consider the case of two minimal sets of generators $x_1,\, \dots\,, x_n$ and $y_1,\, \dots\,, y_n$. We can choose an $n \times n$ matrices A, B over the local ring (R, m, K) such that $Y = XA$ (since the x_i generate) and such that $X = YB$ (since the y_i generate). Then $X = XAB$, so that $X(I - AB) = 0$. Every column of $I - AB$ is a relation on the x_j, and since these are minimal generators the coefficients in any relation are in m. Thus, $I - AB$ has all entries in m, and working mod m, $I - AB \equiv 0$, so that A is invertible modulo m. This implies that its determinant of A is nonzero mod m, and so is a unit of R. But then A is invertible over R. $\square$

The exterior algebra point of view enables us to define the Koszul complex of a map $\theta : P \to R$, where P is a finitely generated projective module that is locally free of constant rank n. Note that P is a homomorphic image of a finitely generated free module G, and the map $G \twoheadrightarrow P$ will split, so that P is finitely presented. Recall that projective is equivalent to locally free for finitely presented modules: see the Theorem on page 103 of the Math 614, Fall 2017 Lecture Notes. The exterior powers $\bigwedge^i(P)$ of P are likewise projective and locally free of constant rank $\binom{n}{i}$, $0 \leq i \leq n$, since the formation of exterior powers commutes with localization. They are also finitely generated and therefore finitely presented. We need to define a map $\bigwedge^i(P) \to \bigwedge^{i-1}(P)$ for every i, and this map is an element of $\mathrm{Hom}_R(\bigwedge^i(P),\, \bigwedge^{i-1}(P))$. Note that $\mathrm{Hom}(\bigwedge^i(P),\, \_)$ commutes with localization here, because $\bigwedge^i(P)$ is finitely presented. We have a unique way of defining these maps if we localize so that P becomes free (this can be achieved on a Zariski open neighborhood of every point: this is the content of problem **5.(a)** in Problem Set #3, and this construction commutes with further localization. Therefore, unique maps exist globally that give a differential for $\mathcal{K}_\bullet(\theta;\, R)$, by the Theorem on the first page of the Math 614 Lecture Notes of November 26. We note that if $f : P \to P$ is an endomorphism of a finitely generated projective module P, we can use the same idea to define a trace and determinant for f, which will agree with the usual ones coming from a matrix for f once we have localized sufficiently that P becomes free.

We want to develop some further sequences associated with Koszul complexes, and we shall make use of the long exact sequence associated with a *mapping cone*, which we describe next.

Given a map $\phi_\bullet : B_\bullet \to A_\bullet$ of complexes, we can associate with it a double complex with two nonzero rows (thought of as indexed by 1 and 0):

$$\begin{tikzcd}
\cdots \arrow[r] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & B_{n+1} \arrow[r] \arrow[d, "\phi_{n+1}"'] & B_n \arrow[r] \arrow[d, "\phi_n"'] & B_{n-1} \arrow[r] \arrow[d, "\phi_{n-1}"'] & \cdots \\
\cdots \arrow[r] & A_{n+1} \arrow[r] \arrow[d] & A_n \arrow[r] \arrow[d] & A_{n-1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

The total complex is called the *mapping cone* of $\phi_\bullet$. The bottom row $A_\bullet$ is a subcomplex. The quotient complex is the top row $B_\bullet$ with degrees shifted down by one. Thus, if $C_\bullet$ is the mapping cone we have the short exact sequence

$$0 \to A_\bullet \to C_\bullet \to B_{\bullet_{-1}} \to 0$$

and so we get

$$\cdots \to H_n(A_\bullet) \to H_n(C_\bullet) \to H_{n-1}(B_\bullet) \to H_{n-1}(A_\bullet) \to \cdots .$$

The connecting homomorphism is easily checked to be given, up to sign, by

$$\phi_{n-1_*} : H_{n-1}(B_\bullet) \to H_{n-1}(A_\bullet).$$

To see this, we choose a cycle $z \in B_{n-1}$. We lift this to the element $0 \oplus z \in C_n = A_n \oplus B_{n-1}$ that maps to z, and now take the image of $0 \oplus z$ in $A_{n-1} \oplus B_{n-2}$, which is $\pm\phi_{n-1}(z) \oplus 0$, and pull this back to $\pm\phi_{n-1}(z) \in A_{n-1}$, which gives the required result.

We now apply this to the Koszul complex $\mathcal{K}(\underline{x};\, M)$, where $\underline{x} = x_1, \ldots, x_n$. Let $\underline{x}^- = x_1, \ldots, x_{n-1}$. Then

$$\mathcal{K}_\bullet(x_1, \ldots, x_n;\, M) = \mathcal{T}_\bullet\big(\mathcal{K}_\bullet(\underline{x}^-;\, R) \otimes \mathcal{K}_\bullet(x_n;\, R)\big) \otimes M \cong \mathcal{T}_\bullet\big(\big(\mathcal{K}_\bullet(\underline{x}^-;\, M) \otimes \mathcal{K}_\bullet(x_n;\, R)\big)$$

which is the mapping cone of the map from $\mathcal{K}_\bullet(\underline{x}^-;\, M)$ to itself induced by multiplication by x_n on every module. The long exact sequence of the mapping cone gives

$$H_n(\underline{x}^-;\, M) \xrightarrow{\pm x_n} H_n(\underline{x}^-;\, M) \to H_n(\underline{x};\, M) \to H_{n-1}(\underline{x}^-; M) \xrightarrow{\pm x_n} H_{n-1}(\underline{x}^-;\, M)$$

which in turn implies:

Theorem. *Let M be any R-module and $x_1, \ldots, x_n$ any sequence of elements of R. Let $\underline{x}$ denote $x_1, \ldots, x_n$ and $\underline{x}^-$ denote $x_1, \ldots, x_{n-1}$. Then for every i there is a short exact sequence:*

$$0 \to H_n(\underline{x}^-;\, M)/xH_n(\underline{x}^-;\, M) \to H_n(\underline{x};\, M) \to \mathrm{Ann}_{H_{n-1}(\underline{x}^-;M)}x_n \to 0.$$

Proof. This is immediate from the long exact sequence above. □

We next note that if R is $\mathbb{N}$ graded and the x_i are homogeneous, then $\mathcal{K}_\bullet(\underline{x};\, R)$ can be $\mathbb{N}$-graded with differentials that preserve degree. Moreover, if M is $\mathbb{Z}$-graded but $[M]_k$ is 0 for $k \ll 0$, then $\mathcal{K}_\bullet(\underline{x};\, M)$ is $\mathbb{Z}$-graded with differentials that preserve degree, and all of the modules occurring are 0 in all sufficiently low negative degrees. This property will also pass to all graded quotients of their graded submodules, and, in particular, every $H_i(\underline{x};\, M)$ will have the property that all modules it is zero in all sufficiently low negative degrees.

To see this, note that if A, B are $\mathbb{Z}$-graded R-modules that are 0 in low degree, we may grade $A \otimes_R B$ by letting $[A \otimes_R B]_k$ be the span of all $a \otimes b$ such that $a \in A_i$ and $b \in B_j$ for some choice of i and j such that $i + j = k$. This gives a $\mathbb{Z}$-grading that vanishes in low degree: if $A_i = 0$ for $i < c$ and $B_j = 0$ for $j < d$, then $[A \otimes_R B]_k = 0$ for $k < c + d$. Next, note that if x_i has degree d_i, $1 \le i \le n$, then $\mathcal{K}_\bullet(x_i;\, R)$ may be thought of as $0 \to R(-d_i) \xrightarrow{x_i} R \to 0$, and this is graded with degree-preserving differentials. The general Koszul complex is constructed by tensoring these together, and then tensoring with M. Note that $R(-d) \otimes_R R(-e) \cong R(-d-e)$ as graded modules, and that $R(-d) \otimes_R M \cong M(-d)$ as graded modules. It follows that $\mathcal{K}_i(\underline{x};\, M)$ is the direct sum of all the modules $M\bigl(-(d_{j_1} + \cdots + d_{j_i})\bigr)$ for $1 \le j_1 < \cdots < j_i \le n$.

Theorem. *Suppose that the R-module $M \neq 0$, and either that (1) M is $\mathbb{Z}$-graded over the $\mathbb{N}$-graded ring R, with all sufficiently small negative graded pieces of M equal to 0, and that $x_1, \ldots, x_n$ are forms of positive degree, or (2) that (R, m, K) is local, M is finitely generated, and that $x_1, \ldots, x_n \in m$. Let $I = (x_1, \ldots, x_n)R$. Then the following conditions are equivalent:*

(1) $H_1(\underline{x};\, M) = 0$.

(2) $H_i(\underline{x};\, M) = 0$ *for all* $i \ge 1$.

(3) *In the case where R and M are Noetherian,* $\mathrm{depth}_I M = n$.

(4) *The elements $x_1, \ldots, x_n$ form a regular sequence on M.*

Proof. The hypothesis implies that $IM \neq M$, by the local or graded form of Nakayama's lemma. We know that (2) and (3) are equivalent in the case where the ring and module are Noetherian. We also know that (4) ⇒ (2) ⇒ (1). It will therefore suffice to show that (1) ⇒ (4). We use induction on n. The case $n = 1$ is obvious, since $H_1(x_1;\, M) = \mathrm{Ann}_M x_1$. Suppose that the result is known for $n - 1$ elements, $n \ge 2$.

Taking $i = 1$ in the preceding Theorem we have a short exact sequence

$$0 \to H_1(\underline{x}^-;\, M)/x_n H_1(\underline{x}^-;\, M) \to H_1(\underline{x};\, M) \to \mathrm{Ann}_{H_0(\underline{x}^-;\, M)} x_n \to 0.$$

Assume that the middle term vanishes. Then all three terms vanish, and so

$$H_1(x_1,\, \ldots\, , x_{n-1}; M) = x_n H_1(x_1,\, \ldots\, , x_{n-1}; M).$$

By Nakayama's lemma, $H_1(x_1,\, \ldots\, , x_{n-1}; M) = 0$, which shows, using the induction hypothesis, that $x_1,\, \ldots\, , x_{n-1}$ is a regular sequence on M. The vanishing of the rightmost term shows that x_n is not a zerodivisor on

$$H_0(x_1,\, \ldots\, , x_{n-1}; M) \cong M/(x_1,\, \ldots\, , x_{n-1})M.$$

Therefore, $x_1,\, \ldots\, , x_n$ is a regular sequence on M, as required. □

Math 615: Lecture of February 14, 2020

We note two important consequences of the final Theorem of the Lecture of February 12.

Corollary. *Under the same hypothesis as for the preceding Theorem (i.e., in certain graded and local situations) a regular sequence $x_1,\, \ldots\, , x_n$ on M is permutable. In other words, if the elements form a regular sequence in one order, they form a regular sequence in every order.*

Proof. Permuting $x_1,\, \ldots\, , x_n$ can be viewed as the result of an action of an invertible matrix — an appropriate permutation matrix. By the results of the preceding lecture, the Koszul homology is not affected by such a permutation. But $x_1,\, \ldots\, , x_n$ is a regular sequence on M if and only if $H_1(x_1,\, \ldots\, , x_n;\, M) = 0$, by the Theorem cited. □

This result can also be proved by elementary means. It suffices to show that any two consecutive elements in the regular sequence can be switched: every permutation can be built up this way. One can work modulo the predecessors of the pair being switched, and so we may assume that the elements are the first two, say x_1, x_2. It is easy to see that it suffices to show that x_2, x_1 is a regular sequence, since $M/(x_1,\, x_2)M = M/(x_2, x_1)M$. The only hard step is to show that x_2 is not a zerodivisor on M. This still requires some form of Nakayama's lemma to hold. The statement that if x_1, x_2 is a regular sequence on M then x_1 is not a zerodivisor on M/x_2M always holds.

Corollary. *Let M be a Noetherian R-module and $\underline{x} = x_1, \ldots, x_n \in R$. If $H_i(\underline{x};\, M) = 0$ for some i then $H_j(\underline{x};\, M) = 0$ for all $j \geq i$.*

Proof. We may replace R by $R/\mathrm{Ann}_R M$ without affecting the Koszul complex or its homology. Therefore, we may assume that R is Noetherian. Let $X_1, \ldots, X_n$ be indeterminates over R, and extend the action of R on M to $S = R[X_1, \ldots, X_n]$ by letting X_i act the way x_i does. This is equivalent to taking the R-algebra map $S \to R$ that fixes $R \subseteq S$ and sends X_i to x_i for $1 \leq i \leq n$, and restricting scalars from R to S. Then M is a finitely generated R-module over the Noetherian ring S, and $\mathcal{K}_\bullet(X_1, \ldots, X_n;\, M) \cong \mathcal{K}_\bullet(\underline{x};\, M)$. The X_i form a regular sequence in S. Replacing R by S and $x_1, \ldots, x_n$ by $X_1, \ldots, X_n$, we see that we may assume without loss of generality that $x_1, \ldots, x_n$ is a regular sequence in R. If $H_j(\underline{x};\, M) \neq 0$ we may choose a prime ideal P of the ring R such that $H_j(\underline{x};\, M)_P \neq 0$. We may replace R by R_P and M by M_P, since $H_t(x_1/1, \ldots, x_n/1;\, M_P) \cong H_t(\underline{x};\, M)_P$ for all P. Thus, we may assume that (R, m) is local. We may also assume that $x_1, \ldots, x_n \in m$: if not, $(x_1, \ldots, x_n)R = R$ kills all the Koszul homology, and all of it vanishes.

If $i = 1$ we are done by the final Theorem of the Lecture of February 12: the vanishing of $H_1(\underline{x};\, M)$ implies that $x_1, \ldots, x_n$ is a regular sequence on M, and that all the higher Koszul homology vanishes. We can now complete the proof by induction on i. Assume that $i > 1$ and the result is known for smaller integers. Form an exact sequence

$$0 \to M' \to R^h \to M \to 0$$

by mapping a finitely generated free module onto M. Since $x_1, \ldots, x_n$ is a regular sequence on R, it is a regular sequence on R^h, and $H_t(\underline{x};\, R^h) = 0$ for all $t \geq 1$. The long exact sequence for Koszul homology then implies at once that $H_t(\underline{x};\, M) \cong H_{t-1}(\underline{x};\, M')$ for all $t > 1$, and so $H_{i-1}(\underline{x};\, M') = 0$ while $H_{j-1}(\underline{x};\, M') \neq 0$ with $j - 1 \geq i - 1$, contradicting the induction hypothesis. □

We shall eventually use this result to prove that if M, N are finitely generated modules over a regular ring R and $\mathrm{Tor}_i^R(M, N) = 0$, then $\mathrm{Tor}_j^R(M, N) = 0$ for all $j \geq i$. This was proved by M. Auslander in the equicharacteristic case and by S. Lichtenbaum in general. In the equicharacteristic case, after localization and completion the values of Tor can be interpreted as Koszul homology over an auxiliary ring. This is not true in the mixed characteristic case, where one also needs spectral sequence arguments to make a comparison with the case where one can interpret values of Tor as Koszul homology. Both arguments make use of the structure of complete regular rings.

We shall soon begin our study of spectral sequences, but before doing that we introduce Grothendieck groups and use them to prove that regular local rings are unique factorization domains, following M. P. Murthy.

Let R be a Noetherian ring. Let $\mathcal{M}$ denote the set of modules

$$\{R^n/M : n \in \mathbb{N},\, M \subseteq R^n\}.$$

Every finitely generated R-module is isomorphic to one in $\mathcal{M}$, which is all that we really need about $\mathcal{S}$: we can also start with some other set of modules with this property without affecting the Grothendieck group, but we use this one for definiteness.

Consider the free abelian group with basis $\mathcal{M}$, and kill the subgroup generated by all elements of the form $M - M' - M''$ where

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

is a short exact sequence of elements of $\mathcal{M}$. The quotient group is called the *Grothendieck group* $G_0(R)$ of R. It is an abelian group generated by the elements $[M]$, where $[M]$ denotes the image of $M \in \mathcal{M}$ in $G_0(R)$. Note that if $M' \cong M$ we have a short exact sequence

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

so that $[M] = [M'] + [0] = [M']$, i.e., isomorphic modules represent the same class in $G_0(R)$.

A map L from $\mathcal{M}$ to an abelian group $(A, +)$ is called *additive* if whenever

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

is exact, then $L(M) = L(M') + L(M'')$. The map γ sending M to $[M] \in G_0(R)$ is additive, and is a universal additive map in the following sense: given any additive map $L : \mathcal{M} \to A$, there is a unique homomorphism $h : G_0(M) \to A$ such that $L = h \circ \gamma$. Since we need $L(M) = h([M])$, if there is such a map it must be induced by the map from the free abelian group with basis $\mathcal{M}$ to A that sends M to $h(M)$. Since h is additive, the elements $M - M' - M''$ coming from short exact sequences

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

are killed, and so there is an induced map $h : G_0(R) \to A$. This is obviously the only possible choice for h.

Over a field K, every finitely generated module is isomorphic with $K^{\oplus n}$ for some $n \in \mathbb{N}$. It follows that $G_0(K)$ is generated by $[K]$, and in fact it is $\mathbb{Z}[K]$, the free abelian group on one generator. The additive map associated with the Grothendieck group sends M to $\dim_K(M)[K]$. If we identify $\mathbb{Z}[K]$ with $\mathbb{Z}$ by sending $[K]$ to 1, this is the dimension map.

If R is a domain with fraction field $\mathcal{F}$, we have an additive map to $\mathbb{Z}$ that sends M to $\dim_{\mathcal{F}} \mathcal{F} \otimes_R M$, which is called the *torsion-free rank* of M. This induces a surjective map $G_0(R) \to \mathbb{Z}$. If R is a domain and $[R]$ generates $G_0(R)$, then $G_0(R) \cong \mathbb{Z}[R] \cong \mathbb{Z}$, with the isomorphism given by the torsion-free rank map.

Notice that if L is additive and

$$0 \to M_n \to \cdots \to M_1 \to M_0 \to 0$$

is exact, then

$$L(M_0) - L(M_1) + \cdots + (-1)^n L(M_n) = 0.$$

If $n \le 2$, this follows from the definition. We use induction. In the general case note that we have a short exact sequence

$$0 \to N \to M_1 \to M_0 \to 0$$

and an exact sequence

$$0 \to M_n \to \cdots \to M_3 \to M_2 \to N \to 0,$$

since

$$\mathrm{Coker}\,(M_3 \to M_2) \cong \mathrm{Ker}\,(M_1 \to M_0) = N.$$

Then

$$(*) \quad L(M_0) - L(M_1) + L(N) = 0,$$

and

$$(**) \quad L(N) - L(M_2) + \cdots + (-1)^{n-1} L(M_n) = 0$$

by the induction hypothesis. Subtracting $(**)$ from $(*)$ yields the result. □

From these comments and our earlier results on regular local rings we get at once:

Theorem. *If R is a regular local ring, $G_0(R) = \mathbb{Z}[R] \cong \mathbb{Z}$.*

Proof. R is a domain, and we have the map given by torsion-free rank. It will suffice to show that $[R]$ generates $G_0(R)$. But if M is any finitely generated R-module, we know that M has a finite free resolution

$$0 \to R^{b_k} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0,$$

and so the element $[M]$ may be expressed as

$$[R^{b_0}] - [R^{b_1}] + \cdots + (-1)^k [R^{b_k}] = b_0[R] - b_1[R] + \cdots + (-1)^k b_k[R] = (b_0 - b_1 + \cdots + (-1)^k b_k)[R]$$

□

Math 615: Lecture of February 17, 2020

Note that given a finite filtration

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

of a finitely generated R-module M and an additive map L we have that

$$L(M) = L(M_n/M_{n-1}) + L(M_{n-1}),$$

and, by induction on n, that

$$L(M) = \sum_{j=1}^{n} L(M_j/M_{j-1}).$$

In particular, $[M] \in G_0(R)$ is

$$\sum_{j=1}^{n} [M_j/M_{j-1}].$$

Theorem. *Let R be a Noetherian ring. $G_0(R)$ is generated by the elements $[R/P]$, as P runs through all prime ideals of R. If P is prime and $x \in R - P$, then $[R/(P + xR)] = 0$, and so if $R/Q_1, \ldots, R/Q_k$ are all the factors in a prime filtration of $[R/(P + xR)]$, we have that $[R/Q_1] + \cdots + [R/Q_k] = 0$. The relations of this type are sufficient to generate all relations on the classes of the prime cyclic modules.*

Proof. The first statement follows from the fact that every finitely generated module over a Noetherian ring R has a finite filtration in which the factors are prime cyclic modules. The fact that $[R/(P + xR)] = 0$ follows from the short exact sequence

$$0 \to R/P \xrightarrow{x} R/P \to R/(P + xR) \to 0,$$

which implies $[R/P] = [R/P] + [R/(P + xR)]$ and so $[R/(P + xR)] = 0$ follows.

Now, for every $M \in \mathcal{M}$, fix a prime cyclic filtration of M. We need to see that if we have a short exact sequence

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

that the relation $[M] = [M'] + [M'']$ is deducible from ones of the specified type. We know that M' will be equal to the sum of the classes of the prime cyclic module coming from its chosen prime filtration, and so will M''. These two prime cyclic filtrations together induce a prime cyclic filtration $\mathcal{F}$ of M, so that the information $[M] = [M'] + [M'']$ is conveyed by setting $[M]$ equal to the sum of the classes of the prime cyclic modules in these specified filtrations of $[M]$ and $[M']$. But $\mathcal{F}$ will not typically by the specified filtration of $[M]$, and so we need to set the sum of the prime cyclic modules in the specified filtration of M equal to the sum of all those occurring in the specified filtrations of M' and M''.

Thus, we get all relations needed to span if for all finitely generated modules M and for all pairs of possibly distinct prime cyclic filtrations of M, we set the sum of the classes of the prime cyclic modules coming from one filtration equal to the corresponding sum for the other. But any two filtrations have a common refinement. Take a common refinement, and refine it further until it is a prime cyclic filtration again. Thus, we get all relations needed to span if for every finitely generated module M and for every pair consisting of a prime cyclic filtration of M and a refinement of it, we set the sum of the classes coming from one filtration to the sum of those in the other. Any two prime cyclic filtrations may then be compared by comaring each two a prime cyclic filtration that refines them both.

In refining a given prime cyclic filtration, each factor R/P is refined. Therefore, we get all relations needed to span if for every R/P and every prime cyclic filtration of R/P, we set $[R/P]$ equal to the sum of the classes in the prime cyclic filtration of R/P. Since $\mathrm{Ass}\,(R/P) = P$, the first submodule of a prime cyclic filtration of R/P will be isomorphic with R/P, and will therefore have the form $x(R/P)$, where $x \in R - P$. If the other factors are $R/Q_1, \ldots, R/Q_k$, then these are the factors of a filtration of $(R/P)/x(R/P) = R/(P + xR)$. Since $[x(R/P)] = [R/P]$, the relation we get is

$$[R/P] = [R/P] + [R/Q_1] + \cdots + [R/Q_k],$$

which is equivalent to

$$[R/Q_1] + \cdots + [R/Q_k] = 0,$$

and so the specified relations suffice to span all relations. □

Corollary. $G_0(R) \cong G_0(R_{\mathrm{red}})$.

Proof. The primes of R_{red} and those of R are in bijective correspondence, and the generators and relations on them given by the preceding Proposition are the same. □

Proposition. *If R and S are Noetherian rings, then $G_0(R \times S) \cong G_0(R) \times G_0(S)$.*

Proof. If M is an $(R \times S)$-module, then with $e = (1, 0)$ and $f = (0, 1)$ we have an isomorphism $M \cong eM \times fM$, where eM is an R-module via $r(em) = (re)(em)$ and fM is an S-module via $s(fm) = (sf)(fm)$. There is an isomorphism $M \cong eM \times fM$. Conversely, given an R-module A and an S-module B, these determine an $R \times S$-module $M = A \times B$, where $(r, s)(a, b) = (ra, sb)$ such that $eM \cong A$ over R and $fM \cong B$ over R. Thus, $(R \times S)$-modules correspond to pairs A, B where A is an R-module and B is an S-module. Moreover, if $h : M \to M'$ then h induces maps $eM \to eM'$ and $fM \to fM'$ that determine h. Said differently, a map from $A \times B \to A' \times B'$ as $(R \times S)$-modules corresponds to a pair of maps $A \to A'$ as R-modules and $B \to B'$ as S-modules. Consequently, a short exact sequence of $(R \times S)$-modules corresponds to a pair consisting of short exact sequences, one of R-modules and the other of S-modules. The stated isomorphism of Grothendieck groups follows at once. □

Proposition. *Let R be an Artin ring.*

(a) *If (R, m, K) is Artin local, $G_0(R) \cong \mathbb{Z} \cdot [K] \cong \mathbb{Z}$, where the additive map $M \mapsto \ell_R(M)$ gives the isomorphism with $\mathbb{Z}$.*

(b) *If R has maximal ideals $m_1, \dots, m_k$, then $G_0(R)$ is the free abelian group on the $[R/m_j]$.*

Proof. For part (b), notice that the R/m_k are generators by Theorem, and there are no non-trivial relations, since if $x \notin m_j$, $R/(m_j + xR) = 0$. Part (a) follows easily from part (b). We may also deduce part (b) from part (a), using the fact that an Artin ring is a finite product of Artin local rings and the preceding Proposition. □

Proposition. *Let R and S be Noetherian rings.*

(a) *If $R \to S$ is a flat homomorphism, there is a a group homomorphism $G_0(R) \to G_0(S)$ sending $[M]_R \mapsto [S \otimes_R M]_S$. Thus, G_0 is a covariant functor from the category of rings and flat homomorphisms to abelian groups.*

(b) *If $S = W^{-1}R$ is a localization, the map described in (a) is surjective.*

(c) *If P is a minimal prime of R, there is a homomorphism $G_0(R) \to \mathbb{Z}$ given by $[M] \mapsto \ell_{R_P}(M_P)$. Of course, if R is a domain and $P = (0)$, this is the torsion-free rank map.*

(d) *If R is a domain, the map $\mathbb{Z} \to G_0(R)$ that sends 1 to $[R]$ is split by the torsion-free rank map. Thus, $G_0(R) = \mathbb{Z}[R] + \overline{G}_0(R)$, where $\overline{G}_0(R) = G_0(R)/\mathbb{Z} \cdot [R]$, the reduced Grothendieck group of R. When R is a domain, the reduced Grothendieck group may be thought of as the subgroup of $G_0(R)$ spanned by the classes of the torsion R-modules.*

(e) *If S is module-finite over R, there is a group homomorphism $G_0(S) \to G_0(R)$ sending $[M]_S$ to $[{}_RM]_R$, where ${}_RM$ denotes M viewed as an R-module via restriction of scalars. In particular, this holds when S is homomorphic image of I. Thus, G_0 is a contravariant functor from the category of rings and module-finite homomorphisms to abelian groups.*

Proof. (a) is immediate from the fact that $S \otimes_R \_$ preserves exactness.

To prove (b), note that if M is a finitely generated module over $W^{-1}R$, it can be written as the cokernel of a matrix of the form (r_{ij}/w_{ij}), where every $r_{ij} \in R$ and every $w_{ij} \in W$. Let w be the product of all the w_{ij}. Then the entries of the matrix all have the form r'_{ij}/w. If we multiply every entry of the matrix by w, which is a unit in S, the cokernel is unaffected: each column of the matrix is multiplied by a unit. Let $M_0 = \text{Coker } (r'_{ij})$. Then $S \otimes_R M_0 \cong M$. This shows the surjectivity of the map of Grothendieck groups.

Part (c) is immediate from the fact that localization is exact coupled with the fact the length is additive. The statement in (d) is obvious, since the torsion-free rank of R is 1.

One has the map in (e) because restriction of scalars is an exact functor from finitely generated S-modules to finitely generated R-modules. One needs that S is module-finite over R to guarantee that when one restricts scalars, a finitely generated S-module becomes a finitely generated R-module. □

If S is faithfully flat or even free over R, the induced map $[M]_R \to [S \otimes_R M]_S$ need not be injective, not even if $S = L \otimes_K R$ where L is a finite field extension of $K \subseteq R$: an example is given in the sequel (see the last paragraph of today's Lecture Notes).

An R-module M is said to have *finite Tor dimension* or *finite flat dimension* over R at most d if $\mathrm{Tor}_i^R(M,\,N) = 0$ for all $i > d$. If $M = 0$, the Tor dimension is defined to be -1. Otherwise, it is the smallest integer d such that $\mathrm{Tor}_i^R(M,\,N) = 0$ for all $i > d$, if such an integer exists, and $+\infty$ otherwise. We leave it as an exercise to show that M has finite Tor dimension at most d if and only if some (equivalently, every) d th module of syzygies of M is flat. Likewise, M has finite Tor dimension at most d if and only if M has a left resolution by flat modules of length at most d. A nonzero module M has Tor dimension 0 if and only of M is flat over R. Of course, if M has finite projective dimension d, then M has Tor dimension at most d.

Proposition. *If S is a Noetherian R-algebra of finite Tor dimension $\leq d$ over the Noetherian ring R, there is a map $G_0(R) \to G_0(S)$ that sends $[M]_R$ to*

$$\theta(M) = \sum_{i=0}^{d} (-1)^i [\mathrm{Tor}_i^R(S,\,M)]_S.$$

Proof. We simply need to check the additivity of the map. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finitely generated R-modules. Then we get a long exact sequence of finitely generated S-modules

$$0 \to \mathrm{Tor}_d^R(S,\,M') \to \mathrm{Tor}_d^R(S,\,M) \to \mathrm{Tor}_d^R(S,\,M'') \to \cdots$$
$$\to \mathrm{Tor}_0^R(S,\,M') \to \mathrm{Tor}_0^R(S,\,M) \to \mathrm{Tor}_0^R(S,\,M'') \to 0$$

and so the alternating sum Σ of the classes of these modules in $G_0(S)$ is 0. We think of these $3d$ modules as in positions $3d-1,\,3d-2,\,\cdots,2,\,1,\,0$ counting from the left. The terms involving M'' are in positions numbered $0,\ ,3,\,6,\,\ldots\,,\,3(d-1)$. Their signs alternate starting with $+$, and so their contribution to Σ is $\theta(M'')$. The terms involving M are in positions numbered $1,\,4,\,7,\,\ldots\,,\,3(d-1)+1$. Their signs alternate starting with $-$, and so their contribution to Σ is $-\theta(M)$. Finally, the terms involving M' are in positions numbered $2,\,5,\,8,\,\ldots\,,\,3(d-1)+2$. Their signs alternate starting with $+$, and so their contribution to Σ is $\theta(M')$. This yields $0 = \Sigma = \theta(M') - \theta(M) + \theta(M'')$, as required. □

Corollary. *If x is not a zerodivisor in the Noetherian ring R, there is a map $G_0(R) \to G_0(R/xR)$ that sends $[M]_R \mapsto [M/xR]_{R/xR} - [\mathrm{Ann}_M\,x]_{R/xR}$.*

Proof. This is the special case of result just above when $S = R/xR$, which has projective dimension at most 1 and, hence, flat dimension at most 1. We have that $\mathrm{Tor}_0^R(R/xR,\,M) \cong (R/xR) \otimes_R M \cong M/xM$, and $\mathrm{Tor}_1^R(R/xR,\,M) \cong \mathrm{Ann}_M x$. An elementary proof of this result may be given by showing that when

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

is exact then so is

$$0 \to \operatorname{Ann}_{M'} x \to \operatorname{Ann}_M x \to \operatorname{Ann}_{M''} x \to M'/xM' \to M/xM \to M''/xM'' \to 0,$$

developing this special case of the long exact sequence for Tor from first principles. □

Corollary. *Let R be Noetherian and let S denote either $R[x]$ or $R[[x]]$, where x is an indeterminate. Since S is flat over R, we have an induced map $G_0(R) \to G_0(S)$. This map is injective.*

Proof. We have that $S/xS \cong R$, where x is not a zerodivisor in S, and so we have a map $G_0(S) \to G_0(R)$. Under the composite map, the class $[M]_R$ of an R-module M maps first to $[M[x]\,]_S$ (respectively, $[M[[x]]\,]_S$), and then to $[M[x]/xM[x]\,]_R$ (respectively, $[M[[x]]/xM[[x]]\,]_R$), since x is not a zerodivisor on $M[x]$ (respectively, $M[[x]]$). In both cases, the quotient is $\cong M$, and so the composite map takes $[M]_R \to [M]_R$. Thus, the composite $G_0(R) \to G_0(S) \to G_0(R)$ is the identity on $G_0(R)$, which implies that $G_0(R) \to G_0(S)$ is injective. □

We next aim to establish the following result, which will imply unique factorization in regular local rings.

Theorem (M. P. Murthy). *Let R be a normal domain and let H be the subgroup of $\overline{G}_0(R)$ spanned by the classes $[R/P]$ for P a prime of height 2 or more. Then*

$$\mathcal{C}\ell\,(R) \cong \overline{G}_0(R)/H.$$

Assuming this for the moment, note the failure of the injectivity of the map from $G_0(R) \to G_0(S)$ where $R = \mathbb{R}[x,\,y]/(x^2+y^2-1)$ and $S = \mathbb{C} \otimes_{\mathbb{R}} R \cong \mathbb{C}[x,\,y]/(x^2+y^2-1)$. We have seen in **6.(b)** of Problem Set #6 from Math 614 that the maximal ideal $P = (x,\,y-1)R$ is not principal in R, from which it will follow that $[P]$ is nonzero in $\mathcal{C}\ell\,(R)$, and so that $[R/P]$ is nonzero in $\overline{G}_0(R)$, and therefore $[R/P]$ is not zero in $G_0(R)$. But P becomes principal when expanded to S. In fact, S is a UFD, for if we let $u = x + yi$ and $v = x - yi$, then $\mathbb{C}[x,\,y] \cong \mathbb{C}[u,\,v]$ (we have made a linear change of variables), and so $S \cong \mathbb{C}[u,\,v]/(uv-1) \cong \mathbb{C}[u][1/u]$. Thus, $[S \otimes R/P]_S = [S/PS]_S = 0$ in $G_0(S)$.

Math 615: Lecture of February 19, 2020

Recall that if R is a normal domain, one defines the *divisor class group* of R, denoted $\mathcal{C}\ell\,(R)$, as follows. First form the the free abelian group on generators in bijective correspondence with the height one prime ideals of R. The elements of this group are called *divisors*. The divisor $\operatorname{div}(I)$ of an ideal $I \neq 0$ whose primary decomposition only involves height one primes (I is said to be of *pure height one*) is then obtained from the primary decomposition of I: if the primary decomposition of I is $P_1^{(k_1)} \cap \cdots \cap P_s^{(k_s)}$ where the P_j are mutually distinct, then $\mathrm{div}\,(I) = \sum_{j=1}^{s} k_j P_j$. We regard the unit ideal as having pure height one in a vacuous sense, and define its divisor to be 0. The divisor $\mathrm{div}\,(r)$ of an element $r \in R - \{0\}$ is the divisor of rR, and, hence, 0 if r is a unit. Then $\mathcal{C}\ell\,(R)$ is the quotient of the free abelian group of divisors by the span of the divisors of nonzero principal ideals. The following is part of a Theorem on the third page of the Math 614 Lecture Notes from December 1, to which we refer the reader for the proof.

Theorem. *Let R be a Noetherian normal domain. If I has pure height one, then so does fI for every nonzero element f of R, and $\mathrm{div}\,(fI) = \mathrm{div}\,(f) + \mathrm{div}\,(I)$. For any two ideals I and J of pure height one, $\mathrm{div}\,(I) = \mathrm{div}\,(J)$ iff $I = J$, while the images of $\mathrm{div}\,(I)$ and $\mathrm{div}\,(J)$ in $\mathcal{C}\ell\,(R)$ are the same iff there are nonzero elements f, g of R such that $fI = gJ$. This holds iff I and J are isomorphic as R-modules. In particular, I is principal if and only if $\mathrm{div}\,(I)$ is 0 in the divisor class group. Hence, R is a UFD if and only if $\mathcal{C}\ell\,(R) = 0$.*

While we are not giving a full proof here, we comment on one point. If $I \cong J$ as an R-module, the isomorphism is given by an element of $\mathrm{Hom}_R(I,\, J)$. If we localize at the prime (0), which is the same as applying $\mathcal{F} \otimes_R \_$, where $\mathcal{F}$ is the fraction field of R, we see that $\mathrm{Hom}_R(I,\, J)$ embeds in $\mathcal{F} \otimes_R \mathrm{Hom}_R(I,\, J) \cong \mathrm{Hom}_{\mathcal{F}}(I\mathcal{F},\, J\mathcal{F}) = \mathrm{Hom}\mathcal{F}(\mathcal{F},\, \mathcal{F}) \cong \mathcal{F}$, that is, every homomorphism from I to J is induced by multiplying by a suitable fraction f/g, $f \in R$, $g \in R - \{0\}$. When this fraction gives an isomorphism we have $(f/g)I = J$ or $fI = gJ$.

Theorem (M. P. Murthy). *Let R be a normal domain and let H be the subgroup of $\overline{G}_0(R)$ spanned by the classes $[R/P]$ for P prime of height 2 or more. Then $\mathcal{C}\ell\,(R) \cong \overline{G}_0(R)/H$ with the map sending $[P] \mapsto [R/P]$ for all height one primes P.*

Before proving this, we note two corollaries. One is that regular local rings have unique factorization. Whether this is true was an open question for many years that was first settled by M. Auslander and D. Buchsbaum by a much more difficult method, utilizing homological methods but based as well on a result of Zariski that showed it suffices to prove the result for regular local rings of dimension 3. Later, I. Kaplansky gave a substantially simpler proof. But I feel that Murthy's argument gives the "right" proof. We have already seen that for a regular local ring R, $\overline{G}_0(R) = 0$. Therefore:

Corollary. *A regular local ring is a UFD.* □

Corollary. *If R is a Dedekind domain, then $\overline{G}_0(R) \cong \mathcal{C}\ell\,(R)$ and $G_0(R) = \mathbb{Z}\cdot[R] \oplus \mathcal{C}\ell\,(R)$.*

Proof. This is clear, since there are no primes of height two or more. □

We now go back and prove Murthy's result.

Proof of the Theorem. We know that $G_0(R)$ is the free group on the classes of the R/P, P prime, modulo relations obtained from prime cyclic filtrations of $R/(P + xR)$, $x \notin P$. We shall show that if we kill $[R]$ and all the $[R/Q]$ for Q of height 2 or more, all relations are also killed except those coming from $P = (0)$, and the image of any relation corresponding to a prime cyclic filtration of R/xR corresponds precisely to $\mathrm{div}\,(x)$. Clearly, if $P \neq 0$ and $x \notin P$, any prime containing $P + xR$ strictly contains P and so has height two or more. Thus, we need only consider relations on the R/P for P of height one coming from prime cyclic filtrations of R/xR, $x \neq 0$. Clearly, R does not occur, since R/xR is a torsion module, and occurrences of R/Q for Q of height ≥ 2 do not matter. We need only show that for every prime P of height one, the number of occurrences of R/P in any prime cyclic filtration of R/xR is exactly k, where $P^{(k)}$ is the P-primary component of xR. But we can do this calculation after localizing at P: note that all factors corresponding to other primes become 0, since some element in the other prime not in P is inverted. Then $xR_P = P^kR_p$, and we need to show that any prime cyclic filtration of R_P/xR_P has k copies of R_P/PR_P, where we know that $xR_P = P^kR_P$. Notice that $(R_P,\, PR_P)$ is a DVR, say (V, tV), and $xR_P = t^kV$. The number of nonzero factors in any prime cyclic filtration of V/t^kV is the length of V/t^kV over V, which is k, as required: the only prime cyclic filtration without repetitions is

$$0 \subset t^{k-1}V \subset t^{k-2}V \subset \cdots \subset t^2V \subset tV \subset V. \quad \square$$

Theorem. $G_0(R) \cong G_0(R[x])$ *under the map that sends* $[M] \mapsto [M[x]]$*, where we have written* $M[x]$ *for* $R[x] \otimes_R M$.

Proof. We have already seen that the map is injective, and even constructed a left inverse for it, which takes

$$[N]_{R[x]} \mapsto [N/xN]_R - [\mathrm{Ann}_N\, x]_R.$$

However, we shall not make use of this left inverse to prove surjectivity. Instead, we prove that every $[S/Q]$, Q prime, is in the image of $G_0(R) \to G_0(R[x])$ by Noetherian induction on $R/(Q \cap R)$. There are two sorts of primes lying over $P \in \mathrm{Spec}\,(R)$. One is $PR[x]$. The other is generated, after localization at $R - P$, by a polynomial $f \in R[x]$ of positive degree with leading coefficient in $R - P$ such that the image of f is irreducible in $\kappa_P[x]$, where $\kappa_P = R_P/PR_P \cong \mathrm{frac}\,(R/P)$. To see this, note that every prime Q lying over P corresponds, via contraction to $R[x]$, to a prime of the fiber $(R-P)^{-1}(R/P)[x] \cong \kappa_P[x]$. The primes in $\kappa_P[x]$ are of two types: there is the (0) ideal, whose contraction to $R[x]$ is $PR[x]$, and there are the maximal ideals, each of which is generated by an irreducible polynomial of positive degree in $\kappa_P[x]$. We can clear the denominators by multiplying by an element of $R-P$, and then lift the nonzero coefficients to $R-P$, to obtain a polynomial f with leading coefficient in $R - P$ as described previously. Note that Q is recovered from P and f as the set of all elements of $R[x]$ multiplied into $P+fR[x]$ by an element of $R-P$. Briefly, $Q = (PR[x] + fR[x]) :_{R[x]} (R - P)$.

Since $R[x]/PR[x] = (R/P)\otimes_R R[x]$ is evidently in the image, we need only show that the primes Q of the form $(PR[x]+fR[x]) :_{R[x]} (R-P)$ are in the image of $G_0(R) \to G_0(R[x])$. We have exact sequences

$$(*) \quad 0 \to (R/P)[x] \xrightarrow{f} (R/P)[x] \to M \to 0,$$

where $M = R[x]/(PR[x] + fR[x])$, and

$$(**) \quad N \to M \to R[x]/Q \to 0.$$

Because $(R-P)^{-1}M = (R-P)^{-1}R[x]/Q$, we have that N is a finitely generated module that is a torsion module over R/P. Since every generator of N is killed by an element of $R-P$, we can choose $a \in R-P$ that kills N. From $(*)$, $[M] = 0$ in $G_0(S)$. From $(**)$, $[R[x]/Q] = -[N]$ in $G_0(R[x])$. Therefore, it suffices to show that $[N]$ is in the image. In a prime cyclic filtration of N, every factor is killed by $P + aR$, and therefore for every $R[x]/Q'$ that occurs, Q' lies over a prime strictly containing P. But then every $[R[x]/Q']$ is in the image by the hypothesis of Noetherian induction. □

Theorem. *Let R be a ring and S a multiplicative system. Then the kernel of $G_0(R) \to G_0(S^{-1}R)$ is spanned by the set of classes $\{[R/P] : P \cap S \neq \emptyset\}$. Hence, for any $x \in R$ there is an exact sequence*

$$G_0(R/xR) \to G_0(R) \to G_0(R_x) \to 0.$$

Proof. The final statement is immediate from the general statement about localization at S, since $G_0(R/xR)$ is spanned by classes $[R/P]_{R/xR}$ such that $x \in P$ and $x \in P$ iff P meets $\{x^n : n \geq 1\}$, and so the image of $G_0(R/xR)$ in $G_0(R)$ is spanned by the classes $[R/P]_R$ for $x \in P$.

To prove the general statement about localization, first note that the specified classes are clearly in the kernel. To show that these span the entire kernel, it suffices to show that all the spanning relations on the classes $[S^{-1}R/QS^{-1}R_Q]$ hold in the quotient of $G_0(R)$ by the span Γ of the classes $[R/P]$ for $P \cap S \neq \emptyset$. Consider a prime cyclic filtration of $S^{-1}R/(PS^{-1}R + (x))$, where x may be chosen in R. We may contract (i.e., take inverse images of) the submodules in this filtration to get a filtration of R/P. Each factor N_i contains an element u_i such that, after localization at S, u_i generates $S^{-1}N_i \cong S^{-1}R/Q_i$. Thus, for each i, we have short exact sequences

$$0 \to Ru_i \to N_i \to C_i \to 0 \qquad \text{and} \qquad 0 \to D_i \to Ru_i \to R/Q_i \to 0,$$

where C_i and D_i vanish after localization at S and so have prime cyclic filtrations with factors $R/\mathcal{Q}_j$ such that $\mathcal{Q}_j$ meets S. Here, we have that $Q_1 = P$. We must show that the relation $\sum_{i>1}[S^{-1}R/S^{-1}Q_i] = 0$ comes from a relation on the $[R/Q_i]$ in $G_0(R)/\Gamma$. But $[R/P] = N_1 + \sum_{i>1}[N_i]$, and for every i,

$$[N_i] = [Ru_i] + [C_i] = [R/Q_i] + [C_i] + [D_i].$$

Since $Q_1 = P$, we have

$$0 = [C_1] + [D_1] + \sum_{i>1}[R/Q_i] + [C_i] + [D_i]$$

in $G_0(R)$, and the conclusion we want follows: as aleady observed, every C_i and every D_i is killed by an element of S, and so has a prime cyclic filtration in which each prime cyclic module has a class in Γ. □

We next define the *Grothendieck group of projective modules* over a Noetherian ring R by forming the free abelian group on generators P in $\mathcal{M}$ (one can work with any set of finitely generated projective modules containing a representative of every isomorphism class) and killing the subgroup spanned by elements $P - P' - P''$, where $0 \to P' \to P \to P'' \to 0$ is exact. In this situation the short exact sequence of projectives is split (this only uses that P'' is projective), and so $P \cong P' \oplus P''$. Thus, the elements that we kill to construct $K_0(R)$ have the form $(P' \oplus P'') - P' - P''$. Note that isomorphic projectives represent the same class in $K_0(R)$.

There is obviously a canonical map $K_0(R) \to G_0(R)$ that takes $[P]$ in $K_0(R)$ to $[P]$ in $G_0(R)$ for every finitely generated projective module over R.

Theorem. *If R is regular, the map $K_0(R) \cong G_0(R)$ is an isomorphism.*

Proof. We want to define a map from $G_0(R)$ to $K_0(R)$. Given a finitely generated R-module M, we can choose a finite projective resolution of M by finitely generated projective modules, say $P_\bullet$, and suppose that the length of this resolution is d. The obvious way to define an inverse map is to send $[M]$ to

$$[P_0] - [P_1] + \cdots + (-1)^d [P_d] \in K_0(R).$$

We must check that this is independent of the choice of the projective resolution. Given another such projective resolution $Q_\bullet$ of M we must show that the two alternating sums are the same in $K_0(R)$ (this is obvious in $G_0(R)$, since both equal $[M]$, but M is not "available" in $K_0(R)$). To prove this, choose a map of complexes $\phi_\bullet : P_\bullet \to Q_\bullet$ such that the induced map of augmentations $M = H_0(P_\bullet) \to H_0(Q_\bullet) = M$ is the identity. Form $C_\bullet$, the mapping cone of ϕ, which is a complex of projective modules. Then $C_n = P_n \oplus Q_{n-1}$. We claim that $C_\bullet$ is exact (not just acyclic): *all* the homology vanishes. To see this, consider the long exact sequence of the mapping cone:

$$\cdots \to H_n(Q_\bullet) \to H_n(C_\bullet) \to H_{n-1}(P_\bullet) \to H_{n-1}(Q_\bullet) \to \cdots .$$

If $n \geq 2$, $H_n(C_\bullet) = 0$ since $H_n(Q_\bullet)$ and $H_{n-1}(P_\bullet)$ both vanish. If $n = 1$, $H_1(C_\bullet)$ vanishes because $H_1(Q_\bullet) = 0$ and the connecting homomorphism $H_0(P_\bullet) \to H_0(Q_\bullet)$ is an isomorphism. If $n = 0$, $H_0(C_\bullet) = 0$ because $H_0(Q_\bullet)$ and $H_{-1}(P_\bullet)$ both vanish.

Thus, the alternating sum of the classes in $C_\bullet$ is 0 in $K_0(R)$, and this is exactly what we want.

Additivity follows because given a short exact sequence of finitely generated modules $0 \to M' \to M \to M'' \to 0$ and projective resolutions $P'_\bullet$ of M' and $P''_\bullet$ of M'' by finitely generated projective modules, one can construct such a resolution for M whose j th term is $P'_j \oplus P''_j$: cf. the middle of page 4 of the Lecture Notes of February 10. □

Math 615: Lecture of February 21, 2020

Note that K_0 is a functor on all maps of Noetherian rings (not just flat maps) because short exact sequences of projectives are split and remain exact no matter what algebra one tensors with. Restriction of scalars from S to R will not induce a map on K_0 unless S is module-finite and *projective* over R.

Observe also that $K_0(R)$ has a commutative ring structure induced by $\_ \otimes_R \_$, with $[R]$ as the multiplicative identity, since the tensor product of two finitely generated projective modules is a projective module, and tensor distributes over direct sum.

Proposition. *Let P and Q be finitely generated projective modules over a Noetherian ring R. Then $[P] = [Q]$ in $K_0(R)$ if and only there is a free module G such that $P \oplus G \cong Q \oplus G$.*

Proof. $[P] = [Q]$ if and only if $[P] - [Q]$ is in the span of the standard relations used to define $K_0(R)$, in which case, for suitable integers h, k,

$$P - Q = \sum_{i=1}^{h} \bigl((P_i \oplus Q_i) - P_i - Q_i\bigr) + \sum_{j=1}^{k} \bigl(P'_j + Q'_j - (P'_j \oplus Q'_j)\bigr)$$

and so

$$P + \sum_{i=1}^{h} (P_i + Q_i) + \sum_{j=1}^{k} (P'_j \oplus Q'_j) = Q + \sum_{i=1}^{h} (P_i \oplus Q_i) + \sum_{j=1}^{k} (P'_j + Q'_j).$$

The fact that this equation holds implies that the number of occurrences of any given projective module on the left hand side is equal to the number of occurrences of that projective module on the right hand side. Therefore, if we change every plus sign (+) to a direct sum sign ($\oplus$), the two sides of the equation are isomorphic modules: the terms occurring in the direct sum on either side are the same except for order. Therefore:

$$P \oplus \bigoplus_{i=1}^{h} (P_i + Q_i) \oplus \bigoplus_{j=1}^{k} (P'_j \oplus Q'_j) = Q \oplus \bigoplus_{i=1}^{h} (P_i \oplus Q_i) \oplus \bigoplus_{j=1}^{k} (P'_j \oplus Q'_j).$$

In other words, if we let

$$N = \bigoplus_{i=1}^{h} (P_i \oplus Q_i) \oplus \bigoplus_{j=1}^{k} (P'_j \oplus Q'_j),$$

then $P \oplus N = Q \oplus N$. But N is projective, and so we can choose N' such that $N \oplus N' \cong G$ is a finitely generated free module. But then

$$P \oplus N \oplus N' \cong Q \oplus N \oplus N',$$

i.e., $P \oplus G \cong Q \oplus G$. □

Corollary. *let R be Noetherian. $K_0(R)$ is generated by $[R]$ if and only if every projective module P has a finitely generated free complement, i.e., if and only if for every finitely generated projective module M there exist integers h and k in $\mathbb{N}$ such that $P \oplus R^h \cong R^k$.* □

We know that

$$K_0(K[x_1, \ldots, x_n]) \cong G_0(K[x_1, \ldots, x_n]) \cong G_0(K) \cong \mathbb{Z}$$

is generated by the class of R. Therefore, every finitely generated projective module over $R = K[x_1, \ldots, x_n]$ has a finitely generated free complement. To prove that every projective module over a R is free, it suffices to show that if $P \oplus R \cong R^n$ then $P \cong R^{n-1}$. The hypothesis implies precisely that P is the kernel of a map $R^n \twoheadrightarrow R$. Such a map is given by a $1 \times n$ matrix $(r_1 \ \ldots \ r_n)$. The surjectivity of the map corresponds to the condition that the r_j generate the unit ideal of R. If $\sum_{j=1}^n r_j s_j = 1$, then the $n \times 1$ column matrix whose entries are $s_1, \ldots, s_n$ mapping $R \to R^n$ gives a splitting. $P \cong R^{n-1}$ implies that this column vector v can be extended to a free basis for R^n, since $R^n = P \oplus Rv$. Since $P \cong R^n/Rv$, P will be free if and only if it has $n-1$ generators, and so P will be free if only if v can be extended to a free basis for R^n. This led to the following question: if one is given one column of a matrix consisting of polynomials over K that generate the unit ideal, can one "complete" the matrix so that it has determinant which is a unit in the polynomial ring? This is equivalent to completing the matrix so that its determinant is 1 if $n \geq 2$: the unit can be absorbed into one of the columns other than the first. This is known as the "unimodular column" problem. However, some authors, who use matrices that act on the right, study the equivalent "unimodular row" problem.

The question was raised by Serre in the mid 1950s and was open until 1976, when it was settled in the affirmative, independently, by D. Quillen and A. Suslin. A bit later, Vaserstein gave another proof which is very short, albeit very tricky. It is true that projective modules over a polynomial ring over a field are free, but it is certainly a non-trivial theorem.

We next want to discuss the functor Ext: in order to do so, we need to discuss some facts about 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. *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: $g \leq g'$ 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 $\geq f$ (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. □

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. *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. □

Math 615: Lecture of February 24, 2020

It is obvious that a homomorphic image 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

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

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. *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

$$\begin{tikzcd}
A_1^{\vee\vee} \arrow[r, "f^{\vee\vee}"] & A_2^{\vee\vee} \\
A_1 \arrow[u, "\theta_{A_1}"] \arrow[r, "f"'] & A_2 \arrow[u, "\theta_{A_2}"']
\end{tikzcd}$$

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. □

Before proving the next result we observe the following. Let R be a C-algebra, let M and N be R-modules, let Q be a C-module, and suppose that we are given a C-bilinear map $B : M \times N \to Q$ such that $B(ru,\, v) = B(u,\, rv)$ for all $r \in R$. Then there is a unique C-linear map $f : M \otimes_R N \to Q$ such that $f(u \otimes v) = B(u, v)$ for all $u \in M$ and $v \in N$. This is a consequence of the easily verified fact that $M \otimes_R N$ is the quotient of $M \otimes_C N$ by the span of all elements of the form $ru \otimes v - u \otimes rv$ for $r \in R$, $u \in M$ and $v \in N$. We are now ready to establish the following easy but very important result:

Theorem (adjointness of tensor and Hom). *Let $C \to R$ be a ring homomorphism, let M be and N be R-modules, and let Q be a C-module. Then there is a natural isomorphism* $\mathrm{Hom}_C(M \otimes_R N,\, Q) \to \mathrm{Hom}_R(M,\, \mathrm{Hom}_C(N,\, Q)$ *as R-modules: the two sides are isomorphic as functors of the three variables M, N, and Q.*

Proof. We define mutually inverse maps explicitly. Given $f : M \otimes_R N \to Q$ as C-modules, let $\Theta(f)$ be the map $M \to \mathrm{Hom}_C(N,\, Q)$ whose value on $u \in M$ is $\beta_{f,u}$, where $\beta_{f,u}(v) = f(u \otimes v)$. Note that the value of $\Theta(rf)$ on u for $r \in R$ is $\beta_{rf,u}$, where $\beta_{rf,u}(v) = (rf)(u \otimes v) = f\big(r(u \otimes v)\big) = f\big((ru) \otimes v)\big)$, while the value of $r\Theta(f)$ on u is $\Theta(f)(ru)$, and the value of that map on $v \in N$ is $\beta_{f,ru}(v) = f\big((ru) \otimes v\big)$. The R-linearity of Θ follows.

On the other hand, given $g : M \to \mathrm{Hom}_C(N,\, Q)$, we can define a C-bilinear map $B_g : M \times N \to Q$ by letting $B_g(u,\, v) = g(u)(v)$. Note that $B_g(ru,\, v) = g(ru)(v) = \big(rg(u)\big)(v) = g(u)(rv) = B_g(u,\, rv)$. Let

$$\Lambda : \mathrm{Hom}_R(M,\, \mathrm{Hom}_C(N,\, Q) \to \mathrm{Hom}_C(M \otimes_R N,\, Q)$$

be such that $\Lambda(g)$ is the linear map corresponding to B_g. The check that Λ and Θ are mutually inverse is straightforward, as is the check of naturality: further details are left to the reader. □

Corollary. *Let R be a C-algebra, let F be a flat R-module, and let W be an injective C-module. Then* $\mathrm{Hom}_C(F,\, W)$ *is an injective R-module.*

Proof. Because of the natural isomorphism

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

we may view the functor

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

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

We can now put things together:

Theorem. *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 the Corollary above, $F^{\vee} = \mathrm{Hom}_{Z}(F, W)$ 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 at the top of page 2, whose demonstration used Zorn's lemma.

Math 615: Lecture of February 26, 2020

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.

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 j th module of cosyzygies. We have the analogue of Schanuel's lemma on syzygies: given two n th 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 $\mathrm{Ker}\,(E^0 \to E^1)$. An n th module of cosyzygies for M is recovered from the injective resolution for every $n \geq 1$ as $\mathrm{Im}\,(E_{n-1} \to E_n)$, or as $\mathrm{Ker}\,(E_n \to E_{n+1})$.

We can define the *injective dimension* $\mathrm{id}_R M$ 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 injective resolution, and it is the length of the shortest such resolution. Then $\mathrm{id}_R M \leq n$, where $n \geq 0$, if and only if M

has an injective resolution of length at most n. If M has no finite injective resolution we define $\mathrm{id}_R M = +\infty$. We note that the following are equivalent conditions on a nonzero module M and nonnegative integer n :

(1) M has injective resolution of length at most n.

(2) Some n th module of cosyzygies of M is injective.

(3) Every n th module of cosyzygies of M is injective.

The reader may also check easily that if M is not injective then the injective dimension of any module of cosyzygies of M is $\mathrm{id}_R M - 1$. More generally, if M has injective dimension $\geq n \geq 1$ then any n th module of cosyzygies has injective dimension $\mathrm{id}_R M - n$.

Given a projective resolution $P_\bullet$ of M and an injective resolution $E^\bullet$ of N, we can form a cohomological double complex $\mathrm{Hom}_R(P_j,\, E_i)$ of which a typical square is

$$\begin{tikzcd}
\mathrm{Hom}_R(P_j,\, E^{i+1}) \arrow[r] & \mathrm{Hom}_R(P_{j+1},\, E^{i+1}) \\
\mathrm{Hom}_R(P_j,\, E^{i}) \arrow[r] \arrow[u] & \mathrm{Hom}_R(P_{j+1},\, E^{i}) \arrow[u]
\end{tikzcd}$$

Every row and every column is exact except at the 0 spot. The homology of the total complex is denoted $\mathrm{Ext}^\bullet_R(M,\, N)$. This is the same as the homology of the complex $\mathrm{Hom}_R(M,\, E^\bullet)$ or of the complex $\mathrm{Hom}_R(P_\bullet,\, N)$. Notice that the arrows are reversed, so that the maps raise the index: a typical map is

$$\mathrm{Hom}_R(P_j,\, N) \to \mathrm{Hom}_R(P_{j+1},\, N).$$

To remove the ambiguity from this definition, one may use the canonical free resolution of M, as in the definition of Tor, for $P_\bullet$, and the canonical injective resolution of N, that comes from embedding each successive module of cosyzygies C of N in an injective by mapping a free module F onto $C\vee$ with one element of the free basis for every element of $C\vee$, and then using the embedding $C \hookrightarrow C^{\vee\vee} \hookrightarrow F^\vee$. However, the value of Ext is independent of the resolutions chosen up to canonical isomorphism. One way to see this is to fix the projective resolution and let the injective resolution vary. No matter how the injective resolution is chosen, the cohomology of the total complex is $H^\bullet(\mathrm{Hom}_R(P_\bullet,\, N)$. Similarly, if we fix the injective resolution and vary the projective resolution the cohomology of the total complex is $H^\bullet(\mathrm{Hom}_R(M,\, E^\bullet)$, and so does not change.

One may also see independence of the projective resolution more directly, using the theory of homotopy of maps of complexes. Given two different projective resolutions $P_\bullet$, $Q_\bullet$ of M, there are maps in each direction that lift the identity map on M, and these are unique up to homotopy. It follows that the composition in either order is homotopic to the identity map on the relevant complex, $P_\bullet$ or $Q_\bullet$. After applying $\mathrm{Hom}_R(\_\,,\, N)$ we still have the maps induced by the homotopy, although, like the maps of complexes, they have reversed direction. This is a homotopy in the cohomological sense: h^n maps the n th term of one complex to the $n-1$ st in the other.

If we develop the theory of Ext purely using injective resolutions, we find that given the following set-up:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & E^0 \arrow[r] & E^1 \arrow[r] & E^2 \arrow[r] & \cdots \\
0 \arrow[r] & M \arrow[r] \arrow[u, "f"] & Q_0 \arrow[r] & Q_1 \arrow[r] & Q_2 \arrow[r] & \cdots
\end{tikzcd}$$

where each row is a complex, the bottom row is exact, and the E_j are injective, one can fill in the vertical arrows, i.e., one can give a map of complexes

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] & E^0 \arrow[r] & E^1 \arrow[r] & E^2 \arrow[r] & \cdots \\
0 \arrow[r] & M \arrow[r] \arrow[u, "f"] & Q_0 \arrow[r] \arrow[u, "\phi^0"] & Q_1 \arrow[r] \arrow[u, "\phi^1"] & Q_2 \arrow[r] \arrow[u, "\phi^2"] & \cdots
\end{tikzcd}$$

which is unique up to homotopy. The homotopy is given by R-linear maps $h^n : Q_n \to E_{n-1}$, and if $\phi^\bullet$, $\psi^\bullet$ are two different liftings of f, then

$$\phi^n - \psi^n = e^{n-1}h^n + h^{n+1}d^n$$

for all n for a suitably chosen homotopy $h^\bullet$.

This theory can be used to check the independence of the values of Ext from the choice of injective resolution, just as in the case of Tor.

It is easy to verify that $\mathrm{Ext}^n_R(M,\, N)$ is a functor of the two variables M, N, contravariant in M (when N is held fixed) and covariant in N (when M is held fixed). Given a map $M \to M'$, the map on Ext is induced by lifting it to a map of projective resolutions, unique up to homotopy. (Note that applying $\mathrm{Hom}_R(\_\,,\, N)$ reverses the arrows.) Likewise, given a map $N \to N'$ the map on Ext is induced by lifting it to a map of injective resolutions, unique up to homotopy. The following result gives a number of basic properties of Ext:

Proposition. *Let R be a ring, and let M, M_i, N,and N_j be R-modules.*

(a) $\mathrm{Ext}^n_R(M,\, N) = 0$ *if* $n < 0$.

(b) $\mathrm{Ext}^0_R(M,\, N) \cong \mathrm{Hom}_R(M,\, N)$ *canonically, as functors of two variables.*

(c) $\mathrm{Ext}^n_R(M,\, N) = 0$ *for all N and all $n \geq 1$ iff* $\mathrm{Ext}^1_R(M,\, N) = 0$ *for all N iff M is projective.*

(d) $\mathrm{Ext}^n_R(M,\, N) = 0$ *for all M and all $n \geq 1$ iff* $\mathrm{Ext}^1_R(M,\, N) = 0$ *for all M iff N is injective.*

(e) *Given a short exact sequence* $0 \to M_2 \to M_1 \to M_0 \to 0$ *there is a functorial long exact sequence for Ext, namely*

$$0 \to \mathrm{Hom}_R(M_0,\, N) \to \mathrm{Hom}_R(M_1,\, N) \to \mathrm{Hom}_R(M_2,\, N) \to \mathrm{Ext}^1_R(M_0,\, N) \to \cdots$$

$$\to \mathrm{Ext}^n_R(M_0,\, N) \to \mathrm{Ext}^n_R(M_1,\, N) \to \mathrm{Ext}^n_R(M_2,\, N) \to \mathrm{Ext}^{n+1}_R(M_0,\, N) \to \cdots .$$

(f) *Given a short exact sequence* $0 \to N_0 \to N_1 \to N_2 \to 0$ *there is a functorial long exact sequence for Ext, namely*

$$0 \to \mathrm{Hom}_R(M,\, N_0) \to \mathrm{Hom}_R(M,\, N_1) \to \mathrm{Hom}_R(M,\, N_2) \to \mathrm{Ext}^1_R(M,\, N_0) \to \cdots$$

$$\to \mathrm{Ext}^n_R(M,\, N_0) \to \mathrm{Ext}^n_R(M,\, N_1) \to \mathrm{Ext}^n_R(M,\, N_2) \to \mathrm{Ext}^{n+1}_R(M,\, N_0) \to \cdots .$$

(g) *The map given by multiplication by* $r \in R$*, acting on the* R*-module* M*, induces the map given by multiplication by* r *on* $\mathrm{Ext}^n_R(M,\, N)$ *for all* n*. The same is true for the map given by multiplication by* r *on* N*.*

Proof. Part (a) is immediate from the definition. Part (b) follows because the exactness of $\cdots \to P_1 \to P_0 \to M \to 0$ implies the exactness of

$$0 \to \mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_R(P_0,\, N) \to \mathrm{Hom}_R(P_1,\, N),$$

so that $\mathrm{Hom}_R(M,\, N)$ may be identified with

$$H^0\big(\mathrm{Hom}_R(P_\bullet,\, N)\big) = \mathrm{Ker}\,\big(\mathrm{Hom}_R(P_0,\, N) \to \mathrm{Hom}_R(P_1,\, N)\big).$$

If $M = P_0$ is projective it has the very short projective resolution $0 \to P_0 \to 0$, from which it is clear that all the higher $\mathrm{Ext}^n(M, N)$ vanish, $n \geq 1$. On the other hand, if all $\mathrm{Ext}^1(M,\, N)$ vanish, then map a free module P onto M, and consider

$$0 \to N \to F \to P \to 0.$$

When we apply $\mathrm{Hom}_R(P,\, \_)$ we get

$$0 \to \mathrm{Hom}_R(P,\, N) \to \mathrm{Hom}_R(P,\, F) \to \mathrm{Hom}_R(P,\, P) \to \mathrm{Ext}^1_R(P,\, N),$$

from the long exact sequence for Ext, and the last term, $\mathrm{Ext}^1_R(P,\, N)$, is 0 by hypothesis. It follows that $\mathrm{Hom}_R(P,\, F) \to \mathrm{Hom}_R(P,\, P)$ is surjective, and so the identity map on P is the image of some map $g : P \to F$. But then g is a splitting of $F \twoheadrightarrow P$, and so P is a direct summand of F and therefore projective. The proof of (d) is entirely similar, and the details are left to the reader. (At the last step, one shows that N is a direct summand of an injective module in which it is embedded, and therefore injective.)

To prove (e) one may Hom the short exact sequence $0 \to M_2 \to M_1 \to M_0 \to 0$ into an injective resolution $E^\bullet$ for N and apply the snake lemma, while for (f) one may hom a projective resolution $P_\bullet$ for M into the short exact sequence $0 \to N_0 \to N_1 \to N_2 \to 0$ and apply the snake lemma. Finally, (g) follows because the map given by multiplication by r on every projective (respectively, injective) module of the resolution lifts multiplication by r on M (respectively, on N) to a map of the projective (respectively, injective) resolution. □

An easy but important fact is that if M and N are finitely generated modules over a Noetherian ring R, all of the modules $\mathrm{Ext}_R^n(M,\,N)$ are finitely generated. The point is the one may compute Ext using a projective resolution $P_\bullet$ of M by finitely generated free modules over R. Then $\mathrm{Hom}(P_\bullet,\,N)$ has terms each of which consists of a direct sum of finitely many copies of N, and so every term is a Noetherian module (although there may be infinitely many terms). It follows that the cohomology is Noetherian. We record this explicitly:

Proposition. *Let R be Noetherian and let M and N be finitely generated R-modules. Then the modules $\mathrm{Ext}_R^n(M,\,N)$ are all Noetherian.* □

The following two results use the behavior of Ext to characterize injective dimension and projective dimension.

Proposition. *Let R be a ring, and $n \geq 0$ an integer. The following conditions on the R-module M are equivalent:*

(1) $\mathrm{pd}_R M \leq n$.

(2) $\mathrm{Ext}_R^{n+1}(M,\,N) = 0$ *for every R-module N.*

(3) $\mathrm{Ext}_R^{j}(M,\,N) = 0$ *for all $j > n$ and every R-module N.*

Proof. It is clear that (1) ⇒ (3) since we may use a projective resolution of M of length at most n to compute $\mathrm{Ext}^j(M,\,N)$, and (3) ⇒ (2) is obvious. We prove that (2) ⇒ (1) by induction on n. The case $n = 0$ is (c) of the preceding Proposition. If $n > 0$, form a short exact sequence $0 \to M_1 \to P \to M \to 0$. The long exact sequence for Ext shows that $\mathrm{Ext}^{n+1}(M,N) \cong \mathrm{Ext}^n(M_1,N) = 0$ for all N, and so M_1 a first module of syzygies of M has projective dimension $\leq n-1$ by the induction hypothesis. It follows that $\mathrm{pd}_R M \leq n$, as required. □

Proposition. *Let R be a ring. Then N is injective if and only if* $\mathrm{Ext}_R^1(R/I,\,N) = 0$ *for every ideal I of R.*

Moreover, for every integer $n \geq 0$ the following conditions on the R-module N are equivalent:

(1) $\mathrm{id}_R N \leq n$.

(2) $\mathrm{Ext}_R^{n+1}(R/I,\,N) = 0$ *for every ideal $I \subseteq R$.*

(3) $\mathrm{Ext}^j_R(M,\,N) = 0$ *for all* $j > n$ *and every* R*-module* M.

Proof. Given an ideal $I \subseteq R$ we have a short exact sequence $0 \to I \subseteq R \to R/I \to 0$ yielding that the following is exact from the long exact sequence for Ext:

$$0 \to \mathrm{Hom}_R(R/I,\,N) \to \mathrm{Hom}_R(R,\,N) \to \mathrm{Hom}_R(I,\,N) \to \mathrm{Ext}^1_R(R/I,\,N).$$

If the rightmost term vanishes, then the map $\mathrm{Hom}_R(R,\,N) \to \mathrm{Hom}_R(I,\,N)$ is surjective, which means that every linear map $I \to N$ extends to a map $R \to N$. This is sufficient for N to be injective by the Proposition at the top of third page of the Lecture Notes from February 21.

It remains to show the equivalence of (1), (2), and (3), which is quite similar to the proof of the preceding result. First, (1) $\Rightarrow$ (3) because an injective resolution of N of length at most n may be use to compute $\mathrm{Ext}^j(M,\,N)$, and (3) $\Rightarrow$ (2) is obvious. We prove that (2) $\Rightarrow$ (1) by induction on n. The case $n = 0$ is the statement we proved in the preceding paragraph. If $n > 0$ we form a short exact sequence $0 \to N \to E \to N' \to 0$ where E is injective. The long exact sequence for Ext shows that $\mathrm{Ext}^{n+1}(R/I, N) \cong \mathrm{Ext}^n(R/I, N') = 0$ for all R/I, and so N', a first module of cosyzygies of N, has injective dimension $\leq n-1$ by the induction hypothesis. It follows that $\mathrm{id}_R N \leq n$, as required. □

We can now show that over a Noetherian regular ring R of Krull dimension d, the projective dimension of *every* module is at most d. We already know this for finitely generated modules. The argument is almost magically simple.

Corollary (J.-P. Serre). *Let* R *be a Noetherian regular ring of Krull dimension* d*. Then the projective dimension of every module, whether finitely generated or not, is at most* d*. Thus, every* d *th module of syzygies is projective.*

Proof. We know that for every ideal I of R, $\mathrm{pd}_R(R/I) \leq d$, since R/I is finitely generated. Thus, for all I and all N, $\mathrm{Ext}^j_R(R/I,\,N) = 0$ for $j > d$, and this implies that for all N, $\mathrm{id}_R N \leq d$. But then, for every R-module M, and every R-module N, $\mathrm{Ext}^j_R(M,\,N) = 0$ for $j > d$, and since this holds for all N, it follows that $\mathrm{pd}_R M \leq d$, as claimed. □

Math 615: Lecture of February 28, 2020

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

$$u_{j_1,\,\ldots\,,j_i} = u_{j_1} \wedge \cdots \wedge u_{j_i}$$

with $1 \le j_1 < \cdots < j_i \le n$ as a basis for $\mathcal{K}_i = \mathcal{K}_i(\underline{x};\, R)$. Let $\_^*$ 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 $\Sigma = \sum_{t=1}^{i}(j_t - 1)$.

We next want to note that, as was the case for Tor, if we have an exact sequence $0 \to M_1 \to P \to M \to 0$, so that M_1 is a first module of syzygies of M over R, the long exact sequence for Ext yields both

$$0 \to \mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_R(P,\, N) \to \mathrm{Hom}_R(M_1,\, N) \to \mathrm{Ext}^1_R(M,\, N) \to 0$$

and isomoorphisms

$$\mathrm{Ext}^i_R(M_1,\, N) \to \mathrm{Ext}^{i+1}_R(M,\, N)$$

for $i > 0$.

Thus, every element of $\mathrm{Ext}^1_R(M,\, N)$ is represented by a map from a first module of syzygies of M to N, and the element of $\mathrm{Ext}^1_R(M,\, N)$ represents the obstruction to extending that map from M_1 to all of P. By induction, if M_i is an ith module of syzygies of M, $i \ge 1$, then

$$\mathrm{Ext}^{i+j}_R(M, N) \cong \mathrm{Ext}^j_R(M_i,\, N),$$

$j \geq 1$. In particular, for $i \geq 1$, we have that $\mathrm{Ext}^i_R(M, N) \cong \mathrm{Ext}^1_R(M_{i-1}, N)$, and an element of $\mathrm{Ext}^i_R(M,\, N)$ will be represented by a map $M_i \to N$, giving the obstruction to extending the map to P_{i-1}, where $0 \to M_i \to P_{i-1} \to M_{i-1} \to 0$ is exact.

This can be seen more directly. Let $P_\bullet$ be a projective resolution of M, and let

$$M_i = \mathrm{Ker}\,(P_{i-1} \to P_{i-2}) = \mathrm{Im}\,(P_i \to P_{i-1})$$

for all $i \geq 1$, so that M_i is an $i\,$th module of syzygies of M. An element of $\mathrm{Ext}^i(M,\, N)$ is represented by a cycle in $\mathrm{Hom}_R(P_i,\, N)$, that is, a map $P_i \to N$ that kills the image of P_{i+1}. But this is the same thing as a map of $P_i/\mathrm{Im}\,(P_{i+1}) \cong M_i$ to N. The boundaries are the maps $P_i \to N$ that arise by composing $P_i \to P_{i-1}$ with a map $P_{i-1} \to N$. The corresponding maps $M_i \to N$ are the ones that extend to P_{i-1}.

Entirely similar marks apply to cosyzygies: one can form $0 \to N \to E \to N^1 \to 0$, where E is injective and N^1 is a first module of cosyzygies of N, and the long exact sequence for Ext yields:

$$0 \to \mathrm{Hom}_R(M,\, N) \to \mathrm{Hom}_R(M,\, E) \to \mathrm{Hom}_R(M,\, N^1) \to \mathrm{Ext}^1_R(M,\, N) \to 0$$

and isomorphisms

$$\mathrm{Ext}^i_R(M,\, N^1) \to \mathrm{Ext}^{i+1}_R(M,\, N)$$

for $i \geq 1$. Likewise, one has isomorphisms

$$\mathrm{Ext}^{i+j}_R(M, N^j) \cong \mathrm{Ext}^j_R(M,\, N^i)$$

when N_i is an $i\,$th module of cosyzygies for N.

Proposition (flat base change in the Noetherian case). *Let R be Noetherian, let S be a flat R-algebra, and let M, N be R-modules. There is a natural isomorphism*

$$S \otimes_R \mathrm{Ext}^j(M,\, N) \to \mathrm{Ext}^j_S(S \otimes_R M,\, S \otimes_R N).$$

Proof. Let $P_\bullet$ be a projective resolution of M by finitely generated (hence, finitely presented) projective modules. Then

$$S \otimes_R \mathrm{Ext}^\bullet_R(M,\, N) \cong S \otimes_R H^\bullet\big(\mathrm{Hom}_R(P_\bullet,\, N)\big) \cong H^\bullet\big(S \otimes_R \mathrm{Hom}_R(P_\bullet,\, N)\big)$$

since S is flat, and since every P_j is finitely presented, this is

$$\cong H^\bullet\big(\mathrm{Hom}_S(S \otimes_R P_\bullet,\, S \otimes_R N)\big) \cong \mathrm{Ext}^\bullet_S(S \otimes_R M,\, S \otimes_R N),$$

since $S \otimes_R P_\bullet$ is a projective resolution of $S \otimes_R M$ over S. It is straightforward to verify that these isomorphisms are independent of the choice of the resolution $P_\bullet$. $\square$

In particular, when R, M, N are Noetherian, Ext commutes with localization and completion.

We briefly describe an alternative approach to the construction of Ext in the category of R-modules which does not use projective or injective modules in the definition. This definition can be adapted to contexts in which there are not enough projective objects and not enough injective objects. We shall not give a complete treatment here: these remarks are only intended to introduce the reader to this circle of ideas. However, we do give examples that show that this point of view leads to new insights about Ext.

We begin with Ext^1. Notice that given a short exact sequence $0 \to A \to B \to C \to 0$ (an extension of C by A) the long exact sequence for exact yields an exact sequence

$$\mathrm{Hom}_R(A,\, A) \to \mathrm{Hom}_R(B,\, A) \to \mathrm{Hom}_R(A,\, A) \to \mathrm{Ext}^1_R(C,\, A),$$

and the identity map on A has an image in $\epsilon \in \mathrm{Ext}^1_R(C,\, A)$.

This element ϵ classifies the extension of C by A in the following sense. Call two such exact sequences $0 \to A \to B \to C \to 0$ and $0 \to A \to B' \to C \to 0$ *equivalent* if there is a map from one to other as follows:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & B' \arrow[r] & C \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[u, "1_A"] & B \arrow[r] \arrow[u, "f"] & C \arrow[r] \arrow[u, "1_C"] & 0
\end{tikzcd}$$

If there is such a map, f is forced to be an isomorphism, and so in this case there is a map the other way. (When we consider higher Ext, there may be a map in one direction but not the other.)

It turns out that two extensions of C by A are equivalent if and only if they give rise to the same element in $\mathrm{Ext}^1_R(C,\, A)$. In fact, suppose that we have such an extension. Write $C = P/C_1$, where P is projective and C_1 is a first module of syzygies of C. Then the map $P \twoheadrightarrow C$ will lift to a map $P \to B$. Then $A \oplus P$ will will map onto B (sending A to B via the given injection $A \hookrightarrow B$), and the map $P \to B$ will map C_1 to A. This map $h : C_1 \to A$ is represents an element of $\mathrm{Ext}^1(C,\, A)$. Conversely, given any element of $\mathrm{Ext}^1_R(C,\, A)$, it is represented by a map $h : C_1 \to A$, and we can construct an extension $A \to B \to C \to 0$ by taking $B = (A \oplus P)/N$, where $N = \{-h(u) \oplus u : u \in C_1\}$, so that every element of C_1 is identified in the quotient with its image in A. Notice that if we kill the image of A in B, $C_1 \subseteq P$ is also killed, and the quotient is C. This explains the map from $\mathrm{Ext}^1_R(C,\, A)$ to equivalence classes of extensions. The remaining details of the proof that $\mathrm{Ext}^1_R(C,\, A)$ classifies extensions are reasonably straightforward.

In describing higher Ext, there is a set-theoretic problem, which we ignore for the moment. Consider exact sequences of length $n+2$, where $n \geq 1$, of the form

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \to C \to 0.$$

We define two such sequences to be *immediately equivalent* (not standard terminology) if there is a map between them that is the identity on A and on C. The intermediate maps need not be isomorphsims when $n \geq 1$. Immediate equivalence generates an equivalence relation. We claim that the equivalence classes are in bijective correspondence with the elements of $\mathrm{Ext}^n_R(C,\, A)$, and we can define $\mathrm{Ext}^n_R(C,\, A)$ in terms of these equivalence classes.

We first give the map in one direction: fix a projective resolution $P_\bullet$ of C. Then the identity map on C lifts to map of the resolution to the exact sequence, and thus proivdes a map $P_n \to A$ that kills the image of P_{n+1}. This map represents an element of $\mathrm{Ext}^n_R(C,\, A)$. In the other direction, given a map of an nth module of syzygies C_n of C to A, call it h, we construct an exact sequence simply by modifying the last two terms of

$$0 \to C_n \to P_{n-1} \to \cdots \to P_0 \to C \to 0.$$

We replace C_n by A, and P_{n-1} by $(A \oplus P_{n-1})/N$ where $N = \{-h(u) \oplus u : u \in C_n\}$.

Here are four insights that come from this point of view.

Given

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \xrightarrow{\alpha} C \to 0$$

representing an element of $\mathrm{Ext}^n_R(C,\, A)$ and

$$0 \to C \xrightarrow{\beta} D_{m-1} \to \cdots \to D_0 \to E \to 0$$

representing an element of $\mathrm{Ext}^m_R(E, C)$, one can form an exact sequence that "merges" them, dropping C, namely

$$0 \to A \to B_{n-1} \to \cdots \to B_0 \xrightarrow{\beta\circ\alpha} D_{m-1} \to \cdots \to D_0 \to E \to 0.$$

This gives a map $\mathrm{Ext}^m_R(E,\, C) \times \mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^{m+n}_R(E,\, A)$ that turns out to be bilinear. It is called the *Yoneda pairing.*

Second, given a ring homorphism $R \to S$ and S-modules A, C, an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

is obviously an exact sequence of R-modules as well. This gives a very understandable map $\mathrm{Ext}^n_S(M,\, N) \to \mathrm{Ext}^n_R(M,\, N)$.

Third, given an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

of R-modules, if S is R-flat we get an exact sequence

$$0 \to S \otimes_R A \to S \otimes_R B_0 \to \cdots \to S \otimes_R B_{n-1} \to S \otimes_R C \to 0.$$

This gives a rather obvious map $\mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_S(S \otimes_R C, S \otimes_R A)$ and hence a map

$$S \otimes_R \mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_S(S \otimes_R C, S \otimes_R A)$$

which is always defined when S is R-flat. We proved earlier that it is an isomorphism under additional hypotheses (if R, C and A are Noetherian).

Fourth, given an exact sequence

$$0 \to A \to B_0 \to \cdots \to B_{n-1} \to C \to 0$$

of R-modules, representing an element of $\mathrm{Ext}^n_R(C,\, A)$, if E is injective over R and $\_^\vee$ denotes $\mathrm{Hom}_R(\_\,,\, E)$, we get an exact sequence

$$0 \to C^\vee \to B^\vee_{n-1} \to \cdots \to B^\vee_0 \to A^\vee \to 0$$

representing an element of $\mathrm{Ext}^n_R(A^\vee,\, C^\vee)$, and so we get a transparently defined map

$$\mathrm{Ext}^n_R(C,\, A) \to \mathrm{Ext}^n_R(A^\vee,\, C^\vee).$$

Math 615: Lecture of March 9, 2020

There is a set-theoretic difficulty with the Yoneda definition of Ext: when $n > 1$ the cardinalities of the modules that can occur are not bounded, and so, even if the isomorphism classes of the modules allowed are restricted, the possible exact sequences form a class rather than a set. This is not an essential difficulty. We have given a construction that provides at least one exact sequence for every element of $\mathrm{Ext}^n_R(C,\, A)$. If one chooses an infinite cardinal that is at least as large as the cardinalities of R, C, and A, one can represent any element of $\mathrm{Ext}^n_R(C,\, A)$ by an exact sequence, of length $n+2$, whose modules are at most of that cardinality. Thus, for any sufficiently large cardinal, one can choose a set of modules that include all isomorphism classes of modules of at most that cardinality, and then consider the equivalence classes of exact sequences from A to C consisting of modules of at most that cardinality. This set will be in bijective correspondence with the elements of $\mathrm{Ext}^n_R(C,\, A)$. If the ring is Noetherian and one wants to work exclusively with finitely generated modules, one can also do that.

It is not difficult to describe the functorial behavior of Ext from the Yoneda point of view. Suppose that we are given R-modules A and C and a map $f : A \to A'$. Given an exact sequence

$$0 \to A \xrightarrow{\alpha} B_n \xrightarrow{\beta} B_{n-1} \to \cdots \to B_1 \xrightarrow{\delta} B_0 \xrightarrow{\gamma} C \to 0$$

representing an element of $\mathrm{Ext}^n_R(C,\, A)$, we expect to be able to construct an exact sequence corresponding to the image of that element in $\mathrm{Ext}^n_R(C,\, A')$. We replace B_n by

$$\frac{A' \oplus B_n}{\{-f(a) \oplus \alpha(a) : a \in A\}}$$

and A by A'. α is replaced by the map α' induced by the map $A' \to A' \oplus B_n$, which is easily seen to be injective, while β is replaced by the homomorphism induced by the map $A' \oplus B \to B_{n-1}$ that kills A' and agrees with β on B.

Similarly, given a map $g : C' \to C$ and an exact sequence representing an element of $\mathrm{Ext}^n_R(C,\, A)$ one expects to be able to construct an exact sequence representing an element of $\mathrm{Ext}^n_R(C',\, A)$. One replaces B_0 by

$$B_0' = \{(b,\, c') \in B \times C' : \gamma(b) = g(c')\}$$

and C by C'. γ is replaced by the restriction of the product projection of $B \times C' \twoheadrightarrow C'$ to B_0': it is still surjective. δ is replaced by the map $\delta' : b_1 \mapsto (\delta(b_1),\, 0)$.

The multiplication by elements of R acting on $\mathrm{Ext}^n_R(C,\, A)$ is recovered by using one of these two constructions either for $f : A \xrightarrow{r} A$ or $g : C \xrightarrow{r} C$, which turn out to give the same result.

Addition in $\mathrm{Ext}^1_R(C, \mathbb{A})$ can be described as follows. Suppose that

$$0 \to A \xrightarrow{\alpha} B \overset{\gamma}{\twoheadrightarrow} C \to 0$$

and

$$0 \to A \xrightarrow{\alpha'} B' \overset{\gamma'}{\twoheadrightarrow} C \to 0$$

are exact. Let

$$B'' = \frac{\{(u,\, u'\} \in B \times B' : \gamma(u) = \gamma(u')\}}{\{(-\alpha(a),\, \alpha'(a)) : a \in A\}}$$

Notice that we have a map $\gamma'' : B'' \twoheadrightarrow C$ whose value on the class of $(u,\, u')$ is $\gamma(u)$, which is the same as $\gamma'(u')$, and a map $\alpha'' : A \to b''$ whose value on A is the class of $(\alpha(a), 0)$, which is the same as the class of $(0,\, \alpha'(a))$. It is not difficult to verify that

$$0 \to A \xrightarrow{\alpha''} B'' \xrightarrow{\gamma''} C \to 0$$

is exact, and represents the sum of the elements corresponding to the two exact sequences initially given.

Of great importance is that the 0 element in $\mathrm{Ext}^1_R(C,\, A)$ corresponds to the split exact sequence

$$0 \to C \to C \oplus A \to A \to 0.$$

In particular, $\operatorname{Ext}^1_R(C,\, A) = 0$ if and only if every exact sequence

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

is split.

The Yoneda point of view gives a transparent interpretation of the connecting homomorphism in the long exact sequence for Ext. Suppose that

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

is exact, and we apply $\operatorname{Hom}_R(\_,\, N)$. The connecting homomorphisms in the long exact sequence for Ext are maps

$$\operatorname{Ext}^n_R(A,\, N) \to \operatorname{Ext}^{n+1}_R(C,\, N).$$

These are obtained, up to sign, from the Yoneda pairing: given an element of $\operatorname{Ext}^n_R(A,\, N)$ represented by an exact sequence:

$$0 \to N \to W_{n-1} \to \cdots \to W_0 \to A \to 0,$$

because $A \cong \operatorname{Ker}(B \to C)$ we also have an exact sequence

$$0 \to N \to W_{n-1} \to \cdots \to W_0 \to B \to C \to 0.$$

Similarly, if we apply $\operatorname{Hom}_R(M,\, \_)$ the connecting homomorphisms map

$$\operatorname{Ext}^n_R(M,\, C) \to \operatorname{Ext}^{n+1}_R(M,\, A).$$

Again, up to sign, they turn out to be given by the Yoneda pairing: the element represented by

$$0 \to C \to V_{n-1} \to \cdots \to V_0 \to M \to 0$$

maps to the element represented by

$$0 \to A \to B \to V_{n-1} \to \cdots \to V_0 \to M \to 0.$$

Ext characterization of depth The following is a very useful way to look at the notion of depth.

Theorem (Ext characterization of depth). *Let $R \to S$ be a homomorphism of Noetherian rings, let I be an ideal of S, let N be a finitely generated R-module with annihilator I, and let M be a finitely generated S-module. The modules $\mathrm{Ext}^j_R(N,\, M)$ are Noetherian S-modules. If $IM = M$ then all of the modules $\mathrm{Ext}^j_R(N,\, M)$ vanish. If $IM \neq M$, and $\mathrm{depth}_I M = d$, then $\mathrm{Ext}^j_R(N,\, M) = 0$ for $j < d$, and $\mathrm{Ext}^d_R(N,\, M) \neq 0$.*

Proof. To see that these Ext modules are Noetherian over S, compute them using a projective resolution $P_\bullet$ of N over R by finitely generated free R-modules. Then $\mathrm{Hom}_R(P_\bullet;\, M)$ consists of finite direct sums of copies of M, and so this complex and its homology consist of Noetherian S-modules.

Next note that $M/IM = 0$ iff $S/IS \otimes_S M = 0$ iff $IS + \mathrm{Ann}_S M = S$. In this case, since the annihilator J of every $\mathrm{Ext}^j_R(N,\, M)$ in S contains IS (because I kills $\mathrm{Ext}^j_R(N,\, M)$ and J is an ideal of S) and contains $\mathrm{Ann}_S M$, we have that $J = S$, so that, for every j, $\mathrm{Ext}^j_R(N,\, M) = 0$.

Now assume that $M \neq IM$, so that $d = \mathrm{depth}_I M$ is finite. We prove the result by induction on d. 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 $d > 0$. Then we can choose a nonzerodivisor $x \in I$ on M, and 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

$$(*_j) \quad 0 \to \mathrm{Ext}^j_R(N,\, M) \to \mathrm{Ext}^j_R(N,\, M/xM) \to \mathrm{Ext}^{j+1}_R(N,\, M) \to 0$$

Since M/xM has depth $d-1$ on N, we have from the induction hypothesis that the modules $\mathrm{Ext}^j_R(N,\, M/xM) = 0$We 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 $\mathrm{Ext}^d_R(N,\,M)$. □

Corollary. *Let $R \to S$ be a homomorphism of Noetherian rings, $f_1,\,\ldots\,,f_n \in R$, $I = (f_1,\,\ldots\,,f_n)R$, and let M be a finitely generated S-module. Then $IM \neq M$ if and only if at least one Koszul homology module $H_i(f_1,\,\ldots\,,f_n;\,M)$ is not 0, in which case the least integer j such that $H_j(f_1,\,\ldots\,,f_n;\,M) \neq 0$ is $n-d$, where d is the depth of M on I, which is the same as the depth of M on IS.*

Proof. We may map $A = Z[X_1,\,\ldots\,,X_n] \to R$ by sending $X_i \to f_i$. Since the Koszul complex $\mathcal{K}_\bullet := \mathcal{K}_\bullet(X_1,\,\ldots\,,X_n;\,A)$ resolves $A[X_1,\,\ldots\,,X_n]/(X_1,\,\ldots\,,X_n)$ over A, the Ext characterization of depth recovers the depth from the nonvanishing cohomology of $\mathrm{Hom}(\mathcal{K}_\bullet, M)$, which may be identify with the cohomology of $\mathrm{Hom}(\mathcal{K}_\bullet, A) \otimes_A M$ numbered backwards using the self-duality of the Koszul complex, which yields the stated result. □

Multiplicities via Koszul homology

We want to prove the following result of J.-P. Serre:

Theorem. *Let $(R,\,m,\,K)$ be a local ring of Krull dimension d, let $\underline{x} = x_1,\,\ldots\,,x_d$ be a system of parameters for R, and let M be a nonzero finitely generated R-module. Let $\dfrac{e}{d!}$ be the coefficient of t^d in the Hilbert polynomial $H(t)$ of M with respect to $I = (x_1,\,\ldots\,,x_d)R$, (thus, $H(t) = \ell(M/I^{t+1}M)$ for all $t \gg 0$). Then the Euler characteristic $\chi(\underline{x};M)$ of the Koszul complex $\mathcal{K}_\bullet(\underline{x};M)$ is equal to e, and therefore is 0 if $\dim(M) < d$ and is positive and equal to the multiplicity of M with respect to I if $\dim(M) = d$.*

Before giving the proof, we discuss the *staggered I-adic filtration* of the Koszul complex $\mathcal{K}_\bullet := \mathcal{K}_\bullet(\underline{x};\,M)$. Let M be a Noetherian module over a Noetherian ring R, let $\underline{x} = x_1,\,\ldots\,,x_d \in R$ and let $I = (x_1,\,\ldots\,,x_d)R$. We put a staggered I-adic filtration on the Koszul complex as follows: we let $\langle\mathcal{K}_i(\underline{x};\,M)\rangle_t = I^{t-i}\mathcal{K}_i(\underline{x};\,M)$, where I^s is defined to be R if $s \leq 0$. The fact that these are subcomplexes is a consequence of the fact that the entries of the matrices for the Koszul complex are elements of I.

We next note that the subcomplex $I^t\mathcal{K}_\bullet(\underline{x};\,M) \subseteq \mathcal{K}_\bullet(\underline{x};\,M)$ may be identified with $\mathcal{K}_\bullet(\underline{x};\,I^tM)$, and that its homology is therefore killed by I.

In consequence, the staggered I-adic filtration yields subcomplexes that are *exact* for all sufficiently large t. There are only finitely many i for which we need to see that this is true, and it so suffices to prove this for each of them individually. Let one such i be given. We to check that for all $t \gg 0$, every z in the kernel of $I^{t-i}\mathcal{K}_i \to I^{t-i+1}\mathcal{K}_{i-1}$ is in the image of $I^{t-i-1}\mathcal{K}_i$. Let Z_i denote the kernel of $\mathcal{K}_i \to \mathcal{K}_{i-1}$. Then $z \in I^{t-i}\mathcal{K}_i \cap Z_i$, and by the Artin-Rees lemma for $t \gg 0$, $z \in I(I^{t-1-i}\mathcal{K}_i \cap Z_i$. But since I kills the homology of $I^{t-1-i}\mathcal{K}_i$, it follows that z maps to 0 in the homology of $I^{t-1-i}\mathcal{K}_i$, and so it is in the image of $I^{t-1-i}\mathcal{K}_{i+1}$, as required.

Proof. We have an exact sequence of complexes

$$0 \to \langle \mathcal{K}_\bullet \rangle_t \to \mathcal{K}_\bullet \to \mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_t \to 0.$$

For all $t \gg 0$, the homology of $\langle \mathcal{K}_\bullet \rangle_t$ vanishes. Hence, the long exact sequence for homology yields isomorphisms:

$$H_i(\mathcal{K}_\bullet) \cong H_i(\mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_t)$$

for all $t \gg 0$. Thus, the Euler characteristic of the complex $\mathcal{K}_\bullet$, which we are studying, is the same as $\chi(\mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_t)$ for all $t \gg 0$. The modules in $\mathcal{K}_\bullet / \langle \mathcal{K}_\bullet \rangle_t$ have finite length, and so the alternating sum of the lengths of the homology modules is the same as the alternating sum of the lengths of the modules $\mathcal{K}_i / I^{t-i}\mathcal{K}_i$ for all $t \gg 0$. Now, $\mathcal{K}_i / I^{t-i}\mathcal{K}_i$ is the direct sum of $\displaystyle\binom{d}{i}$ copies of $M/I^{t-i}M$, and so for all $t \gg 0$ we have

$$\chi(\underline{x};\, M) = \sum_{i=0}^{d} (-1)^i \binom{d}{i} \ell(M/I^{t-i}M) = \sum_{i=0}^{d} (-1)^i \binom{d}{i} H(t-i-1).$$

For any polynomial P of t, $(\Delta^d P)(t) = \sum_{i=0}(-1)^i \binom{d}{i} P(t-i)$ by a straightforward induction on d, where Δ^d is the dth iteration of the operator Δ. The rightmost expression displayed above is therefore Δ^d applied to the polynomial $t \mapsto H(t-1)$. The fact that $M/(x_1, \ldots, x_d)M$ has finite length implies that $d \geq \delta := \dim(M)$. Each iteration of Δ decreases the degree of the polynomial input by one (after the polynomial reaches a constant, further iterations simply produce the 0 polynomial) and multiplies the leading term by the degree. Since $H(t-1)$, like $H(t)$, has leading term $\dfrac{e}{\delta!}t^\delta$, we see that if $d = \delta$ then Δ^d applied to $H(t-1)$ produces the constant e, while if $d > \delta$, the result is 0. □

Properties of Cohen-Macaulay rings

Theorem. *The following conditions on a local ring $(R, \mathfrak{m}, K)$ of Krull dimension d are equivalent.*

(a) There exists a system of parameters for R that is a regular sequence.

(b) Every system of parameters for R is a regular sequence.

(c) $\dim(R) = \operatorname{depth}_{\mathfrak{m}} R$.

If these equivalent conditions hold, the local ring R is called Cohen-Macaulay.

Proof. Since a nonzerodivisor is part of a system of parameters, a regular sequence in R is part of a system of parameters. Hence, (c) implies (a). Since every system of parameters, say $\underline{x}$, generates an ideal with radical $\mathfrak{m}$, the depth of R is $\dim(R)$ if and only if depth of R on $(\underline{x})$ is $\dim(R)$, and this is equivalent to the vanishing of the Koszul homology $H_i(\underline{x}; R)$ for $1 \leq i \leq d$. But this implies $\underline{x}$ is a regular sequence independent of the choice of $\underline{x}$. □

Theorem. *Let R be a Noetherian ring. The following conditions are equivalent:*

(a) The local ring of R at every maximal ideal is Cohen-Macaulay.

(b) The local ring of R at every prime ideal is Cohen-Macaulay.

(c) For every proper ideal I of R, the depth of R on I is the same as the height of I.

(d) If $f_1, \ldots, f_h$ are elements of R generating an ideal I of height h, then all associated primes of I are minimal of height h.

If these equivalent conditions hold, R is called Cohen-Macaulay. *Moreover, if R is Cohen-Macaulay and the situation of part (d) holds, R/I is also Cohen-Macaulay.*

Proof. Clearly, (b) ⇒ (a). To show that (a) ⇒ (d), we may localize at an associated prime P of I. Then $f_1, \ldots, f_h$ becomes part of a system of parameters for R_P, and so it is a regular sequence. It must be a maximal regular sequence: since R/P embeds in R/I, this remains true after localization, which shows that R_P/I_P has depth 0 on PR_P. But since R_P is Cohen-Macaulay local, we then have $h = \dim(R_P) = \text{height}\,(P)$.

To prove that (d) ⇒ (c), let $f_1, \ldots, f_k$ be a maximal regular sequence in I. It remains a regular sequence in every local ring at a prime containing I, which shows that the height h if I is at least k. Since $f_1, \ldots, f_k$ is a maximal regular sequence in I, it has an associated prime P that contains I. By the assumption of (d), P has height k, and so $k = \text{height}\,(P) \geq he(I) = h$, the other inequality.

Finally, (c) ⇒ (b) since for any prime P of height h, the we have a regular sequence in P of length h, and this remains true when we localize at P.

The final statement reduces to the case of R_P for primes $P \supseteq I$. But then the generators of I become part of a system of parameters in a Cohen-Macaulay local ring, and when we pass to R_P/IR_P, the depth and dimension both drop by h. □

Proposition. *Let R be a module-finite extension of a regular local ring $(A, \mathfrak{m})$ that is local or is torsion-free as an A-module. Then R is Cohen-Macaulay if and only if it is a free (equivalently, flat, equivalently projective) A-module.*

Proof. If R is local, a system of parameters for A is aso a system of parameters for R, and the result now follows at once from the Auslander-Buchsbaum theorem. Every maximal ideal Q of R lies over $\mathfrak{m}$, and it is clear from the lying over theorem that the height of Q is at most the dimension of A, and from the going down theorem (A is normal) that the height of Q is at least the dimension of A. Let $\underline{x}$ be a system of parameters for A. Then it is also a system of parameters in R_Q. Hence, if R is flat over A, it is a regular sequence in R_Q and R_Q is Cohen-Macaulay. On the other hand, if each R_Q is Cohen-Macaulay, then $\underline{x}$ is a regular sequence in each R_Q. It follows that it is a regular sequence in R. The result now follows again from the Auslander-Buchsbaum theorem. □

The graded situation is especially nice. We first note:

Lemma. *Let $K[x_1, \dots, x_d]$ be a polynomial ring over a field K. Let M be $\mathbb{Z}$-graded module such that $M_{-N} = 0$ for all $N \gg 0$. Then M is free over R if and only if $x_1, \dots, x_d$ is a regular sequence on M.*

Proof. It is clear that if M is free, $x_1, \dots, x_d$ is a regular sequence. Let $\mathfrak{m} = (x_1, \dots, x_d)R$. The images of the homogeneous elements span $M/\mathfrak{m}M$ over K and so have a subset that is a basis $\overline{u}_j$, $J \in J$ (the index set J may be infinite), where the u_j are homogeneous elements of R. By the graded form of Nakayama's lemma, the u_j span M over R, and it suffices to show that they have no nonzero relation. We use induction on d. The case $d = 0$ is clear. If there is a relation $\sum_{j \in J_0} f_j u_j = 0$ choose such a relation in which the largest degree of an f_j occurring in minimum. If x_1 divides all the f_j, then since it is a nonzerodivisor on M we may factor it out to get a relation with coefficients of lower degree. If not, we get a nonzero relation working with R/x_1R and M/x_1M, which contradicts the induction hypothesis. □

Proposition. *Let S be a finitely generated K-algebra that is a module-finite torsion-free extension of the polynomial ring $R = K[F_1, \dots, F_d]$. Then S is a Cohen-Macaulay module if and only it is projective as an R-module.*

If S is module-finite extension of the polynomial ring $K[F_1, \dots, F_d]$ that is graded (so that the F_i are elements of S of positive degree) with $S_0 = K$, then the following conditions are equivalent:

(a) S is Cohen-Macaulay.

(b) The $F_1, \dots, F_d$ are a regular sequence in S.

(c) S is R-free.

(d) $S_\mathfrak{m}$ is Cohen-Macaulay, where $\mathfrak{m}$ is the homogeneous maximal deal of S.

Proof. The first statement follows at once from the Proposition above.

Now consider the graded case. Then (b) and (c) are equivalent by the Lemma above. When these conditions hold, S is R-free and so torsion-free, and so is S is Cohen-Macaulay, which is part (a). Clearly, (a) ⇒ (d). Thus, it suffices to prove that (d) ⇒ (b). By induction on the length of the regular sequence, it suffices to show that if T is $\mathbb{N}$-graded with $T_0 = K$ and homogeneous maximal ideal $\mathfrak{n}$ then if f is homogeneous nonzerodivisor in $T_\mathfrak{n}$, it is a nonzerodivisor in T. This follows because $T \to T_\mathfrak{n}$ is injective: the associated primes of T are homogeneous, and so no element of $T - \mathfrak{n}$ is a zerodivisor in T. □

A Noetherian ring is called *catenary* if given any two primes $P \subseteq Q$ in the ring, are maximal chains (also called it saturated chains) of primes from P to Q have the same length. Homomorphic images and localization of catenary rings are catenary.

Note that by the third problem of Problem Set #3, every nonzero submodule of a Cohen-Macaulay module N of Krull dimension δ has dimension at least δ and, hence, dimension δ. This means that every associated prime P of N is such that $\dim(R/P) = \delta$. In particular, for every minimal prime P of a Cohen-Macaulay local ring R, $\dim(R/P) = \dim(R)$.

Theorem. *Cohen-Macaulay rings and, hence, regular rings are catenary. In a Cohen-Macaulay local ring R, for every prime P,* $\dim(R/P) + \dim(R_P) = \dim(R)$

Proof. We can replace the ring R by R_Q and so assume that Q is maximal. We can also kill a maximal regular sequence in P, so that P is minimal. By the discussion above, $\dim(R//P) = \dim(R)$ and it will suffice to show that every saturated chain of primes from P to the maximal ideal Q has length equal to $\dim(R)$. We use induction on the dimension of R. Suppose we have a strict maximal chain $P = P_0 \subset P_1 \subset \cdots \subset P_i \subset \cdots \subset P_k = Q$, so that there is no prime strictly between P and P_1. P_1 cannot be contained in the union of the minimal primes of R, or it would be contained in one of them. Choose $x \in P_1$ not in ay minimal prime. Then x is not a zerodivisor in R, and the dimension of R/xR, which is again Cohen-Macaulay, is $\dim(R) - 1$. Then $P_1/xR \subset \cdots \subset P_i/xR \subset \cdots \subset P_k/xR$ is a maximal chain in R/xR, and it follows from the induction hypothesis that $k - 1 = \dim(R/xR) = \dim(R) - 1$ so that $k = \dim(R)$.

To prove the final statement choose a saturated chain from P to the maximal ideal whose length is $\dim(R/P)$ and a saturated chain descending from P to a minimal prime of R whose length is $\dim(R_P)$. We may put these together to form a saturated chain from the maximal ideal to a minimal prime of R, which we have already shown has length equal to $\dim(R)$. □

Theorem. *If R is Cohen-Macaulay (respectively, regular), then so are the polynomial and formal power series rings $R[x_1, \ldots, x_n]$ and $R[[x_1, \ldots, x_n]]$.*

Proof. By a straightforward induction, it suffices to consider the case $n = 1$, and we abbreviate $x := x_1$. Let Q be a maximal iddeal of $S = R[x]$ lying over P in R. We may replace R by R_P and so assume that P is maximal. Let $\kappa = R/P$. Then Q corresponds to a maximal ideal of $R[x]/P[x] \cong \kappa[x]$, and so is generated by $P[x]$ and a monic polynomial f of $R[x]$ that is irreducible in $\kappa[x]$. If R is regular, then a regular system of parameters for P together with f generate Q, which imples that $R[x]_Q$ is regular, since its maximal ideal is generated by a regular sequence (note that $R[x]_Q$ is faithfully flat over R). If R is Cohen-Macaulay, choose a maximal regular in R. It is still regular in $R[x]_Q$, by flatness, and so we may pass to the quotients of R and $R[x]_Q$ by this regular sequence. Then $\dim(R) = 0$, and $\dim)R[x]_Q = 1$. Because the image of f is monic, it is not a zerodivisor in $R[x]$ and hence not a zerodivisor in $R[x]_Q$.

Now let Q be maximal in $S := R[[x]]$. Then $x \in Q$, for otherwise x has an inverse f in R/Q and $1 - xf \in Q$. This is a contradiction, since $1 - xf$ has inverse

$$1 + xf + x^2f^2 + \cdots + x^kf^k + \cdots \in S.$$

It follows that Q is generated by x and P, where P is a maximal ideal of R. Then S_Q is Cohen-Macaulay (respectively, regular) since x is a nonzerodivisor in S and S_Q and $S_Q/xS_Q \cong R_P$. □

Ext duals of Cohen-Macaulay modules over regular rings Let M be a finitely generated Cohen-Macaulay module of dimension n over a regular local ring $(R, \mathfrak{m}, K)$ of

Krull dimension d, where $0 \le n \le d$. We shall use the notation $M^\vee$ for $\mathrm{Ext}^{d-n}(M,\, R)$. This gives a kind of "dual" Cohen-Macaulay module. More precisely:

Theorem. *Let $(R,\, \mathfrak{m},\, K)$, d, M, and n be as in the paragraph above. The functor $M \to M^\vee$ is a contravariant exact functor from Cohen-Macaulay modules of Krull dimension n to Cohen-Macaulay modules of Krull dimension n. What is more:*

(a) $\mathrm{Ext}^j(M,\, R) = 0$ except when $j = n - d$

(b) $M^{\vee\vee} \cong M$, and a minimal resolution of M or $M^\vee$ can be be obtained by applying $\mathrm{Hom}_R(\_\,,\, R)$ to the minimal resolution of the other.

(c) M and $M^\vee$ have the same annihilator and the same dimension.

(d) For any prime P, $(M_P)^\vee \cong (M^\vee)_P$.

(e) If x is a nonzerodivisor on M, $(M/xM)^\vee \cong M^\vee/xM^\vee$.

(f) If $M = R/(x_1,\, \dots\,, x_h)R$ is a quotient of R by a regular sequence, $M^\vee \cong M$ (not naturally). In particular, $K^\vee \cong K$.

(g) If M has finite length, so does $M^\vee$, and their lengths are equal.

(h) The least number of generators of a finite length module M is equal to $\dim_K \mathrm{Ann}_{\mathfrak{m}} M^\vee$. That is, for a finite length module and its dual, the least number of generators of each is the same as the K-vector space dimension of the socle in the other.

(i) The type of M is the dimension of the least number generators of $M^\vee$.

Proof. Note that the Auslander-Biuchsbaum theorem implies that $\mathrm{pd}_R M = \mathrm{depth}_R - \mathrm{depth}_{\mathfrak{m}} M = d - n$, which is also $\dim(M)$, since M is Cohen-Macaulay. Note that by the third problem of Problem Set #3, every nonzero submodule of M has dimension at least d and, hence, dimension d. This means that for every associated prime P of M, $\dim(R/P) = d$, so that all associated primes of M are minimal. Since R is regular, we have that for of these P, the height of P is $n - d$, and so the height of $I = \mathrm{Ann}_R M$ is also $n - d$. Therefore, the depth of R on I is $n - d$. By the Ext characterization of depth, $\mathrm{Ext}^i_R(M, R)$ vanishes for $i < n - d$, and since $\mathrm{pd}_R M = n - d$, $\mathrm{Ext}^i_R(M, R)$ vanishes for $i > n - d$. Thus, there is a unique nonvanishing $\mathrm{Ext}^j_R(M, R)$ which occurs when $j = n - d$. Let $h := n - d$.

Consider a minimal resolution of M,

$$(*) \qquad 0 \longrightarrow R^{b_h} \xrightarrow{A_h} \cdots \xrightarrow{A_{i+1}} R^{b_i} \xrightarrow{A_i} \cdots \xrightarrow{A_1} R^{b_0} \to 0$$

where the cokernel of the rightmost map is M. If we apply $\mathrm{Hom}_R(\_\,, R)$ and uses dual bases for the free modules we obtain

$$0 \longrightarrow R^{b_0} \xrightarrow{A_1^{\mathrm{tr}}} \cdots \xrightarrow{A_i^{\mathrm{tr}}} R^{b_i} \xrightarrow{A_{i+1}^{\mathrm{tr}}} \cdots \xrightarrow{A_h^{\mathrm{tr}}} R^{b_h} \to 0$$

where A^{tr} indicates the transpose of the matrix A. Because $\mathrm{Ext}^j(M,\, R) = 0$ except when $j = h$, the complex above is exact except at the rightmost spot, where the cohomology is the cokernel of A_h^{tr} and is $\mathrm{Ext}^h(M,\, R) = M^\vee$. Thus, the display gives a minimal free resolution of $M^\vee$. Thus, $\mathrm{pd}_R M^\vee = n - d$, and so the depth of $M^\vee$ on $\mathfrak{m}$ is d. $M^\vee = \mathrm{Ext}^h(M,\, R)$ is killed by I, and so its dimension is at most $\dim(R/I) = d$. Hence, its dimension must be d, and it is Cohen-Macaulay. If we use the resolution displayed in $(*)$ to compute $M^{\vee\vee}$ we return to the resolution of M and see that $M^{\vee\vee} \cong M$. Thus, the annihilator of $M^\vee$, which contains I, kills M, and it follows that $\mathrm{Ann}_R M^\vee = \mathrm{Ann}_R M$. The fact that $\_^{\,\vee}$ is exact on short exact sequences of Cohen-Macaulay modules of dimension n is now immediate from the long seqence for Ext and the fact that there will be only one nonvanishing term arising from each of three modules, all at the spots indexed by $h = n - d$. hange

We have now established all of the statements except (d) — (g). Note that a prime P is in the support of M iff it is in the support of $M^\vee$. When we localize at a prime in the support, the height h of the annihilator does not change, since all minimal primes of the annihilator have height h. Part (d) now follows because Ext commutes with localization for finitely generated modules over a Noetherian ring.

Part (e) follows by applying the long exact sequence for Ext arising from

$$0 \longrightarrow M \xrightarrow{\cdot x} M \longrightarrow M/xM \longrightarrow 0$$

and $\mathrm{Hom}_R(\_,\, R)$. The only nonzero terms are

$$0 \longrightarrow \mathrm{Ext}_R^h(M,\, R) \xrightarrow{\cdot x} \mathrm{Ext}_R^h(M,\, R) \longrightarrow \mathrm{Ext}_R^{h+1}(M/xM,\, R) \longrightarrow 0$$

which is just what we want.

The result in (f) is immediate from using the Koszul complex $\mathcal{K}_\bullet(x_1, \dots, x_h;\, R)$ as a free resolution of $R/(x_1, \dots, x_h)R$ to compute the Ext dual. Alternatively, $R^\vee = \mathrm{Hom}_R(R, R) \cong R$, and one may apply (e) repeatedly. The statement about K then follows from the fact that $\mathfrak{m}$ is larenerated by a regul.ar sequence.

One then obtains (g) by induction on the length (the case of length 1 is just that $K^\vee \cong K$) and the fact that if $0 \to K \to M \to N \to 0$ is exact, where N has length $n-1$, then $0 \to N^\vee \to M^\vee \to K^\vee \to 0$ is exact.er

Let $(x_1, \dots, x_d)$ generate $\mathfrak{m}$. Then $M^{\oplus d}M \to M/\mathfrak{m}M \to 0$ is exact, where the first map takes $(u_1, \dots, u_d) \mapsto \sum_{i-1}^d x_i u_i$ Applying $\_^{\,\vee}$ gives an exact sequence $0 \to (M/\mathfrak{m}M)^\vee\mathfrak{m} \to M \to M^{\oplus d}$ where the last map takes $u \mapsto (x_1u,\, \dots,\, x_du)$. But the kernel of the last map is $\mathrm{Ann}_M\mathfrak{m}$, which is therefore $\cong (M/\mathfrak{m}M)\vee$. It follows that the K-vector space dimension of $\mathrm{Ann}_M\mathfrak{m}$ is the same as the K-vector space dimension of $(MmfM)^\vee$, which is the same as the K-vector space dimension of $M/\mathfrak{m}M$. This proves (h).

Finally, for part (i), the truth of the statement is unaffected when we replace M by M/xM, using part (e). By repeated application of this fact, we may reduce to the case where M has finite length. The result is then immediate from part (h). □

Invariant theory, Cohen-Macaulay rings, and tight closure

In the next part of the course we study ideas connected with the rings of invariants of linearly reductive algebraic groups acting on polynomial rings, including a proof that they are Cohen-Macaulay. In the process, we introduce ideas from tight closure theory.

To keep prerequisites from algebraic geometry to a minimum, in our study we will take the ground field K to be an algebraically closed field. For the kinds of results that we will be considering, this is no disadvantage: typically, one can deduce results over any infinite field by passing to the algebraic closure.

Linear algebraic groups and their modules

$\mathrm{GL}(n,\,K)$ has the structure of a closed algebraic set, and that the same is true for the $\mathrm{GL}_n(V)$, the group of K-automorphisms of a finite-dimensional vector space V. One gives $\mathrm{GL}_n(V)$ the structure of a closed algebraic set by choosing a basis for V. If $\dim(V) = n$, this gives an identification of V with $\mathrm{GL}(n,\,K)$. The coordinate ring is obtained from the polynomial ring in n^2 variables corresponding to the entries of the $n \times n$ matrix, and adjoining the reciprocal of the determinant of the matrix $\bigl(x_{ij}\bigr)$. However, the structure of V as an algebraic set is independent of the choice of basis: if one takes a different basis, the identification of $GL(n,\,K)$ with V changes, but this is via an automorphism of $\mathrm{GL}(n,\,K)$ given by conjugating by the change of basis matrix. This map is not only a group automorphism: it is also an automorphism in the category of closed algebraic sets.

A *linear algebraic group* G is a Zariski closed subgroup of some $\mathrm{GL}(n,\,K)$. Thus, G has the structure of closed algebraic set.

The product of two closed algebraic sets has the structure of a closed algebraic set. If $X = V(I)$ where $I \subseteq K[x_1,\,\dots\,,x_m]$, so that $X \subseteq \mathbb{A}^m_K$, and $Y = V(J)$ where $J = K[y_1,\,\dots\,,y_n]$, so that $Y \subseteq \mathbb{A}^n_K$ (the variables are taken to be $m+n$ algebraically independent elements) then $X \times Y$ may be identified with $V(IT + JT) \subseteq \mathbb{A}^{m+n}_K$, where $T = K[x_1,\,\dots\,,x_m,\,y_1,\,\dots\,,y_n]$.

It is easy to show that if G is a linear algebraic group, then the map $G \times G \to G$ that corresponds to the group multiplication is regular, as well as the inverse map $G \to G$: this follows from the fact that this is true when $G = \mathrm{GL}(n,\,K)$.

An *action* of a linear algebraic group G on a finite-dimensional vector space V is then a group action $G \times V \to V$ such that the defining map is a morphism of closed algebraic sets, i.e., a regular map over K. The image of $(\gamma,\,v)$ is denoted $\gamma(v)$. Alternatively, it is given by a homomorphism $h : G \to GL_K(V)$: the action is recovered by the rule $\gamma(v) = h(\gamma)(v)$. We then say that V is G-module (over K, but usually we do not mention the field K).

If $W \subseteq V$ is a K-vector subspace such that W is stable under the action of G, the restriction of the map $G \times V \to V$ gives W the structure of a G-module, and we shall say that W is a *G-submodule* of V.

We extend the notion of G-module to infinite-dimensional K-vector spaces as follows: an action of G on an infinite-dimensional vector space V is allowed if V is a directed union of finite-dimensional spaces W such that the restricted action makes W into a G-module.

The direct sum of G-modules becomes a G-module in an obvious way. A G-stable subspace of an infinite-dimensional G-module is again a G-module. If V is a G-module and $W \subseteq V$, then V/W has the structure of G-module such that for all $\gamma \in G$ and $v \in V$, $\gamma(v + W) = \gamma(v) + W$.

A G-module map $f : V \to W$ is a K-linear map such that for all $\gamma \in G$ and $v \in V$, $f\bigl(\gamma(v)\bigr) = \gamma\bigl(f(v)\bigr)$. The inclusion of a G-submodule $W \subseteq V$ is a G-module map, as is the quotient map $V \twoheadrightarrow V/W$.

A nonzero G-module M is called *irreducible* or *simple* if it has no nonzero proper submodule. If M is irreducible it is necessarily finite-dimensional, as it is a directed union of finite-dimensional G-submodules.

A linear algebraic group is called *linearly reductive* if every finite-dimensional G-module is a direct sum of irreducible G-modules. Over an field, the finite groups G such that the order of G is invertible in the field are linearly reductive, and so is an algebraic torus, i.e., a finite product of copies of $GL(1,\, K)$. In characteristic $p > 0$, these are the main examples. But over $\mathbb{C}$ the semisimple groups are linearly reductive as well. We shall comment further about this later.

Linearly reductive linear algebraic groups

Theorem. *Let G be a linearly reductive linear algebraic group and let $W \subseteq V$ be G-modules. Then there is a family of irreducible submodules $\{M_\lambda\}_{\lambda\in\Lambda}$ in V such that*

$$V = W + \sum_{\lambda\in\Lambda} M_\lambda$$

and the sum is direct. Hence, if

$$W' = \sum_{\lambda\in\Lambda} M_\lambda,$$

then $V = W \oplus W'$, so that W' is a G-module complement for W in V.

In particular, we may take $W = 0$, and so V itself is a direct sum of irreducible submodules, even if it is infinite-dimensional.

Proof. Consider the set of families of irreducible submodues

$$\{M_\lambda\}_{\lambda\in\Lambda}$$

of V such that the sum

$$W + \sum_{\lambda\in\Lambda} M_\lambda$$

is direct, i.e., such that every module occurring has intersection 0 with the sum of the other modules occurring. The empty set is such a family, and the union of chain of such families is such a family. Hence, there is a maximal such family, which we denote $\{M_\lambda\}_{\lambda\in\Lambda}$. We claim that $V = V'$, where

$$V' = W + \sum_{\lambda\in\Lambda} M_\lambda.$$

If not, there is a finite-dimensional submodule V_0 of V that is not contained in V'. V_0 is a direct sum of irreducibles: one of these, call it M_0, must also fail to be contained in V'. Then $M_0 \cap V'$ is a proper G-submodule of M_0, and so it is 0. But then the family can be enlarged by including M_0 as a new member, a contradiction. □

If V is G-module, let V^G be the *subspace of invariants*, i.e.,

$$V^G = \{v \in V : \text{for all } \gamma \in G,\ \gamma(v) = v\}.$$

Then V^G is the largest G-submodule of V on which G acts trivially, and it is a direct sum (although not in a unique way) of one-dimensional G-modules on which G acts trivially. Note that if M is an irreducible G-module on which G acts on non-trivially, then $M^G = 0$, for otherwise M^G is a proper nonzero G-submodule of M.

Theorem. *Let V be a G-module, where G is linearly reductive. Then V^G has a* unique *G-module complement V_G, which may also be characterized as the sum of all irreducible submodules M of V on which G acts non-trivially.*

Proof. Let W be any G-module complement for V^G. Let M be any irreducible in G on which G acts non-trivially. If $M \cap W \neq 0$, the $M \cap W = M$, and so $M \subseteq W$ as required. Otherwise M injects into $V/W \cong V^G$, which implies that G acts trivially on M, a contradiction. Thus, every irreducible on which G acts nontrivially is contained in W. But W is a direct sum of irreducibles, and G must act non-trivially on each of these, since there are no invariants in W. Therefore, W is the sum of all irreducible submodules of G on which G acts non-trivially, which proves that W is unique. □

We also have:

Proposition. *If $f : V \to W$ is a map of G-modules, then $f : V^G \to W^G$, i.e., f induces a map of the respective G-invariant subspaces of V and W by restriction. Moreover, $f : V_G \to W_G$. Thus, f preserves the direct sum decompositions $V = V^G \oplus V_G$ and $W = W^G \oplus W_G$.*

Proof. If v is invariant so that $\gamma(v) = v$ for all $\gamma \in G$, then $\gamma\big(f(v)\big) = f\big(\gamma(v)\big) = f(v)$ for all $\gamma \in G$. Thus, $F(V^G) \subseteq W^G$.

Now consider any irreducible M on which G acts non-trivially. The kernel of f intersected with M is a G-submodule of M, and, hence, is 0 or M. If it is 0, then M injects into W, and the image is an isomorphic copy of M, which means that $f(M)$ is an irreducible

G-submodule of W on which G acts non-trivially. Hence, $f(M) \subseteq W_G$. On the other hand, if the kernel contains all of M, the image is $0 \subseteq W_G$. □

Dicussion. Let G be a linear algebraic group that is not necessarily lineaarly reductive. Consider a short exact sequence of G-modules

$$0 \to W \to V \to Y \to 0.$$

Clearly, $W^G \subseteq Y^G$, and the kernel of the map $V^G \to Y^G$ is, evidently, $V^G \cap W$, which is obviously W^G. Hence, for any linear algebraic group, we always have that

$$0 \to W^G \to Y^G \to V^G$$

is exact. In general, however, the map $Y^G \to V^G$ need not be onto. However:

Corollary. *If G is linearly reductive and $0 \to W \to V \to Y \to 0$ is an exact sequence of G-modules, then $0 \to W^G \to V^G \to Y^G \to 0$ is exact.*

Proof. The map $V \to Y$ is the direct sum of the maps $V^G \to Y^G$ and $V_G \to Y_G$. Hence, it is surjective if and only if both $V^G \to Y^G$ and $V_G \to Y_G$ are surjective, which, in particular, shows that $V^G \to Y^G$ is surjective. □

When G is linearly reductive, we have a canonical G-module retraction $\rho_V : V \twoheadrightarrow V^G$ that is obtained by killing V_G. This map is called the *Reynolds operator.* Note that if we are given a short exact sequence of G-modules $0 \to W \to Y \to V \to 0$, then we have a commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & W_G \arrow[r] \arrow[d] & V_G \arrow[r] \arrow[d] & Y_G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & W \arrow[r] \arrow[d, "\rho_W"'] & V \arrow[r] \arrow[d, "\rho_V"'] & Y \arrow[r] \arrow[d, "\rho_Y"'] & 0 \\
0 \arrow[r] & W^G \arrow[r] \arrow[d] & V^G \arrow[r] \arrow[d] & Y^G \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

The columns are split exact, and the rows are exact: the middle row is the direct sum of the rows above and below it.

The property that when $V \to W$ is a surjection of finite-dimensional G-modules then $V^G \to W^G$ is surjective actually characterizes linearly reductive groups. To see this, first note that if V and W are finite-dimensional G-modules, we can put a G-module structure on $\mathrm{Hom}_K(V, W)$ (this is simply the vector space of all K-linear maps) as follows: for all $\gamma \in G$ and all $f : V \to W$, $\gamma(f)(v) = \gamma(f(\gamma^{-1}v))$. This is easily verified to give $\mathrm{Hom}_K(V, W)$ the structure of a G-module. Moreover:

Lemma. *Let V, W be finite-dimensional G-modules. Then $\mathrm{Hom}_K(V,\, W)^G$ is the K-vector space of G-module maps from V to W.*

Proof. Suppose that $f : V \to W$. Then f is fixed by G if and only if for all $\gamma \in G$ and for all $v \in V$, $\gamma\big(f(\gamma^{-1}v)\big) = f(v)$, i.e., $f(\gamma^{-1}v) = \gamma^{-1}f(v)$. Since γ^{-1} takes on every value in G as γ varies, we have that f is fixed by G iff f is a G-module homomorphism. □

Theorem. *Let G be a linear algebraic group. G is linearly reductive if and only if for every surjective G-module map of finite-dimensional G-modules $V \twoheadrightarrow W$, the map $V^G \to W^G$ is also surjective.*

Proof. It suffices to show that every finite-dimensional G-module V is a direct sum of irreducible G-modules: if not, let V be a counter-example of smallest possible vector space dimension. Then V is not irreducible, and we may choose a maximal proper G-submodule $M \neq 0$, so that $W = V/M$ is irreducible. It suffices to show that the exact sequence

$$(*) \quad 0 \to M \to V \xrightarrow{f} W \to 0$$

splits as a sequence of G-modules, since in that case we have that $V \cong M \oplus W$ and $\dim_K(M) < \dim_K(V)$. It is, of course, split as a sequence of K-vector spaces. Apply $\mathrm{Hom}_K(W,\, \_)$, where this is simply Hom as K-vector spaces. Then

$$0 \to \mathrm{Hom}_K(W,\, M) \to \mathrm{Hom}_K(W,\, V) \xrightarrow{f_*} \mathrm{Hom}_K(W,\, W) \to 0$$

is exact (since the sequence $(*)$ is split as a sequence of K-vector spaces), and the map f_*, which sends $g : W \to V$ to $f \circ g$, is therefore surjective. This is a sequence of G-modules, and so the map

$$\mathrm{Hom}_K(W,\, V)^G \to \mathrm{Hom}_K(W,\, W)^G$$

is surjective. That is, the set of G-module maps from $W \to V$ maps onto the set of G-module maps from $W \to W$. Hence, there is a G-module map $g : W \to V$ such that $f_*(g) = f \circ g$ is the identity map on W, and so $(*)$ is split as a sequence of G-modules. □

Remark. The existence of a functorial Reynolds operator that retracts every finite-dimensional G-module onto its invariant submodule and so, for every G-module map $V \to W$, provides a commutative diagram:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\rho_V"'] & > W \arrow[d, "\rho_W"] \\ V^G \arrow[r, "f"'] & W^G \end{tikzcd}$$

already implies that when the top arrow is surjective, so is the bottom arrow. For if $w \in W^G$ we may choose an arbitrary element $v \in V$ such that $f(v) = w$, and then

$$f\big(\rho_V(v)\big) = \rho_W\big(f(v)\big) = \rho_G(w) = w,$$

as required. Thus, the existence of a functorial retraction onto the modules of invariants is also equivalent to the condition that G be linearly reductive.

Remark. If G is a finite group such that the order $|G|$ of G is invertible in K, the Reynolds operator is given by:

$$\rho(v) = \frac{1}{|G|}\sum_{g\in G} g(v),$$

i.e., averaging over the group G.

It turns out that linear reductive linear algebraic groups over the complex numbers $\mathbb{C}$ are precisely those that have a Zariski dense compact real Lie subgroup H. Then H has Haar measure, a translation-invariant measure μ such that $\mu(H) = 1$, and the Reynolds operator can be obtained by averaging over the group:

$$\rho(v) = \int_{\gamma\in H} \gamma(v)\, d\mu.$$

Early proofs of finite generation for rings of invariants of semisimple groups over $\mathbb{C}$ made use of this idea. Purely algebraic proofs have been available for a long time: these involve the study of modules over the Lie algebra. See, for example, [A. Borel, *Linear Algebraic Groups*, Benjamin, New York, 1969].

Lecture of March 11

The additive group $G = (K, +)$ of the field K may be identified with the group of upper triangular 2×2 unipotent matrices

$$\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in K\},$$

since

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

for all a, $b \in K$. This group is not linearly reductive. Let $V = K^2$, thought of a column vectors, and let G act in the obvious way, by left multiplication on column vectors. Let $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Then $V^G = Ke_1$ is a G-stable subspace of K^2, i.e., e_1 is an eigenvectxor of every matrix in G corresponding to the eigenvalue 1. However, Ke_1 has no G-stable complement in K^2: such a complement would be one-dimensional and that would require matrices such as $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$ to have a second eigenvector. □

The Reynolds operator for ring actions and finite generation of R^G

We next want to study the situation where G is a linearly reductive linear algebraic group acting on a K-algebra R by ring automorphisms.

Theorem. *Let G be a linearly reductive algebraic group and let R be a K-algebra that is a G-module such that G acts on R by K-algebra automorphisms. Then the Reynolds operator $R \to R^G$ is R^G-linear.*

Proof. The Reynolds operator arises from the decomposition $R = R^G \oplus R_G$. It suffices to show that R_G is an R^G-module. Let $M \subseteq R_G$ be a typical irreducible G-submodule of R on which G acts non-trivially. Let $a \in R^G$, and consider the map $M \twoheadrightarrow aM$ that sends $r \mapsto ar$ for all $r \in M$. This is a map of G-modules, because for all $\gamma \in G$, $\gamma(ar) = \gamma(a)\gamma(r) = a\gamma(r)$. The kernel is therefore a G-submodule of M. If the kernel is M, then $aM = 0 \subseteq R_G$. If the kernel is 0, then $M \cong aM$ as G-modules. It follows that G acts non-trivially on the irreducible G-module aM, and so $aM \subseteq R_G$, as required. □

We have the following:

Lemma. *Let $A \subseteq R$ be a ring extension such that A is a direct summand of R as an A-module, i.e., there is an A-linear map $R \to A$ that restricts to the identity map on A.*

(a) *For every ideal I of A, $IR \cap A = I$.*

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

(c) *If R is Noetherian and A is an $\mathbb{N}$-graded algebra over $A_0 = K$, a field, then A is a finitely generated K-algebra.*

Proof. (a) Suppose we have $a = f_1r_1 + \cdots + f_kr_k$ where $a \in A$, the $f_j \in I \subseteq A$, and the $r_j \in R$. Then $\rho(a) = a$, and by the A-linearity of ρ, we have that $a = \rho(a) = f_1\rho(r_1) + \cdots + f_k\rho(r_k) \in I$, as required, since each $\rho(r_j) \in A$.

(b) Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an infinite non-decreasing chain of ideals in A. Since R is Noetherian, then chain I_jR is eventually stable, and so for some k, $I_kR = I_{k+h}R$ for all $h \geq 0$. Intersecting with A and applying (a), we have that $I_k = I_{k+h}$ for all $h \geq 0$, as required.

(c) By part (b), A is Noetherian, and so its maximal ideal is finitely generated as an ideal. We can take the generators to be forms of positive degree, say $F_1, \ldots, F_h$. Let $B = K[F_1, \ldots, F_h] \subseteq A$. It suffices to show that $B = A$. If not, we can choose a homogeneous element $F \in A - B$ of least degree. Since F is in the maximal ideal of A, we can write $F = \sum_{j=1}^{h} G_jF_j$, and by taking homogenous components we may assume that if $G_j \neq 0$, then $\deg(G_j) = \deg(F) - \deg(F_j) < \deg(F)$, and so every $G_j \in B$ by the fact that F has least degree in $A - B$. But then $F \in B$ as well. □

Corollary. *If G is a linearly reductive linear algebraic group acting by K-automorphisms on a finitely generated K-algebra R, then R^G is finitely generated.*

Proof. If R is graded and the action preserves degree, this follows from part (c) of the Lemma above. In the general case, we can choose a finite-dimensional vector space $V \subseteq R$ that is G-stable and contains generators of R. We may then form the symmetric algebra

S of V over K, which is a polynomial ring over K whose space of forms of degree 1 is is isomorphic with V. We may let G act on V using the G-module structure of G, and this action extends to the polynmial ring S. The map $S \to R$ that sends each element of $V = [S]_1$ to itself, but considered as an element of $V \subseteq R$ extends uniquely to a K-algebra homomorphism $S \to R$. Since V generates R, this map is surjective. It is easy to see that this is also a map of G-modules. Hence, since we have a surjection $S \twoheadrightarrow R$, we also have a surjection $S^G \twoheadrightarrow R^G$. S^G is finitely generated over K by the graded case already considered, and so R^G is finitely generated over K. □

Hilbert's fourteenth problem asks whether every ring of invariants of a linear algebraic group acting on a polynomial ring is finitely generated. This turns out to be false: the first counter-example was given by M. Nagata. It involved the action of the product of a large number of copies of the additive group of the field. Finite generation does hold when the group is linearly reductive and in some other important cases. We mention one here.

Theorem (Emmy Noether). *Let G be a finite group acting on a finitely generated K-algebra R. Then R^G is a finitely generated K-algebra.*

Proof. Let $R = K[r_1, \ldots, r_k]$. Suppose that $|G| = n$, say $G = \{\gamma_1, \ldots, \gamma_n\}$. For each r_i, consider the elements $\gamma_1(r_i), \ldots, \gamma_n(r_i)$. The elementary symmetric functions of these elements are invariant, and give coefficients for an equation of integral dependence of r_i, namely $\prod_{j=1}^n \bigl(z - \gamma_j(r_i)\bigr) = 0$. Hence, if R_0 is generated over K by the k sets of elementary symmetric functions of elements $\gamma_1(r_i), \ldots, \gamma_n(r_i)$, $1 \le i \le k$, then R_0 is finitely generated over K, and $R_0 \subseteq R^G \subseteq R$. Each r_i is integral over R_0, and so R is integral and finitely generated over R_0. Hence, R is module-finite over R_0, which is Noetherian. It follows that R^G is module-finite over R_0 and, hence, finitely generated over K. □

The Cohen-Macaulay property for certain rings of invariants

Our next main objective is to prove the following:

Theorem. *Let G be a linearly reductive linear algebraic group over a field K, acting by K-automorphisms on a polynomial ring $R = K[x_1, \ldots, x_n]$ by a degree-preserving action, i.e., an action that extends an action of G on $[R]_1$. Then R^G is a Cohen-Macaulay ring.*

The proof will occupy us for a while. One of the subtle points is that a homogeneous system of parameters of R^G, which will generate an ideal of height $d = \dim(R^G)$ in R^G, typically generates an ideal of smaller height in R: in fact, it is hard to say anything special about the expansion to R of the ideal generated by a homogeneous system of parameters of R^G.

Before proceeding with material that will be needed for the argument, we give some examples.

Examples of actions on of matrix groups on polynomial rings

In giving the examples below, I am not going to worry about whether the action is a right action or a left action. If one has a right action (so that $(v)(gg') = ((v)g)g'$ one can replace it by a left action such that $(g, v) \mapsto vg^{-1}$ (the invariants are the same), and conversely. The point is that $g \mapsto g^{-1}$ is an isomorphism of a group G with G^{op}. A left action on a ring yields a right action on the variety, a left action on a vector space yields a right action on the linear functionals on that vector space, and so forth.

Consider an infinite field K and let X, Y be $r\times t$ and $t\times s$ matrices of indeterminates over K, where $1 \leq t \leq r \leq s$. Let $S = K[X, Y]$ denote the polynomial ring in $rt + st$ variables generated by the entries. Let $\alpha \in \mathrm{GL}(t, K) := G$ act by sending the entries of X, Y to the that corresponding entries of $X\alpha^{-1}$, αY. It is easy to see that the entries of the product matrix XY are invariant, and one can prove that they generate the ring $S^G = K[XY]$, and that if Z is an $r \times s$ matrix of indeterminates, then $S^G = K[XY] \cong K[Z]/I_{t+1}$: that is, the relations on the entries of XY are generated by the vanishing of the size $t + 1$ minors. The minors do give relations because, thinking over the fraction field of $[K, Y]$, the map of vector spaces whose matrix is XY factors through a vector space of dimension t, and so has rank at most t. It is much harder to show that the minors generate all relations. By the theorem we aim to prove, S^G is Cohen-Macaulay in the characteristic 0 case. This is true in characteristic $p > 0$ as well, but needs different methods: time permitting we will address the issue in characteristic $p > 0$. ne This example is quite interesting even when $t = 1$. If we let the transpose of X be $\big(x_1,\ \cdots, .x_r\big)$ and $Y = \big(y_1,\ \cdots, .y_s\big)$, then S^G is the Segre product $K[x_iy_j : 1 \leq i \leq r, .1 \leq j \leq s]$ of the polynomial rings $K[x_1, \ldots, x_r]$ and $K[s_1, \ldots, s_]$. Notice that the height of the maximal ideal $\mathfrak{m}$ of the ring of invariants, which is $r + s - 1$ typically drops to $\min\{r,\ s\}$ when it is extended to S.

Now suppose instead that $\alpha \in \mathrm{SL}(r, K)$ acts on $S = K[X]$ as above so that the entries of X are sent to the corresponding entries of αX. It turns out that the ring of invariants S^G is the ring generated by the size r minors of X. This is the homogeneous coordinate ring of a Grassmann variety, and the minors satisfy, typically, well-known quadratic relations called the *Plücker* relations. The special linear group is linearly reductive in characteristic 0, and so the theorem on p. 124 implies these rings are Cohen-Macaulay if K has characteristic 0. Again, this is true in positive characteristic as well, by other methods. Note that in this example, the height of the maximal ideal of S^G is $rs - r^2 + 1$, but if that maximal ideal is expanded to to S, the ideal has height $s - r + 1$, which is smaller if $r > 1$.

We now begin what will turn out to be a lengthy journey towards the proof of the theorem on p. 124. In the process, we will motivate the underlying ideas of tight closure theory.

The argument we give will depend on reduction to characteristic $p > 0$, which is odd, because there are relatively few linearly reductive groups in positive characteristic. Another proof is known: cf. [J.-F. Boutot, *Singularités rationelles par les groupes réductifs*, Invent. Math. **88** (1987) 65–68]. However, that argument needs resolution of singularities, Grothendieck duality, and the Grauert-Riemenschneider vanishing theorem. The first proof of this Theorem, which used reduction to prime characteristic $p > 0$, was given in

[M. Hochster and J. L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. in Math. **13** (1974) 115–175], but the argument we give here follows a line of thought introduced in [M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda Theorem*, J.A.M.S. **3** (1990) 31–116]. The theorem is actually true whenever A is a graded ring that is a direct summand over itself of a polynomial ring $K[x_1, \ldots, x_n]$. In fact, whenever A is a direct summand of a regular ring R as an A-module, if A contains a field it must be Cohen-Macaulay, but the argument for the general case, which can be achieved along the same lines as the argument given here, is much more technical. Quite recently, techniques of perfectoid geometry have been used to remove the condition that the regular ring contain a field, but the argument in this case still depends on arguments in characteristic $p > 0$.

Here is a sharper form of the Theorem:

Theorem. *Let R be a polynomial ring over a field K, let A be a K-subalgebra of R generated by forms, and let $F_1, \ldots, F_d$ be a homogeneous system of parameters of A such that for every i, $1 \le i \le d-1$, $(F_1, \ldots, F_i)R \cap A = (F_1, \ldots, F_i)A$. Then A is a Cohen-Macaulay ring.*

If $A = R^G$ for a linearly reductive linear algebraic group G, then every ideal of A is contracted from R, and so we have that the ideals $(F_1, \ldots, F_i)A$ are contracted from R.

We shall first prove the Theorem above in characteristic $p > 0$. The proof depends on the following somewhat technical fact:

Theorem (colon-capturing). *Let A be an $\mathbb{N}$-graded domain finitely generated over a field K of prime characteristic $p > 0$. Let $F_1, \ldots, F_d$ be a homogeneous system of parameters for A. Suppose that one has a relation:*

$$u_{i+1}F_{i+1} = u_1F_1 + \cdots + u_iF_i$$

for some i. Then there exists an element $c \in A - \{0\}$ such that for all nonnegative integers $e \gg 0$,

$$(*) \quad cu_{k+1}^{p^e} \in (F_1^{p^e}, \ldots, F_i^{p^e})A.$$

Before proving this fact, we want to make several comments. When working in prime characteristic $p > 0$, it will be typographically convenient to use the letter q to stand for p^e, where $e \in \mathbb{N}$. Thus, the statement $(*)$ can be expressed instead as

$$(**) \quad cu_{k+1}^{q} \in (F_1^{q}, \ldots, F_i^{q})A.$$

Consider an ideal $J \subseteq A$, where A is any ring of prime characteristic $p > 0$. Then we shall use the notation $J^{[q]}$ for the ideal $(u^q : u \in A)A$, i.e., the ideal generated by all qth powers of elements of J. If J has generators u_i, then $J^{[q]}$ has generators u_i^q, since

$$(r_{i_1}u_{i_1} + \cdots + r_{i_h}u_{i_h})^q = r_{i_1}^q u_{i_1}^q + \cdots + r_{i_h}^q u_{i_h}^q,$$

but $J^{[q]}$ is independent of the choice of generators of J. Note that $J^{[q]} \subseteq J^q$, but, unless J is principal, J^q tends to be considerably larger: it contains all products of q generators of J, while $J^{[q]}$ contains only q th powers of generators of J.

The condition in $(**)$ for all $q \gg 0$ with fixed $c \neq 0$ may be construed, heuristically, as asserting that the element u_{i+1} is "almost" in the ideal generated by $F_1, \ldots, F_i$. We can make this thought somewhat less vague as follows: take q th roots of both sides in a suitable integral extension of A (one must adjoing sufficieintly many q th roots of elements in A). From the equation

$$(\#) \quad cu_{i+1}^q = F_1^q u_1 + \cdots + F_i^q u_i$$

one gets

$$(\#\#) \quad c^{1/q} u_{i+1} = F_1 u_1^{1/q} + \cdots + F_i u_k^{1/q}.$$

As $q \to \infty$, $1/q$ approaches 0, and so one may think of $c^{1/q}$ as approaching 1 in a vague heuristic sense. Thus, elements getting "arbitrarily close to 1" are multiplying u_{i+1} into $(F_1, \ldots, F_i)$, although in a somewhat larger ring than A.

Proof of the Theorem on colon-capturing. A is module-finite over $B = K[F_1, \ldots, F_d]$. Let $v_1, \ldots, v_h$ be a maximal sequence of elements of A that are linearly indpendent over B, so that $G = Bv_1 + \cdots Bv_h$ is a free B-module of rank h. Here, h will be the same as the degree of the extension of fraction fields, $[\mathrm{frac}\,(A) : \mathrm{frac}\,(B)]$. Consequently, A/G is a torsion-module over the domain B: we can see this as follows. If $v \in A - G$, it must have a nonzero multiple in G: otherwise $v_1, \ldots, v_h, v$ are linearly independent over B, contradicting the choice of h. Hence, each generator of A has a nonzero multiple in G. By taking the product of the multipliers, we obtain a nonzero element $c \in B \subseteq A$ such that $cA \subseteq G$. It turns out that c has the property we require.

Suppose that we have a relation

$$F_{i+1} u_{i+1} = F_1 u_1 + \cdots + F_i u_i,$$

where the $u_j \in A$. Taking q th powers where $q = p^e$ we have:

$$F_{i+1}^q u_{i+1}^q = F_1^q u_1^q + \cdots + F_i^q u_i^q,$$

and multiplying by c gives

$$(\#) \quad F_{i+1}^q (cu_{i+1}^q) = F_1^q (cu_1^q) + \cdots + F_i^q (cu_i^q).$$

Since each of the elements $cF_j^q \in cA \subseteq G$, we may think of $(\#)$ as a relation on $F_1^q, \ldots, F_{i+1}^q$ with coefficients in the free B-module G. Since $F_1^q, \ldots, F_{i+1}^q$ is a regular sequence on B, it is a regular sequence on G, and we can conclude that

$$cu_{i+1}^q \in (F_1^q, \ldots, F_i^q)G \subseteq (F_1^q, \ldots, F_i^q)A,$$

for all $q = p^e$, as required. □

We shall prove the following Lemma: we postpone giving the argument for a bit.

Lemma. *Let R be the polynomial ring $K[x_1, \dots, x_n]$. Let J be any ideal of R. Suppose that there exists $c \in R - \{0\}$ and $f \in R$ such that $cf^q \in J^{[q]}$ for all $q \gg 0$. Then $f \in J$.*

Assuming this result for the moment, we give the proof of the sharper form of the Theorem on the Cohen-Macaulay proprerty for rings of invariants. The argument is amazingly easy now!

Proof of the sharper theorem. We want to show that $F_1, \dots, F_d$ is a regular sequence in A. Suppose that $uF_{i+1} \in (F_1, \dots, F_i)A = I$. By the Theorem on colon-capturing above, we have that there exists $c \neq 0$ in A such that $cu^q \in I^{[q]}$ for all $q \gg 0$. Then we may expand I to R to obtain $cu^q \in (IR)^{[q]}$ for all $q \gg 0$. By the Lemma above, we then have $u \in IR$, so that $u \in IR \cap A = I$ by hypothesis. □

It remains to prove the Lemma.

Lecture of March 13

If R is a ring of prime characteristic p we write $F_R : R \to R$ for the *Frobenius endomorphism*: $F_R(r) = r^p$. If $e \in \mathbb{N}$, we write F_R^e for the composition of F_R with itself e times, the iterated Frobenius endomorphism. Thus, $F_R^e(r) = r^{p^e}$. The subscript $_R$ is often omitted.

Quite generally, if R is a regular Noetherian ring, $F^e : R \to R$ is faithfully flat. We shall not prove this fact in general at this point, but we do want to prove that when R is a polynomial ring over a field K, $F^e : R \to R$ makes the right hand copy of R into a free R-module over the left hand copy of R. Note that F^e is an injective homomorphism, since the polynomial ring has no nonzero nilpotents. The image of R under this map is $R^q = \{r^q : r \in R\}$, where $q = p^e$.

We first note the following:

Lemma. *If T is free as S-algebra and S is free as an R-algebra, then T is free as an R-algebra. In fact, if $\{t_j\}_{j \in \mathcal{J}}$ is a free basis for T over S and $\{s_i\}_{i \,\in \mathcal{I}}$ is a free basis for S over R then the set of products $\{t_j s_i : j \in \mathcal{J},\, i \in \mathcal{I}\}$ is a free basis for T over R.*

Proof. If $t \in T$, we can write $t = \sum_{k=1}^n u_k t_{j_k}$, where the $u_k \in S$, and then we may express every u_k as an R-linear combination of finitely many of the elemnts s_i. It follows that the specified products span. If some R-linear combination of the products is 0, we may enlarge the set so that it consists of elements $s_{i_h} t_{j_k}$ for $1 \le h \le m$ and $1 \le k \le n$. If

$$\sum_{1 \le h \le m, 1 \le k \le n} r_{hk} s_{i_h} t_{j_k} = 0$$

where the $r_{hk} \in R$. We can write this as

$$\sum_{k=1}^{n}(\sum_{h=1}^{m} r_{hk}s_{i_h})t_{j_k} = 0,$$

from which we first conclude that every $\sum_{h=1}^{m} r_{hk}s_{i_h} = 0$ and then that every $r_{hk} = 0$. □

Proposition. *If B is a free A-algebra, $x_1, \ldots, x_n$ are indeterminates, and $k_1, \ldots, k_n$ are positive integers, then $B[x_1, \ldots, x_n]$ is free over $A[x_1^{k_1}, \ldots, x_n^{k_n}]$.*

Proof. By a straightforward induction, this reduces at once to the case where $n = 1$. We let $x = x_1$ and $k = k_1$. Then $B[x] \cong A[x] \otimes_A B$ is free over $A[x]$. By the preceding Lemma, it suffices to show that $A[x]$ is free over $A[x^k]$. But it is quite easy to verify that the elements x^a for $0 \leq x \leq a - 1$ are a free basis. □

Theorem. *Let K be field and let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over K. Then $F_R^e : R \to R$ makes the right hand copy of R into a free module over the left hand copy of R.*

Proof. The image of R under F^e is $R^q = K^q[x_1^q, \ldots, x_n^q]$. It suffices to show that R is free over R^q. Note that since K^q is a field, K is free over K^q. The result is now immediate from the preceding Proposition. □

Lectures of March 16–18

In this lecture, we will prove that taking colons of ideals commutes with flat base change in the Noetherian case (and somewhat more generally). Because we already know that when R is a polynomial ring the iterated Frobenius endomorphism $F^e : R \to R$ is flat (and even makes R into a free module over itself) and because the $\_^{[q]}$ operation may be viewed as base change using the Frobenius endomorphism, it follows that $I^{[q]} :_R J^{[q]} = (I :_R J)^{[q]}$ when R is a polynomial ring. We shall see eventually that this is also true when R is *regular* of prime characteristic $p > 0$. This is used to show in the Theorem that follows that if R is polynomial, $c \neq 0$ and $cu^q \in I^{[q]}$ for all $q \gg 0$, then $u \in I$. This may be thought of as saying that if u is "almost" in I in this rather technical sense, and the ring is polynomial, then u actually is in I. This idea is the beginning of tight closure theory, as we shall see later

We then begin process of extending these ideas to polynomial rings over fields of equal characteristic 0. There are several ideas involved. One starts out over a field of characteristic 0. One replaces the field by a finitely generated $\mathbb{Z}$-subalgebra A that contains all needed coefficients. We give a version of Noether normalization over domains. This result enables us to show that when one kills a maximal ideal in a finitely generated $\mathbb{Z}$-algebra

A, the quotient is a field of characteristic $p > 0$ — in fact, a finite field. The idea of many proofs the go from fields of equal characteristic zero to characteristic $p > 0$ is to "descend" to a finitely generated $\mathbb{Z}$-algebra and then kill a suitable maximal ideal to get to characteristic p. Typically, a Zariski dense set of the maximal ideals can be used. If one does this carefully, one can show that a counter-example to the theorem of interest over a field of characteristic 0 leads to a counterexample in characteristic $p > 0$, and then one has reduced to proving the result in a positive characteristic situation.

A technical point that comes up is that carrying through the details may require one to know that various rings and modules that come up are A-free. The result on generic freeness that we prove enables us to achieve this after localizing at one nonzero element of A. Note that the new ring A_a is still a finitely generated $\mathbb{Z}$-algebra. The supply of maximal ideals on A one might use is diminished, but still Zariski dense in the maximal spectrum of the original choice of A. We have given a very strong form of the generic freeness here. The following more modest statement is enough for most purposes here. Let A be a Noetherian domain, R a finitely generated A-module, and M a finitely generated R-module. Then there an element $a \in A - \{0\}$ such that M_a is A_a-free. Note that this is also true if $M = R$. A mildly stronger form asserts that if N is a finitely generated A-submodule of M, one can choose $a \in A - \{0\}$ such that $(M/N)_a$ is A_a-free. Note the following consequence:

If one has

$$0 \to N_a \to M_a \to (M/N)_a \to 0$$

and $(M/N)_a$ is A_a-free, the sequence remains exact when one tensors with $\kappa = A_a/\mu$, where μ is a maximal ideal of A_a. This may be used to keep the image of N_a in M_a nonzero when one tensors with κ. (0f course, once the cokernel is free, or even flat, exactness is preserved when we tensor with any A_a-module, because $\mathrm{Tor}_1^{A_a}\big((M/N)_a, \_\big)$ vanishes no matter what the second input is.

We now proceed with the detailed treatment.

We need the following:

Lemma. *Let $R \to S$ be flat, and let $I \subseteq R$, $J \subseteq R$ be ideals such that $J = (f_1, \ldots, f_k)R$ is finitely generated. Then $(I :_R J)S = IS :_S JS$.*

Proof. Consider the map $R \to (R/I)^{\oplus k}$ that sends $r \mapsto (\overline{f_1 r}, \ldots, \overline{f_k r})$ where $\overline{u}$ denotes the image of $u \in R$ modulo I. The kernel of this map is precisely $I :_R J$, i.e.,

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

is exact. Thus, this sequence remains exact when we apply $S \otimes_R \_$ to obtain:

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

The kernel of $\phi : S \to (S/IS)^{\oplus k}$ is therefore the image of $(I :_R J) \otimes_R S \to S$, which is $(I :_R J)S$. (The map is injective, so that $(I :_R J) \otimes_R S \cong (I :_R J)S$. In general, if $R \to S$

is flat and $\mathfrak{A}$ is an ideal of R, when $S \otimes_R \_$ is applied to the injection $0 \to \mathfrak{A} \to R$ it yields an isomorphism $\mathfrak{A} \otimes_R S \cong \mathfrak{A}S$.) But the definition of ϕ implies that the kernel is $IS :_S JS$. □

Remark. When $\phi : R \to S$ and I is an ideal of R, IS is generated by the images of the elements of I under ϕ. Suppose that R is a ring of prime characteristic $p > 0$ and let $S = R$, made into an R-algebra by means of the structural homomorphism $F^e : R \to R$. Tn for any ideal I of R, $IS = I^{[q]}$.

Then:

Theorem. *Let R be a polynomial ring $K[x_1, \ldots, x_n]$ over a field K of characteristic $p > 0$. For any two ideals I, $J \subseteq R$, $I^{[q]} :_R J^{[q]} = (I :_R J)^{[q]}$.*

Proof. Since $F^e : R \to R$ is flat, this is immediate from the Remark just above and the Lemma. □

The following result now completes, in the case of prime characteristic $p > 0$, the proof of the sharper form of the Theorem on the Cohen-Macaulay property for rings of invariants stated at the top of p. 4 of the Lecture Notes of March 11.

Theorem. *Let R be a polynomial ring $K[x_1, \ldots, x_n]$ over a field K of characteristic $p > 0$. Let I be an ideal of R, let $u \in r$, and let $c \in R - \{0\}$. Suppose that $cu^q \in I^{[q]}$ for all $q = p^e \gg 0$. Then $u \in I$.*

Proof. The fact that $cu^q \in I^{[q]}$ for all $q \gg 0$ may be restated as $c \in I^q :_R (uR)^{[q]}$ for all $q \gg 0$. By the Theorem just above, this means that $c \in (I :_R uR)^{[q]}$ for all $q \gg 0$. If $u \notin I$, then $I :_R uR$ is a proper ideal and is contain in some maximal ideal m of R. Then for some q_0 we have

$$c \in \bigcap_{q \geq q_0} (I :_R Ru)^{[q]} \subseteq \bigcap_{q \geq q_0} m^{[q]} \subseteq \bigcap_{q \geq q_0} (mRm)^{[q]} \subseteq \bigcap_{q \geq q_0} (mR_m)^q = 0,$$

and so $c = 0$, a contradiction. Hence, we must have $u \in I$ after all. □

Our next objective is to prove the Theorem for fields of characteristic 0 as well, by reducing to the characteristic p case.

First step: moving towards characteristic p

We now suppose that we have a counter-example to the Theorem stated at the top of p. 4 over a field K of equal characteristic 0. In the sequel, we want to replace K, insofar as possible, by a finitely generated $\mathbb{Z}$-subalgebra $D \subseteq K$. We then obtain a counterexample by killing a maximal ideal μ of D: it turns out that D/μ must be a finite field.

In order to carry our ideas through, we first need to prove some preliminary results. One is the fact just stated about maximal ideals in finitely generated $\mathbb{Z}$-algebras. However, we also need results of the following kind: suppose that $A_D \subseteq R_D$ are finitely generated D-algebras. Then one can localize at one nonzero element $d \in D-\{0\}$ such that $(R_D/A_D)_d$ is flat over D_d. We shall prove one of the strongest known results of this type. This will enable us to preserve an inclusion $A_D \subseteq R_D$ while killing a maximal ideal of D. We shall need to be able to do this and also preserve various other inclusions like this in order to give the detailed argument.

We first review the Noether Normalization Theorem over a domain. We begin with:

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

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

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

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

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

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

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

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

Theorem (Noether normalization over a domain). *Let T be a finitely generated extension algebra of a Noetherian domain D. Then there is an element $d \in D - \{0\}$ such that T_d is a module-finite extension of a polynomial ring $D_d[z_1, \ldots, z_h]$ over D_d.*

Proof. We use induction on the number n of generators of T over D. If $n = 0$ then $T = D$. We may take $h = 0$. Now suppose that $n \geq 1$ and that we know the result for algebras generated by $n-1$ or fewer elements. Suppose that $T = D[\theta_1, \ldots, \theta_n]$ has n generators. If the θ_i are algebraically independent over K then we are done: we may take $h = n$ and $z_i = \theta_i$, $1 \leq i \leq n$. Therefore we may assume that we have a nonzero polynomial $f(x_1, \ldots, x_n) \in D[x_1, \ldots, x_n]$ such that $f(\theta_1, \ldots, \theta_n) = 0$. Instead of using the original θ_j as generators of our K-algebra, note that we may use instead the elements

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

where N is chosen for f as in the preceding Lemma. With ϕ as in that Lemma, we have that these new algebra generators satisfy $\phi(f) = f(x_1 + x_n^N, \ldots, x_{n-1} + x_n^{N^{n-1}}, x_n)$ which we shall write as g. We replace D by D_d, where d is the coefficient of x_n^m in g. After multiplying by $1/d$, we have that g is monic in x_n with coefficients in $D_d[x_1, \ldots, x_{n-1}]$. This means that θ_n' is integral over $D_d[\theta_1', \ldots, \theta_{n-1}'] = T_0$, and so T_d is module-finite over T_0. Since T_0 has $n-1$ generators over D_d, we have by the induction hypothesis that $(T_0)_{d'}$ is module-finite over a polynomial ring $D_{dd'}[z_1, \ldots, z_{d-1}] \subseteq (T_0)_{d'}$ for some nonzero $d' \in D$, and then $T_{dd'}$ is module-finite over $D_{dd'}[z_1, \ldots, z_h]$ as well. □

Theorem. *Let κ be a field that is a finitely generated $\mathbb{Z}$-algebra. Then κ is a finite field. Hence, if μ is any maximal ideal of a finitely generated $\mathbb{Z}$-algebra D, then D/μ is a finite field.*

Proof. If $\mathbb{Z}$ injects into κ (we shall see that this cannot happen) then κ is a module-finite extension of a polynomial ring $\mathbb{Z}[1/d][x_1, \ldots, x_h]$ where $d \in \mathbb{Z} - \{0\}$ (we need not localize κ at d, since d must already be invertible in the field κ). If p is a prime not dividing d, then p is not invertible in $\mathbb{Z}_d$, nor in the polynomial ring, and hence cannot be invertible in a module-finite extension of the polynomial ring, a contradiction.

Hence, $\mathbb{Z}$ does not inject into κ, which implies that κ has characteristic $p > 0$ and is finitely generated over $\mathbb{Z}/pZ$ for some prime $p > 0$. Then κ is module-finite over a polynomial ring $(\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_h]$. Since κ has dimension 0, we must have $h = 0$, i.e., that κ is module-finite over $\mathbb{Z}/p\mathbb{Z}$, which implies that κ is a finite field. □

Second step: generic freeness

Before proving a strong form of generic freeness, we need:

Lemma. *Let D be any ring. let*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k \subseteq \cdots \subseteq M$$

be a non-decreasing possibly infinite sequence of submodules of the module M over D, and suppose that $\bigcup_{k=1}^{\infty} M_k = M$. If M_{k+1}/M_k is free over D for all $k \geq 0$, then M is free.

Proof. Choose a free basis for every M_{k+1}/M_k and for every $k \geq 0$, let $\mathcal{B}_k$ be a set of elements in M_{k+1} that maps onto the chosen free basis for M_{k+1}/M_k. In particular, $\mathcal{B}_1$ is a free basis for $M_1 \cong M_1/0$. We first claim that $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$ is a free basis for M_{k+1} for every $k \geq 0$. We already have this for $k = 0$, and we use induction. Thus, we may assume that $\mathcal{B}_{k-1}$ is a free basis for $\mathcal{M}_k$, and we must show that $\mathcal{B}_k$ is a free basis for $\mathcal{M}_{k+1}$. This is clear from the fact that the D-linear map $M_{k+1}/M_k \to M_{k+1}$ that sends each element of the chosen free basis of M_{k+1}/M_k to the element of $\mathcal{B}_k$ that lifts it is a splitting of the exact sequence

$$0 \to M_k \to M_{k+1} \to M_{k+1}/M_k \to 0.$$

It then follows at once that $\mathcal{B} = \bigcup_{k=0}^{\infty} \mathcal{B}_k$ is a free basis for M: first, there can be no non-trivial relations, for such a relation involves only finitely many basis elements and so would give a non-trivial relation on the elements of some $\mathcal{B}_k$. Second, since $\mathcal{B}$ evidently contains a set that spans M_k for every k and $\bigcup_{k=1}^{\infty} M_k = M$, $\mathcal{B}$ spans M. □

Theorem (strong form of generic freeness). *Let D be a Noetherian domain, and let $D = T_0 \to T_1 \to T_2 \to \cdots \to T_s$ be a sequence of maps of finitely generated T_0-algebras. Let M be a finitely generated T_s-module, and for every i, where $0 \leq i \leq s$, let N_i be a finitely generated T_i-submodule of M. Let $Q = M/(N_0 + \cdots + N_s)$. Then there exists a nonzero element d in D such that Q_d is D_d-free.*

Proof. By inserting additional algebras in the chain, we may assume without loss of generality that every T_{i+1} is generated over the image of T_i by one element. We use induction on s. Note also that we can view Q as the quotient of $M' = M/N_s$ by the sum of the images of $N_1, \ldots, N_{s-1}$, so that there is no loss of generality in assuming that $N_s = 0$.

If $s = 0$ we simply have a finitely generated D-module M. In this case, take a maximal sequence of elements $u_1, \ldots, u_h \in M$ that are linearly independent over D, so that $G = Du_1 + \cdots + Du_h$ is free over D. (Such a sequence must be finite, or one would have an infinite strictly ascending chain of submodules of M spanned by the initial segments of the sequence $u_1, u_2, u_3, \ldots$.) It follows that M/G is a torsion-module over D: for every element u of $M - G$ there must be a nonzero element of D that multiplies u into G, or else we may take $u_{h+1} = u$ to get a longer sequence. Thus, there is an element d_j of $D - \{0\}$ that multiplies each element v_j of a finite set of generators for M into G. Let d be a nonzero common multiple of these d_j. Then $M_d = G_d$ is free over D_d.

Now suppose that $s \geq 1$. Take a finite set $\mathcal{S}$ of generators for M that includes a finite set of generators for each of the N_i. Let N be the T_{s-1} submodule of M generated by all of these. By the induction hypothesis, we can choose $d' \in D - \{0\}$ such that $N/(N_0 + \cdots + N_{s-1})$ becomes free when we localize at d'. If we can choose d such that M/N becomes free, then localizing at dd' solves the problem. Let θ be an element of T_s that generates T_s over the image of T_{s-1}. Let $M_0 = 0$ and let $M_i = N + \theta N + \cdots + \theta^{i-1}N$ for $i \geq 1$, so that $M_1 = N$, $M_2 = N + \theta N$, $M_3 = N + \theta N + \theta^2 N$, and so forth. Let $W_i = M_i/M_{i-1}$ for $i \geq 1$. We claim that there are surjections

$$N = W_1 \twoheadrightarrow W_2 \twoheadrightarrow \cdots \twoheadrightarrow W_k \twoheadrightarrow \cdots,$$

where the map $W_i \to W_{i+1}$ is induced by multiplication by θ, which takes $M_i \to M_{i+1}$ for every i. The image of the map on numerators contains $\theta^i N$, which spans the quotient, so that these are all surjections. The kernels of the maps $N \to W_i$ form an ascending sequence of T_{s-1}-submodules of N, and so the kernels are all eventually the same. This implies that there exists k such that for all $i \geq k$, $W_i \cong W_k$. By the induction hypothesis for each of the modules W_j we can choose $d_j \in D - \{0\}$ such that $(W_j)_{d_j}$ is free over D_{d_j}. Let d be a common multiple of these d_j. By the Lemma above, $(M/N)_d$ is free over D_d. $\square$

Third step: descent to a finitely generated algebra over the integers

The next step in our effort to prove the sharper form of the result on the Cohen-Macaulay property for rings of invariants is to "replace" K by a finitely generated $\mathbb{Z}$-subalgebra D of K. The idea is to make D sufficiently large so that all of the salient features of a counter-example can be discussed in D-algebras instead of K-algebras. We then localize D at one element so as to make certain quotients free, using the Theorem on generic freeness. Finally, we kill a maximal ideal of D and so produce a counter-example to the characteristic $p > 0$ form of the Theorem. Since we have already proved the result in positive characteristic, this is a contradiction, and will complete the proof of the Theorem.

We have a field K of chracteristic 0, a polynomial ring $R = K[x_1, \ldots, x_n]$, a K-subalgebra A of R finitely generated over K by forms $u_1, \ldots, u_s$, and a homogeneous system of parameters $F_1, \ldots, F_d$ for A. We also know that for $1 \leq i \leq d-1$,

$$(F_1, \ldots, F_i)R \cap A = (F_1, \ldots, F_i)A.$$

We want to prove that $F_1, \ldots, F_d$ is a regular sequence. Suppose not, and suppose that

$$(\dagger) \quad GF_{i+1} = G_1F_1 + \cdots + G_iF_i$$

where $G_1, \ldots, G_i$, $G \in A$ and $G \notin (F_1, \ldots, F_i)A$, where $i \leq d-1$. We want to show that we can construct an example with the same properties in prime characteristic $p > 0$.

Since $F_1, \ldots, F_d$ is a homogeneous system of parameters for A, every u_j has a power in the ideal generated by $F_1, \ldots, F_d$. Hence, for every j we can choose $m_j \geq 1$ and an equation

$$u_j^{m_j} = w_{j,1}F_1 + \cdots + w_{j,d}F_d,$$

where the $w_{j,k} \in A$. Moreover, every F_t, G_t, and G, as well as all the $w_{j,k}$, can be expressed as polynomials in $u_1, \ldots, u_s$ with coefficients in K, say $F_k = P_k(u_1, \ldots, u_s)$, $G_k = Q_k(u_1, \ldots, u_s)$ for $1 \leq k \leq d$, $G = Q(u_1, \ldots, u_s)$, and $w_{j,k} = H_{j,k}(u_1, \ldots, u_s)$. As a first attempt at constructing the domain D, we take the $\mathbb{Z}$-subalgebra of K generated by all coefficients of the u_j (as polynomials in $x_1, \ldots, x_n$), the P_k, the Q_k, Q, and the $H_{j,k}$. However, we may (and shall) enlarge D further, specifically, by localizing at one nonzero element.

Let $R_D = D[x_1, \ldots, x_n]$, and let $A_D = D[u_1, \ldots, u_s] \subseteq R_D$. The elements F_j, G_j, G, and $w_{j,k}$ are in A_D, and we still have the relation $(\dagger)$ holding in A_D. Moreover, every u_j is in the radical of the ideal generated by $(F_1, \dots, F_d)$ in A_d, and so Rad $\bigl((F_1, \dots, F_d)A_D\bigr)$ is a homogeneous prime ideal of A_D, call it $\mathcal{Q}_D$. It is spanned over D by all forms of positive degree. We have that $A_D/\mathcal{Q}_D = D$.

We are now ready for the dénouement, which involves applying the result on generic freeness to preserve this situation while passing to positive characteristic.

Lecture of March 20

The first part of this lecture provides the final step in proving the Theorem on p. 124 and its sharp form stated on p. 126: the latter is valid in equal characteristic 0 and in characteristic $p > 0$. I am designating the material after the completion of the proof as optional (and will not be tested on quizzes or in problem sets) but I want to give a brief discussion of what is covered here. Consider a 2×3 matrix of indeterminates over the complex numbers. The ring R generated by the three 2×2 minors is a ring of invariants of an action of $\mathrm{SL}(2, \mathbb{C})$ on the polynomial ring S generated by the six variables x_{ij} that are the entries of the matrix. One has a splitting of $R \hookrightarrow S$ as R-modules given by the Reynolds operator. It turns out that one can give such a splitting even if one replaces $\mathbb{C}$ by $\mathbb{Q}$. However, if one works instead over a field of characteristic $p > 0$, there is not splitting. This implies that one works over $\mathbb{Q}$, to define the values of the splitting on all monomials in the x_{ij}, one must be using every prime integer as a denominator. In the detailed discussion, there is an introduction to local cohomology theory.

The final step: the application of generic freeness

We have the following:

Lemma. *If $0 \to N \to M \to G \to 0$ is an exact sequence of D-modules and G is D-free, then the sequence is split, so that $M \cong N \oplus G$. In this case, for any D-module or D-algebra Q, the sequence $0 \to Q \otimes_D N \to Q \otimes_D M \to Q \otimes_D G \to 0$ is exact.*

Proof. To construct a splitting $f : G \to M$ choose a free basis $\mathcal{B}$ for G and for every element $b \in \mathcal{B}$, define $f(b)$ to be an element of M that maps to b. Exactness is preserved by $Q \otimes_D \_$ becaue tensor product commutes with direct sum. $\square$

We are now ready to complete the proof.

There are several exact sequences that we are going to want to preserve while passing to characteristic $p > 0$. Since A has Krull dimension d and is module-finite over $K[F_1, \dots, F_d]$, we know that $F_1, \dots, F_d$ are algebraically independent over K and, hence, over the smaller ring D. This yields

$$(1) \quad 0 \to D[F_1, \dots, F_d] \to A_D \to A_D/D[F_1, \dots, F_d] \to 0$$

where $D[F_1, \, \ldots \, , F_d]$ is a polynomial ring over D. After localizing at one element of $D-\{0\}$ we may assume that all these modules are D-free, and, henceforth we assume this. We shall make a number of further localizations like this, but only finitely many. Note that localizing further preserves freeness. So long as there are only finitely many localizations at one element, D remains a finitely generated $\mathbb{Z}$-algebra.

Second, we have

$$(2) \quad 0 \to A_D \to R_D \to R_D/A_D \to 0.$$

We may assume that D has been localized at one more element so that the terms of the exact sequence above are D-free.

For every j, the ideal $(F_1, \, \ldots \, , F_j)A$ is contracted from $R = K[x_1, \, \ldots \, , x_n]$. This implies that the map $A/(F_1, \, \ldots \, , F_j)A \to R/(F_1, \, \ldots \, , F_j)R$ is injective. This map arises from the map

$$(*) \quad A_D/(F_1, \, \ldots \, , F_j)A_D \to R_D/(F_1, \, \ldots \, , F_D)R_D$$

in two steps: we may tensor over D with the fraction field $\mathcal{F}$ of D, and then we may tensor over $\mathcal{F} \subseteq K$ with K. After we tensor with K, we know that the map is injective. Since K is faithfully flat (in fact, free) over its subfield $\mathcal{F}$, $(*)$ is injective once we tensor with $\mathcal{F}$. Therefore the kernel, if any, is torsion over D. Hence, if we localize at one element of $D - \{0\}$ so that $A_D/(F_1, \, \ldots \, , F_j)A_D$ becomes D-free, the map $(*)$ is injective. We may also localize at one element of $D - \{0\}$ so that the cokernel is free over D, and therefore we have for every j an exact sequence

$$(3) \quad 0 \to A_D/(F_1, \, \ldots \, , F_j)A_D \to R_D/(F_1, \, \ldots \, , F_D)R_D \to \frac{R_D/(F_1, \, \ldots \, , F_D)R_D}{A_D/(F_1, \, \ldots \, , F_j)A_D} \to 0$$

consisting of free D-modules.

Finally, we have that $G\big(A/(F_1, \, \ldots \, , F_i)A\big) \neq 0$. It follows that $G\big(A_D/(F_1, \, \ldots \, , F_i)A_D\big)$ is not a D-torsion module, since it is nonzero after we apply $K \otimes_D \_$. Hence, after localizing further at one element of $D - \{0\}$, we may assume that

$$(4) \quad 0 \to G\big(A_D/(F_1, \, \ldots \, , F_i)A_D\big) \to A_D/(F_1, \, \ldots \, , F_i)A_D \to A_D/(F_1, \, \ldots \, , F_i, \, G)A_D \to 0$$

is an exact sequence of free D-modules such that the module $G\big(A_D/(F_1, \, \ldots \, , F_i)A_D\big)$ is not zero.

We now choose a maximal ideal μ of D. Then $\kappa = D/\mu$ is a finite field, and has prime characteristic $p > 0$ for some p. We write A_κ and R_κ for $\kappa \otimes_D A_D = A_D/\mu A_D$ and $\kappa \otimes_D R_D = R_D/\mu R_D \cong \kappa[x_1, \, \ldots \, , x_n]$, respectively. We use $\overline{w}$ to indicate the image $1 \otimes w$ of w in A_κ or R_κ. By the preceding Lemma, the sequences displayed in (1), (2), (3), and (4) remain exact after applying $\kappa \otimes_D \_$.

From (1) we have an injection of $\kappa[F_1, \, \ldots \, , F_d]$, which is a polynomial ring, into A_κ. This shows that the dimension of A_κ is at least d. Since the homogeneous maximal ideal of A_κ is generated by the $\overline{u}_j$ and these are nilpotent on the ideal $(\overline{F}_1, \, \ldots \, , \overline{F}_d)A_\kappa$, we have that $\overline{F}_1, \ldots, \overline{F}_d$ is a homogeneous system of parameters for A_κ. From (2) we have an injection $A_\kappa \hookrightarrow R_\kappa$. From (3), we have that $(\overline{F}_1, \ldots, \overline{F}_j)A_\kappa$ is contracted from R_κ for every j. From (4), we have $\overline{G}$ is not in $(\overline{F}_1, \ldots, \overline{F}_i)A_\kappa$, although we still have that

$$\overline{G}\,\overline{F}_{i+1} = \overline{G}_1\overline{F}_1 + \cdots + \overline{G}_i\overline{F}_i$$

in A_κ, so that A_κ is not Cohen-Macaulay. This contradicts the positive characteristic version of the Theorem, which we have already proved. □

Note: we have completed the proof of the sharper form of the result on the Cohen-Macaulay property for rings of invariants stated on p. 4 of the Lecture Notes of March 11 in all characteristics now, and, consequently, we have completed as well the proof of the Theorem stated in the middle of p. 3 of the Lecture Notes of March 11.

Optional material

Remarks. It might seem more natural to prove the Theorem stated in the mdidle of p. 3 of the Lecture Notes of March 11 by preserving the Reynolds operator, i.e., that the ring of invariants is a direct summand, while passing to characteristic p. It turns out that this is not possible, as we shall see below. What we actually did was to preserve finitely many specific consequences of the existence of the Reynolds operator, namely the contractedness of the ideals $(F_1, \ldots, F_j)A$ from R, while passing to characteristic p, and this was sufficient to get the proof to work.

Consider the action of $G = \mathrm{SL}(2, K)$ on $\mathbb{C}[X]$, where $X = \bigl(x_{i,j}\bigr)$ is a 2×3 matrix of indeterminates that sends the entries of X to the corresponding entries of γX for all $\gamma \in G$. It turns out that the ring of invariants in this case is $\mathbb{C}[\Delta_1, \Delta_2, \Delta_3]$, where Δ_j is the determinant of the submatrix of X obtained by deleting the j th column of X. In this case Δ_1, Δ_2, and Δ_3 are algebraically independent: this is true even if we special the entries of the matrix X so as to obtain

$$\begin{pmatrix} 1 & 1 & (y-z)/x \\ 0 & x & y \end{pmatrix},$$

where x, y, and z are indeterminates. It is easy to "descend" the inclusion $A = R^G = \mathbb{C}[\Delta_1, \Delta_2, \Delta_3] \subseteq \mathbb{C}[X]$ to an inclusion of finitely generated $\mathbb{Z}$-algebras: one can take $D = \mathbb{Z}$, and consider the inclusion $\mathbb{Z}[\Delta_1, \Delta_2, \Delta_3] \subseteq \mathbb{Z}[X]$. However, this is *not* split after we localize at one integer of $\mathbb{Z} - \{0\}$, nor even if we localize at all positive prime integers except a single prime $p > 0$. The Reynolds operator needs the presence of *all* prime integers $p \neq 0$ in the denominators. Note that if the map were split after localizing at all integers not divisible by p, we could then apply $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \_$ and get a splitting of the map $(\mathbb{Z}/p\mathbb{Z})[\Delta_1, \Delta_2, \Delta_3] \subseteq (\mathbb{Z}/p\mathbb{Z})[X]$. But we shall see below that this map is *not* split.

At the same time, we want to note that in the Theorem on generic freeness, it is important that the algebras T_i are nested, with maps $T_0 \to T_1 \to T_2 \to \cdots \to T_s$. The result is false if one kills a sum of submodules over mutually incomparable subalgebras, or even a sum of such subalgebras.

Both our proof that $(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\, \Delta_2,\, \Delta_3] \subseteq (\mathbb{Z}/p\mathbb{Z})[X]$ does not split and our example of the fallure of generic freeness when the T_i are incomparable are based on looking at the same example.

Namely, we consider the module

$$H = \frac{\mathbb{Z}[X]_{\Delta_1\Delta_2\Delta_3}}{\mathbb{Z}[X]_{\Delta_2\Delta_3} + \mathbb{Z}[X]_{\Delta_1\Delta_3} + \mathbb{Z}[X]_{\Delta_1\Delta_2}}$$

where X is the same 2×3 matrix of indeterminates discussed in the action of $\mathrm{SL}(2,\, \mathbb{C})$ above and $D = T_0 = \mathbb{Z}$. Note that the numerator and the three summands in the denominator are all finitely generated $\mathbb{Z}$-algebras. We shall see that $\mathbb{Q} \otimes_{\mathbb{Z}} H$ is a nonzero vector space over the rational numbers $\mathbb{Q}$, and that H is a divisible abelian group, i.e., that $nH = H$ for every nonzero integer n. It follows that if we localizate at any nonzero integer $n \in \mathbb{Z}$, H_n is nonzero, and is not free over $\mathbb{Z}_n$. If it were free over $\mathbb{Z}_n$, it could not be divisible by p for any integer p that does not divide n, since it is simply a direct sum of copies of $\mathbb{Z}_n$.

It remains to prove the assertions that $\mathbb{Q} \otimes H \neq 0$, that $pH = H$ for every nonzero prime integer $p > 0$, and that the map $(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\, \Delta_2\, \Delta_3] \to (\mathbb{Z}/p\mathbb{Z})[X]$ is non-split for every prime integer $p > 0$.

We first note that if $Z_1,\, Z_2, Z_3$ are indeterminates and B is any base ring, then

$$H(B,\, Z) = \frac{B[Z_1,\, Z_2,\, Z_3]_{Z_1Z_2Z_3}}{B[Z_1,\, Z_2,\, Z_3]_{Z_2Z_3} + B[Z_1,\, Z_2,\, Z_3]_{Z_1Z_3} + B[Z_1,\, Z_2,\, Z_3]_{Z_1Z_2}}$$

is nonzero: in fact, the numerator is the free B-module spanned by *all* monomnials $Z_1^{a_1}Z_2^{a_2}Z_3^{a_3}$ where $a_1,\, a_2,\, a_3 \in \mathbb{Z}$, and the denominator is the free B-module spanned by all such monomials in which one of the integers $a_1,\, a_2,\, a_3$ is nonnegative. Hence, the quotient may be identified with the free B-module spanned by all monomials $Z_1^{a_1}Z_2^{a_2}Z_3^{a_3}$ such that $a_1, a_2, a_3 < 0$. Since $\Delta_1,\, \Delta_2,\, \Delta_3$ are algebraically independent over $\mathbb{C}$ and, hence, over $\mathbb{Q}$, we have that $H(\mathbb{Q},\, \Delta_1,\, \Delta_2,\, \Delta_3) = H(\mathbb{Q},\, \Delta)$ is a nonzero vector space over $\mathbb{Q}$. We have a comutative diagram:

$$\begin{tikzcd}
H(\mathbb{C},\, \Delta) \arrow[r, "\iota"] & H(\mathbb{C},\, \Delta) \otimes_{\mathbb{C}[\Delta]} \mathbb{C}[X] \\
H(\mathbb{Q},\, \Delta) \arrow[u] \arrow[r] & H(\mathbb{Q},\, \Delta) \otimes_{\mathbb{Q}[\Delta_1,\, \Delta_2,\, \Delta_3]} \mathbb{Q}[X] \arrow[u]
\end{tikzcd} .$$

The top row may be thought of as obtained from the bottom row by applying $\mathbb{C} \otimes_{\mathbb{Q}} \_$.

We next observe that because $\iota : \mathbb{C}[\Delta_1,\, \Delta_2,\, \Delta_3] \subseteq \mathbb{C}[X]$ is split by the Reynolds operator for the action of $\mathrm{SL}(2,\, \mathbb{C})$, and the top row is obtained by tensoring this inclusion over $\mathbb{C}[\Delta_1,\, \Delta_2,\, \Delta_3]$ with $H(\mathbb{C},\, \Delta)$, the top arrow is an injection. Since $\mathbb{C}$ is free and therefore faithfully flat over $\mathbb{Q}$, the arrow in the bottom row is also an injection. Thus,

$H(\mathbb{Q},\,\Delta) \otimes_{\mathbb{Q}[\Delta_1,\,\Delta_2,\,\Delta_3]} \mathbb{Q}[X]$ is a nonzero vector space over $\mathbb{Q}$, and this is the same as the result of apply $\mathbb{Q} \otimes_{\mathbb{Z}} \_$ to

$$H(\mathbb{Z},\,\Delta) \otimes_{\mathbb{Z}[\Delta_1,\,\Delta_2,\,\Delta_3]} \mathbb{Z}[X] = \frac{\mathbb{Z}[X]_{\Delta_1\Delta_2\Delta_3}}{\mathbb{Z}[X]_{\Delta_2\Delta_3} + \mathbb{Z}[X]_{\Delta_1\Delta_3} + \mathbb{Z}[X]_{\Delta_1\Delta_2}}$$

which is the module H described earlier.

Finally, we shall show that $H = pH$ for every prime integer $p > 0$, and from this we deduce that $(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\,\Delta_2,\,\Delta_3] \to (\mathbb{Z}/p\mathbb{Z})[X]$ is non-split for every prime integer $p > 0$. Note that $H/pH = (\mathbb{Z}/p\mathbb{Z}) \otimes_{\mathbb{Z}} H$. If $(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\,\Delta_2,\,\Delta_3] \to (\mathbb{Z}/p\mathbb{Z})[X]$ splits over $(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\,\Delta_2,\,\Delta_3]$ then by applying $\_ \otimes_{\mathbb{Z}/p\mathbb{Z}} H(\mathbb{Z}/p\mathbb{Z}, \Delta)$ we obtain in injection

$$H(\mathbb{Z}/p\mathbb{Z}, \Delta) \to H/pH.$$

The lefthand term is not zero, and this will imply that $H/pH \neq 0$. Thus, by showing that $H/pH = 0$, we also show that

$$(\mathbb{Z}/p\mathbb{Z})[\Delta_1,\,\Delta_2,\,\Delta_3] \to (\mathbb{Z}/p\mathbb{Z})[X]$$

does not split.

The final step involves some explicit use of local cohomology theory. We refer to to the Lecture of December 8 from Math 711, Fall 2006, which contains a concise treatment of the material we need here as well as further references, but we give a brief description.

First recall that if M, N are modules over R, the modules $\mathrm{Ext}^i_R(M,\,N)$ are defined as follows. Choose a free (or projective) resolution of M, i.e., an exact complex

$$\cdots \to P_i \to \cdots \to P_0 \to M \to 0$$

such that the P_i are free (or projective). This complex will frequently be infinite. Let $P_\bullet$ be the complex obtained by replacing M by 0, i.e.,

$$\cdots \to P_i \to \cdots \to P_0 \to 0.$$

Apply the contravariant functor $\mathrm{Hom}_R(\_,\,N)$ to this complex to obtain:

$$0 \to \mathrm{Hom}_R(P_0,\,N) \to \cdots \to \mathrm{Hom}_R(P_i,\,N) \to \cdots\,.$$

Then $\mathrm{Ext}^i_R(M,\,N)$ is the cohomology of the complex at the $\mathrm{Hom}_R(P_i,\,N)$ spot (this is still the kernel of the outgoing map at that spot modulo the image of the incoming map: it is called *cohomology* because the maps increase the indices).

If R is Noetherian, $I = (f_1,\,\ldots\,,f_s)$ is an ideal of R, and M is any R-module, the ith *local cohomology module* of M with support in I is defined as

$$\varinjlim_t \mathrm{Ext}^i(R/I_t,\,M)$$

where I_t runs through any sequence of ideals cofinal with the powers of I. In particular, we may take $I_t = I^t$ for all t, but, as we shall see below, other choices of I can be advantageous. It follows that $H^i_I(M)$ depends only on the the radical of I and not on I itself.

The main result that we are going to assume without proof here is that $H^i_I(M)$ is also the cohomology at the i th spot of the complex

$$(*) \quad 0 \to M \to \bigoplus_{1 \le j \le s} M_{f_i} \to \cdots \to \bigoplus_{1 \le j_1 < j_2 < \cdots j_i \le s} M_{f_{j_1} f_{j_2} \cdots f_{j_i}} \to \cdots \to M_{f_1 f_2 \cdots f_s} \to 0.$$

If we think of the i th term as a direct sum and the $i+1$ st term as a direct product, the maps are determined by specifying maps $M_{f_{j_1} \cdots f_{j_i}} \to M_{f_{k_1} \cdots f_{k_{i+1}}}$, where $j_1 < \cdots < j_i$ and $k_1 < \cdots < k_{i+1}$. The map is 0 unless, $\{j_1, \ldots, j_i\}$ is obtained from $\{k_1, \ldots, k_{i+1}\}$ by omitting one term, sayt k_t, and then the map is $(-1)^{t-1}\theta$ where θ is the natural map induced by localizing "further" at f_{k_t}.

By the description of local cohomology in $(*)$ above, the module

$$H/pH = \frac{(\mathbb{Z}/p\mathbb{Z})[X]_{\Delta_1 \Delta_2 \Delta_3}}{(\mathbb{Z}/p\mathbb{Z})[X]_{\Delta_2 \Delta_3} + (\mathbb{Z}/p\mathbb{Z})[X]_{\Delta_1 \Delta_3} + (\mathbb{Z}/p\mathbb{Z})[X]_{\Delta_1 \Delta_2}}$$

is precisely the local cohomology module $H^3_I\big((\mathbb{Z}/p\mathbb{Z})[X]\big)$ where $I = (\Delta_1, \Delta_2, \Delta_3)S$, where $S = (\mathbb{Z}/p\mathbb{Z})[X]$. On the other hand, from the definition above this local cohomology module is

$$\varinjlim{}_t \operatorname{Ext}^3_S(S/I_t, S),$$

where I_t is any sequence of ideals cofinal with the powers of I. In our case, we use $I_t = I^{[p^t]}$. The proof is completed by showing that for all t, there is a free resolution of R/I_t over R of length 2. Hence, every $\operatorname{Ext}^3_S(S/I_t, S)$ vanishes. For $I = I_1$ itself, we leave it as an exercise to show that

$$0 \to S^2 \xrightarrow{\beta} S^3 \xrightarrow{\alpha} S \to S/I \to 0$$

is such a resolution, where $\alpha = \big(\Delta_1 \ \ -\Delta_2 \ \ \Delta_3\big)$ and the matrix of β is the transpose of X. The case of I_t follows at once by applying $S \otimes_S \_$, where the map $S \to S$ is the t th iteration F^t of the Frobenius endomorphism, to this complex. Since S is faithfully flat over itself via this map, the new complex is exact, and provides a free resolution of S/I_t of length 2. □

Lecture of March 23

This lecture begins a detailed study of rings of invariants of algebraic tori, i.e., groups of the form $\mathrm{GL}(1, K)^s$, over an algebraically closed field K. Some results hold without restriction on the field. In fact, for algebras finitely generated over a field, the Cohen-Macaulay property is unaffected by base change of the field to its algebraic closure, and one can often make use of this fact. See the Lemma on the next page.

I will regard a great deal of the material in this lecture as optional, but I will summarize some main points, and I hope you will, at a minimum, read and understand the main results. For several results, I will specify that the theorem is not optional.

One point is that a linear algebraic group G acts on its coordinate ring $K[G]$. Every finite-dimensional G-module N occurs as a G-submodule of a direct sum of copies of $K[G]$. From this one can deduce that a linear algebraic group is linearly reductive if and only if $K[G]$ decomposes, as a G-module, into a direct sum of irreducibles, and all irreducible G-modules arise in this way. See the Corollary to the Theorem on p. 145 of the notes. All irreducible G-modules over $\mathrm{GL}(1, K)^s$ have dimension one as K-vector space, and the action is determined by an s-tuple of integers: if the element of $\mathbb{Z}^s$ is $k_1, \ldots, k_s$, then one gets a G-module structure on the K-vector space spanned by x by letting $(\gamma_1, \ldots, \gamma_s) \in \mathrm{GL}(1, K)^s$ act on x by $(\gamma_1, \ldots, \gamma_s) : x \mapsto \gamma_1^{k_1} \cdots \gamma_k^{k_s} x$.

It turns out the given a degree-preseriving action of $\mathrm{GL}(1, s)^K$ on a polynomial ring in n variables over an algebraically close field K, one can choose the variables so that each variable spans, over K, a one-dimensional G-stable irreducible submodule, so that one has one s-tuple of integers as above for eavery variable.

Required material. For actions of this form, the ring of invariants is spanned over K by all monomials $x_1 a_1 \cdots x_n^{a_n}$, where the vector of exponents $\alpha = (a_1, \ldots, a_n)$ runs through all nonnegative integer solutions of a system of linear equations over $\mathbb{Z}$. See the Theorem on p. 147. In consequence, rings of this form are Cohen-Macaulay. The fact that the ring defined by the vanishing of the 2×2 minors of a matrix of indeterminates is, consequently, Cohen-Macaulay is also required material.

The last part of this lecture begins work on the proof of the result that any normal subring of $K[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}]$ (the Laurent polynomials in $x_1, \ldots, x_n$) is Cohen-Macaulay. Such rings are often called *toric.* The result is a consequence of the theorem discussed in the preceding paragraph and a quite detailed analysis of additive subsemgroups of $\mathbb{Z}^n$, and will extend into the next lecture. The detailed analysis of subsemigroups of $\mathbb{Z}^n$ is optional, but the result that normal rings generated by monomials are Cohen-Macaulay is required.

We begin by proving the lemma discussed above.

Lemma. *(a) Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a flat local homomorphism of Noetherian rings whose fiber is zero-dimensional. Then R is Cohen-Macaulay if and only if S is Cohen-Macaulay.*

(b) Let $R \to S$ be a faithfully flat homomorphism of Noetherian rings such that every maximal ideal of S lies over a maximal ideal of R, and for every maximal ideal $\mathfrak{m}$ of R, the fiber $S/\mathfrak{m}S$ is zero-dimensional. The R is Cohen-Macaulay if and only if S is $Cohen-Macaulay$.

(c) Let R be a finitely generated algebra over a field K and let L be an algebraic field extension of K. Then R is Cohen-Macaulay if and only if $S = L \otimes_K R$ is Cohen-Macaulay.

Proof. For part (a), let $x_1, \ldots, x_d$ be a system of parameters for R. If it is a regular sequence, then flatness implies that it is also a regular sequence in S, and since $S/\mathfrak{m}S$ is zero-dimensional, $\mathfrak{n}$ is nilpotent modulo $\mathfrak{m}S$ and so modulo $(x_1, \ldots, x_d)S$.

On the other hand, minimal primes of S lie over minimal primes of R: if Q is minimal in S with contraction P, then $R_P \to S_Q$ is faithfully flat and so injective, and since QS_Q is nilpotent, the same holds for PR_P. For the converse, there is nothing to prove when R has dimension 0. We use induction on the dimension of R. Suppose S is Cohen-Macaulay and let $x_1 = x$ be part an element of R not in any minimal prime. Then indt is not in any minimal prime of S, and so is part of a system of parameters for both R and x. Since S is faithfully flat and it is not a zerodivisor in S, it is not a zerodivisor in R. We can now complete the proof by induction by considering $R/xR \to S/xS$. □

(b) If $\mathfrak{m}$ is a maximal ideal of R there is a maximal ideal $\mathfrak{n}$ of S containing $\mathfrak{m}S$, and since S/fmS is 0 dimensional, $R_{\mathfrak{m}} \to S_{\mathfrak{n}}$ satisfies (a). Hence, if S is Cohen-Macaulay so is R. But if $\mathfrak{n}$ is maximal in S and lies over $\mathfrak{m}$ in R, then $\mathfrak{m}$ is maximal and, again $R_{\mathfrak{m}} \to S_{\mathfrak{n}}$ satisfies (a). Thus, if R is Cohen-Macaulay, so is S. □

(c) $S = L \otimes_K R$ is faithfully flat over R. If $\mathfrak{m}$ is maximal in R, we know that $R/\mathfrak{m}$ is a finitely generated zero-dimensional K-algebra, and so module-finite over K, by Noether normalization. Hence, S/fmS is module-finte over L and zero-dimensional. Moreover, if $\mathfrak{n}$ is a maximal ideal of S lying over a prime P in R, then R/P injects as a K-algebra into the module-finite L-algebra S/fn, which is integral over K, since L is. Hence R/P is zero-dimensional and P is maximal. □

Remark. With more work, one can remove the condition that L be algebraic over K in part (c). However, note that maximal ideals of S need not lie over maximal ideals of R when L is not algebraic over K. E.g., let $L = K(t)$ be a transcendental extension. In $L[x]$ the ideal $x - t$ is maximal, but lies over the 0 ideal in $K[x]$.

We next want to prove that the algebraic torus $\mathrm{GL}(1, K)^s$, which we shall refer to simply as a *torus*, is linearly reductive, as asserted earlier, over every algebraically closed field K, regardless of characteristic. The notation G_{m} is also used for the multiplicative group of K viewed as a linear algebraic group via its isomorphism with $\mathrm{GL}(1, K)$.

Until further notice, K denotes an algebraically closed field. Let G be any linear algebraic group over K. Let $K[G]$ be its coordinate ring, whose elements may be thought of as thein regular maps of the closed algebraic set G to K. (This notation has some danger of ambiguity, since $K[G]$ is also used to denote the group ring of G over K, but we shall only use this notation for the coordinate ring here.) The right action of G on itself by multiplication (i.e., γ acts so that $\eta \mapsto \eta\gamma$) induces a (left) action of G on the K-vector space $K[G]$. Thus, if $f \in K[G]$, $\gamma(f)$ denotes the function whose value on $\eta \in G$ is $f(\eta\gamma)$. Since right multiplication by γ is a regular map of $G \to G$, the composition with $f : G \to K$ is also regular.

Discussion: regularity of the action of G on $K[G]$. We study the map

$$G \times K[G] \to K[G]$$

and prove that it gives an action in our sense. Let $f \in K[G]$. Let μ be the multiplication map $G \times G \to G$. The function $(\eta, \gamma) \mapsto f(\eta\gamma)$ is the composite $f \circ \mu$, and so is a regular function on $G \times G$. Therefore, it is an element of

$$K[G \times G] \cong K[G] \otimes_K K[G],$$

and consequently can be written in the form

$$\sum_{i=1}^{k} g_i \otimes h_i$$

where the g_i, $h_i \in K[G]$. This means that for every fixed γ,

$$(*) \quad \gamma(f) = \sum_{t=1}^{k} h_t(\gamma) g_t.$$

Hence, all of the functions $\gamma(f)$ are in the K-span of the g_i, and this is finite-dimensional. It follows that $K[G]$ is a union of finite-dimensional G-stable subspaces V. Let $f_1, \ldots, f_n$ be a basis for one such V. For every f_i in the basis we have a formula like $(*)$ of the form

$$(*_i) \quad \gamma(f_i) = \sum_{t=1}^{k} h_{it}(\gamma) g_{it}.$$

A priori, k may vary with i but we can work with the largest value of k that occurs. Hence, for $c_1, \ldots, c_n \in K^n$ we have

$$(**) \quad \gamma(\sum_{i=1}^{n} c_i f_i) = \sum_{t=1}^{k} \sum_{i=1}^{n} c_i h_{it}(\gamma) g_{it}.$$

Let Θ be a K-vector space retraction of the K-span of the g_{it} to V. Since Θ fixes the element on the left hand side, which is in V, applying Θ to both sides yields:

$$(\#) \quad \gamma(\sum_{i=1}^{n} c_i f_i) = \sum_{t=1}^{k} \sum_{i=1}^{n} c_i h_{it}(\gamma)\Theta(g_{it}).$$

Here, each $\Theta(g_{it})$ is a fixed linear combination of $f_1, \ldots, f_n$, and although we do not carry this out explicitly, the right hand side can now be rewritten as a linear combination of $f_1, \ldots, f_n$ such that coefficients occurring are polynomials in the regular functions h_{it} on G and the coefficients $c_1, \ldots, c_n$ parametrizing $V \cong K^n$. It follows at once that the action of G on V is regular for every such V. □

We next note:

Theorem. *Let G be a linear algebraic group over a field K, and let N be a finite dimensional G-module. Then N is isomorphic with a submodule of $K[G]^{\oplus h}$ for some h.*

Proof. Let $\theta : N \to K$ be an arbitrary K-linear map. We define a K-linear map

$$\theta^{\vee} : N \to K[G]$$

which will turn out to be a map of G-modules as follows: if $v \in N$, let $\theta^{\vee}(v)$ denote the function on G whose value on $\gamma \in G$ is $\theta\bigl(\gamma(v)\bigr)$. Since the map $G \times N \to N$ that gives the action of G on N is a regular map, for fixed $v \in N$ the composite

$$G \cong G \times \{v\} \subseteq G \times N \to N$$

is a regular map from $G \to N$ whose composite with the linear functional $\theta : N \to K$ is evidently regular as well. Hence, $\theta^{\vee}(v) \in K[G]$. This map is clearly linear in v, since θ and the action of γ on N are K-linear. Moreover, for any $\eta \in G$ and $v \in N$, $\theta^{\vee}\bigl(\eta(v)\bigr) = \eta\bigl(\theta^{\vee}(v)\bigr)$: the value of either one on $\gamma \in G$ is, from the appropriate definition, $\theta\bigl(\gamma(\eta(v))\bigr)$.

Choose a basis $\theta_1, \ldots, \theta_h$ for $\mathrm{Hom}_K(N, K)$. Then the map $N \to K[G]^{\oplus h}$ that sends $v \mapsto \theta_1^{\vee}(v) \oplus \cdots \oplus \theta_h^{\vee}(v)$ is a G-module injection of N into $K[G]^{\oplus h}$. To see this, note that if $v \neq 0$, it is part of a basis, and there is a linear functional whose value on v is not 0. It follows that for some i, $\theta_i(v) \neq 0$. But then $\theta_i^{\vee}(v) \neq 0$, since its value on the identity element of G is $\theta_i(v) \neq 0$. □

Lemma. *If M is G-module and is a direct sum of irreducibles $\{N_\lambda\}_{\lambda\in\Lambda}$, then every G-submodule N of M is isomorphic to the direct sum of the irreducibles in a subfamily of $\{N_\lambda\}_{\lambda\in\Lambda}$, and N has a complement that is the (internal) direct sum of a subfamily of the $\{N_\lambda\}_{\lambda\in\Lambda}$.*

Proof. Let N be a given submodule of M. We first construct a complement N' of the specified form. By Zorn's Lemma there is a maximal subfamily of $\{N_\lambda\}_{\lambda\in\Lambda}$ whose (direct) sum N' is disjoint from N. We claim that $M = N \oplus N'$. We need only check that $M = N + N'$. If not, some irreducible N_{λ_0} in the family is not contained in $N + N'$. But then its intersection with $N + N'$ must be 0, and we can enlarge the subfamily by using N_{λ_0} as well.

By the same argument, N' has a complement N'' in M that is a direct sum of a subfamily of $\{N_\lambda\}_{\lambda \in \Lambda}$. Then since $M = N \oplus N'$, $N \cong M/N'$, while since $M = N'' \oplus N'$, $M/N' \cong N''$. Thus, $N \cong N''$, which shows that N is isomorphic with a direct sum of a subfamily of the irreducibles as required. □

Corollary of the Theorem. *If G is a linear algebraic group over K and $K[G]$ is a direct sum of irreducible G-modules $\{N_\lambda\}_{\lambda\in\Lambda}$, then G is linearly reductive, and every G-module is isomorphic to a direct sum of irreducible G-modules in this family. In particular, up to isomorphism, every irreducible G-module is in this family.*

Proof. By the Theorem above, every finite-dimensional G-module N is a submodule of $K[G]^{\oplus h}$ for some h, and this module is evidently a direct sum of irreducibles from the same family. The result now follows from the Lemma just above. □

We next want to apply this Corollary to the case where $G = \mathrm{GL}(1,\, K)^s$ is a torus. Fix an s-tuple of integers $k_1, \, \ldots \, , k_s \in \mathbb{Z}^s$. One example of an action of G on a one-dimensional vector space Kx is the action such that $\gamma = (\gamma_1, \, \ldots \, , \gamma_s)$ sends

$$x \mapsto \gamma_1^{k_1} \cdots \gamma_s^{k_s} x$$

for all $\gamma \in G$. Because the vector space is one-dimensional, this G-module is clearly irreducible. We can now prove that for this G, every G-module is a direct sum of irreducibles of this type.

Theorem. *Let K be a field and let $G = \mathrm{GL}(1,\, K)^s$ be a torus. Then G is linearly reductive, and every G-module is a direct sum of one-dimensional G-modules of the type described just above.*

Proof. $K[G]$ is the tensor product of s copies of the coordinate ring of $GL(1,\, K)$, and may be identified with $K[x_1,\, x_1^{-1}, \, \ldots \, , \, x_s, \, x_s^{-1}]$. The action of G on this ring is such that $\gamma = (\gamma_1, \, \ldots \, , \gamma_s)$ sends $x_i \mapsto \gamma_i x_i$, $1 \leq i \leq s$. It follows at once that $\mu = x_1^{k_1} \cdots x_s^{k_s}$, where $(k_1, \, \ldots \, , k_s) \in \mathbb{Z}^s$, is mapped to $\gamma_1^{k_1} \cdots \gamma_s^{k_s} \mu$ for every $\gamma = (\gamma_1, \, \ldots \, , \gamma_s) \in G$, and so $K[G]$ is the direct sum of copies of G-modules as described just above, one for every monomial μ. The result is now immediate from the Corollary of the Theorem. □

Discussion: degree-preserving actions of a torus on a polynomial ring. We keep the assumption that K is an algebraically field, although we shall occasionally be able to relax it in the statements of some results: this will always be made explicit. The last statement in the Theorem below is an example.

Let $G = \mathrm{GL}(1,\, K)^s$ act by degree-preserving K-algebra automorphisms on the polynomial ring R in n variables over K so that R is a G-module. Giving such an action is the same as making the one forms $[R]_1$ of R into a G-module: the action then extends uniquely and automatically to R. Given such an action we may write $[R]_1$ as a direct sum of one-dimensional irreducible G-modules as above. Therefore, we may choose a basis $x_1, \dots, x_n$ for $[R]_1$ over K so that for every j, Kx_j is a G-stable submodule. It follows that for every j we can choose integers $k_{1,j}, \dots, k_{s,j} \in \mathbb{Z}$ such that for all $\gamma = (\gamma_1, \dots, \gamma_s) \in G$, γ sends

$$x_j \mapsto \gamma_1^{k_{1,j}} \cdots \gamma_s^{k_{s,j}} x_j.$$

Thus, the action of G on $R = K[x_1, \dots, x_n]$ is completely determined by the $s \times n$ matrix $\bigl(k_{i.j}\bigr)$ of integers. Every action comes from such a matrix, and for every such matrix there is a corresponding action.

Now consider any monomial $\mu = x_1^{a_1} \cdots x_n^{a_n}$ of R. For all $\gamma = (\gamma_1, \dots, \gamma_s) \in G$, γ sends

$$\mu \mapsto \bigl(\prod_{i=1}^{s} (\gamma_i^{k_{i,1}a_1 + \cdots + k_{i,n}a_n})\bigr)\mu.$$

It is now easy to see that the ring of invariants is spanned over K by all monomials $x_1^{a_1} \cdots x_n^{a_n}$ such that the s homogeneous linear equations

$$\sum_{j=1}^{n} k_{i,j} a_j = 0$$

are satisfied.

We have proved:

Theorem. *A ring generated by monomials arises as the ring of invariants of an action of a torus as above if and only if the ring is spanned over K by the monomials x^α where α runs through the solutions in $\mathbb{N}^n$ of some family of s homogenous linear equations over $\mathbb{Z}$ in n unknowns. Consequently, any such ring is Cohen-Macaulay, whether the field is algebraically closed or not.* □

Of course, the Cohen-Macaulay property follows because of our result on rings of invariants of linearly reductive linear algebraic groups acting on polynomial rings. If the field K is not algebraically closed, we may use the fact that the Cohen-Macaulay property is not affected when we tensor over K with its algebraic closure $\overline{K}$, by the Lemma at the top of p. 143.

Example: the ring defined by the vanishing of the 2×2 minors of a generic matrix. Let $G = GL(1, K)$ acting on $K[x_1, \dots, x_r, y_1, \dots, y_s]$, where $x_1, \dots, x_r, y_1, \dots, y_s$ are $r + s$ algebraically independent elements, so that if $\gamma \in G$, then $x_i \mapsto \gamma x_i$ for $1 \le i \le r$ and $y_i \mapsto \gamma^{-1} y_i$ for $1 \le i \le s$. Here, there is only one copy of the multiplicative group, and so there is only one equation in the system:

$$x_1^{a_1} \cdots x_r^{a_r} y_1^{b_1} \cdots y_s^{b_s}$$

is invariant if and only if

$$a_1 + \cdots + a_r - b_1 - \cdots - b_s = 0.$$

That is, the ring of invariants is spanned over K by all monomials μ such that the total degree of μ in the variables $x_1, \ldots, x_r$, which is $a_1 + \cdots a_r$, is equal to the total degre of μ in the variables $y_1, \ldots, y_s$, which is $b_1 + \cdots + b_s$.

Each such monomial can written as product of terms $x_i y_j$, usually not uniquely, by pairing each of the x_i occurring in the monomial with one of the y_j occurring. It follows that

$$R^G = K[x_i y_j : 1 \leq i \leq r, \, 1 \leq j \leq s].$$

Consider an $r \times s$ matrix of new indeterminates $Z = \bigl(z_{i,j}\bigr)$. There is a K-algebra surjection

$$K[Z] \twoheadrightarrow K[x_i y_j : 1 \leq i \leq r, \, 1 \leq j \leq s] = R^G$$

that sends $z_{i,j} \mapsto x_i y_j$ for all i and j. The ideal $I_2(Z)$ is easily checked to be in the kernel, so that we have a surjection $K[Z]/I_2(Z) \twoheadrightarrow R^G$. It is now easy to check that this map is injective, given the result of problem 6., 7. of Problem Set #3, Math 615, Winter 2016, namely, that $I_2(Z)$ is prime. We will give a different proof that this ideal is prime in a future lecture. Assuming this, let $\mathcal{F}$ be the fraction field of the domain $D = K[Z]/I_2(Z)$, and let $\overline{z}_{i,j}$ be the image of $z_{i,j}$. It is clear that $z_{1,1}$ has too small a degree to be in $I_2(Z)$, and so $\overline{z}_{1,1} \neq 0$. Since the 2×2 minors of the image $\overline{Z}$ of Z vanish, the matrix $\overline{Z}$ has rank 1 over $\mathcal{F}$. It follows that the i th row of $\overline{Z}$ is $\overline{z}_{i,1}/\overline{z}_{1,1}$ times the first row. Define a a K-algebra map $K[x_1, \ldots, x_r, \, y_1, \ldots, y_s] \to \mathcal{F}$ by $x_i \mapsto \overline{z}_{i,1}/\overline{z}_{1,1}$ for $1 \leq i \leq r$ and and $y_j \mapsto \overline{z}_{1,j}$ for $1 \leq j \leq s$. Then the restriction to R^G is a K-algebra map $R^G \to K[Z]/I_2(Z)$ that sends $x_i y_j \mapsto \overline{z}_{i,j}$ for all i, j and so is an inverse for ϕ. □

We can now conclude:

Theorem. *Let Z be an $r \times s$ matrix of indeterminates over any field K. Then $K[Z]/I_2(Z)$ is a Cohen-Macaulay domain.* □

We want to prove a somewhat more general result. Recall that a domain D is called *normal* or *integrally closed* if every element of its fraction field that is integral over D is in D.

Theorem. *Let $x_1, \ldots, x_n$ be indeterminates over the field K and let S be any finitely generated normal subring of $K[x_1, \, 1/x_1, \ldots, \, x_n, \, 1/x_n]$ generated by monomials. Then S is Cohen-Macaulay.*

Recall that if $\mathcal{M}$ is a semigroup under multiplication with identity 1, disjoint from the ring B, the semigroup ring $B\langle\mathcal{M}\rangle$ is the free B-module with basis $\mathcal{M}$ with multiplication defined so that if $b, \, b' \in B$ and $\mu, \, \mu' \in \mathcal{M}$ then $(b\mu)(b'\mu') = (bb')(\mu\mu')$. The general rule for multiplication is then forced by the distributive law. More precisely,

$$\sum_i b_i \mu_i \sum_j b'_j \mu'_j = \sum_\nu (\sum_{\mu_i \mu'_j = \nu} b_i b'_j) \nu$$

where μ, $\mu' \in \mathcal{M}$. It is understood that there are only finitely many nonzero terms in each summation on the left hand side, and this forces the same to be true in the summation on the right hand side.

We will prove the Theorem by showing that each such ring can be obtained from a monomial ring which has the Cohen-Macaulay property by virtue of our Theorem on rings of invariants of tori by adjoining variables and their inverses.

We shall therefore want to characterize the semigroups of exponent vectors in $\mathbb{N}^n$ corresponding to rings of invariants of tori. We already know that such a semigroup is the set of solutions of a finite system of homogeneous linear equations with integer coefficients (we could also say rational coefficients, since an equation can be replace by a nonzero integer multiple to clear denominators). That is, such a semigroup is the intersection of a vector subspace of $\mathbb{Q}^n$ with $\mathbb{N}^n$. It also follows that H is a such a semigroup if and only if it has the following two properties:

(1) If α, $\alpha' \in H$ and $\beta = \alpha - \alpha' \in \mathbb{N}^n$ then $\beta \in H$.

(2) If $\beta \in \mathbb{N}^n$ and $k\beta \in H$ for some integer $k > 0$, then $\beta \in H$.

If H is the intersection of a $\mathbb{Q}$-subspace of $\mathbb{Q}^n$ with $\mathbb{N}^n$, then it must be the intersection of the subspace it spans with $\mathbb{N}$. The abelian group that H spans is

$$H - H = \{\alpha - \alpha' : \alpha,\, \alpha' \in H\}.$$

Let $\mathbb{Q}^+ = \{u \in \mathbb{Q} : u > 0\}$. The vector space that H spans is then

$$\mathbb{Q}^+(H - H) = \{u\beta : u \in \mathbb{Q}^+,\, \beta \in H - H\}.$$

In fact, this vector space is also

$$\bigcup_{m=1}^{\infty} \frac{1}{m}\,(H - H)$$

where

$$\frac{1}{m}(H - H) = \{\frac{\beta}{m} : \beta \in H - H\}.$$

The fact that H is the intersection of a $\mathbb{Q}$-vector subspace of $\mathbb{Q}^n$ with $\mathbb{N}^n$ if and only if (1) and (2) hold follows at once.

Lecture of March 25

We continue the study of subrings of polynomial and Laurent polynomial rings generated by monomials. We do this by studying the vectors of exponents in $\mathbb{Z}^n$ (if there are n variables): the set of vectors is an additive subsemigroup of $\mathbb{Z}^n$. Such a semigroup H determines a subring of $S = K[x_1,\, 1/x_1,\, \ldots\, ,\, x_n,\, 1/x_n]$ for every field K, namely $K[x^H] = K[x_1^{a_1} \cdots x_n^{a_n} : (a_1,\, \ldots\, , a_n) \in H]$. It turns out that this ring is integrally closed in its fraction field (also called normal) if and only if H is *normal* in the sense defined below (the definition and theorem are given in the third and fourth paragraphs of the next page). Note that the condition for normality depends only on the semigroup H, and not on its embedding in $\mathbb{Z}^n$. The condition for normality of the algebra depends only on the semigroup, not on the field. Also note that the algebra one gets need not be Noetherian: see the Example at the top of the third page of the notes for this lecture.

The notion of a *full* subsemgroup of $\mathbb{N}^n$ is also introduced, in the middle of the third page of the notes for this lecture, following the example. Observe that in this case, negative exponents are not allowed. Moreover, whether $H \subseteq \mathbb{N}^n$ is full depends on the embedding in $\mathbb{N}^n$, not just on the semggroup H. The importance of this notion is that when H is full, the ring $K[x^H]$ is a direct summand, as a module over itself, of the polynomial ring $K[x_1,\, \ldots\, , x_n]$. Hence, for full semigroups, $K[x^H]$ is Cohen-Macaulay.

Another major result is that a finitely generated normal subsemigroup is isomorphic with the direct sum of a group $\mathbb{Z}^K$ and a full subsemigroup of some $\mathbb{Z}^s$. From this one sees that given a finitely generated normal subring R of the Laurent polynomials S or of the usual polynomial ring, R is Cohen-Macaulay! A key point in the proof of this is that if a subsemigroup of Z^n does not contain a nonzero element u and its inverse $-u$, then it is isomorphic with a full subsemgroup of some $\mathbb{N}^s$. The proof of this fact depends on studying convex geometry over the rational numbers $\mathbb{Q}$. I am designating this material optional.

We next want to consider when a K-subalgebra of $S = K[x_1,\, 1/x_1,\, \ldots\, ,\, x_n,\, 1/x_n]$ generated by monomials is normal. This is entirely a property of the semigroup of monomials involved, and does not depend on the base field.

We shall typically work with the additive semigroup of exponent vectors, which is a subsemigroup H of $\mathbb{Z}^n$. If $\alpha = (a_1,\, \ldots\, , a_n) \in \mathbb{Z}^n$, we write x^α for $x_1^{a_1} \cdots x_n^{a_n}$. Then the K-subalgebras of S generated by monomials correspond bijectively to the subsemigroups H of $\mathbb{Z}^n$: given H, the corresponding subalgebra is the K-span of $\{x^\alpha : \alpha \in H\}$.

If H is an additive (which we intend to imply commutative) f semigroup such that cancellation holds, i.e., if $\alpha, \alpha', \beta \in H$ and $\alpha + \beta = \alpha' + \beta$ then $\alpha = \alpha'$, then there is an essentially unique way to enlarge H to group that is generated by H. Define an equivalence relation on $H \times H$ by the rule $(\alpha,\, \beta) \sim (\alpha',\, \beta')$ precisely when $\alpha + \beta' = \alpha' + \beta$. The equivalence classes form a semigroup such that

$$[(\alpha_1, \beta_1) + [(\alpha_2, \beta_2)] = [(\alpha_1 + \alpha_2,\, \beta_1 + \beta_2)].$$

H embeds in this new semigroup by sending $\alpha \mapsto [(\alpha, 0)]$. The 0 element is represented by $(0, 0)$ and also by those elements of the form (α, α). There are now inverses since $[(\alpha, \beta)] + [(\beta, \alpha)] = [(\alpha + \beta, \alpha + \beta)] = [(0, 0)]$. In particular, $[(\beta, 0)]$ has additive inverse $[(0, \beta)]$. Thus, the new semigroup is a group, and if we identify $\alpha \in H$ with its image, then every element of this group has the form $\alpha - \beta$ for choices of α, $\beta \in H$. We denote this group $H - H$. If we have any other injection of H into a semigroup G that is a group, then the subgroup of G generated by H is isomorphic with $H - H$.

In particular, when H is a subsemigroup of $\mathbb{Z}^n$, the group $H - H$ depends only on H, not on its embedding in $\mathbb{Z}^n$.

We define $H \subseteq \mathbb{Z}^n$ to be *normal* if whenever α, $\alpha' \in H$ and there is a positive integer k such that $k(h - h') \in H$, then $h - h' \in H$.

Theorem. *For every field K, $R = K[x^\alpha : \alpha \in H]$ is normal if and only if H is normal.*

Proof. First suppose that the subalgebra R is normal, and that $k(\alpha - \alpha') \in H$, where k is a positive integer. Then x^α, $x^{\alpha'} \in R$, and $f = x^\alpha / x^{\alpha'} = x^{\alpha - \alpha'}$ is an element of the fraction field integral over R, since $f^k \in R$. Hence, $f \in R$, and so $\alpha - \alpha' \in H$.

We next show that the condition that H be normal is sufficient for R to be normal. Suppose that we can solve the problem when K is an infinite field, e.g., an algebraically closed field. If K is finite, let L be an infinite field containing K. Then

$$R = K[x_1, 1/x_1, \dots, x_n, 1/x_n] \cap L[x^\alpha : \alpha \in H],$$

and since both the rings being intersected are normal, R is normal as well.

Therefore we may assume that K is infinite. The group of invertible diagonal matrices $\mathcal{D}_n$ acts on S, and R is stable. One can then show thiat that the integral closure of R will be spanned by monomials. Consider the ring obtained by adjoining the inverses of all monomials in R. This ring R_1 corresponds to $H - H$, which is isomorphic with a free abelian group $\mathbb{Z}^h$, and so R_1 is isomorphic with a localized polynomial ring obtained by adjoining h algebraically independent elements and their inverses to K. Thus, R_1 is normal, and so any monomial in the normalization of R is in R_1.

It follows that if R is not normal, then there is a monomial $\mu = x^\alpha / x^{\alpha'}$, where $\alpha, \alpha' \in H$, that is integral over R and not in R. Choose a monic polynomial $F(Z)$ with coefficients in R of degree k satisfied by μ. Assign Z the same monomial degree as μ. Then the sum of the terms whose monomial degree is μ^k must also vanish when we substitute $Z = \mu$, and so we have an equation of integral dependence that is monomially graded. Since R is a domain, there is no loss of generality in assuming that the constant term is nonzero: if necessary, we may factor out a power of Z. We continue to call the degree k. Then μ^k has the same monomial degree ν as the constant term $c\nu$, where $c \in K - \{0\}$, and ν is a monomial in R. This shows that $k(\alpha - \alpha') \in H$, and so $\alpha - \alpha' \in H$ and $\mu \in R$ after all. □

Example. Let K be any field, let $\lambda \geq 0$ be a real number, and let

$$H_\lambda = \{(a,\, b) \in \mathbb{N}^2 : a/b > \lambda\}.$$

It is easy to see that if $0 \leq \lambda < \lambda'$ then H_λ is strictly larger than $H_{\lambda'}$. Morever, every H_λ is a normal semigroup. Let $R_\lambda = K[x^\alpha : \alpha \in H_\lambda]$. This gives an uncountable chain $\{R_\lambda\}_{\lambda \geq 0}$ of normal subrings of $K[x_1,\, x_2]$. None of the rings R_λ is Noetherian: if R_λ were Noetherian, the fact that it is $\mathbb{N}$-graded over K would imply that it is finitely generated by elements

$$x_1^{a_1} x_2^{b_1},\, \ldots\,,\, x_1^{a_n} x_2^{b_n}$$

with every $a_j/b_j > \lambda$. Let $s > \lambda$ be the minimum of the rational numbers $a_1/b_1,\, \ldots\,,\, a_n/b_n$. Then

$$K[x_1^{a_1} x_2^{b_1},\, \ldots\,,\, x_1^{a_n} x_2^{b_n}]$$

does not contain any monomial $x^a y^b$ with $a/b < s$, and so cannot be equal to R_λ. □

The Example above shows that the condition of being normal is too weak to imply that a semigroup is finitely generated. We next want to consider a much stronger condition on subsemigroups of $\mathbb{N}^n$ which implies *both* normality and finite generation.

We say that a subsemigroup $H \subseteq \mathbb{N}^n$ is *full* if whenever $\alpha, \alpha' \in H$ and $\alpha - \alpha' \in \mathbb{N}^n$ then $\alpha - \alpha' \in \mathbb{N}$. We observed at the end of the previous lecture that the subsemigroups obtained from rings of invariants of torus actions on polynomial rings are full.

It is obvious that full subsemigroups are normal, for if $k(\alpha - \alpha') \in H$, then $k(\alpha - \alpha') \in \mathbb{N}^n$, and since $k > 0$, this implies that $\alpha - \alpha' \in H$. Something much stronger is true.

Theorem. *Let H be a full subsemigroup of $\mathbb{N}^n$. Let $R = K[x^\alpha : \alpha \in H]$, where K is any field. Then $R \hookrightarrow K[x_1,\, \ldots\,, x_n]$ is split. Hence:*

(a) *R is a finitely generated K-algebra, and so H is a finitely generated semigroup.*

(b) *R is Cohen-Macaulay.*

Proof. Let W be the K-span of the monomials x^β for $\beta \in \mathbb{N}^n - H$. Evidently, $K[x_1,\, \ldots\,, x_n] = R \oplus W$ as K-vector spaces. To complete the proof that we have a splitting, it suffices to show that W is an R-module. This comes down to the assertion that if $\alpha' \in H$, so that $x^{\alpha'} \in R$, and $\beta \in \mathbb{N}^n - H$, so that $x^\beta \in W$, then $x^{\alpha'} x^\beta \in W$. Suppose not. Then $x^{\alpha' + \beta} = x^\alpha$, where $\alpha \in H$. But thihs means that $\beta = \alpha - \alpha' \in \mathbb{N}^n$. By the definition of full subsemigroup, $\beta \in H$, a contradiction.

The first statement in part (a) follows from the Lemma at the top of p. 2 of the Lecture Notes of March 11, and the second statement in part (a) is an Immediate consequence. Part (b) the follows from the Theorem at the top of p. 4 of the Lecture Notes of March 11. □

We shall complete the proof that finitely generated normal K-subalgebras of S are Cohen-Macaulay by proving the following

Theorem. *Let H be a finitely generated normal subsemigroup of $\mathbb{Z}^n$. Then $H \cong \mathbb{Z}^k \oplus H'$, where H' is isomorphic to a full subsemigroup of $\mathbb{N}^n$.*

It will then follow that $K[x^\alpha : \alpha \in H]$ is the polynomial ring in k variables with the inverses of the variables adjoined over $K[x^\alpha : \alpha \in H']$. Thus, the remaining work is in the proof of the Theorem just above, most of which we postpone for a bit. However, we can immediately give the part of the argument in which we split off $\mathbb{Z}^k$.

First part of the proof of the Theorem. First, replace $\mathbb{Z}^n$ by $H - H \subseteq \mathbb{Z}^n$. Since a subgroup of $\mathbb{Z}^n$ will also be a finitely generated free abelian group, we may assume that $H - H = \mathbb{Z}^n$ (the property of being a normal semigroup is not affected). Let G be the set of all elements of H with additive inverses in H. Then G contains 0 and is closed under addition. It follows that G is a subgroup of $\mathbb{Z}^n$, and so $G \cong \mathbb{Z}^k$ for some $k \in \mathbb{N}$. We next claim that $\mathbb{Z}^n/G$ is torsion-free. Suppose $\beta \in \mathbb{Z}^n = H - H$ and $k\beta \in G$. Then $k(-\beta) \in G$ as well, and both β and $-\beta$ are in $\mathbb{Z}^n = H - H$. It follows that β and $-\beta$ are both in H, and so $\beta \in G$, as required.

Thus, $\mathbb{Z}^n/G$ is a finitely generated torsion-free abelian group, and it follows that it is free. Thus,

$$0 \to G \to \mathbb{Z}^n \to \mathbb{Z}^n/G \to 0$$

splits. Let $G' \cong \mathbb{Z}^h \cong \mathbb{Z}^n/G$ be a free complement for G in H. Every element $\beta \in H$ can be expressed uniquely as $\alpha + \alpha'$ where $\alpha \in G$ and $\alpha' \in G'$. But $-\alpha \in H$, and so $\alpha' \in H$. Thus, $H = G \oplus H'$, where $H' = H \cap G'$, and may also be viewed as the image of H under the projection $\mathbb{Z}^n = G \oplus G' \cong G \times G' \twoheadrightarrow G'$. It follows that H' is a finitely generated subsemigroup of G'. Evidently, H' does not contain the additive inverse of any of its nonzero elements, since $G \cap H' = 0$. Moreover, H' is normal: if $\beta \in H - H'$ and $\kappa\beta \in H'$, then $\beta \in H$, and may be written uniquely as $\alpha + \alpha'$ with $\alpha \in G$ and $\alpha' \in H'$. Then $k\alpha + k\alpha' \in H'$, and so $k\alpha = 0$. It follows that $\alpha = 0$, and $\beta = \alpha' \in H'$, as required. The proof of the Theorem above therefore reduces to establishing the following

Lemma. *Let H be a finitely generated normal subsemigroup of $\mathbb{Z}^n$ such that there is no nonzero element with an additive inverse in H. Then H is isomorphic with a full subsemigroup of $\mathbb{N}^s$ for some nonnegative integer s.*

The proof of this Lemma will be carried through by studying a class of semigroups in $\mathbb{Q}^n$ that are closed under multiplication by elements of $\mathbb{Q}^+$, the positive rational numbers. What we need is an understanding of convex geometry over $\mathbb{Q}$.

Optional material

Geometry in vector spaces over the rational numbers

The results in this section are proved over $\mathbb{Q}$: the statements and proofs are valid with no changes whatsoever if $\mathbb{Q}$ is replaced by any field between $\mathbb{Q}$ and $\mathbb{R}$, including $\mathbb{R}$, or any ordered field. The results are, in fact, more "standard" over $\mathbb{R}$.

Let V be a vector space over $\mathbb{Q}$. By a $\mathbb{Q}^+$*-subsemigroup* C of V we mean a subsemigroup that is closed under multiplication by elements of $\mathbb{Q}^+$. (It would also be natural to refer to C as a *convex cone*: it will be closed under taking all linear combinations with nonnegative coefficients, and will be a union of "rays" emanating from the origin.) Henceforth, V will be assumed finite-dimensional. We say that C is *finitely generated over* $\mathbb{Q}^+$ if it has finitely many elements $\alpha_1, \ldots, \alpha_h$ such that every element of C is a $\mathbb{Q}^+$-linear combination of the elements $\alpha_1, \ldots, \alpha_h$. We write V^* for the $\mathbb{Q}$-vector space $\mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$, which is finite-dimensional of the same dimension as V. Its elements will be called *linear functionals* on V.

If L is a nonzero linear functional on V, the set $\{\alpha \in V : L(\alpha) \geq 0\}$ is called a *half-space.* The set $\{\alpha \in V : L(\alpha) \leq 0\}$ is also a half-space, since we may replace L by $-L$. We can always choose a basis for V consisting of $n-1$ vectors $e_1, \ldots, e_{n-1}$ in the kernel of V and a vector e_n on which L has the value 1. If we identify V with $\mathbb{Q}^n$ using this basis, the half-space determined by L is is identified with $\{(q_1, \ldots, q_n) \in \mathbb{Q}^n : q_n \geq 0\}$: we refer to this as the *standard example* of a half-space. A half-space is a $\mathbb{Q}^+$-subsemigroup that is finitely generated: it suffices to see this for the standard example. Then generators are the vectors $e_1, \ldots, e_{n-1}, -e_1, \ldots, -e_{n-1}$, and e_n.

We shall say that a $\mathbb{Q}^+$-subsemigroup C *has no line* or is a $\mathbb{Q}^+$-subsemigroup *with no line* if there is no nonzero vector in C whose additive inverse is in C: it is equivalent that C does not contain a one-dimensional vector subspace of the ambient space.

If C is a finitely generated $\mathbb{Q}^+$-subsemigroup we may take any set of generators, and choose a minimal subset with the property of generating C over $\mathbb{Q}^+$. We shall call these elements *a minimal set of generators of* C.

Lemma. *Let V be a finite-dimensional $\mathbb{Q}$-vector space.*

(a) *Every finite intersection of half-spaces in V is a finitely generated $\mathbb{Q}^+$-subsemigroup.*

(b) *Let C be be any $\mathbb{Q}^+$-subsemigroup in V. Let W be the subset of C consisting of elements with an additive inverse in C. Then W is a vector subspace of V, and if W' is a vector space complement for W in V, then $C = W \oplus C'$, where $C' = C \cap W'$ is also the projection of C on W'. C' is a finitely generated $\mathbb{Q}^+$-subsemigroup with no line.*

(c) *If C is a $\mathbb{Q}^+$-subsemigroup with no line, $\alpha_1, \ldots, \alpha_h \in C$, $c_1, \ldots, c_h \in \mathbb{Q}^+$, and $c_1\alpha_1 + \cdots + c_h\alpha_h = 0$, then $\alpha_1 = \cdots = \alpha_h = 0$.*

(d) *Let C be a finitely generated $\mathbb{Q}^+$-subsemigroup with no line and let α, β be part of a minimal set of generators for C. Then $C_1 = C + \mathbb{Q}\alpha$, which is the $\mathbb{Q}^+$-subsemigroup generated by C and $-\alpha$, does not contain $-\beta$.*

Proof. For part (a) we use induction on the number of half-spaces. We have already proved the result in the discussion above if there is just one half-space. Thus, we may assume that the intersection of all but one of the half-spaces is a finitely generated $\mathbb{Q}^+$-subsemigroup C, and it suffices to show that the intersection of C with remaining half-space is finitely generated. After a change of basis, we may assume that the last half-space D is the standard example. Let $\alpha_1, \ldots, \alpha_h$ generate C, and let c_j be the last coordinate of α_j, $1 \le j \le h$. We may multiply each α_j by $1/|c_j|$ if $c_j \ne 0$ and so assume that every nonzero c_j is 1 or -1. Then

$$C \cap D = \{q_1\alpha_1 + \cdots + q_h\alpha_h : q_j \in \mathbb{Q}_j^+ \text{ for all } j \text{ and } \sum_{j=1}^{h} q_j c_j \ge 0\}.$$

It therefore suffices to show that

$$E = \{(q_1, \ldots, q_h) \in (\mathbb{Q}^+)^h : \sum_{j=1}^{h} q_j c_j \ge 0\}$$

is finitely generated as a $\mathbb{Q}^+$-subsemigroup, because we have a surjective map $E \twoheadrightarrow C \cap D$ sending

$$(q_1, \ldots, q_h) \mapsto q_1\alpha_1 + \cdots + q_h\alpha_h.$$

This map will carry a finite set of generators for E to a finite set of generators for $C \cap D$. We may assume that coordinates have been permuted so that we have $c_1 = \cdots = c_a = 1$, $c_{a+1} = \cdots = c_{a+b} = -1$, and the remaining c_j are 0. It is easy to verify that the e_i for $1 \le i \le a$, the $e_i + e_j$ for $1 \le i \le a$ and $a+1 \le j \le b$, and the e_k for $a+b+1 \le k \le h$ generate E over $\mathbb{Q}^+$.

Part (b) is entirely similar to the construction of the splitting $H = G \oplus H'$ except that it is much simpler in the present context, and the proof is left as an exercise.

For part (c), if some c_j is not 0, say c_h, then

$$-\alpha_h = \frac{c_1}{c_h}\alpha_1 + \cdots + \frac{c_{h-1}}{c_h}\alpha_{h-1},$$

contradicting the assumption that C has no line.

Finally, for part (d), suppose

$$-\beta = \eta - c\alpha,$$

where we may assume $c > 0$ or else $-\beta \in H$. The element η can be written as a nonnegative linear combination of α, β, and the other minimal generators, say

$$\eta = q\alpha + r\beta + \eta',$$

where η' does not involve α or β. Then

$$-\beta = q\alpha + r\beta + \eta' - c\alpha,$$

and so

$$(q-c)\alpha + (r+1)\beta + \eta' = 0.$$

If $q \geq c$ this contradicts part (c). If $q < c$, then

$$\alpha = \frac{r+1}{c-q}\beta + \frac{1}{c-q}\eta',$$

which means that α is not needed as a generator, a contradiction. □

Proposition. *Let V be a finite-dimensional vector space over $\mathbb{Q}$ and let $C \subseteq V$ be a finitely generated $\mathbb{Q}^+$-subsemigroup. If C is proper, then C is contained in a half-space, i.e., there is a nonzero linear functional that is nonnegative on C. If $\alpha \in C$ and $-\alpha \notin C$ then one can choose L nonnegative on C so that $L(\alpha) > 0$. If C contains no line, one can choose L so that it is positive on all nonzero elements of C.*

Proof. We use induction on $\dim_{\mathbb{Q}}(V)$, and assume that all of the statements are true for vector spaces of smaller dimension. We may replace V by $C - C$, and so assume that C spans V. If $\dim(V) = 1$ then C is either $\{0\}$, a half-line, or all of V, and the result is trivial.

In general, we have a decomposition $C = W + C'$ where W is a vector space as in part (b) of the Lemma, and $C' \subseteq W'$, a complement for W. If $W \neq 0$ then all of the statements can now be deduced from the induction hypothesis applied to $C' \subseteq W'$: one extends the functional on W' by letting it be 0 on W. Note that if $\alpha \in C$ and $-\alpha \notin C$ then $\alpha = \beta + \alpha'$ where $\beta \in W$ and $\alpha' \in C' - \{0\}$, and has no additive inverse in C'.

This means that we can assume without loss of generality that C has no line, and we may choose minimal generators $\alpha_1, \ldots, \alpha_h$. We must have $h \geq 2$, or else $\dim_{\mathbb{Q}}(V) \leq 1$, since C spans V. It will suffice to construct a linear functional L_i that is positive on α_i and nonnegative on C for every i. The sum of these linear functionals will be positive on all of $C - \{0\}$, since every element is nonnegative linear combination of the α_i. Thus, it suffices to construct such a functional that is nonnegative on, say, α_1. Let $\alpha = \alpha_2$ and $\beta = \alpha_1$. We apply part (d) of the Lemma above, and replace C by $C_1 = C + \mathbb{Q}\alpha$. Then β does not have an inverse, but C_1 contains a line, and so we can construct a linear functional nonnegative on C_1 and positive on $\beta = \alpha_1$ by reducing to a lower-dimensional case, as in the preceding paragraph. □

Theorem. *Let V be a finite-dimensional vector space over $\mathbb{Q}$. Then $C \subseteq V$ is a finitely generated $\mathbb{Q}^+$-subsemigroup if and only if C is a finite-intersection of half-spaces.*

Proof. The "if" part is part (a) of the Lemma. It remains to see that every $\mathbb{Q}^+$-subsemigroup is a finite intersection of half-spaces. Let $\alpha_1, \ldots, \alpha_h$ be a finite set of generators. The set of linear functionals nonnegative on α_i is a half-space H_i in the dual vector space V^*, and so the intersection of the H_i is a finitely generated $\mathbb{Q}^+$-subsemigroup in V^*. Let $L_1, \ldots, L_s$ be generators. It suffices to show that C is the intersection of the half-spaces determined by the L_j. Let β be any vector not in C. It will suffice to show that there exists a linear functional that is nonnegative on C and negative on β, for this functional is a nonnegative linear combination of the L_j, and so at least one of the L_j will have the same property. Consider

$$C_1 = C + \mathbb{Q}^+(-\beta),$$

the $\mathbb{Q}^+$-subsemigroup generated by C and $-\beta$. If $\beta \in C_1$ we have

$$\beta = \alpha - c\beta$$

with $\alpha \in C$ and $c > 0$ and then

$$\beta = \frac{1}{1+c}\alpha \in C,$$

a contradiction. Since $\beta \notin C_1$, by the Proposition above there is a linear functional that is positive on $-\beta$ and nonnegative on C_1, and this has the required property. □

Lecture of March 27

In the first part of this lecture we use the optional results on convexity over the rational numbers from the previous lecture to finish the proof of a missing Lemma, and with that we will have completed the proof that normal rings generated by monomials are Cohen-Macaulay.

We then begin our introduction to tight closure theory. In fact, the basic idea of tight closure is in the proof of our theorem on colon-capturing in positive characteristic.

In this paragraph, all rings are Noetherian, of prime characteristic $p > 0$. For simplicity, think of the case where R is a domain, and consider an ideal I. Suppose that $u \in R$. The idea is that if there is a fixed nonzero element $c \in R$ such that $cu^{p^e} \in I^{[p^e]}$ for all $e \gg 0$ (where $I^{[p^e]} = (f^{p^e} : f \in I)R)$ then u is "almost" in I in some sense. It turns out that when R is regular, this condition implies that u *is* in I. When R is not regular, this condition becomes a definition: u is said to be in the *tight closure* of I. The word "tight" is used because this closure is a "tight fit" for the ideal, i.e., it is small compared to other closures. We will extend this notion to a closure operation on submodules of finitely generated modules.

It turns out that many rings besides regular rings have the property that every ideal is tightly closed. For example, the rings of the form $K[X]/I_t(X)$, where X is a matrix of indeterminates and $I_t(X)$ is the ideal generated by the $t \times t$ minors of X have this property. The same is true for the ring generated by the $r \times r$ minors of an $r \times s$ matrix of indeterminates, where $1 \leq r \leq s$, and for normal subrings of the Laurent polynomials over a field that are generated by finitely many monomials. A number of theorems that hold for regular rings hold much more generally if one changes the conclusion, for example, so that instead of saying that an element satisfying certain condition is in an ideal, one says instead that it is in the tight closure of the ideal.

Rings in which every ideal is tightly closed are called *weakly* F-*regular*. If the same condition holds for all localizations, the ring is called F-*regular*. Major results include the fact that weakly F-regular rings are both Cohen-Macaulay and normal.

We shall also indicate how the theory may be extended to Noetherian rings containing a field of characteristic 0.

We now return to the final step in the proof of the Cohen-Macaulay property for normal rings generated by monomials.

In the previous lecture we established the results that we need about convex geometry over the rational numbers, and we are now ready to prove the Lemma on p. 150 of the

Lecture Notes of March 25, which will also complete the proof that normal subrings of $K[x_1, 1/x_1, \ldots, x_n, 1/x_n]$ generated by finitely many monomials are Cohen-Macaulay.

Proof of the Lemma on embedding normal subsemigroups as full subsemigroups of $\mathbb{N}^s$*.* Let $H \subseteq \mathbb{Z}^n$ be a finitely generated normal subsemigroup that does not contain the additive inverse of any of its nonzero elements. We want to show that H can be embedded as a full subsemigroup in $\mathbb{N}^s$ for some s. First note that $H - H$ is a free abelian group, and so we may replace $\mathbb{Z}^n$ by $H - H$. Henceforth, we assume that $H - H = \mathbb{Z}^n$. This does not affect the condition that H be normal. Second, let $C = \mathbb{Q}^+H$ be the $\mathbb{Q}^+$-subsemigroup generated by H. It is generated over $\mathbb{Q}^+$ by the generators of H, and so is finitely generated as a $\mathbb{Q}^+$-subsemigroup of $\mathbb{Q}^n$. It contains no line, for if we had β and $-\beta$ both in $\mathbb{Q}^+H$, we could choose a positive integer N such that $N\alpha, -N\alpha \in H$, a contradiction.

Let $\alpha_1, \ldots, \alpha_h$ be nonzero generators of H, and, hence, of C. Let $V = \mathbb{Q}^n$ and $V^* = \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$. Let $C' \subseteq V^*$ be the set of all linear functionals in V^* that are nonnegative on C. Since all elements of C are nonnegative rational linear combinations of $\alpha_1, \ldots, \alpha_h$,

$$C' = G_1 \cap \cdots \cap G_h,$$

where

$$G_j = \{L \in V^* : L(\alpha_j) \geq 0\}$$

for $1 \leq j \leq h$. We may think of α_j as an element of $(V^*)^* \cong V$. Then every G_j is a half-space in V^*, and so C' is a fintely generated $\mathbb{Q}^+$-subsemigroup in V^*. Choose $L_1, \ldots, L_s \in V^*$ that generate C' over $\mathbb{Q}^+$. Each $L_i(\alpha_j)$ is nonnegative rational number. We may therefore replace L_i by a multiple by a suitable positive integer, and so assume that for all i, j, the value of $L_i(\alpha_j)$ is in $\mathbb{N}$. Since every element of H is a linear combination of the α_j with coefficients in $\mathbb{N}$, it follows that all values of every L_i on H are in $\mathbb{N}$. We therefore have a map

$$\Phi = (L_1, \ldots, L_s) : H \to \mathbb{N}^s$$

where

$$\alpha \mapsto \bigl(L_1(\alpha), \ldots, L_s(\alpha)\bigr).$$

To complete the proof, we shall show that this map is one-to-one and that its image in $\mathbb{N}^s$ is a full subsemigroup of $\mathbb{N}^s$. First, suppose that $\alpha, \beta \in H$ are distinct. Then $\alpha - \beta$ is nonzero, and so either $\alpha - \beta \notin H$ or $\beta - \alpha \notin H$. Suppose, say, that $\alpha - \beta \notin H$. The $\alpha - \beta \notin C$ as well: otherwise, $k(\alpha - \beta) \in H$ for some integer $k > 0$, and, since H is normal, we then have $\alpha - \beta \in H$, a contradiction. Hence, there is a linear functional nonnegative on C and negaqtive on $\alpha - \beta$. This linear functional is in C' and so is a nonnegative rational linear combination of the L_i. It follows that some L_i is negative on $\alpha - \beta$. But then $L_i(\alpha) \neq L_i(\beta)$. Thus, Φ is injective.

Finally, we need to show that the image of H under Φ is a full subsemigroup of $\mathbb{N}^s$. Suppose that $\Phi(\alpha) - \Phi(\alpha') \in \mathbb{N}^s$. We want to show that $\alpha - \alpha' \in H$. But $\Phi(\alpha - \alpha') \in \mathbb{N}^s$, and so $L_i(\alpha - \alpha') \geq 0$ for al i. If $\alpha - \alpha' \notin C$, we know that there is a linear functional L that is nonnegative on C and negative on $\alpha - \alpha'$. But then $L \in C'$, and this is impossible because every L_i is nonnegative on $\alpha - \alpha'$. Thus, $\alpha - \alpha' \in C$. But then for some positive integer k, we have that $k(\alpha - \alpha') \in H$, and so $\alpha - \alpha' \in H$, since H is normal. □

Tight closure

We have shown in a graded instance that a direct summand of a polynomial ring is Cohen-Macaulay, and we have applied that result to show that finitely generated integrally closed rings generated by monomials are also Cohen-Macaulay.

The idea of the proof can be used to establish the result in much greater generality. In fact, it is known that if R is a Noetherian regular ring containing a field and $A \subseteq R$ is a direct summand of R as A-modules, then A is Cohen-Macaulay. Recently, perfectoid methods have been used to extend this result to the case where R is a regular ring that does not necessarily contain a field, like a polynomial or formal power series ring in finitely many variables over $\mathbb{Z}$ or over a Noetherian discrete valuation domain, e.g., over the p-adic integers. But the perfectoid proof rests on positive characteristic results.

The tool that one needs to establish this result in characteristic $p > 0$ is called *tight closure theory.* A similar theory, defined by reduction to positive characteristic, exists for Noetherian rings containing the rationals. Whether there exists a comparable theory for rings that need not contain a field is a very important open question, and new ideas from perfectoid geometry may provide a solution.

We are going to develop part of the theory in positive characteristic, and explain how the theory is extended to rings that contain $\mathbb{Q}$ without giving full details. We shall also explain why having such a theory would solve many open problems in mixed characteristic.

We begin by defining tight closure for ideals in Noetherian rings of positive prime characteristic p, and discussing some of its good properties. The notion was introduced implicitly in the Theorem on colon-capturing, which is the second Theorem on p. 126 of the Lecture Notes of March 11, but the explicit definition was not made at that point.

Definition: tight closure. Let R be a Noetherian ring of prime characteristic $p > 0$, let I be an ideal of R, and let $f \in R$. We say that f is in the *tight closure* of I if there exists an element $c \in R$, not in any minimal prime of R, such that for all $e \gg 0$, $cf^{p^e} \in I^{[p^e]}$. The set of elements in the tight closure of I is called the *tight closure* of I, and is denoted I^*.

In the earlier Theorem on colon-capturing, R was a domain. Notice that when R is a domain, the condition that c not be in any minimal prime of R is simply the condition that c not be 0. We note some elementary properties of the tight closure operation. Until further notice, R is a Noetherian ring of prime characteristic $p > 0$.

(1) *I^* is an ideal of R, and $I \subseteq I^*$. If $I \subseteq J \subseteq R$ are ideals, then $I^* \subseteq J^*$.*

As we did earlier in this context, we use q to stand for p^e. If $cf^q \in I^{[q]}$ for all $q \gg 0$, then $c(rf)^q \in I^{[q]}$ for all $q \gg 0$. If also $c'g^q \in I^{[q]}$ for all $q \gg 0$, then $(cc')(f+g)^q =$

$c'cf^q + cc'g^q \in I^{[q]}$ for all $q \gg 0$. If $f \in I$ then $1 \cdot f^q \in I^{[q]}$ for all q, which shows that $I \subseteq I^*$. The fact that $I \subseteq J \Rightarrow I^* \subseteq J^*$ is obvious from the definition. $\square$

We shall use the notation R° for the set of elements of R not in any minimal prime of R. The element c used in checking whether a given element of $u \in R$ is in I^* is allowed to depend on u. However, there is a single element $c \in R^\circ$ that can be used for all elements of I^*: that is, if $u \in I^*$, then $cu^q \in I^{[q]}$ for all $q \gg 0$. The point is that I^* is finitely generated: suppose that $u_1, \ldots, u_h$ are generators. Let $c_j \in R^\circ$ be such that $c_j u_j^q \in I^{[q]}$ for all $q \gg 0$, $1 \leq j \leq h$. Let $c = c_1 \cdots c_h$. Then since every $u \in I^*$ is an R-linear combination of $u_1, \ldots, u_h$, we have that $cu^q \in I^{[q]}$ for all $q \gg 0$. This implies that $c(I^*)^{[q]} \subseteq I^{[q]}$ for all $q \gg 0$.

One can use this to see that $(I^*)^* = I^*$. For suppose that u is such that $c'u^q \in (I^*)^{[q]}$ for all $q \gg 0$. Then $(cc')u^q = c(c'u^q) \in c(I^*)^{[q]} \subseteq I^{[q]}$ for all $q \gg 0$, and so $u \in I^*$. We state this formally:

(2) *If I is any ideal of R, $(I^*)^* = I^*$.*

We note that if R is a domain or if I is not contained in any minimal prime of R, then $u \in I^*$ iff there exists $c \in R^\circ$ such that $cu^q \in I^{[q]}$ for all q. In the second case we can choose $c' \in I - R^\circ$. If $cu^q \in I^{[q]}$ for $q \geq q_0$, we can replace c by $c(c')^{q_0}$. In the domain case we can use this idea unless $I = (0)$. But then $I^* = (0)$, and we automatically have that $cu^q \in I^{[q]}$ for all q when $u \in I^*$, since $u = 0$.

We also note:

(3) *If $R \subseteq S$ are domains, and $I \subseteq R$ is an ideal, $I^* \subseteq (IS)^*$, where I^* is taken in R and $(IS)^*$ in S.*

This is immediate from the definition of tight closure, since nonzero elements of R map to nonzero elements of S and $I^{[q]} \subseteq (IS)^{[q]} = I^{[q]}S$. More generally, this holds when $R \to S$ is a homomorphism such that R° maps into S°. In fact, under mild conditions on the rings, for any map $R \to S$ (it need not be injective) the tight closure of every ideal $I \subseteq R$ maps into the tight closure of IS in S, but the proofs are difficult.

Note that Theorem on colon-capturing from p. 4 of the Lecture Notes of March 11 can now be re-stated as follows:

Theorem (colon-capturing). *Let A be an $\mathbb{N}$-graded domain finitely generated over a field K of prime characteristic $p > 0$. Let $F_1, \ldots, F_d$ be a homogeneous system of parameters for A. Then for $0 \leq i \leq d-1$, $(F_1, \ldots, F_i)A :_A F_{i+1} \subseteq (F_1, \ldots, F_i)^*$.* $\square$

We shall see that there is a local version of this result. Mild conditions on the local ring are needed: for the reader is familiar with the notion of "excellent" local ring, we note that being excellent suffices. It is also sufficient if the ring is a homomorphic image of a regular local ring or even of a Cohen-Macaulay local ring. Since we shall show that every complete local ring is a homomorphic image of a regular local ring, the result is valid in the complete case.

(4) *If A is a local domain of characteristic $p > 0$ that is a homomorphic image of a Cohen-Macaulay ring and $f_1, \dots, f_d$ is a system of parameters for A, then for $1 \leq i \leq d-1$, $(f_1, \dots, f_i)A :_A f_{i+1} \subseteq \bigl((f_1, \dots, f_i)A\bigr)^*$.*

The proof is postponed.

We next note that the second theorem on p. 131 of the Lecture Notes of March 16–18 may now be stated as follows:

Lemma. *Every ideal of the polynomial ring $K[x_1, \dots, x_n]$ over a field K of prime characteristic $p > 0$ is tightly closed.* □

We shall eventually show the following:

(5) *If R is a regular Noetherian ring of characteristic $p > 0$, then every ideal of R is tightly closed.*

The key point in the proof is that the Frobenius endomorphism is flat for all regular rings of characteristic $p > 0$. We shall prove this making use of the structure theory of complete local rings.

We note that given a theory of tight closure satisfying conditions (1) — (5), one immediately gets the following:

Theorem. *Let R be a regular ring of characteristic $p > 0$ and let $A \subseteq R$ be a subring such that A is a direct summand of R as A-modules. Then A is Cohen-Macaulay.*

Sketch of proof, assuming (1) — (5). The issue is local on A. Assume that (A, m) is local. One may replace A by its completion and R by its completion at mR. Thus, we may assume that the Theorem on colon-capturing holds for A, i.e., that (4) holds. Let $f_1, \dots, f_d$ be a system of parameters for A. Suppose $uf_{i+1} \in (f_1, \dots, f_i)A$. Then $u \in \bigl((f_1, \dots, f_i)A\bigr)^*$ by (4). By (3), we have that $u \in \bigl((f_1, \dots, f_i)R\bigr)^*$. By (5), we have that $u \in (f_1, \dots, f_i)R \cap A$. Since A is a direct summand of R, it follows that $u \in (f_1, \dots, f_i)A$. Thus, $f_1, \dots, f_d$ is a regular sequence in A, and A is Cohen-Macaulay. □

Thus, the development of a sufficiently good tight closure theory in characteristic $p > 0$ yields a proof that direct summands of regular rings are Cohen-Macaulay.

There is also a theory of tight closure for Noetherian rings containing $\mathbb{Q}$ that has properties (1) — (5). It is defined in a convoluted way using reduction to positive characteristic p. In consequence, it is known that direct summands of regular rings are Cohen-Macaulay in equal characteristic 0. This was an open question for a long time if the ring does not contain a field, but has recently been settled using perfectoid methods.

We shall also see that the existence of a good tight closure theory has many other applications.

Lecture of March 30

In this lecture we extend the theory of tight closure to submodules of finitely generated modules. We then indicate how to extend the theory to rings that contain a field of characteristic 0.

The way the theory is set up for modules, suppose R, which has prime characteristic $p > 0$, is the ring and $N \subseteq M$ are finitely generated R-modules. Let $u \in M$. Let G be a finitely generated free module that maps on M, let H be the inverse image of N in G and let $v \in G$ map to u under $G \twoheadrightarrow M$. Let $\overline{u}$ be the image of u in M/N. It will turn out that u is in the tight closure of N in M if and only if $\overline{u}$ is in the tight closure of 0 in M/N, and also if and only if v is in the tight closure of H in G. Thus, it suffices to give the definition of when an element is in the tight closure for a free module $G \cong R^h$. The definition is the same as for ideals if we define w^q, when $w = (f_1, \ldots, f_h)$, to be $(f_1^q, \ldots, f_h^q)$ and let $H^{[q]}$ denote the R-span of $\{w^q : w \in H\}$. Then $v \in H^*$ in G if and only if there exists c not in any minimal prime of R such that for all $a = p^e \gg 0$, $cv^q \in H^{[q]}$. The case of ideals is simply the case where $h = 1$.

The definition of tight closure when the ring is a finitely generated $\mathbb{Q}$-algebra is given by replacing $\mathbb{Q}$ by a localization of $\mathbb{Z}$ at one integer, and then considering what happens module prime integers.

Tight closure for modules

We want to extend tight closure theory to modules. Suppose we are given $N \subseteq M$, finitely generated modules over a Noetherian ring R of prime characteristic $p > 0$. We can define v^{p^e} for $v \in R^h$ as follows: if $v = (f_1, \ldots, f_h)$, then $v^{p^e} = (f_1^{p^e}, \ldots, f_h^{p^e})$. If $G \subseteq R^h$ we define G^{p^e} as the R-span of all the elements $\{v^{p^e} : v \in G\}$. One gets the same module if one takes only the R-span of the p^e th powers of generators of G. This agrees with our definition of $I^{[p^e]}$ when $I \subseteq R$ is an ideal. If $G \subseteq R^h$, we define $G^*_{R^h}$, the *tight closure* of G in R^h as the set of elements $v \in R^h$ such that for some $c \in R^\circ$, $cv^q \in G^{[q]}$ for all $q \gg 0$, where q is p^e.

Given $N \subseteq M$ where M is finitely generated over R, we define the *tight closure* N^*_M of N in M as follows. Map a free module $R^h \twoheadrightarrow M$, and let G be the inverse image of N in R^h, so that we also have a surjection $G \twoheadrightarrow N$. Let v be any element of R^h that maps to u. Then $u \in N^*$ precisely if $v \in G^*_{R^h}$ as defined above. This is independent of the choice of v mapping to u. It is also independent of the choice of surjection $R^h \twoheadrightarrow M$.

It is understood that the tight closure of an ideal is taken in R unless otherwise specified.

Note that:

(0) *$u \in N^*_M$ if and only if the image $\overline{u}$ of u in M/N is in $0^*_{M/N}$.*

As in the ideal case:

(1) N^*_M *is a submodule of* M *and* $N \subseteq N^*_M$. *If* $N \subseteq Q \subseteq M$ *then* $N^*_M \subseteq Q^*_M$.

(2) If $N \subseteq M$, then $(N^*_M)^*_M = N^*_M$.

An example of tight closure

Let K be any field of characteristic $p > 0$ with $p \neq 3$. Let

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

This is a normal ring with an isolated singularity. It is Cohen-Macaulay. It is also a standard graded K-algebra. (This ring is sometimes called a *cubical cone*. It is also the homogeneous coordinate ring of an elliptic curve.)

We claim that $z^2 \in (x,\, y)^* - (x,\, y)$ in R. In fact, if we kill $I = (x,\, y)R$, we have $R/I = K[Z]/(Z^3)$, and the image of Z^2 is not 0. Take $c = z$ (the choices $c = x$ and $c = y$ also work). We need to check that

$$z(z^{2q}) \in (x^q,\, y^q)$$

for all $q \gg 0$. Let ρ be the remainder when $2q + 1$ is divided by 3, so that $\rho = 0$ or $\rho = 2$. We can write $2q + 1 = 3k + \rho$. Then

$$c(z^2)^q = z^{2q+1} = z^{3k+\rho} = (z^3)^k z^\rho = (-1)^k (x^3 + y^3)^k z^\rho.$$

To conclude the proof that $z^2 \in (x,\, y)^*$, it suffices to show that $(x^3 + y^3)^k \in (x^q,\, y^q)$. But otherwise we have $i + j = k$ with $i \geq 0$ and $j \geq 0$, and this implies that $3i \leq q - 1$ and that $3j \leq q - 1$. Adding these inequalities gives $3k = 3i + 3j \leq (q - 1) + (q - 1) = 2q - 2$, so that $2q + 1 - \rho \leq 2q - 2$ which implies that $\rho \geq 3$, a contradiction. □

This gives a non-trivial example where the tight closure of an ideal is larger than the ideal.

Defining tight closure for Noetherian rings containing the rational numbers

We want to discuss very briefly how one extends the theory to all Noetherian rings containing $\mathbb{Q}$. For a detailed account see, [M. Hochster and C. Huneke, *Tight closure in equal characteristic zero*, preprint] available at

`http://www.math.lsa.umich.edu/~hochster/msr.html`

— the notion discussed here corresponds to ${}^{*\mathrm{eq}}$. There is also an exposition in [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].

We first define a notion of tight closure in finitely generated $\mathbb{Q}$-algebras. In fact, any finitely generated $\mathbb{Q}$-algebra can be obtained as the tensor product over $\mathbb{Z}$ of $\mathbb{Q}$ with a finitely generated $\mathbb{Z}$-algebra. If our original $\mathbb{Q}$ algebra is $R = \mathbb{Q}[X_1, \, \ldots \, , X_n]/(F_1, \, \ldots \, , F_m)$, note that one can choose a single integer d divisible by all denominators in the polynomials $F_1, \, \ldots \, , F_m$, and then

$$R = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}[1/d][X_1, \, \ldots \, , X_n]/(F_1, \, \ldots \, , F_m).$$

We want to keep track of the behavior of this finitely generated $\mathbb{Z}$-algebra as we localize at finitely many nonzero integers: of course, this has the same effect as localizing $\mathbb{Z}$ at a single nonzero integer. Therefore we shall think of our finitely generated $\mathbb{Q}$-algebra R as $\mathbb{Q} \otimes_D R_D$, where $D = \mathbb{Z}[1/d]$ is the localization of $\mathbb{Z}$ at a single nonzero integer. But we shall allow that integer d to change so that it has more factors: in effect, as we localize further, we exclude finitely many more prime integers from consideration. By localizing at one element of $\mathbb{Z} - \{0\} \in D$ we may assume that R_D is D-free, by the Theorem on generic freeness. If B is D-algebra, which typically will be either $\mathbb{Q}$ or $\kappa = D/pD$ for some prime integer $p > 0$ not invertible in D, we write R_B for $B \otimes_D R_B$. Thus, $R = R_{\mathbb{Q}}$. Moreover, if M_D is an R_D-module, we write M_B for $B \otimes_D M_D$.

Given a finitely generated R-module M, we may think of it as the cokernel of a finite matrix with entries in D. This matrix will have entries in R_D if we localize D sufficiently, so that we have an R_D-module M_D such that $\mathbb{Q} \otimes_D M_D \cong M$. If D is large enough, we can assume that a given element of M is in D. If N is a finitely generated submodule of M, we may assume that D is large enough to contain a given finite set of generators of N over R, and we consider the R_D-submodule N_D of M_D generated by these elements. By localizing D at one more nonzero integer, we may assume that all of the terms of

$$0 \to N_D \to M_D \to M_D/N_D \to 0$$

are D-free. It follows that

$$0 \to N_B \to M_B \to M_B/N_B \to 0$$

is exact for every D-algebra B. We then have that $N \subseteq M$ arises from the inclusion $N_D \subseteq M_D$ by applying $\mathbb{Q} \otimes_D \_$. Note that when $M = R$ and $N = I$ is an ideal of R, we localize so that R_D/I_D is D-free.

Now suppose whether we want to test whether $u \in M$ is in the tight closure of N in M in *the affine* $\mathbb{Q}$*-algebra* sense. We choose R_D and $N_D \subseteq M_D$ as above, and take D sufficiently large that $u \in M_D$. We then define $u \in N^*_M$ if the image of $1 \otimes u$ of u is in $N^*_\kappa \subseteq M_\kappa$, where $\kappa = D/pD = \mathbb{Z}/p\mathbb{Z}$, for all but finitely many prime integers $p > 0$ that are prime in D. This condition can be shown to be independent of the choice of D, R_D, and $N_D \subseteq M_D$. This turns out to give a very good notion of tight closure when the base ring is a finitely generated $\mathbb{Q}$-algebra.

Example. Consider $R = \mathbb{Q}[X, \, Y, \, Z]/(X^3 + Y^3 + Z^3) = \mathbb{Q}[x, \, y, \, z]$. Then in this ring we have $z^2 \in (x, \, y)^*$, just as we did in positive characterisitic $p \neq 3$. In fact, we can take

$D = \mathbb{Z}$ and $R_D = \mathbb{Z}[X, Y, Z]/(X^3 + Y^3 + Z^3)$. We can let $I_D = (x, y)R_D$. For every $p \neq 3$, with $\kappa = \mathbb{Z}/p\mathbb{Z}$, the image of z^2 in $R_\kappa = \kappa[X, Y, Z]/(X^3 + Y^3 + Z^3)$ is in the tight closure, in the characteristic $p > 0$ sense, of $I_\kappa = (x, y)_\kappa$.

This notion can be extended to arbitrary Noetherian rings containing $\mathbb{Q}$ as follows. Let S be any such ring, let M be a finitely generated S-module and $N \subseteq M$ a submodule. Let $u \in M$. Then we define $u \in N^*_M$ if for every map $S \to C$, where C is a complete local domain, there exists and affine $\mathbb{Q}$-algebra R_0, a finitely generated R_0-module M_0, a submodule $N_0 \subseteq M_0$, an element $u_0 \in M_0$, and a map $R_0 \to C$ such that:

(1) $C \otimes_{R_0} M_0 \cong C \otimes_S M$.

(2) The image of $C \otimes_{R_0} N_0$ in $C \otimes_{R_0} M_0 \cong C \otimes_S M$ is the same as the image of $C \otimes_S N$ in $C \otimes_S M$.

(3) The image $1 \otimes u_0$ of u_0 in $C \otimes_{R_0} M_0 \cong C \otimes_S M$ is the same as the $1 \otimes u$ of u in $C \otimes M$.

(4) The element u_0 is in the tight closure of N_0 in M_0 in the affine $\mathbb{Q}$-algebra sense.

That, is roughly speaking, u is in the tight closure of $N \subseteq M$ if for every base change to a complete local domain, the new u, N, M also arise by base change from an instance of tight closure over an affine $\mathbb{Q}$-algebra.

This is a highly technical, convoluted definition, and working with it presents substantial technical difficulties. Nonetheless, with the help of some very deep results about the behavior of complete local rings, including a form of the Artin Approximation Theorem, one can show that this notion satisfies the conditions (1) — (5) discussed in the Lecture Notes for March 27 on pages 160–162. for a "good" tight closure theory. For the colon-capturing property (4) it suffices if the local ring is an *excellent* domain: we shall not define the property of being excellent here, but all rings that are localizations of finitely generated algebras over either a complete local ring (fields are included) or over $\mathbb{Z}$ are excellent.

We shall not pursue these ideas further in this course, but this should give the reader some feeling for how one extends the theory to all Noetherian rings containing $\mathbb{Q}$ in a manner that ultimately rests on reduction to characteristic $p > 0$.

Lecture of April 1

Another use of tight closure: contracted expansions from module-finite extension rings

In this lecture we discuss the problem of understanding $IS \cap R$ when R is a Noetherian domain and S is a module-finite or integral extension. If R contains the rational numbers $\mathbb{Q}$ and is normal, the situation is simple: it turns out that $IS \cap R = I$. In characteristic $p > 0$ the problem is much more difficult. Even when R is normal, $IS \cap R$ can be strictly larger than I. But we shall show that $IS \cap R \subseteq I^*$, which provides another use for tight closure. One can also consider the union of the ideals $IS \cap R$ as S runs through all module-finite extensions of R (it turns out not to matter whether the extension is also a domain), which gives a new kind of closure of I, called the *plus* closure I^+ such that $I \subseteq I^+ \subseteq I^*$ in positive characteristic p.

We also discuss the status of several questions about tight closure that were either open questions for a considerable length of time and then resolved, or that continue to be open questions.

Let R be a domain. Suppose that $R \subseteq S$ is a module-finite extension. In general, $I \subseteq IS \subseteq R$, but $IS \cap R$ may be larger than I. The main case is where S is also a domain. For S has a minimal prime $\mathfrak{p}$ disjoint from the multiplicative system $R - \{0\}$, and R injects into $\overline{S} = S/\mathfrak{p}$, which is a domain module-finite over R. Moreover, if $r \in R$ is in IS, then the image of r in $S/\mathfrak{p}$ is in $I\overline{S}$.

Suppose that $f \in R$, $g \in R - \{0\}$, and f/g is integral over R but not in R, which means that $f \notin gR$. We may take $S = R[f/g]$. Then $f \in gS \cap R - gR$, so that when R is not normal even principal ideals fail to be contracted from module-finite extensions. But if R is normal and contains $\mathbb{Q}$, then every ideal is contracted from every module-finite extension S. To see this, first note that it suffices to consider the case where S is a domain, by the argument above. Let $\mathcal{K}$ and $\mathcal{L}$ be the respective fraction fields of R and S. Multiplication by an element of $\mathcal{L}$ gives a map $\mathcal{L} \to \mathcal{L}$ which is $\mathcal{K}$-linear. If we simply think of this map as an endomorphism of the finite-dimensional $\mathcal{K}$-vector space $\mathcal{L}$, we may take its trace: i.e., pick a basis for $\mathcal{L}$ over $\mathcal{K}$, and take the sum of the diagonal entries of the matrix of the multiplication map with respect to this basis. This is independent of the choice of basis.

This trace map $\mathrm{Tr}_{\mathcal{L}/\mathcal{K}} : \mathcal{L} \to \mathcal{K}$ is $\mathcal{K}$-linear (hence, R-linear) and has value h on 1, where $h = [\mathcal{L} : \mathcal{K}]$. When R is a normal Noetherian ring, it turns out that the values of this map on S are in R. (One can see this as follows. First, R is the intersection of its localizations R_P at height one primes P. For if f, $g \in R$, $g \neq 0$, and f/g is in the fraction field of R but not in R, then $f \notin gR$. The associated primes of gR have height one, because R is normal. Using the primary decomposition of gR, we see that $f \notin \mathfrak{A}$ for some ideal $\mathfrak{A}$ primary to an associated P of gR of height one, and since elements of $R - P$

are not zerodivisors on $\mathfrak{A}$, $f \notin \mathfrak{A}R_P$ and so $f \notin gR_P$, i.e., $f/g \notin R_P$. If $Tr_{\mathcal{L}/\mathcal{K}}$ has a value on S not in R, we may preserve this while localizing at a height one prime P of R. But then we may replace R, S by R_P, S_P and assume that $R = R_P$ is a Noetherian discrete valuation ring. Since S is a torsion-free module over R, it is free, and has a free basis over R, say $s_1, \, \ldots \, , s_j$, consisting of elements of S. This is also a basis for $\mathcal{L}$ over $\mathcal{K}$, and can be used to calculate the trace of s. But now the matrix for multiplication by s has entries in R: for every s_i we have

$$ss_i = \sum_{j=1}^{h} r_{ij}s_j$$

with the $r_{ij} \in R$. But then the trace is $\sum_{i=1}^{h} r_{ii}$ and is in R after all. The condition that R be Noetherian is not really needed: for example, in the general case, an integrally closed domain can be shown to be a directed union of Noetherian integrally closed domains, from which the general case can be deduced. There are several other lines of argument.)

Finally, $\dfrac{1}{h}\mathrm{Tr}_{\mathcal{L}/\mathcal{K}} : S \to R$ splits $R \hookrightarrow S$ as a map of R-modules: by R-linearity, the fact that 1 maps to itself implies that the same holds for every element of R. Since we have a splitting, it follows that every ideal of R is contracted from S.

Although ideals are contracted from module finite-extensions of normal Noetherian domains that contain $\mathbb{Q}$, this is false in positive characteristic p.

Example. Let $R = K[X, \, Y, \, Z]/(X^3+Y^3+Z^3)$ where K is a field of characteristic 2. Then $z^2 \notin (x, \, y)R$, as noted earlier. But if we make a module-finite domain extension S of R that contains $x^{1/2}$, $y^{1/2}$, and $z^{1/2}$, then since $z^3 = x^3 + y^3$ (we are in characteristic 2, so that minus signs are not needed) we have $z^{3/2} = x^{3/2} + y^{3/2}$ (since squaring commtutes with addition and elements have at most one square root in domains of characteristic 2, taking square roots also commutes with addition in domains of characteristic 2). But then

$$z^2 = z^{1/2}z^{3/2} = z^{1/2}(xx^{1/2} + yy^{1/2}) = x^{1/2}z^{1/2}x + y^{1/2}z^{1/2}y \in (x, \, y)S \cap R - R.$$

However, tight closure "captures" the contracted expansion to a module-finite extension, which gives another proof that $z^2 \in (x, y)^*$ in the Example just above.

Theorem. *Let R be a Noetherian domain, and let S be any integral extension of R. Then for every ideal I of R, $IS \cap R \subseteq I^*$.*

Proof. Suppose that $f \in R$ and

$$(*) \quad f = \sum_{i=1}^{h} f_j s_j$$

where the $f_j \in I$ and the $s_j \in S$. We may replace S by $R[s_1, \, \ldots \, , s_h] \, \subseteq S$, and so assume that S is module-finite over R. Second, we may kill a minimal prime of S disjoint from

$R-\{0\}$ and so assume that S is a module-finite domain extension of R. Choose a maximal set of R-linearly independent elements of S, say $u_1, \ldots, u_k$, so that $Ru_1 + \cdots + Ru_k$ is R-torsion. It follows that some nonzero element $r \in R$, we have that

$$S \cong rS \subseteq Ru_1 + \cdots + Ru_k.$$

Thus, we have an embedding $S \hookrightarrow R^k$. Suppose that $1 \in S$ has as its image in R^k an element whose i th coordinate is nonzero, so that the composite map $S \hookrightarrow R^k \xrightarrow{\pi_i} R$ is nonzero on the element $1 \in S$, where π_i is the i th coordinate projection of $R^k \twoheadrightarrow R$. This gives an R-linear map $\theta : S \to R$ such that $\theta(1) = c \in R$ is nonzero. Now take q th powers of both sides of $(*)$, yielding

$$(**) \quad f^q \cdot 1 = \sum_{i=1}^{h} f_j^q s_j^q.$$

Since θ is R-linear and $f, f_1, \ldots, f_h \in R$, this yields

$$f^q\theta(1) = \sum_{i=1}^{h} f_j^q \theta(s_j^q),$$

and so $cf^q \in I^{[q]}$ for all q. This implies that $f \in I^*$. $\square$

Open questions: tight closure, plus closure, and localization

We want to consider some open questions in tight closure theory, and some related problems about when rings split from their module-finite extension algebras. After we do this, we shall prove some specific results in the characteristic p theory. It will turn out that to proceed further, we will need the structure theory of complete local rings, which we will develop next.

One of the longest standing and most important questions about tight closure is when tight closure commutes with localization. E.g., if R is Noetherian of prime characteristic $p > 0$, I is an ideal of R, and W is a multiplicative system of R, when is $W^{-1}(I^*_R)$ the same as $(W^{-1})^*_{W^{-1}R}$? It is easy to prove that $W^{-1}(I^*_R) \subseteq (W^{-1})^*_{W^{-1}R}$. This was an open question for more than twenty years. It is known to be true in many cases, but false in general, by a result of [H. Brenner and P. Monsky, See, for example, [I. Aberbach, M. Hochster, and C. Huneke, *Localization of tight closure and and modules of finite phantom projective dimension*, J. Reine Angew. Math. (Crelle's Journal) **434** (1993), 67–114], and [M. Hochster and C. Huneke, *Test exponents and localization of tight closure*, Michigan Math. J. **48** (2000), 305–329] for a discussion of the problem.

We saw in the Theorem proved on p. 168 of this lecture that tight closure "captures" contracted extension from module-finite and even integral extensions. We shall add this as (6) to our list of desirable properties for a tight closure theory, which becomes the following:

(0) *$u \in N^*_M$ if and only if the image $\overline{u}$ of u in M/N is in $0^*_{M/N}$.*

(1) *N^*_M is a submodule of M and $N \subseteq N^*_M$. If $N \subseteq Q \subseteq M$ then $N^*_M \subseteq Q^*_M$.*

(2) If $N \subseteq M$, then $(N^*_M)^*_M = N^*_M$.

(3) *If $R \subseteq S$ are domains, and $I \subseteq R$ is an ideal, $I^* \subseteq (IS)^*$, where I^* is taken in R and $(IS)^*$ in S.*

(4) *If A is a local domain then, under mild conditions on A (the class of rings allowed should include local rings of a finitely generated algebra over a complete local ring or over $\mathbb{Z}$), and $f_1, \ldots, f_d$ is a system of parameters for A, then for $1 \le i \le d-1$, $(f_1, \ldots, f_i)A :_A f_{i+1} \subseteq \bigl((f_1, \ldots, f_i)A\bigr)^*$.*

(5) If R is regular, then $I^* = I$ for every ideal I of R.

(6) For every module-finite extension ring R of S and every ideal I of R, $IS \cap R \subseteq I^*$.

These are all properties of tight closure in prime characteristic $p > 0$, and also of the theory of tight closure for Noetherian rings containing $\mathbb{Q}$ that we described in the Lecture of March 30. In characteristic $p > 0$, (4) holds for homomorphic images of Cohen-Macaulay rings, and for excellent local rings. If $R \supseteq \mathbb{Q}$, (4) holds if R is excellent. We will prove that (4) holds in prime characteristic for homomorphic images of Cohen-Macaulay rings quite soon. We have proved (5) in prime characteristic $p > 0$ for polynomial rings over a field, but not yet for all regular rings. To give the proof for all regular rings we need to prove that the Frobenius endomorphism is flat for all such rings, and we shall eventually use the structure theory of complete local rings to do this.

An extremely important open question is whether there exists a closure theory satisfying (1) — (6) for Noetherian rings that need not contain a field.

The Theorem proved on p. 168 of this lecture makes it natural to consider the following variant notion of closure. Let R be any integral domain. Let R^+ denote the integral closure of R in an algebraic closure $\overline{\mathcal{K}}$ of its fraction field $\mathcal{K}$. We refer to this ring as the *absolute integral closure* of R. R^+ is unique up to non-unique isomorphism, just as the algebraic closure of a field is. Any module-finite (or integral) extension domain S of R has fraction field algebraic over $\mathcal{K}$, and so S embeds in $\overline{\mathcal{K}}$. It follows that S embeds in R^+, since the elements of S are integral over R. Thus, R^+ contains an R-subalgebra isomorphic to any other integral extension domain of R: it is a maximal extension domain with respect to the property of being integral over R. R^+ is the directed union of its finitely generated subrings, which are module-finite over R. R^+ is also charactized as follows: it is a domain that is an integral extension of R, and every monic polynomial with coefficients in R^+ factors into monic linear polynomials over R^+.

Given an ideal $I \subseteq R$, the following two conditions on $f \in R$ are equivalent:

(1) $f \in IR^+ \cap R$.

(2) For some module-finite extension S of R, $f \in IS \cap R$.

The set of such elements, which is $IR^+ \cap R$, is denoted I^+, and is called the *plus* *closure* of I. (The definition can be extended to modules $N \subseteq M$ by defining N^+_M to be the kernel of the map $M \to R^+ \otimes_R (M/N)$.)

By the Theorem on p. 168 of the notes for this lecture, which is property (6) above in characteristic $p > 0$, we have that

$$I \subseteq I^+ \subseteq I^*$$

in prime characteristic $p > 0$. Whether $I^+ = I^*$ in general under mild conditions for Noetherian rings of prime characteristic $p > 0$ is another very important open question. It is not known to be true even in finitely generated algebras of Krull dimension 2 over a field.

However, there are some substantial positive results. It is known that under the mild conditions on the local domain R (e.g., when R is excellent), if I is generated by part of a system of parameters for R, then $I^+ = I^*$. See [K. E. Smith, *Tight closure of parameter ideals*, Inventiones Math. **115** (1994) 41–60]. Moreover, H. Brenner [H. Brenner, *Tight closure and plus closure in dimension two*, Amer. J. Math. **128** (2006) 531–539] proved that if R is the homogeneous coordinate ring of a smooth projective curve over the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$ for some prime integer $p > 0$, then $I^* = I^+$ for homogeneous ideals primary to the homogeneous maximal ideal. In [G. Dietz, *Closure operations in positive characteristic and big Cohen-Macaulay algebras*, Thesis, Univ. of Michigan, 2005] the condition that the ideal be homogeneous is removed: in fact, there is a corresponding result for modules $N \subseteq M$ when M/N has finite length. Brenner's methods involve the theory of semi-stable vector bundles over a smooth curve (in fact, one needs the notion of a *strongly* semi-stable vector bundle, where "strongly" means that the bundle remains semi-stable after pullback by the Frobenius map).

One reason for the great interest in whether plus closure commutes with tight closure is that it is known that plus closure commutes with localization. Hence, if $I^* = I^+$ in general (under mild conditions on the ring) one gets the result that tight closure commutes with localization.

The notion of plus closure is of almost no help in understanding tight closure when the ring contains the rationals. The reason for this is the result established using field trace in the first two pages of the notes for this lecture, which we restate formally here.

Theorem. *Let R be a normal Noetherian domain with fraction field $\mathcal{K}$ and let S be a module-finite extension domain with fraction field $\mathcal{L}$. Let $h = [\mathcal{L} : \mathcal{K}]$. If $\mathbb{Q} \subseteq R$, or, more generally, if h has an inverse in R, then $\frac{1}{h}\mathrm{Tr}_{\mathcal{L}/\mathcal{K}}$ gives an R-module retraction $S \to R$.* □

It follows that if $\mathbb{Q} \subseteq R$ and R is a normal domain, then $I^+ = I$ for every ideal I of R. Many normal rings (in some sense most normal rings) that are essentially of finite type over $\mathbb{Q}$ are not Cohen-Macaulay, and so contain parameter ideals that are not tightly closed. This shows that plus closure is not a greatly useful notion in Noetherian domains that contain $\mathbb{Q}$.

Lecture of April 3

In this lecture we begin discussion of *weakly F-regular rings*: these are the Noetherian rings of characteristic $p > 0$ such that every ideal is tightly closed. In particular, regular rings are weakly F-regular. It will turn out that R is weakly F-regular if and only if its localization at every *maximal ideal* is weakly F-regular. There are many examples when the ring is not regular. See the Examples on the next page. It is not known even for very good rings (finitely generated algebras over an algebraically closed field, for example) whether weak F-regularity is preserved by localization at an arbitrary prime. If that is true, it is preserved by localization at any multiplicative system. It is conjectured that under mild conditions on R, the two notions should be equivalent: the question has been open for over thirty-three years. Weakly F-regular rings are automatically normal and, under very mild assumptions, Cohen-Macaulay. We have mostly talked about normal domains in the past. More generally, a finite product of normal domains is also called *normal.* With this definition, the problem of whether a ring is normal is local: R is normal if and only if all local rings of R are normal domains.

We also define a *splinter* to be a Noetherian domain that splits, as a module over itself, from every module-finite ring extension. This condition turns out to imply normality, and, for rings containing $\mathbb{Q}$, normality characterizes the splinters. In characteristic p, this condition holds if the ring is weakly F-regular, and it is known to be equivalent to weak F-regularity for Cohen-Macaulay rings whose local rings have type 1 (these are called *Gorenstein rings*).

Weakly F-regular rings and F-regular rings

We define a Noetherian ring R of prime characteristic $p > 0$ to be *weakly F-regular* if every ideal is equal to its tight closure, i.e., every ideal is tightly closed. We define R to be *F-regular* if all of its localizations are weakly F-regular. It is not known whether weakly F-regular implies F-regular, even for domains finitely generated over a field. This would follow if tight closure were known to commute with localization.

We have already proved that polynomial rings over a field of positive characteristic are weakly F-regular, and we shall prove that every regular ring of positive characteristic is F-regular. This is one reason for the terminology. The “F” suggests the involvement of the Frobenius endomorphism.

We shall soon show that a weakly F-regular ring is normal, and, if it is a homomorphic image of a Cohen-Macaulay ring, is itself Cohen-Macaulay.

Theorem. *A direct summand A of a weakly F-regular domain is weakly F-regular, and a direct summand of an F-regular domain is F-regular.*

Proof. Assume that R is weakly F-regular. If $f \in I_A^*$, then $f \in (IR)^* \cap A = IR \cap A = I$. Since the direct summand condition is preserved by localization on A, it follows that a direct summand of an F-regular domain is F-regular. □

Examples of F-regular rings. Fix a field K of characteristic $p > 0$. Normal rings finitely generated over K by monomials are direct summand of regular rings, and so are F-regular. If X is an $r \times s$ matrix of indeterminates over K with $1 \leq t \leq r \leq s$, then it is known that $K[X]/I_t(X)$ is F-regular, and that the ring generated by the $r \times r$ minors of X over K is F-regular (this is the homogeneous coordinate ring of the Grassmann variety). See [M. Hochster and C. Huneke, *Tight closure of parameter ideals and splitting in module-finite extensions*, J. of Algebraic Geometry **3** (1994) 599–670], Theorem (7.14). We have already observed that these rings are direct summands of polynomial rings when K has characteristic 0, but this is not true in any obvious way when the characteristic is positive.

Splitting from module-finite extension rings

It is natural to attempt to characterize the Noetherian domains R such that R is a direct summand, as an R-module, of every module-finite extension ring S. We define a Noetherian domain R with this property to be a *splinter*. We then have the following result, which was actually proved in the preceding lecture, although it was not made explicit there.

Theorem. *Let R be a Noetherian domain.*

(a) *If R is a splinter, then every ideal of R is contracted from every integral extension.*

(b) *If R is a splinter, then R is normal.*

(c) *R is a splinter if and only if it is a direct summand of every module-finite domain extension.*

(d) *If $\mathbb{Q} \subseteq R$, then R is a splinter if and only if R is normal.*

Proof. For part (a), suppose $f, f_1, \ldots, f_h \in R$ and $f = \sum_{i=1}^h f_i s_i$ with the s_i in S. Then we have the same situation when S is replaced by $R[s_1, \ldots, s_h]$. Hence, it suffices to show that every ideal of R is contracted from every module-finite extension S. But then we have an R-linear retraction $\phi : S \to R$, and the result is part (a) of the Lemma at the top of p. 2 of the Lecture of March 30.

Part (b) has already been established in the fourth paragraph on p. 159 of the Lecture of March 30.

For part (c), we have already observed that S has a minimal prime $\mathfrak{p}$ disjoint from $R - \{0\}$, and it suffices to split the injection $R \hookrightarrow S/\mathfrak{p}$.

Finally, for part (d), the existence of the required splitting when S is a domain is proved at the bottom of p. 4 and top of p. 5 of the Lecture Notes of March 30, using field trace, and restated on p. 3 here. □

The example on p. 5 of the Lecture Notes of March 30 shows that in positive characteristic p, a normal domain need not be a splinter. The property of being a splinter in characteristic p is closely related to the property of being weakly F-regular.

We first note the following fact: we shall not give the proof in these lectures, but refer the reader to [M. Hochster, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. **51** (1973) 25–43] and [M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977) 463–488].

Theorem. *Let R be a normal Noetherian domain. Then R is a direct summand of a module-finite extension of S if and only if every ideal of R is contracted from S.*

Of course, we know the "only if" part.

Corollary. *Let R be a normal Noetherian domain of positive characteristic p. Then R is a splinter if and only if for every ideal $I \subseteq R$, $I = I^+$.*

Corollary. *If R is a normal Noetherian domain and R is weakly F-regular, then R is a splinter.*

Proof. This is immediate from the preceding result, since $I^+ \subseteq I^*$. □

We shall see quite soon that if R is weakly F-regular it is automatic that R is normal. If plus closure is the same as tight closure, then it would follow that R is weakly F-regular if and only if R is a splinter. This is an open question.

We have already observed that in characteristic $p > 0$, regular rings are weakly F-regular, although we have not prove this. Assuming this for the moment we have:

Corollary. *A regular ring that contains a field is a direct summand of every module-finite extension ring.*

This was conjectured by the author in 1969, and was been open question for regular rings that do not contain a field, such as polynomial rings over the integers, for 50 years. The case of dimension 3 was settled affirmatively in [R. C. Heitmann, *The direct summand conjecture in dimension three*, Annals of Math. (2) **156** (2002) 695–712]. The general case was settled by Y. André in 2016, and then a simpler proof was given by B. Bhatt.

It is also a major open question whether there exists a tight closure theory satisfying conditions (0) — (6) of p. 1 for Noetherian rings that need not contain a field. The existence of such a theory would imply that direct summands of regular rings are Cohen-Macaulay in general, and that regular rings are direct summands of all of their module-finite extensions in general. Such a theory would also settle many other open questions.

Lecture of April 6

In the first part of this lecture we consider only Noetherian rings of positive prime characteristic p. We prove that the tight closure of (0) is the nilradical, and we can conclude that weakly F-regular rings are reduced. We also study tight closure in products of rings, and prove that a finite product of weakly F-regular rings is weakly F-regular. We prove that if every principal ideal of a ring is tightly closed, then the ring is a finite product of normal domains (we adjust terminology, and call these finite products of normal domains *normal* as well.

The second part of the lecture reviews and refines properties of Cohen-Macaulay rings, especially those connected with chain conditions, and introduces the notion of *universally catenary*: R is universally catenary if every finitely generated R-algebra (this includes homomorphic images) is catenary. Cohen-Macaulay rings are universally catenary.

More on tight closure, weak F-regularity, and the Cohen-Macaulay property

We next want to study weakly F-rings, i.e., Noetherian rings of prime characteristic $p > 0$ such that every ideal is tightly closed. Until further notice, all given rings R are assumed to be Noetherian, of prime characteristic $p > 0$.

Proposition. *The tight closure of the (0) ideal in R is the ideal of all nilpotent elements. Hence, if $(0) = (0)^*$, the R is reduced. In particular, every weakly F-regular ring is reduced.*

Proof. If u is nilpotent then $1 \cdot u^q = 0$ for all $q \gg 0$. Conversely, if $c \in R^\circ$ and $cu^q = 0$ for all $q \gg 0$, then for every minimal prime $\mathfrak{p}$ we have that $cu^q \in \mathfrak{p}$ for some q. Since $c \notin \mathfrak{p}$, we have that $u^q \in \mathfrak{p}$ and so $u \in \mathfrak{p}$. But the intersection of the minimal primes is the set of nilpotent elements of R, and so u is nilpotent. The remaining statements are now obvious. □

Proposition. *Suppose that $R = S \times T$ is a product ring, with $S,\, T \neq 0$. Then for every ideal $I \times J$ of $S \times T$, where $I \subseteq S$ and $J \subseteq T$ are ideals, $(I \times J)^*_R = I^*_S \times J^*_T$.*

Proof. The first point is that $(S \times T)^\circ = (S^\circ) \times (T^\circ)$. Hence if $cs^q \in I^{[q]}$ for all $q \gg 0$ and $dt^q \in J^{[q]}$ for all $q \gg 0$, we have that

$$(c,\, d)(s,\, t)^q \in I^{[q]} \times J^{[q]} = (I \times J)^{[q]}$$

for all $q \gg 0$. The converse is also immediate. □

Corollary. *A finite product $R_1 \times \cdots \times R_h$ is weakly F-regular if and only if every factor is weakly F-regular.* □

Theorem. *If every principal ideal of R is tightly closed, then R is a product of normal domains.*

Proof. The fact that $(0) = (0)^*$ implies that R is reduced. We first show that R is a product of domains. If there are two or more minimal primes, the minimal primes can be partitioned into two nonempty sets. Call the intersection of one set I and the intersection of the other set J. Then $I \cap J = 0$, and $I + J$ is not contained in any minimal prime $\mathfrak{p}$, for otherwise, $\mathfrak{p}$ would have to contain both a minimal prime of I and a minimal prime of J, and would be equal to both of these. Hence we can choose $f \in I$ and $g \in J$ such that $f + g$ is not in any minimal prime of R, and so is a nonzerodivisor. Note that $fg \in I \cap J$, and so $fg = 0$. Now

$$(f+g)f^q = f^{q+1} = f(f+g)^q$$

for all q, so that $f \in (f+g)^* = (f+g)R$. Thus, we can choose $r \in R$ such that $f = r(f+g) = rf + rg$, and the $f - rf = rg$. Since $f \in I$ and $g \in J$, both sides must vanish, and so $f = rf$ and $rg = 0$. Now $r(f+g) = rf = f$, and

$$r^2(f+g) = r(rf+rg) = r(f+0) = rf = f,$$

so that

$$(f+g)(r^2 - r) = 0.$$

Since $f + g$ is not a zerodivisor, we have that $r^2 - r = 0$. Since $rf = f$ is not 0 (or $f + g$ would be in the minimal primes containing g) $r \neq 0$. Since $rg = 0$, $r \neq 1$. Therefore, R contains a non-trivial idempotent, and is a product of two rings. Both have the property that principal ideals are tightly closed, because a principal ideal of $S \times T$ is the product of a principal ideal of S and a principal ideal of T, and we may apply the Proposition above.

We may apply this argument repeatedly and so write R as a finite product of rings with the property that every principal ideal is tightly closed, and such that none of the factors is a product. Each of the factors must have just one minimal prime, and so is a domain. It remains to see that if principal ideals are tightly closed in a domain R, then R is normal. Suppose that $f,\, g \in R$, $g \neq 0$, and f/g is integral over R. Let $S = R[f/g]$, which is module-finite over R. Then $f = g(f/g) \in gS$, and so $f \in (gR)^*$. But $(gR)^* = gR$, and so $f \in gR$, i.e., $f/g \in R$, as required. □

We next want to show that, under mild conditions on R, if R is weakly F-regular then R is Cohen-Macaulay. To prove this, we will need to generalize the results on colon-capturing that we have already obtained in finitely generated $\mathbb{N}$-graded algebras over a field.

We first review some facts about Cohen-Macaulay rings. This material is in the Lecture of March 11.

We recall that if $(R,\, \mathfrak{m},\, K)$ is a Cohen-Macaulay local ring, then for every minimal prime $\mathfrak{p}$ of R, $\dim(R/\mathfrak{p}) = \dim(R)$.

Thus, a Cohen-Macaulay local ring cannot exhibit the kind of behavior one observes in $R = K[[x,\, y,\, z]]/\bigl((x,\, y) \cap (z)\bigr)$: 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.

We also recall that 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. If R is catenary, then so is R/I for every ideal I, since primes containing I are in bijective correspondence with primes of R containing I, and saturated chains of primes in R/I joining P/I to Q/I, where $I \subseteq P \subseteq Q$ and P, Q are primes of R, correspond to saturated chains of primes of R joining P to Q. Similarly, any localization of a catenary ring is catenary. M. Nagata gave the first examples of Noetherian rings that are not catenary: there is a local domain $(R,\, \mathfrak{m},\, K)$ of dimension 3, for example, containing saturated chains $0 \subset Q \subset m$ and $0 \subset P_1 \subset P_2 \subset m$, where all inclusions are strict. See [M. Nagata, *Local rings*, Interscience, New York, 1962], Appendx A1, pp. 204–205. Although Q has height one and $\dim(R) = 3$, the dimension of R/Q is 1. Nagata also showed that even when a Noetherian ring is catenary, the polynomial ring in one variable over it need not be.

A Noetherian ring R is called *universally catenary* if every finitely generated R-algebra is catenary. This is equivalent to assuming that all polynomial rings in finitely many variables over R are catenary, since all finitely generated R-algebras are homomorphic images of such polynomial rings, and a homomorphic image of a catenary ring is catenary (because, if $I \subseteq P \subseteq Q$, the chains of primes between P and Q correspond bijectively with the chains of primes between P/I and Q/I in R/I). Note also that , similarly, all localizations of catenary rings are catenary, and it follows easily that localizations of universally catenary rings are universally catenary. Cohen-Macaulay rings are universally catenary, as we show in the two results below. The following result strengthens a bit what we know about about chains of primes in Cohen-Macaulay rings.

Theorem. *A Cohen-Macaulay ring R is catenary, and for any two prime ideals $P \subseteq Q$ in R, every saturated chain of prime ideals joining P to Q has length* $\mathrm{height}\,(Q) - \mathrm{height}\,(P)$.

Proof. For the first part, the issues are unaffected by localizing at Q. Thus, we may assume that R is local and that Q is the maximal ideal. There is part of a system of parameters of length $h = \mathrm{height}\,(P)$ contained in P, call it $x_1, \, \ldots\,, x_h$. This sequence is a regular sequence on R and in so on R_P, which implies that its image in R_P is system of parameters. We now replace R by $R/(x_1, \, \ldots\,, x_h)$. Both the dimension and depth of R have decreased by h, so that R is still Cohen-Macaulay. Q and P are replaced by their images, which have heights $\dim(R) - h$ and 0, and $\dim(R) - h = \dim(R/(x_1, \, \ldots\,, x_h)$. We have therefore reduced to the case where R 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'. Choose an element x in P_1 not in any minimal prime, and an element y of P_1' not in any minimal prime. Then xy 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. □

Corollary. *Cohen-Macaulay rings are universally catenary, i.e., a finitely generated algebra over a Cohen-Macaulay ring is catenary.*

Proof. Such an algebra is a homomorphic image of a polynomial ring in finitely many variables over a Cohen-Macaulay ring, which is again Cohen-Macaulay, and homomorphic images of catenary rings are catenary. □

Lecture of April 8

Throughout this lecture we will work with Noetherian rings of positive prime characteristic p. The first main goal is to prove a result on colon-capturing for tight closure in rings that are homomorphic images of Cohen-Macaulay rings. The condition that a ring be a homomorphic image of a Cohen-Macaulay ring is not very restrictive: it typically holds for the Noetherian rings that come up in algebraic geometry, algebraic combinatorics, several complex variables (e.g., convergent power series rings) and algebraic number theory. In fact, the rings that come up are usually homomorphic images of regular rings. The property of being a homomorphic image of a Cohen-Macaulay ring passes to finitely generated algebras and to all localizations at multiplicative systems. Note that every ring that is finitely generated either over a field or over a complete local ring has this property (as we shall see later, every complete local ring is a homomorphic image of a complete regular local ring).

The argument for colon-capturing needs a preliminary lemma on prime avoidance for cosets, which is used in the proof of another lemma on lifting systems of parameters from quotients S/P to S.

It is then shown that a ring is weakly F-regular if and only if all of its localizations at *maximal* ideals are weakly F-regular. We emphasize that it is *not* known whether the localizations of a weakly F-regular ring at non-maximal primes must again be weakly F-regular (the stronger property defines F-*regularity* without the modifier "weakly"). Coupled with the colon-capturing result, this proves that every weakly F-regular ring that is a homomorphic image of a Cohen-Macaulay ring is Cohen-Macaulay.

Here are the two preliminary results needed for the theorem on colon-capturing.

Lemma (prime avoidance for cosets). *Let S be any commutative ring, $x \in S$, $I \subseteq S$ an ideal and $P_1, \dots, P_k$ 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. □

Lemma. *Let S be a Cohen-Macaulay local ring, let P be a prime ideal of S of height h, and let $x_1, \ldots, x_{i+1}$ be part of a system of parameters of $R = S/P$. Let $y_1, \ldots, y_h \in P$ be part of a system of parameters for S (we have a regular sequence on S of length h since the depth of S on P is the height of P, and this will be part of a system of parameters). Then there exist elements*

$\widetilde{x}_1, \ldots, \widetilde{x}_{i+1}$ of S such that

$\widetilde{x}_j$ maps to x_j modulo P, $1 \leq j \leq i+1$, and $y_1, \ldots, y_h, \widetilde{x}_1, \ldots, \widetilde{x}_{i+1}$ is part of a system of parameters for S.

Proof. We construct the $\widetilde{x}_j$ recursively. Suppose that the $\widetilde{x}_j$ for $j < k+1 \leq i+1$ have been chosen so that $y_1, \ldots, y_h, \widetilde{x}_1, \ldots, \widetilde{x}_k$ is part of a system of parameters for S. Here, k is allowed to be 0 (i.e., we may be choosing $\widetilde{x}_1$). We want to choose an element of $x_{k+1} + P$ that is not in any minimal prime of $y_1, \ldots, y_h, \widetilde{x}_1, \ldots, \widetilde{x}_k$, and these all have height at most $h + k$. By the Lemma on prime avoidance for cosets, if $\widetilde{x}_{k+1} + P$ is contained in the union, then $Sx_{k+1} + P$ is contained in one of them, say Q. Working modulo P we have that Q/P is a minimal prime $x_1, \ldots, x_{k+1}$ of height at most $h + k - h = k$. This is a contradiction, since $x_1, \ldots, x_{k+1}$ is part of a system of parameters in S/P, and so any minimal prime must have height at least $k + 1$. □

Theorem (colon-capturing). *Let $(R, \mathfrak{m}, K)$ be a local domain of prime characteristic $p > 0$, and suppose that R is a homomorphic image of a Cohen-Macaulay ring of characteristic p. Let $x_1, \ldots, x_{i+1}$ by part of a system of parameters in R. Then*

$$(x_1, \ldots, x_i) :_R x_{i+1} \subseteq (x_1, \ldots, x_i)^*.$$

Proof. Suppose that $R = S/P$, where S is Cohen-Macaulay of characteristic p, and let Q be the inverse image of m in S. Then R is also a homomorphic image of S_Q, since $S_Q/PS_Q \cong (S/P)_Q = R_Q = R_m = R$. Hence, we may assume that S is local. Choose $y_1, \ldots, y_h$ and $\widetilde{x}_1, \ldots, \widetilde{x}_{i+1}$ as in the preceding Lemma. Since P is a minimal prime of $(y_1, \ldots, y_h)$ in S, we can choose $\widetilde{c} \in S - P$ and an integer $N > 0$ such that $\widetilde{c}P^N \in (y_1, \ldots, y_h)S$. Let $c \neq 0$ be the image of $\widetilde{c}$ in R. Suppose that $fx_{i+1} = f_1x_1 + \cdots + f_ix_i$ in R. Then we can choose elements $\widetilde{f}$ and $\widetilde{f}_1, \ldots, \widetilde{f}_i$ in S that lift f and $f_1, \ldots, f_i$ respectively to S. This yields an equation

$$\widetilde{f}\widetilde{x}_{i+1} = \widetilde{f}_1\widetilde{x}_1 + \cdots + \widetilde{f}_i\widetilde{x}_i + \Delta$$

in S, where $\Delta \in P$. Then for all $p^e = q \geq N$ we have

$$\widetilde{f}^q\widetilde{x}_{i+1}^q = \widetilde{f_1}^q\widetilde{x}_1^q + \cdots + \widetilde{f}_i^q\widetilde{x}_i^q + \Delta^q$$

We may multiply both sides by $\widetilde{c}$, and use the fact that $\widetilde{c}\Delta^q \in cP^N \subseteq (y_1, \ldots, y_h)$ to conclude that

$$(*) \quad \widetilde{c}\widetilde{f}^q\widetilde{x}_{i+1}^q \in (\widetilde{x}_1^q, \ldots, \widetilde{x}_i^q, y_1, \ldots, y_h)S$$

But $y_1, \, \dots \, , y_h, \, \widetilde{x}_1^q, \, \dots \, , \widetilde{x}_{i+1}^q$ is a permutable regular sequence in S, and so $(*)$ implies that

$$\widetilde{c}\widetilde{f}^q \in (\widetilde{x}_1^q, \, \dots \, , \widetilde{x}_i^q, \, y_1, \, \dots \, , y_h)S.$$

When we consider this modulo P, We have that $(y_1, \, \dots \, , y_h)$ is killed, and so

$$cf^q \in (x_1^q, \, \dots \, , x_i^q)$$

for all $q \geq N$, and this gives the desired conclusion. $\square$

Weak F-regularity: localization at maximal ideals and the Cohen-Macaulay property

We next want to prove that the property of being weakly F-regular is local on the maximal ideals of R. From this we will deduce that a weakly F-regular ring that is a homomorphic image of a Cohen-Macaulay ring is Cohen-Macaulay. We need two preliminary results.

Lemma. *Let R be any Noetherian ring, let M be a finitely generated R-module and $N \subseteq M$ a submodule. Then N is the intersection of a (usually infinite) family of submodules Q of M such that every M/Q is killed by a power of a maximal ideal of R.*

In particular, every ideal I of R is an intersection of ideals that are primary to a maximal ideal of R.

Proof. Let $u \in M - N$. Consider the family of submodules $M_1 \subseteq M$ such that $N \subseteq M$ and $u \notin M_1$. This family is nonempty, since it contains N. Therefore it has a maximal element Q. It will suffice to show that M/Q is killed by a power of a maximal ideal of R. Note that every nonzero submodule of M/Q contains the image of u, or else its inverse image in M will strictly contain Q but will not contain u.

We may replace M by M/Q and u by its image in M/Q. It therefore suffices to show that if $u \neq 0$ is in every nonzero submodule of M, then M is killed by a power of a maximal ideal, which is equivalent to the assertion that $\mathrm{Ass}\,(M)$ consists of a single maximal ideal. Let $P \in \mathrm{Ass}\,(M)$ and suppose that $P = \mathrm{Ann}_R v$, where $v \neq 0$ is in M. Then $Rv \cong R/P$, and every nonzero element has annihilator P. But $u \in Rv$, and so $P = \mathrm{Ann}_R u$. It follows that every associated prime of M is the same as $\mathrm{Ann}_R u$, and so there is only one associated prime. It remains to show that P is maximal. Suppose not, and consider $R/P \hookrightarrow M$. It will suffice to show that there is no element in all the nonzero ideals of R/P. Thus, it suffices to show that if $S = R/P$ is a Noetherian domain of dimension at least one, there is no nonzero element in all the nonzero ideals. This is true, in fact, even if we localize at a nonzero prime ideal m of S, for in S_m, there is no element in all of the ideals $m^n S_m$. $\square$

Proposition. *Let R be a Noetherian ring of prime characteristic $p > 0$, and let $\mathfrak{A}$ be an ideal of R.*

(a) *If $\theta : R \to S$ is such that S is flat Noetherian R-algebra and, in particular, if S is a localization of R, then $\theta(\mathfrak{A}^*_R) \subseteq (\mathfrak{A}S)^*_S$.*

(b) *Let m be a maximal ideal of R and suppose that $\mathfrak{A}$ is an m-primary ideal. Let $f \in R$. Then $f \in \mathfrak{A}^*_R$ if and only if $f/1 \in (\mathfrak{A}R_m)^*_{R_m}$.*

(c) *Under the hypotheses of part (b), $\mathfrak{A}$ is tightly closed in R if and only if $\mathfrak{A}R_m$ is tightly closed in R_m.*

Proof. (a) Let $f \in \mathfrak{A}^*_R$. The equation $cf^q \in \mathfrak{A}^{[q]}$ implies $\theta(c)\theta(f)^q \in (\mathfrak{A}S)^{[q]}$, and so we need only see that if $c \in R^\circ$ then $c \in S^\circ$. Suppose, to the contrary, that c is in a minimal prime $\mathfrak{q}$ of S. It suffices to see that the contraction $\mathfrak{p}$ of $\mathfrak{q}$ to R is minimal. But $R_\mathfrak{p} \to S_\mathfrak{q}$ is still faithfully flat, and the maximal ideal of $S_\mathfrak{q}$ is nilpotent, which implies that $\mathfrak{p}R_\mathfrak{p}$ is nilpotent, and so $\mathfrak{p}$ is minimal.

For part (b), we see from (a) that if $f \in \mathfrak{A}^*$ then $f \in (\mathfrak{A}R_m)^*$. We need to prove the converse. Suppose that $c_1 \in R_m^\circ$ has the property that $cf_1^q \in \mathfrak{A}^{[q]}R_m = (\mathfrak{A}R_m)^{[q]}$ for all $q \gg 0$. Then c_1 has the form c/w where $c \in R$ 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 $c \in R$. We next want to replace c by an element with the same image in R_m that is not in any minimal prime of R. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the minimal primes of R that are contained in m, so that the ideals $\mathfrak{p}_jR_m$ for $1 \le j \le k$ are *all* of the minimal primes of R_m. It follows that the image of $\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$ is nilpotent in R_m, 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 R_m. If $c + I$ is contained in the union of the minimal primes of R, then by the coset form of prime avoidance, 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 $1 \le j \le k$. But then $c \in \mathfrak{p}_j$, a contradiction, since $c/1$ is not in any minimal prime of R°. Hence, we can choose $f \in I$ such that $c + f \in R^\circ$, and $c + f$ also maps to $c/1$ in R. We change notation and assume $c \in R^\circ$. Then $cf^q/1 \in \mathfrak{A}^{[q]}R_m$ for all $q \gg 0$. Since $\mathfrak{A}^{[q]}$ is primary to m, the ring $R/\mathfrak{A}^{[q]}$ has only one maximal ideal, $m/\mathfrak{A}^{[q]}$, and is already local. Hence,

$$R/\mathfrak{A}^{[q]} \cong (R/fA^{[q]})_m = R_m/\mathfrak{A}^{[q]}R_m.$$

It follows that $cf^q \in \mathfrak{A}^{[q]}$ for all $q \gg 0$, and so $f \in \mathfrak{A}^*_R$, as required.

Part (c) is immediate from part (b) and the observation above that $R_m/\mathfrak{A}R_m = R/\mathfrak{A}$, so that any element of $R_m/\mathfrak{A}R_m$ is represented by an element of R. □

Remark. Part (a) holds for any map $R \to S$ of Noetherian rings of prime characteristic $p > 0$ such that R° maps into S°. We have already seen another example, namely when $R \hookrightarrow S$ are domains.

Theorem. *The following conditions on R are equivalent.*

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

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

(3) *For every maximal ideal m of R, R_m is weakly F-regular.*

Proof. Statements (2) and (3) are equivalent by part (c) of the preceding Proposition, and (1) ⇒ (2) is clear. Assume (2), and let I be any ideal of R. We need only show that I is tightly closed. If not, let $f \in I^* - I$. Since I is the intersection of the ideals containing I that are primary to maximal ideals, there is an ideal $\mathfrak{A}$ of R primary to a maximal ideal m such that $I \subseteq \mathfrak{A}$ and $f \notin \mathfrak{A}$. Since $\mathfrak{A}$ is tightly closed and $I \subseteq \mathfrak{A}$, we have $I^* \subseteq \mathfrak{A}$, and so $f \in \mathfrak{A}$, a contradiction. □

Theorem. *Let R be a Noetherian ring of positive prime characteristic p that is a homomorphic image of a Cohen-Macaulay ring. If R is weakly F-regular, then R is Cohen-Macaulay.*

Proof. By the preceding result, it suffices to check this for $R_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of R: the hypothesis of weak F-regularity is preserved. Thus, we may assume that R is local. We then know that R is normal, and so R is a domain, and it follows that the theorem on colon-capturing stated on the second page of the notes for this lecture holds. Hence, if $x_1, \ldots, x_d$ is a system of parameters for R, and $J_i = (x_1, \ldots, x_i)R$, $0 \leq i < d$, then $J_i :_R x_{i+1} \subseteq J_i^*$ and $J_i^* = J_i$. But the statement $J_i :_R x_{i+1} = J_i$ means that the image of x_{i+1} is not a zerodivisor in R/J_i, $0 \leq< d$, which means that $x_1, \ldots, x_d$ is a regular sequence on R. □

Lecture of April 10

In this lecture we give brief discussions first of excellent rings, and then of F-rational rings in positive prime characteristic. The material in these subsections is primarily expository and is optional — it will not be needed for any quiz or problem set.

The condition of excellence is a convenient hypothesis: excellent rings have many of the same properties that finitely generated algebras over a field have.

F-rational rings are defined here as Noetherian rings R of positive prime characteristic p that are quotients of Cohen-Macaulay rings such that, for every local ring $R_{\mathfrak{m}}$ of the ring R at a maximal ideal $\mathfrak{m}$, the local ring is equidimensional (the quotient of $R_{\mathfrak{m}}$ by any minimal prime has the same dimension as $R_{\mathfrak{m}}$) and the ideal generated by one (equivalently, every) system of parameters is tightly closed. This condition implies that the ring is Cohen-Macaulay and normal, and turns out to be strictly weaker than F-regularity.

We then begin our summary of the structure theory of complete local rings. That subsection has a separate introduction. The statements of some of the results (these will be clearly indicated) are required material. Complete proofs of the results stated in these notes will be provided in a Supplement, which will be both posted and distributed by e-mail. But going through the proofs of the results is optional.

Excellent rings

Alexander Grothendieck introduced a class of Noetherian rings called *excellent* rings in his massive work, *Éléments de géométrie algébrique* IV, Publications Mathématiques de l'IHÉS **24** (1965), Section 7. These rings have many of the important properties shared by finitely generated algebras over a field (as mentioned above), or over the integers, or over a compete local ring. We give the definition and mention some basic properties, but we do not give a detailed treatment. However, in the sequel we will occasionally mention that a result about, for example, tight closure, generalizes to the excellent case.

One of the most important ideas underlying the usefulness of this notion is that for an excellent local ring R, there is an especially good way of showing that desirable properties of the completion $\widehat{R}$ are shared by R: this follows largely from the definition of a G-ring, discussed below. I feel that one of the most readable treatments of the theory of excellent rings is given in the book *Commutative Algebra* by H. Matsumura, Benjamin, New York, 1970.

A Noetherian K-algebra S is called *geometrically regular* over K (or $K \to S$ is called *geometrically regular*) if for every for every finite algebraic extension L of K, $L \otimes_K S$ is regular. This implies that S is regular, since it holds when $L = K$. If $L_0 \subseteq L$ are finite algebraic field extensions and $L \otimes_K S$ is regular, then $L_0 \otimes_K S$ is regular, because $L \otimes_K S$ is faithfully flat over $L_0 \otimes_K S$. Thus, the larger L is, the harder it is to satisfy the condition. However, if S is regular then $L \otimes_K R$ is regular whenever L is *separable finite algebraic* over K. Thus, if K has characteristic 0, or is perfect (and, of course, if K is algebraically closed), R is geometrically regular over K if and only if it is regular. If K has characteristic p, every finite algebraic extension is contained in a finite algebraic extension which consists of a finite purely inseparable extension followed by a finite separable extension. Hence, $K \to R$ is geometrically regular if and only if for every purely inseparable finite algebraic extension L of K, we have that $L \otimes_K R$ is regular. Note that if R is an algebraic extension field of K, it is geometrically regular if and only if it is separable over K: otherwise, there will be nilpotents in $L \otimes KR$ when L is the splitting field of the minimal polynomial of an element of R that is not separable over K.

More generally, a map $R \to S$ of Noetherian rings is called *geometrically regular* if and only if it is flat with geometrically regular fibers. That is S is R-flat and for every prime P of R, with $\kappa_P = R_P/PR_P \cong \mathrm{frac}\,(R/P)$, the fiber $\kappa_P \otimes_R S$ is geometrically regular over κ_P.[1]

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

This condition can fail even for a Noetherian discrete valuation domain V in characteristic $p > 0$. Let k be a perfect field of characteristic p and let $K = k(t_1, \ldots, t_n, \ldots)$ be the field generated by an infinite sequence of indeterminates over K. Let $K_0 = K^p$ and $K_n = K_0(t_1, \ldots, t_n)$, which will contain $t_1, \ldots, t_n$ but only t_h^p if $h > n$. Let $V_n = K_n[[x]] \subseteq K[[x]]$, which is a Noetherian discrete valuation domain with maximal ideal xV_n. Let $V = \cup_{n=0}^{\infty} V_n$, which is easily verified to be a Noetherian discrete valuation domain with maximal ideal xV. We still have $V \subseteq K[[x]]$, and it is easy to check that $\widehat{V}$ may be identified with $V[[x]]$. This means that the fraction field of $\widehat{V}$ is a purely inseparable the fraction field of V, and this extension is not geometrically regular.

We can finally give the definition of *excellence*. 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. Therere are many ways to give this hypotheses with a superficially weaker assumption about the openness of the regular locus.

Excellent rings include the integers, fields, complete local rings, convergent power series rings, and are closed under taking quotients, localization, and formation of finitely generated algebras. The rings that come up in algebraic geometry, algebraic number theory, algebraic combinatorics, and several complex variables are excellent. Excellent rings tend very strongly to share the good behavior exhibited by rings that are finitely generated over a field. Here are some examples.

[1] For those familiar with the notion of *smoothness*, when S is finitely presented as a R-algebra, S is smooth over R if and only if it is geometrically regular over R. There is a complete treatment in the Lecture Notes from Math 615, Winter 2017.

In connection with (4) of the list of properties that follows, note that the completion of an excellent local domain need *not* be a domain: if $S = K[x, y]$, where K is a field of characteristic different from 2 (there are similar examples in characteristic 2) $\mathfrak{m} = (x, y)S$ and $R = S_{\mathfrak{m}}/(y^2 - x^2(1 + x)$, then R is a domain (because $y^2 - x^2(1 + x)$ is irreducible, even over $K(x, y)$) but $\widehat{R}$ has two minimal primes (because $y^2 - x^2(1 + x)$ reduces in the completion $K[[x, y]]$: the point is that since $1 + x$ has a square root in $K[[x]]$, so does $x^2(1 + x)$.

For a detailed treatment of the items (5) and (6), we refer to M. Hochster and C. Huneke, *F-regularity, test elements, and smooth base change*, Trans. Amer. Math. Soc. **346** (1994), 1–62.

Recall that a local ring R is *equidimensional* if for every minimal prime $\mathfrak{p}$ of R, the Krull dimension of $R/\mathfrak{p}$ is the same as the Krull dimension of R.

(1) The normalization of an excellent domain R is a finitely generated R-module.

(2) The completion of a reduced excellent local ring is reduced.

(3) The completion of a normal excellent local domain is normal.

(4) The completion of any excellent reduced, equidimensional local ring R is reduced and equidimensional. In particular, the completion of an excellent local domain is reduced and equidimensional.

(5) (Colon-capturing in excellent local rings.) If R is an excellent equidimensional ring of positive prime characteristic, $x_1, \dots, x_d$ is a system of parameters, and $J_i := (x_1, \dots, x_i)R$, $J_i :_R x_{i+1} \subseteq J_i^*$.

(6) (Existence of test elements.) Let R be a localization of a reduced finitely generated algebra over an excellent semilocal ring of positive prime characteristic. Let $c \in R$ be any element not in any minimal prime of R such that R_c is regular (such elements exist). Then c has a power that is a test element for tight closure in R.

F-rational rings

We have defined a Noetherian ring of positive prime characteristic p to be F-*rational* if it is a homomorphic image of a Cohen-Macaulay ring R and for the localization at each maximal ideal, the local ring is equidimensional and one (equivalently, every) system of parameters is tightly closed. For a detailed treatment see M. Hochster and C. Huneke, *F-regularity, test elements, and smooth base change*, Trans. Amer. Math. Soc. **346** (1994), 1–62, especially Theorem 4.2. One can show a local ring $(R, \mathfrak{m})$ satisfying this condition is a normal domain. In the domain case, the problem of showing that if one system of parameters is tightly closed then all systems of iis tightly closed, is addressed in Problem Set 5. Once one knows this it follows that if $x_1, \dots, x_d$ is a system of parameters, then all of the ideals $J_i = (vectxi)R$, $0 \leq i \leq d$ are tightly closed since

$$J_i = \bigcap_{t=1}^{\infty}(x_1, \dots, x_i, x_{i+1}^t, \dots, x_d^t)R$$

(since J_i is closed in the $\mathfrak{m}$-adic topology on R). Thus, in an F-rational local ring, every ideal generated by part of a system of parameters is tightly closed. The colon-capturing theorem for quotients of Cohen-Macaulay rings may be applied, and then exactly the same proof as used in the Theorem at the end of the preceding lecture shows that R is Cohen-Macaulay. Thus, every F-rational ring is Cohen-Macaulay as well as normal.

This paragraph assumes additional background in algebraic geometry. A finitely generated algebra over a field K of characteristic 0 is said to have *rational singularities* if is Cohen-Macaulay, normal, and the higher direct images of the structure sheaf of a desingularization are 0. (This characterization is redundant, and there are other characterizations.) This notion is independent of base change of the field. In considering an algebra like this over a field K, K may be replaced by a subfield that is finitely generated over $\mathbb{Q}$ and contains the coefficients of the defining equations of the radical ideal that is used to define the algebra as a quotient of a polynomial ring. In fact, one can choose a finitely generated $\mathbb{Z}$-algebra $A \subseteq K$ and a finitely generated A-algebra R_A such that the coordinate ring of the original algebraic set is $R = K \otimes_A R_A$. By a theorem of Karen Smith and Nobuo Hara (cf. Karen E. Smith, *F-rational rings have rational singularities*, Amer. J. Math. **119** (1997), 159–180 and Nobuo Hara, *A characterization of rational singularities in terms of injectivity of Frobenius maps*, Amer. J. Math. **120** (1998) 981–996 R has rational singularities if and only if for all maximal ideals μ in Zariski open dense subset of the maximal spectrum of A, with $\kappa := A/\mu$ (note that this is a *finite* field) one has that $R_\kappa := \kappa \otimes_A R_A$ is F-rational. Thus, notions of "good behavior" defined in terms of tight closure and other positive characteristic phenomena can be used to characterize related notions of "good behavior" over fields of characteristic 0. There are many other examples, and there is a considerable literature on the relationship between characteristic p properties and properties defined over fields of characteristic 0.

Lecture of April 13

In this lecture we give a summary of the structure theory of complete local rings. The statements of some of the results (these will be clearly indicated) are required material. Complete proofs of the results stated in these notes will be provided in a Supplement, which will be both posted and distributed by e-mail. But going through the proofs of the results is optional.

Summary of the structure theory of complete local rings over a field

We begin with some of the structure theory of complete local rings in the case where the ring contains a field. One key point is that if $(R, \mathfrak{m}, K)$ is a complete local ring that contains a field, then R contains a field $\widetilde{K}$ such that the canonical surjection $R \twoheadrightarrow R/\mathfrak{m} = K$ carries $\widetilde{K}$ isomorphically onto K. $\widetilde{K}$ is called a *coefficient field* for R. This means that if a complete local ring contains any field, it contains an isomorphic copy of its residue class field. If R contains a field of characteristic 0, one may take any maximal subfield of R (such exist by Zorn's lemma) as the coefficient field. The proof of the result is much more difficult in characteristic $p > 0$. However, if K is perfect, the choice of $\widetilde{K}$ is unique: it must be $\bigcap_e F^e(R)$, the set of all elements of R that have p^e th roots in R for all $e \geq 1$. This does turn out to be a field: it is disjoint from $\mathfrak{m}$, since any element in it that is in $\mathfrak{m}$ must be in $\mathfrak{m}^{[p^e]}$ for all e and, hence, 0.

In equal characteristic 0 and other positive characteristic cases, the choice of $\widetilde{K}$ is usually not unique. However, it is typical to use the same letter K for both a choice of $\widetilde{K}$, i.e., a choice of coefficient field, as for the residue class field, and we usually do so in the sequel.

Two very important points in the structure theory: if $K \hookrightarrow R$ is a coefficient field for the complete local ring $(R, \mathfrak{m}, K)$, and $x_1, \ldots, x_n \in \mathfrak{m}$, there is unique continuous (with respect to the respective maximal ideal-adic topologies) K-algebra map from the formal power series ring $\theta : K[[X_1, \ldots, X_n]] \to R$ such that $X_i \mapsto x_i$, $1 \leq i \leq n$. If $x_1, \ldots, x_n$ generate $\mathfrak{m}$, this map is surjective. If $n = d = \dim(R)$ and $x_1, \ldots, x_d$ is a system of parameters for R, the map is injective, and R is module-finite over the image. Thus, if R is regular, $n = d$, and $x_1, \ldots, x_d$ is a minimal set of generators of $\mathfrak{m}$ (i.e., a regular system of parameters), then $\theta : K[[X_1, \ldots, X_d] \to R$ is an isomorphism. Thus, every complete local ring containing a field is a homomorphic image of a formal power series ring, and is also module-finite over a subring (necessarily of the same dimension) which is a formal power series ring. Both of these statements are analogues of statements that are true for finitely generated algebras over a field and polynomial rings. The second statement is analogous to Noether normalization. It also follows that a complete local ring containing a field is regular iff it is isomorphic with a formal power series ring $K[[x_1, \ldots, x_d]]$.

There is a very satisfactory structure theory for complete local rings that do not necessarily contain a field. These have what is called *mixed characteristic*: the residue class field has characteristic $p > 0$, while the ring itself has characteristic 0 or p^h for some $h \geq 2$. Complete Noetherian discrete valuation domains V in which a prime integer p generates the maximal ideal (like the p-adic integers) can be used as coefficient rings in the domain case (there cannot be a coefficient field, but the residue field is the residue field of one of these coefficient rings). In other cases, there may be a coefficient ring of the form V/p^hV. It is still true in mixed characteristic that every complete local ring is a homomorphic image of a formal power series ring $V[[X_1, \, \ldots \, , X_n]]$ with V as above. Every complete local domain R of mixed characteristic is module-finite over a subring of the form $V[[X_2, \, \ldots \, , \, X_d]$ where the images of $p, X_2, \, \ldots \, , \, X_d$ form a system of parameters in R. Moreover, every mixed characteristic complete regular local ring has either the form $V[[X_2, \, \ldots \, , \, X_d]$ (if p is not in the square of the maximal ideal) or else has the form $V[[X_2, \, \ldots \, , \, X_d, \, X_{d+1}]/(f)$, where $f = p - g$ and g is in the square of the maximal ideal of the formal power series ring. There is a complete treatment in the Supplement, but we won't use the mixed characteristic theory in this course.

We shall use the structure theory of complete local regular local rings in equal characteristic p to show that in prime characteristic $p > 0$, the Frobenius endomorphism and its iterations, i.e., its powers under compostion, are flat. It is then immediate that they are faithfully flat, since the extension of the maximal ideal $\mathfrak{m}$ underF^e is $\mathfrak{m}^{[p^e]}$, which is contained in $\mathfrak{m}$ and so a proper ideal. This will enable us to prove that all regular rings are F-regular in characteristic $p > 0$.

The Discussion that follows and the *statements* of the three Theorems on the next page are required material. The full proofs are given in the Supplement and are not required.

Discussion. Let $(R, \mathfrak{m}, . K)$ be a complete local ring that is an A-algebra for some ring A and let $x_1, \ldots , x_n \in \mathfrak{m}$. We have a unique A-homomorphism θ_0 of the polynomial ring $A[X_1, \, \ldots \, , X_n] \to R$ such that $X_i \mapsto x_i$, $1 \leq i \leq n$. This extends uniquely to the power series ring $B := A[[X_1, \, \ldots \, , X_n]]$ if we require continuity with respect to the $(X_1, \, \ldots \, , X_n)B$-adic and fm-adic topologies. To see this, consider an element $u \in B$ and let u_h be the sum of all terms of u involving only monomials in the power series for u of degree at most h. Then u is the limit of the u_n, which are polynomials, in the $(X_1, \, \ldots \, , X_n)B$-adic topology. Note that $\theta_0(u_{h+1}) - \theta_0(u_h)$ is an A-linear combination of monomials of degree $h + 1$ in the elements $x_i = \theta(X_i)$, and so is in $\mathfrak{m}^{h+1}$. Hence, the elements $\theta_0(u_h)$ form a Cauchy sequence in R, and have a unique limit in R, which we denote $\theta(u)$. Clearly, the continuity assumption forces the homomorphism extending θ_0 to be θ. It is easy to check that θ preserves addition and multiplication, that it is A-linear, and that it extends θ_0. This proves the existence and uniqueness of θ. In fact, if $\underline{i} := (i_1, \, \ldots \, , i_n)$ varies in $\mathbb{N}^n$, then

$$\theta : \sum_{\underline{i}} a_{\underline{i}} X^{i_1} \cdots X_n^{i_n} \mapsto \sum_{\underline{i}} a_{\underline{i}} x_1^{i_1} \cdots x_n^{i_n}.$$

We can now state:

Theorem. *Let notation be as in the preceding discussion.*

(a) If $A \to R \to K$ is a surjection and $x_1, \ldots, x_n$ generate $\mathfrak{m}$, then $\theta : A[[X_1, \ldots, X_n]] \to R$ is surjective.

(b) Let $K \hookrightarrow R$ be a coefficent field for R, so that $K \hookrightarrow R \twoheadrightarrow K$ is an isomorphism. Suppose that $x_1, \ldots, x_d$ is a system of parameters for R and that $n = d$. Then $\theta : K[[X_1, \ldots, X_n]] \to R$ is injective, and R is module-finite over the image, which is isomorphic to a formal power series ring.

(c) Suppose that R is regular, that $K \hookrightarrow R$ is a coefficient field, and the $x_1, \ldots, x_n$ is a regular system of parameters, i.e., a system of parameters that generates $\mathfrak{m}$. Then $\theta : K[[X_1, \ldots, X_n]]$ is an isomorphism.

For the proof, we refer to the Supplement on complete local rings, but the *statement* of this result is required material. We note that in part (b), the image of the map θ is often denoted $K[[x_1, \ldots, x_d]]$.

Since an Artin local ring that contains a field is automatically complete, we have:

Corollary. *An Artin local ring R that contains a field contains a coefficient field K, and so is a finite-dimensional vector space over K.*

The final statement in the Corollary just above is immediate from the fact that the length of the Artin local ring is finite and, when there is a coefficient field, length coincides with vector space dimension over the coefficient field.

The statement of the following very important result is required:

Theorem. *Every complete local ring that contains a field has a coefficient field.*

The proof is given in the Supplement.

Given the preceding two results, we immediately have the following result, whose statement is required material:

Theorem. *Let R be a complete local ring that contains a field.*

(a) R is a homomorphic image of a formal power series ring $K[[X_1, \ldots, X_n]]$.

(b) (Formal Noether normalization.) If $x_1, \ldots, x_d$ is a system of parameters for R, then R is module finite over the formal power series subring $K[[x_1, \ldots, x_d]]$.

(c) If R is regular local and $x_1, \ldots, x_d$ is a regular system of parameters, then R is isomorphic with the formal power series ring $K[[x_1, \ldots, x_d]]$. $\square$

Remark. The structure theorems show that formal power series rings over K have a great many K-automorphisms. We illustrate this point with one example. Consider the formal power series ring $K[[x, y, z]]$, with $\mathfrak{m} = (x, y, z)$. The elements $u := x + y^2 + z^3$, $v := y + x^7 + xz^{11}$, and $w := z + x^{13} + y^{19} + x^{67}y^{23}z^{101}$ are a regular system of parameters, since they generate $\mathfrak{m}/\mathfrak{m}^2$. Thus, $K[[u, v, w]] \subseteq K[[x, y, z]]$ is actually an equality, and x, y, and z can all be expressed as power series in u, v, and w. Moreover, there is an $\mathfrak{m}$-adically continuous K-automorphism of this formal power series ring that maps x, y, and z to u, v, and w, respectively. The higher degree terms in the expressions for u, v, and w were chosen more or less randomly.

Lecture of April 15

In this Lecture we first give two proofs of the (faithful) flatness of the Frobenius endomorphism (and, hence, of its iterates) for regular rings of positive prime characteristic p. Both reduce to the local case. The first then reduces to the complete case and utilizes the structure theory of complete regular local rings over a field. The second makes use of Problem **6.** in Problem Set #4, but ultimately depends on the homological characterization of regular local rings and understanding of Tor. The flatness of Frobenius is then used to prove that every ideal is tightly closed in a regular ring of positive prime characteristic p: in fact every submodule of every finitely generated module is tightly closed.

The remainder of the material is optional. First, the important that if every ideal is tightly closed, then every submodule of every module is tightly closed is proved *in complete generality.* The treatment uses one result in the literature that is not established in the course. Along the way, there is a discussion of Gorenstein local rings and of approximately Gorenstein local rings. It is shown that a Gorenstein Artin local ring is injective as a module over itself in the case where the ring contains a field. This is true more generally. A final section gives a treatment of tight closure for modules using the Frobenius functors introduced in Problem **5.** of the Problem Set #5. This approach makes it clear that the definition we gave earlier for tight closure of N in M is independent of the choices we made (such as the free module that is mapped onto M).

The flatness of the Frobenius endomorphism for all regular rings of positive prime characteristic

We next want to establish the assertion made earlier that the Frobenius endomorphism is flat for every regular Noetherian ring of prime characteristic $p > 0$. Faithful flatness is then obvious. We give two proofs of this: the first relies on the structure theory of complete local rings. In both proofs, we want to reduce to the case where the ring is local. In the first proof we then reduce to the case where the ring is complete local. We first observe the following:

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

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

and there is a commutative diagram

$$\begin{tikzcd}
S \otimes_R N \arrow[r, "\iota"] \arrow[d, "f"'] & S \otimes_R M \arrow[d, "g"'] \\
S \otimes_R \big(N/(m^tM \cap N)\big) \arrow[r, "\iota'"] & S \otimes_R \big(M/m^tM\big)
\end{tikzcd}.$$

The image $f(u)$ of u in $S \otimes_R \big(\big(N/(m^tM \cap N)\big)$ 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, $m^tM \cap N \subseteq m^hN$. Hence, the proof will be complete provided that we can show that the image of u is nonzero in

$$S \otimes_R (N/m^hN) \cong S \otimes_R \big((R/m^h) \otimes_R N\big) \cong (R/m^h) \otimes_R (S \otimes_R N) \cong (S \otimes_R N)/m^h(S \otimes_R N).$$

But

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

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

Lemma. *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 $N \subseteq M$ is flat 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 $N \subseteq M$, 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. □

We are now ready to prove:

Theorem. *Let R be a regular Noetherian ring of prime characteristic $p > 0$. Then the Frobenius endomorphism $F : R \to R$ is flat.*

Proof. To distinguish the two copies of R, we let S denote the right hand copy, so that $F : R \to S$. The issue of flatness is local on R, and if P is prime, then $(R - P)^{-1}S$ is the localization of S at the unique prime Q lying over P (if we remember that S is R, then Q is P), since the p th power of every element of $S - Q$ is in the image of $R - P$. Hence, there is no loss of generality in replacing R by R_P, and we henceforth assume that $(R, \mathfrak{m}, K)$ is local.

By the preceding Lemma, $F : R \to R$ is flat if and only if the induced map $\widehat{R} \to \widehat{R}$ is flat, and this map is easily checked to be the Frobenius endomorphism on $\widehat{R}$. We have now reduced to the case where R is a complete regular local ring. By the structure theory for complete regular local rings, we have $R = K[[x_1, \ldots, x_n]]$ where K is a field of characteristic p. By the final Theorem of the Lecture Notes of March 13, $F : K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ makes $K[x_1, \ldots, x_n]$ into a free algebra over itself. It follows that it is flat over itself, and this remains true when we localize at $(x_1, \ldots, x_n)$. By the preceding Lemma, we still have flatness after we complete both rings. Completing yields

$$F : K[[x_1, \ldots, x_n]] \to K[[x_1, \ldots, x_n]],$$

which proves the flatness result we need. □

Second proof of the flatness of Frobenius in regular rings This argument is very short, but depends both on the homological characterization of regular local rings and the use of the functor Tor. Consider $F : R \to R$. By Problem **6.** of Problem Set #4, it suffices to show that given a system of parameters $x_1, \ldots, x_d$ for R, its image under F is a regular sequence is the target copy of R. This is obvious, since the image $x_1^p, \ldots, x_d^p$ is a system of parameters for the target copy of R. □

Remark. It is also true that a Noetherian ring of positive prime characteristic p is regular if and only if the Frobenius endomorphism is flat. Cf. E. Kunz, *Characterizations of regular lcoal rings of characteristic* p, Amer. J. Math. **91** (1969) 772–784.

Regular rings are weakly F-regular: the general case

We can now give the application of this result that we have been intending for some time. We first generalize a previous lemma about flatness and its application to the Frobenius endomorphism over regular rings.

Lemma. *Let $R \to S$ be a flat ring homomorphism, let $H \subseteq G$ be R-modules, and let N be a finitely generated submodule of G. Identify $S \otimes_R H$ and $S \otimes_R N$ with submodules of $S \otimes_R G$. Then $(S \otimes_R H) :_S (S \otimes_R N) = S \otimes (H :_R N)$.*

Let $u_1, \dots, u_n$ generate N and consider the composite map $R \to G^{\oplus n} \twoheadrightarrow (G/H)^{\oplus n}$ such that the map on the left sends $r \mapsto (ru_1, \dots, ru_n)$ and the map on the right is the direct sum of n copies of the quotient surjection $G \twoheadrightarrow G/H$. The kernel of this map is $H : RN$, so that $0 \to H :_R N \to R \to (G/H)^{\oplus n}$ is exact. When we apply $S \otimes_R \_$, the fact that S is R-flat implies that

$$0 \to S \otimes_R (H :_R N) \to S \to \big((S \otimes G)/(S \otimes H)\big)^{\oplus n}$$

is exact. The required result follows because the kernel of the map on the right is also $(S \otimes_R H) :_S (S \otimes_R N)$. □

If we apply this when $S = R$ is regular, $R \to R$ is the eth iteration of the Frobenius endomorphism, G is free, and N is generated by one element u, we obtain:

Corollary. *If R is regular of characteristic $p > 0$, G is free, $H \subseteq G$, and $u \in G$, then for all $q = p^e$, $e \in \mathbb{N}$, we have that $H^{[q]} :_R u^q = (H :_R u)^{[q]}$.* □

Theorem. *Let R be a regular Noetherian ring of prime characteristic $p > 0$. Then every ideal I of R is tightly closed. In fact, every submodule of every finitely generated module is tightly closed.*

Proof. It suffices to prove the second assertion, and by it suffices to prove that every submodule H of every finitely generated free R-module G is tightly closed.

Suppose $u \in H^* - H$ in G and $c \in R$ not in any minimal prime and satisfies $cu^q \in H^{[q]}$ for all $q \gg 0$. We may replace R by its localization at a maximal ideal $\mathfrak{m}$ in the support of $(I + Ru)/I$, G by $G_\mathfrak{m}$, H by $H_\mathfrak{m} \subseteq G_\mathfrak{m}$ and u by its image in the local ring $R_\mathfrak{m}$. The image of c in $R_\mathfrak{m}$ is still not in any minimal prime, i.e., it is not 0. Hence, we still have that $u \in H^*_\mathfrak{m} - H_\mathfrak{m}$ in $G_\mathfrak{m}$. Thus, we may assume without loss of generality that R is local. Then for some q_0,

$$c \in \bigcap_{q \geq q_0} H^{[q]} :_R u^q = \bigcap_{q \geq q_0} (H :_R u)^{[q]} \subseteq \bigcap_{q \geq q_0} m^{[q]} \subseteq \bigcap_{q \geq q_0} m^q = (0),$$

a contradiction. The leftmost equality in the display follows from the Corollary above. □

If every ideal is tightly closed, then every submodule of every finitely generated module is tightly closed

The rest of this lecture consists entirely of optional material, first a section devoted to the proof of the characteristic $p > 0$ fact stated just above. Thus, either condition may be used to define weakly F-regular rings. The material is self-contained, except for one fact not proved in this course. A reference is provided. The "external" statement that we need is shown in boldface in the first full paragraph of the page after the next.

The last part of the lecture, also optional, gives a treatment of tight closure for modules using Frobenius functors.

Discussion. It is always true that if a Noetherian ring of positive prime characteristic is weakly F-regular in the sense that every ideal is tightly closed, then every submodule of every finitely generated module is tightly closed. In this discussion we explain why, but part of the argument relies on a reference to material outside the course. We also need a fact about zero-dimensional Gorenstein rings, but a self-contained treatment for the case where the ring contains a field is provided.

Beginning of the argument. Suppose that every ideal of R is tightly closed. Suppose $N \subseteq M$ are finitely generated modules such that $u \in M$ is in the tight closure of N but not in N. Then this remains true when we localize at a suitable maximal ideal of R, one that contains the annihilator of the class of u in M/N. Hence, we may assume without loss of generality that $(R,\, \mathfrak{m},\, K)$ is local. Second, we may replace N by a maximal submodule N' of M such that $N \subseteq N'$ and $u \notin N'$. We replace M by M/N' and u by its image in M/N'. Thus, we may assume that u is in every nonzero submodule of M and is in the tight closure of 0 but not 0. This implies that the only associated prime of M is $\mathfrak{m}$: if $P \neq 0\mathfrak{m}$ were associated, so $R/P \hookrightarrow M$ and u would in (the image of) all the powers of $\mathfrak{m}/P$, and the intersection of those powers is 0. It follows that M has finite length, and we can choose n such that $\mathfrak{m}^n$ kills M.]. Moreover, since u is in every nonzero submodule of M, it must be, up to a unit multiplier, the unique nonzero element in the socle of M (if the socle had dimenson two or more as K-vector space, u could not be a multiple of each of two linearly independent elements in the socle).

Digression: Gorenstein and approximately Gorenstein rings. Because every ideal of the local ring R is tightly closed, we know that R is normal. The paper [M. Hochster, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977) 463–488] introduces and studies the notion of *approximately Gorenstein rings*. A local ring $(R,\, \mathfrak{m},\, K)$ is called *Gorenstein* if it is Cohen-Macaulay of type 1. (It is not obvious but true that this property passes to localizations of the ring at prime ideals: see the notes on Local Cohomology that have been added to the Web page for the course.) A Noetherian ring is then define to be Gorenstein if its localizations at all prime ideals are Gorenstein). The type condition means that if $x_1,\, \dots\, , x_d$ is any system of parameters, where d is the dimenson of R, then the Artin ring $R/(x_1,\, \dots\, , x_d)R$ has a one-dimensional socle, and this is equivalent to the condition that the socle, which is the annihilator of $\mathfrak{m}$ in $R/(x_1,\, \dots\, , x_d)R$, is isomorphic to one copy of $R/\mathfrak{m}$. Under this assumption it is easy to see that the socle is contained in every nonzero submodule, because every nonzero submodule has at least one element killed by m.[2] In general, the condition for a local ring of dimenson 0 (i.e., an Artin local ring) to be Gorenstein is that the socle be one-dimensional: in dimension 0, the Cohen-Macaulay assumption is automatic.

A local ring $(R,\, \mathfrak{m},\, K)$ is called *approximately Gorenstein* if for every power $\mathfrak{m}^n$ of the maximal ideal, there is an $\mathfrak{m}$-primary ideal I such that $I \subseteq \mathfrak{m}^n$ and R/I is Gorenstein.

[2] If the submodule is N take s maximum such that $\mathfrak{m}^s N \neq 0$, and then every element of $\mathfrak{m}^s N$ is in the socle. Here, s may be 0, in which case N itself is killed by $\mathfrak{m}$.

Note that an $\mathfrak{m}$-primary ideal I_n has the property that R/I_n is Gorenstein if and only if I is *irreducible*, i.e., not the intersection of two strictly larger ideals. Every Gorenstein ring R is approximately Gorenstein: if R is 0-dimensional, we can take all the I_n to be 0, while if the dimension of R is $d > 0$ and $x_1, \ldots, x_d$ is a system of parameters for R, we may take $I_n = (x_1^n, \ldots, x_d^n)R$. It is clear that R/I_n is Gorenstein, since $x_1^n, \ldots, x_d^n$ is a system of parameters for R.

It turns out that being approximately Gorenstein is not a strong condition on R. In the paper referenced above, the condition is characterized, and it is shown that **every normal local ring is approximately Gorenstein**, which is what we need here.[3]

The other fact that we need is that *a 0-dimensional Gorenstein local ring is an injective module over itself.*[4] This is a very important result and is proved, for example, in the addition to the Web page on Local Cohomology, which has been posted. We give a self-contained proof here for the case where the ring contains a field (assuming the existence of coefficient fields from the structure theory), which is the only case we need.

Proof that a 0-dimensional Gorenstein local ring that contains a field is injective as a module over itself. Let $(R, \mathfrak{m}, K)$ be a 0-dimensional local ring with a one-dimensional socle. Suppose that R contains a field. Then R has a coefficient field $K \subseteq R$: we fix such a coefficient field. We shall show that $E = \mathrm{Hom}_K(R, K)$ is an injective R-module (the R-module structure on the first input gives an R-module structure on E) and that it is isomorphic with R. This proves that R is injective as an R-module. The fact that E is injective follows from the following isomorphism of functors: $M \to \mathrm{Hom}_R(M, E)$ and $M \to \mathrm{Hom}_K(M \otimes_R, K)$. The latter is clearly exact, and the isomorphism is a consequence of the adjointness of tensor and Hom: $\mathrm{Hom}_K(M \otimes_R, K) \cong \mathrm{Hom}_R\big(M, \mathrm{Hom}_K(R, K)\big)$. To show that $R \cong \mathrm{Hom}_K(R, K)$ as an R-module, first note that since length is the same as K-vector space dimension here, they have the same length. To complete the proof, let $K \cong Ku = Ru$ be the socle in R. Choose a K-linear map $\theta : R \to K$ such that $u \mapsto 1$. We shall show that θ is not killed by any nonzero r in R. It follows that $R \cong R\theta \subseteq E$. But then since $R\theta$ has the same length as E, they are equal. To see that $r\theta \neq 0$, note that rR must meet Ku, and it follows that there exists $a \in R$ such that $ar = u$. Then $r\theta(a) = \theta(ar) = \theta(u) = 1$, so $r\theta$ is not 0. $\square$

Conclusion of the argument. We now come back to the situation at the end of the paragraph labeled **Beginning of the argument.** As already observed we know that R is normal, and so R is approximately Gorenstein. Thus, R has an irreducible $\mathfrak{m}$-primary ideal I such that $I \subseteq \mathfrak{m}^n$, where $\mathfrak{m}^n$ kills M. Hence, M is a module over $A := R/I$, which is a 0-dimensional Gorenstein ring. Consider the map from $Ru \cong K = R/\mathfrak{m}$ to R/I that identifies u with a generator of the socle in A, which is one copy of $R/\mathfrak{m}$. Since A is injective as an A-module, this extends to an A-linear map $\alpha : M \to A$. This map must be injective: if the kernel were nonzero it would contain u, and u does not map to 0. Thus,

[3] It is also shown that every local ring that has depth at least two on its maximal ideal is approximately Gorenstein, and that every reduced excellent local ring is approximately Gorenstein.

[4] In fact, a local ring is Gorenstein if and only if it has finite injective dimension as a module over itself. In this case, the Cohen-Macaulay property follows. Moreover, the injective dimension is always the same as the Krull dimension. Again, this is proved in the addition to the Web page on Local Cohomology.

$M \hookrightarrow R/I$, and this is also an embedding as an R-modules. Since u is in the tight closure of 0 on M, its image v in R/I is in the tight closure of 0 in R/I. Suppose v is the image of w in R. Then w is in the tight closure of I in R, but not in I, a contradiction. $\square$

A functorial treatment of tight closure for modules

The material in this section is optional, although it may be helpful to read the more detailed treatment here of the Frobenius functors (also called *Peskine-Szpiro functors*) that are introduced in Problem **5.** of the Problem Set #5. The new treatment makes it clear that whether an element of M is in the tight closure of a submodule $N \subseteq M$ is independent of the choices (such as a free module mapping onto M) in our original definition. The fact that this definition is equivalent to the earlier one is proved at the end of the lecture.

Remark. Let S be Noetherian of positive prime characteristic p. It is important to note that if R is a homomorphic of S, and $N \subseteq M$ are Noetherian R modules, then the tight closure of N in M **depends very heavily** on whether one is worknig over R or S. This is already true in the case of ideals. E.g., let $S = K[[x, y]]$ and $R = S/(x^3 - y^2)S \cong K[[t^2, t^3]]$. Working over S, the submodule xR of R is tightly closed, since S is regular. But working over R, the tight closure of xR is $(x, y)R$ (note that $K[[t]]$ is a module-finite extension of R, and the image of y is $t^3 \in xK[[t]] \cap R = t^2K[[t]] \cap K[[t^2, t^3]]$.

Much more about tight closure may be found in the addition to the Web page entitled *Foundations of Tight Closure Theory*, which are lecture notes from a course on tight closure.

If R is a ring, we use the notation R° to denote the set of elements in R not in any minimal prime. These are the elements that are available to be the constant element of R used as a multiplier in the definition of tight closure.

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

Base change. If $f : R \to S$ is an ring homomorphism, there is a base change functor $S \otimes_R \_$ from R-modules to S-modules. It takes the R-module M to the R-module $S \otimes_R M$ and the map $h : M \to N$ to the unique S-linear map $S \otimes_R M \to S \otimes_R N$ that sends $s \otimes u \mapsto s \otimes h(u)$ for all $s \in S$ and $u \in M$. This map may be denoted $\mathrm{id}_S \otimes_R h$ 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 $\bigl(r_{ij}\bigr)$ to the cokernel of the matrix $\bigl(f(r_{ij})\bigr)$.

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

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

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

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

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

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

The Frobenius functors. Let R be a ring of positive prime 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 $\mathcal{F}_R^e$. This is the same as the base change functor for the homomorphism $F^e : R \to R$, where $F^e(r) = r^{p^e}$ for all $r \in R$, by the iterated application of (11) above. When the ring is clear from context, the subscript ${}_R$ is omitted, and we simply write $\mathcal{F}$ or $\mathcal{F}^e$.

We then have, from the corresponding facts above:

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

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

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

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

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

(6) $\mathcal{F}^e$ is right exact: if
$$M' \to M \to M'' \to 0$$
is exact, then so is
$$\mathcal{F}^e(M') \to \mathcal{F}^e(M) \to \mathcal{F}^e(M'') \to 0.$$

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

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

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

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

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

We also note the following: given a homomorphism $g : R \to S$ of rings of positive prime 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 positive prime 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.

Tight closure for modules Let R be a ring of positive prime characteristic p and let $N \subseteq M$ be finitely generated R-modules. 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 $c \in R^\circ$,

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

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

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

(a) *N^*_M is an R-module.*

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

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

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

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

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

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

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

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

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

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

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

Let R and S be Noetherian rings of positive prime 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. *Let $R \to S$ be a homomorphism of Noetherian rings of positive prime 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. □

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

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

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

Proof. The final statement is just a special case of the Theorem. The "only if" part follows from the preceding Proposition. It remains to prove that if u is in the tight closure modulo every P_i, then it is in the tight closure. This means that for every i there exists $c_i \in R - P_i$ such that for all $q \gg 0$, $c_iu^q \in N^{[q]} + P_iF^e(M)$, 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 ith 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 $c^q u^q \in N^{[q]}$ for all $q \geq q_1 q_0$. $\square$

Let R have minimal primes $P_1, \ldots, P_n$, and let $J = P_! \cap \cdots \cap P_n$, the ideal of nilpotent elements of R, so that $R_{\text{red}} = R/J$. 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. *Let R be a ring of positive prime characteristic p , 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 $R_{\text{red}} = R/J$.*

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

We also note the following easy fact:

Proposition. *Let R be a ring of positive prime characteristic p . 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 $N^{[q_0q]}$. $\square$

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

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

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

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

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

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

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

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

The following result, used earlier without proof, is very useful in thinking about tight closure.

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

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

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

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

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

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

We earlier 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 then have the problem of proving that the notion is independent of the choice of free basis. Moreover, with the earlier approach, we needed 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.

Lecture of April 17

We first discuss the tight closure proof that direct summands of regular rings are Cohen-Macaulay. This is the only part of this material that is not optional.

We then introduce the notion of integral dependence on an ideal and integral closure of ideals. A Supplement on integral closure has been provided. We then give the amazingly easy tight closure proof of a strengthend form of the Briançon-Skoda theorem. All of this material is optional in the sense that it will not be covered on the last quiz.

Direct summands of regular rings are Cohen-Macaulay

The following result application of tight closure theory is immediate from what we have already done.

Theorem. *A direct summand R of a weakly F-regular domain S is weakly F-regular. Hence, a direct summand of a regular ring of positive prime characteristic p that is a homomorphic image of a Cohen-Macaulay ring is Cohen-Macaulay.*

Proof. The first statement is part of the Theorem stated at the bottom of the first page of the Lecture of April 3. The second statement is the immediate from the final Theorem of the Lecture of April 8. □

Again, material in the lecture notes beyond this point will not be tested in the remaining quiz.

Discussion. The restriction that R be a homomorphic image of a Cohen-Macaulay ring is not needed. One can localize R at a maximal ideal and then S at prime lying over the maximal ideal of R while maintaining the property that every ideal of R is contracted from S, and so assume that both are local. One can then complete R with respect to its maximal ideal $\mathfrak{m}$ and S with respect to $\mathfrak{m}S$ and so assume that R is complete, and that every ideal is contracted from S. Now R is a homomorphic image of a regular ring, and one has colon-capturing. If $x_1, \dots, x_d$ is a system of parameters for R, and $I_i = (xi_1, \dots, i_)$ for $0 \leq i \leq d-1$, then $I_i : x_{i+1} \subseteq I*$ in R, and this is contained in $(I_iS)^*$ in S and in R. But $(I_iS)^* = IS$ since S is regular, and $I_iS \cap R = I_i$. □

The extension of tight closure theory to rings containing the rational numbers gives a proof of the same result for rings containing the rationals, and the result has recently been extended to mixed characteristic by perfectoid methods.

The Briançon-Skoda theorem

This section is optional.

We first discuss the notion of the integral closure of an ideal in the Noetherian case.

Theorem. *Let R be Noetherian, I an ideal, and let $r \in R$. The following conditions are equivalent, and define the condition that an element $r \in R$ be integral over an ideal I of R.*

(1) *There is an element c not in any minimal prime of R such that $cr^n \in I^n$ for all $n \gg 0$ (equivalently, for infinitely many values of n).*
(2) *There is an element c not in any minimal prime of R such that $cr^n \in I^n$ for infinitely many values of n.*
(3) *For every map of R into a Noetherian discrete valuation domain V, the image of r is IV.*
(4) *For every minimal prime $\mathfrak{p}$ of R and Noetherian discrete valuation domain between $R/\mathfrak{p}$ and its fraction field, the image of r is in IV.*
(5) *rt is integral over the Rees ring $R[It] \subseteq R[t]$ (the latter is the polynomial ring in one variable t overR).*
(6) *For some positive integer n, the element r satisfies a polynomial equation of the form*
$$r^n + i_1r^{n-1} + \cdots + i_jr^{n-j} + \cdots + i_{n-1}r + i_n = 0$$
where the coefficient $i_j \in I^j$.

Note that it suffices if $r^n \in I^n$: let $i_n := r^n$, and use the equation $r^n - i_n = 0$.

For our purposes here, we will take (2) as the definition of when an element is integral over an ideal in the Noetherian case. When R is not Noetherian, (5) and (6) are equivalent and imply the other conditions and either may be taken as the definition of when r is in the integral closure of I. In all cases, the set of elements integral over I is an ideal called the *integral closure* of I, and denoted $\overline{I}$. There is a treatment of integral closure of ideals in a new Supplement on the Web page. There is a great deal more on the subject in the Lecture Notes for Math 615, Winter 2019.

We first note:

Theorem. *Let R be a Noetherian ring of positive prime characteristic p. If $r \in I^*$, then $r \in \overline{I}$. In other words, $I^* \subseteq \overline{I}$.*

Tight closure is typically much smaller than integral closure. For example in $K[x, y]$ or $K[[x, y]]$, where x, y are indeterminates, the ideal (x^n, y^n) is tightly closed for all integers n. But its integral closure contains $(x, y)^n$, since if $i+j = n$, $(x^iy^j)^n = (x^n)^i(y^n)^j \in (x^n, y^n)^n$.

The following result was first proven for algebras over the complex numbers and convergent power series rings over the complex numbers by analytic methods.

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

There are many refined versions, but, for simplicity, we only consider this statement here.

Later, an algebraic proof of the Briançon-Skoda theorem was given by J. Lipman and A. Sathaye that is valid in all characteristics, including mixed characteristic: we refer to the Lecture Notes from Math 615, Winter 2019 for a full treatment.

Tight closure theory permits an extremely simple proof of a stronger result in the case where the ring contains a field, which we want to give here. We first want to note two corollaries of the Briançon-Skoda theorem, but we refer to the Lecture Notes from Math 615, Winter 2019 for the details of how they follow from it.

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

This answers affirmatively a question raised by John Mather.

Second:

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

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

Here is the tight closure version in characteristic $p > 0$.

Theorem (Generalized Briançon-Skoda theorem). *Let R be a ring of positive prime characteristic p . Let $I = (f_1, \dots, f_n)$ be an ideal of R generated by n elements. Then $\overline{I^n} \subseteq I^*$.*

Proof. Suppose $r \in \overline{I^n}$ and c is an element not in any minimal prime of R such that $cr^h \in I^h$ for all $h \gg 0$. Then when $h = q = p^e \gg 0$ we have $cr^q \in \big((f_1, \dots, f_n)^h\big)^q = (f_1, \dots, f_n)^{nq} \subseteq (f_1^q, \dots, f_n^q)$ because, in a monomial of degree nq in n elements, at least one of the exponents on one of the elements must be at least q. Hence, $cr^q \in I^{[q]}$ for all $q \in 0$. □

We now recover the usual Briançon-Skoda theorem not just for regular rings, but for every weakly F-regular ring, since in that case $I^* = I$.

Remark. One easily gets the same result for algebras containing the rational numbers using the notion of tight closure in equal characteristic 0 that was discussed briefly earlier, and this recovers the original Briançon-Skoda theorem.

Lecture of April 20

Let $1 \leq t \leq r \leq s$ and let K be a field. This final lecture is devoted to proving that over any field K, if one considers the polynomial ring $S = K[x_{ij} : 1 \leq i \leq r,\, 1 \leq j \leq s]$ in the entries of an $r \times s$ matrix $X = \bigl(x_{ij}\bigr)$ then $I_t(X)$, the ideal generated by the $t \times t$ minors of X is prime, and the ring $S/I_t(X)$ is a Cohen-Macaulay domain. It is, in fact, also normal.

There are several ways to approach the problem of proving that large classes of ideals are prime. One is the method of Hodge algebras (also called algebras with straighten law), and you can read about them in the book of W. Bruns and J. Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics **39**, Revised Edition, Cambridge University Press, 1993. We shall prove the result here using a different method: that of *principal radical systems*, initially developed in J. A. Eagon and M. Hochster, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93** (1971) 1020–1058. This method typically involves enlarging the class of ideals considered to a very large family consisting of radical ideals, containing the prime ideals of the primary decomposition of every ideal in the family, and with the property that whenever I is in the family, there is an ideal in the family generated by I and one additional element. One then establishes that the family consists entirely of radical ideals by what amounts to Noetherian induction: one proves the result for a given ideal in the family assuming it for all the larger ideals in the family. The base of the induction is easy because the maximal elements of the family are generated by subsets of the indeterminates. One uses the fact that $I + fS$ is radical to deduce that I is radical. This leads to an understanding of all of the ideals and of their primary decompositions. The application is usually to finitely generated graded algebras over a field K.

The Cohen-Macaulay property for the primes and some of the radical ideals in the family is then deduced, again by Noetherian induction, by one of two methods. In some cases, one uses that there is a nonzerodivisor f modulo I such that $I + fS$ is in the family. One can then deduce the Cohen-Macaulay property for S/I from the Cohen-Macaulay property for $S/(I + fR) \cong (S/I)/f(S/I)$, where one knows inductively that for the larger ideal $I + fS$, the quotient $S/(I + fS)$ is Cohen-Macaulay. In other cases, one deduces that $S/(I \cap J)$ is Cohen-Macaulay from the Cohen-Macaulay property for the quotients by the larger ideals I, J, and $I + J$. There are also techniques that work for more complicated intersections, but we will not need them for the case of determinantal ideals. In the situation where one has homogenous ideals I, J in a polynomial ring. it turns out that if I and J both have height h while $I + J$ has height $h + 1$ and all of S/I, S/J, and $S/(I + J)$ are Cohen-Macaulay, then $S/(I \cap J)$ is also Cohen-Macaulay. This is deduced using the fact that there is a short exact sequence

$$0 \to S/(I \cap J) \to (S/I) \oplus (S/J) \to S/(I + J) \to 0$$

along with standard facts about depth: see page 213 (the fifth page of the notes for this lecture), and its Corollary on the following page.

For pedagogical reasons we first give the proof that ideals of minors define Cohen-Macaulay domains for the case of 2×2 minors, and then we consider the general case. This is not efficient, but should make the ideals of the argument clearer.

The method of principal radical systems is based on two simple lemmas, stated below.

Lemma. *Let R be a Noetherian ring that is either local or $\mathbb{N}$-graded, and let $x \in R$ be in the maximal ideal or be a form of positive degree. Suppose that N is the nilradical of R, that N is prime, that $x \notin N$, and that R/xR is reduced. Then $N = 0$, i.e., R is a domain.*

Proof. Suppose that $u \in N$. Since R/xR is reduced, we must have that $u = xv$ for some $v \in R$. Since $xv \in N$, $x \notin N$, and N is prime, we must have that $v \in N$. Therefore $N = xN$. By Nakayama's lemma for local or graded rings, $N = 0$. □

By applying this Lemma to R/I in the situation below, we obtain:

Corollary. *Let R be a Noetherian ring that is either local or $\mathbb{N}$-graded, and let $x \in R$ be in the maximal ideal or be a form of positive degree. Suppose that I is a (homogeneous in the graded case) proper ideal of R with radical P, where P is prime, that $x \notin P$, and that $P + xR$ is radical. Then $I = P$, i.e., I is prime.*

The next Lemma has various generalizations that may prove useful, but we shall stick with the simplest case.

Lemma. *Let R be Noetherian, let I be an ideal of R, let J be the radical of I, and suppose that $J \subseteq P$ where P is prime. Suppose that $I + xR$ is radical where $x \notin P$, and that $xP \subseteq I$. Then $I = J$, i.e., I is radical.*

Proof. Suppose that $u \in J$. Then $u \in I + xR$, say $u = i + xr$, where $i \in I$ and $r \in R$. Then $xr = u - i \in J \subseteq P$, and so $r \in P$. Since $xP \subseteq I$, we have that $xr \in I$ and so $u = i + xr \subseteq I$. □

We want to use these lemmas to prove the following result:

Theorem. *Let K be a field, let r and s be positive integers, let t be an integer with $1 \leq t \leq \min\{r, s\}$, and let X be an $r \times s$ matrix of indeterminates over K. Then $I_t(X)$ is a prime ideal, i.e., $K[X]/I_t(X)$ is a domain.*

The proof will take a while. The idea is to include $I_t(X)$ in a much larger, but finite, family of ideals to which we can apply the lemmas above. The ideals are typically radical rather than prime. The result is proved by reverse induction, in that the largest ideal(s) in the family are shown to be radical first. The family has the property that for each ideal I in it that is not maximal in the family, there is a larger ideal of the form $I + xR$ in the family, which will be known to be radical from the induction hypothesis.

We shall show first that the ideals $I_t(X)$ have radicals that are prime. Thus, once we show that they are radical, it will follow that they are prime.

Note that if L is the algebraic closure of K and R is a K-algebra, $R \subseteq L \otimes_K R$, and so to show that R is reduced or a domain it suffices to show the corresponding fact for $L \otimes_K R$. Thus, the problem we are discussing reduces to the case where K is algebraically closed, and we assume this from here on. This will enable us to take a naive approach to the material we need from algebraic geometry, which will involve only basic facts about closed algebraic sets in affine spaces $\mathbb{A}^N_K$.

Note that showing that $\mathrm{Rad}\,(I_t(X))$ is prime is equivalent to showing that $V(I_t(X))$ is an irreducible closed algebraic set. We think of points of $\mathbb{A}^{rs}_K$ as corresponding to $r \times s$ matrices over K. Then $V(I_t(X))$ is precisely the set of $r \times s$ matrices of rank $\leq t-1$.

Proposition. *Let r, s, and t be as above. Let A be an $r \times s$ matrix over a field K. Then A has rank $\leq t-1$ if and only if A factors BC where B is an $r \times (t-1)$ matrix over K and C is a $(t-1) \times s$ matrix over K.*

Proof. We think of A as giving a linear map $K^s \to K^r$, where K^s is interpreted as $s \times 1$ columns. The rank is at most $t-1$ if and only if the image has dimension $\leq t-1$, i.e., if and only if the map factors $K^s \to K^h \to K^r$ where $h \leq t-1$. We may think of K^{t-1} as $K^h \oplus K^{t-1-h}$ and extend the map $K^h \to K^r$ to the additional summand K^{t-1-h} by letting it be 0. This gives a factorization $K^s \to K^{t-1} \to K^r$ for A which yields that $A = BC$, as required, while any linear map with such a factorization obviously has rank at most $t-1$. □

Corollary. *With notation as above, $V(I_t(X))$ is irreducible.*

Proof. Think of $\mathbb{A}^{(r+s)(t-1)} \cong \mathbb{A}^{r(t-1)}_K \times \mathbb{A}^{(t-1)s}_K$ as indexing pairs of matrices $(B,\, C)$ where B is $r \times (t-1)$ and C is $(t-1) \times s$. We have a map $\mathbb{A}^{(r+s)(t-1)} \to V((I_t(X))$ that sends $(B,\, C) \mapsto BC$, and by the preceding Proposition this map is surjective. Since $\mathbb{A}^{(r+s)(t-1)}$ is irreducible and the image of an irreducible is irreducible, $V(I_t(X))$ is irreducible. □

Of course, this establishes that $\mathrm{Rad}\,(I_t(X))$ is prime.

For heuristic reasons, we now carry through the proof that $I_t(X)$ is radical first for the case where $t = 2$. Let $J_{k,h,a}(X) = J_{k,h,a}$ denote the ideal generated by the entries of the first h rows of X, the first k columns of X, and the first a entries of the $(h+1)$ st row of X. Here, $0 \leq k \leq s$, $0 \leq h \leq r$, and $0 \leq a \leq s$. If $h = r$ or $k = s$ all the variables have been killed and $a = 0$ is forced. We also abbreviate $J_{k,h,0} = J_{k,h}$ and $J_{0,0,a} = J_a$. Note that $J_{k,h,a} = J_{k,0} + J_{0,h,a}$. If $a \leq k$, $J_{k,h,a} = J_{k,h}$. Certain ideals have more than one description: e.g., if $h < r$, $J_{k,h,s} = J_{k,h+1,0}$.

We shall prove by induction that all of the ideals $I_2(X) + J_{k,h,a}(X)$ are radical, and prime if $a = 0$. We assume the result for smaller matrices of indeterminates. Evidently, $I_2(X) + J_{s,r} = J_{s,r}$ is the ideal generated by all the indeterminates and is maximal. We now consider one ideal $I = I_2(X) + J_{k,h,a}(X)$ in the family, and assume that all larger ideals in the family are radical. We need to show that I is radical.

We can simplify things a bit as follows. Let X' be the $(r-h)\times(s-k)$ matrix in the lower right corner of X. As noted above we may assume that $a \geq k$. Then we have an obvious isomorphism

$$K[X]/\bigl(I_2(X)+J_{k,h,a}(X)\bigr) \cong K[X']/\bigl(I_2(X')+J_{a-k}(X')\bigr)$$

induced by the K-algebra surjection $K[X] \twoheadrightarrow K[X']$ that fixes each indeterminate in X' while sending the other indeterminates to 0. Since we know the result for the smaller matrix X' if either h or k is positive, there is no loss of generality in assuming that $h=k=0$. Likewise, we may assume that $0 \leq a \leq s-1$. Finally, if either r or s is 1, then $I_2(X)=0$, and the ideal is generated by a subset of the variables and is clearly prime. Henceforth we assume that $r, s \geq 2$.

Thus, $I = I_2(X)+J_a$ where $0 \leq a \leq s-1$. Let $x = x_{1,a+1}$. Since we know that larger ideals in the family are radical, we have that $I_2(X)+J_{a+1}$ is radical, and this is $I+(x)$. We consider two cases.

(1) $a=0$. In this case, we know that $\mathrm{Rad}\,(I)$ is prime. The result now follows from the corollary to the first lemma, provided that we know that x is not in the radical of I. This follows because we can specialize x_{11} to 1 and all other variables to 0 and we get a point of $V(I)$ where $x_{11} \neq 0$. □

(2) $1 \leq a \leq s-1$. For every i,j such that $2 \leq i \leq r$, $1 \leq j \leq a$, consider the 2×2 submatrix of X formed by the intersection of the first and $i\,th$ rows of X with the j th and $a+1$ st columns, namely:

$$\begin{pmatrix} x_{1,j} & x_{1,a+1} \\ x_{i,j} & x_{i,a+1} \end{pmatrix}.$$

The determinant of this matrix is in $I_2(X)$, and so $x_{1,j}x_{i,a+1} - x_{i,j}x \in I_2(X) \subseteq I$. Since $x_{1,j} \in J_a \subseteq I$ as well, we have that $xx_{i,j} \in I$. Let $P = I_2(X)+J_{a,0}(X)$. This is a larger ideal of our family, and is therefore radical, by the induction hypothesis. But the quotient by it is $\cong K[X']/I_2(X')$, where X' is the submatrix of X formed by the last $s-a$ columns of X, and so the radical is prime. Thus, P is a prime ideal containing J, and is generated over I by the elements $x_{i,j}$, $2 \leq i \leq r$, $1 \leq j \leq a$. It follows that $xP \subseteq I$. Finally, $x \notin P$, since we get a point of $V(P)$ by specializing so that $x_{1,a+1}=1$ while every other indeterminate is specialized to 0. The fact that I is radical now follows from the second lemma. □

We next want to use the work that we have done on the ideals $I_2(X)$ to prove that the rings $K[X]/I_2(X)$ are all Cohen-Macaulay rings. We first need to calculate the dimensions of the rings $K[X]/I_2(X)$.

Proposition. *Let X be an $r\times s$ matrix of indeterminates. The localization of $R = K[X]/I_2(X)$ at the element $x = x_{1,1}$ is isomorphic with the localization of the polynomial ring $S = K[x_{i,1}, x_{1,j} : 1 \leq i \leq r,\ 1 \leq j \leq s]$ at the element $x = x_{1,1}$. Hence,* $\dim(R) = \dim(R_x) = r+s-1$.

Proof. For $i \geq 2$, $j \geq 2$ the equation given by the vanishing of the 2×2 minor formed the first and i th rows and the first and j th columns is

$$x_{1,1}x_{i,j} - x_{1,j}x_{i,1} = 0$$

which is equivalent to

$$(*) \quad x_{i,j} = x_{1,j}x_{i,1}/x$$

in R_x. Consider the K-algebra homomorphism $K[X] \to S_x$ that fixes $x_{i,j}$ if $i = 1$ or if $j = 1$, and otherwise sends $x_{i,j} \mapsto x_{1,j}x_{i,1}/x$. It is straightforward to verify that the map kills $I_2(X)$ and so induces a surjection $R_x \twoheadrightarrow S_x$. The inclusion $S \subseteq K[X]$ induces a map $S_x \to R_x$. The composition $(R_x \to S_x) \circ (S_x \to R_x)$ is clearly the identity on S_x, and the composition $(S_x \to R_x) \circ (R_x \to S_x)$ is the identity on R_x because of the displayed relations $(*)$. The statement about dimensions is clear, since $\dim(S_x) = \dim(S) = r + s - 1$. □

We may also argue as follows in calculating the dimension of R, which is the same as the dimension of $V(I_2(X))$. Consider the open set where the first row of the matrix is nonzero. The first row varies in $\mathbb{A}^s_K$ (with the origin deleted), i.e., in a variety of dimension s. Each of the other $r-1$ rows is a scalar times the first row, and so one expects the dimension to be $s + (r-1) = r + s - 1$.

Theorem. *With r, s, X as above, each of the rings $K[X]/I_2(X)$ is Cohen-Macaulay.*

Before proving this, we note the following.

Lemma. *If I and J are any ideals of any ring R, there is an exact sequence:*

$$0 \to R/(I \cap J) \to R/I \oplus R/J \to R/(I+J) \to 0$$

where the first map sends $r + (I \cap J) \mapsto (r + I) \oplus (-r + J)$ and the second map sends $(r + I) \oplus (r' + J) \mapsto (r + r') + (I + J)$.

Proof. It is straightforward to check that the maps are well-defined and R-linear. The first map is injective, since $r + (I \cap J)$ is in the kernel iff $r \in I$ and $r \in J$. The second map obviously kills the kernel, and is clearly surjective, Finally, $(r+I) \oplus (r'+J)$ is in the kernel of the second map iff $r + r' \in I + J$, i.e., $r + r' = i + j$ with $i \in I$ and $j \in J$. But then $r - i = r' + j = r_0$, and $(r + I) \oplus (r' + J)$ is the image of $r_0 + (I \cap J)$. □

In the case of an $\mathbb{N}$-graded Noetherian ring R with $R_0 = K$, a field, and homogeneous maximal ideal m, R is Cohen-Macaulay if and only if $\operatorname{depth}_m R = \dim(R)$. We also have:

Corollary. *Let hypotheses be as in the preceding Lemma. Suppose that R is a finitely generated $\mathbb{N}$-graded algebra over a field K with $R_0 = K$ and that I, J are ideals such that R/I, R/J are Cohen-Macaulay of dimension $d-1$ and $R/(IJ)$ is Cohen-Macaulay of dimension $d-2$. Then $R/(I \cap J)$ is Cohen-Macaulay of dimension $d-1$.*

Proof. We need only check that the depth of $R/(I \cap J)$ i on its maximal ideal, or on $\mathfrak{m}$, the maximal ideal of R, is $d-1$. Since the depth $R/(I+J)$ on $\mathfrak{m}$ is $d-2$ and the depth of $(R/I) \oplus (R/J)$ on $\mathfrak{m}$ is $d-1$, this is immediate from the long exact sequence for Ext. □

Proof of the Theorem. We use induction, and so we may assume the result if either or both of the dimensions of the matrix X are decreased. R is a domain and $x = x_{1,1}$ is therefore a nonzerodivisor. It will therefore suffice to prove that R/xR is Cohen-Macaulay. In R/xR, the fact that $x_{i,1}x_{1,j} - x_{1,1}x_{i,j} = 0$ shows that any minimal prime of x either contains all the $x_{1,j}$ or all of the $x_{i,1}$. Let P be the ideal $I_2(X) + (x_{1,j} : 1 \leq j \leq s)$ and Q the ideal $I_2(X) + (x_{i,1} : 1 \leq i \leq r)$. It follows that $V(x) = V(P) \cup V(Q)$. Since all of these ideals are radical, we have that $xR = P \cap Q$.

Let X', X'', and X''' be the matrices obtained from X be deleting, respectively, the first row, the first column, and both the first column and row. Then $R/P \cong K[X']/I_2(X')$ is a Cohen-Macaulay domain of dimension $(r-1)+s-1 = r+s-2$ by the induction hypothesis. $R/Q \cong K[X'']/Q$ is, similarly, a Cohen-Macaulay domain of dimension $r + (s-1) - 1 = r+s-2$. Moreover, $K[X]/(P+Q) \cong K[X''']/I_2(X''')$ is a Cohen-Macaulay domain of dimension $(r-1)+(s-1)-1 = r+s-3$, again using the induction hypothesis. We can now make of the short exact sequence

$$0 \to R/xR \to R/P \oplus R/Q \to R/(P+Q) \to 0.$$

Since the module in the middle has depth $r+s-2$ on m and the module on the right has depth $r+s-3$ on m, the module on the left has has depth $r+s-2$ on m. (One may use the long exact sequence for $\mathrm{Ext}_R(K, \_)$, or for Koszul homology, or for local cohomology to show this.) Since x is not a zerodivisor in the domain R, it follows that $\mathrm{depth}_m(R) = r+s-1$, which is $\dim(R)$. Therefore, R is Cohen-Macaulay. □

We now want to generalize all this to the case of $t \times t$ minors. We introduce two notations that will be useful in dealing with matrices. If A is a matrix, we write $A|_t$ for the submatrix formed from the first h columns of A. If A and B are matrices of sizes $r \times t$ and $r \times u$, respectively, we write $A\#B$ for the $r \times (t+u)$ matrix obtained by *concatenating* A and B: the first t columns of $A\#B$ give A, while the last u columns give B.

The following elementary fact will prove critical in our analysis. It generalizes the fact that when the two by two minors of a matrix vanish and the entries of the first row in the first v columns are 0, then the rest of the entries of the first row kill the elements in the first v columns.

Lemma (killing minors). *Let $A = (a_{ij})$ be a matrix and $1 < v < w$ integers such that the $(k+1) \times (k+1)$ minors of $A|_w$ vanish. Suppose also that $a_{1j} = 0$ for $1 \leq j \leq v$. Then for $v < j \leq w$, a_{1j} kills $I_k(A|_v)$.*

Proof. Fix j and fix a $k \times k$ minor of $A|_v$. If the minor involves the first row of A, it is 0, since the first row of $A|_v$ is 0. Therefore we may assume that the minor involves k rows of A other than the first and k columns of A that are actually columns of $A|_v$. Let

B denote the $k \times k$ submatrix of A determined by these rows and columns. Consider the $(k+1) \times (k+1)$ submatrix of A that involves, additionally, the first row of A and the j th column of A. This submatrix has the block form $\begin{pmatrix} 0 & a_{1,j} \\ B & C \end{pmatrix}$ where 0 denotes a $1 \times k$ block and C denotes a $k \times 1$ block. The determinant of this matrix is 0 by hypothesis, and is equal to $\pm a_{i,j} \det(B)$. The result follows. □

Now suppose that we want to create a family of ideals that can be used to prove that ideals of the form $I_3(X)$ are prime. If we kill the variables in the first v columns of the first row, we are led to consider ideals in which the 2×2 minors of the first v columns are 0 and the 3×3 minors of the entire matrix are 0. In addition, some of the entries of the first row are 0. Eventually we may lose the entire first row.

When we consider building an appropriate family for $I_4(X)$, we are led to consider ideals of the form $I_3(X|_v) + I_4(X) + I_a(X)$. But once the first row is gone, and we start to kill entries of te second row, we see that we need to consider ideals of the form $I_2(X|_u)+I_3(X_v)+I_4(X)+I_a(X)$. This suggests studying the large class that we are about to introduce.

Let X be an $r \times s$ matrix and $1 \leq t \leq \min r,\, s$ as before. Let $\sigma = (s_0,\, s_1,\, \ldots\,, s_{t-1})$, where the s_j are nonnegative integers $\leq s$ and $s_{t-1} = s$. We denote by $I_\sigma(X)$ the ideal

$$I_1(X|_{s_0}) + I_2(X|_{s_1}) + \cdots + I_t(X|_{s_{t-1}}).$$

We shall prove:

Theorem. *Let K be a field, and X an $r \times s$ matrix of indeterminates over K with r, s, t as above. Then all of the ideals $I_\sigma(X) + I_{k,h,a}(X)$ are radical, where $\sigma = (s_1, \ldots, s_{t-1})$ as above.*

We shall also prove that certain ideals among these are prime, and the the quotients by these primes are Cohen-Macaulay, but before we state the precise result, we want to introduce some restrictions on the elements σ and k, h, a used to describe the ideals.

Exactly as in our analysis of the case where $t = 2$, if $k > 0$ or $h > 0$ we can consider instead an ideal of the same type defined using a matrix of indeterminates with at least one dimension strictly smaller than r or s. Henceforth, we assume that $h = k = 0$. Having a positive value for s_0 has the same effect as having the same value for k. We may likewise assume that $s_0 = 0$. If we are not killing any $j \times j$ minors in our sum $I_\sigma(X)$, we assume that $s_{j-1} = j - 1$. Note that $X|_{j-1}$ has rank at most $j - 1$ automatically. Also note that if the size j minors vanish for the first u columns, the same is true for the size $j+1$ minors. This enables us to assume that $s_{j-1} \leq s_j$. But we can say more: the size $j+1$ minors will vanish for $X|_{u+1}$ as well, since a $j+1$ size minor that involves the last column may be expanded with respect to that column, and the cofactors are size k minors of $X|_u$. Henceforth, we may assume without loss of generality that $0 < s_1 < s_2 \cdots < s_{t-1} = s$. When this condition holds, we shall say that σ is *standard.* Note that when we want to work with $I_t(X)$, we work instead with $I_\sigma(X)$ for $\sigma = (0, 1, 2, 3, \ldots, t-2, s)$.

We can now state a more precise version of the theorem that we are aiming to prove.

Theorem. *Let K, X, r, s, t, k, h, σ, and a be as above. Then $I_\sigma(X) + J_{k,h,a}(X)$ is radical.*

If σ is standard and $a = s_k$ for some k (the case where $k = 0$, when $s_k = 0$, is included), then $P = I_\sigma(X) + I_{s_k}(X)$ is prime, and the ring $K[X]/P$ is Cohen-Macaulay.

The proof will occupy as for a while, but is, in fact, quite similar to the argument for the case where $t = 2$.

We first prove:

Lemma. *Let $0 \leq k < t \leq r$ be integers and K a field. Let L be a nonzero linear functional on K^r and let $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{t-1}$ be a nondecreasing chain of subspaces of K^r such that L vanishes on V_k (hence, on all of $V_1, \ldots, V_k$) and $\dim_K(V_j) \leq j$ for $1 \leq j \leq t-1$. Then there exists a chain of subspaces $0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_{t-1}$ in K^r such that L vanishes on W_k, $V_j \subseteq W_j$ for $1 \leq j \leq t-1$, and $\dim(W_j) = j$ for $1 \leq j \leq t-1$.*

Proof. We construct the W_j by reverse induction on j. We may evidently choose $W_{t-1} \subseteq K^r$ such that $V_{t-1} \subseteq W_{t-1}$ and $\dim_K(W_{t-1}) = t-1$, since $\dim(V_{t-1}) \leq t-1 < r$. If $W_{j+1}, \ldots, W_{t-1}$ have already been chosen satisfying the required conditions, $j > 1$, then there are two cases. If $j \neq k$, simply chose W_j of dimension j lying between $V_j \subseteq W_{j+1}$, which is possible since $\dim(V_j) \leq j$ and $\dim(W_{j+1}) = j+1$. If $j = k$, let H denote the kernel of L, a codimension one subspace of K^r. We now have to choose W_k of dimension k so that it contains V_k and is contained in $H \cap W_{k+1}$. But the dimension of $H \cap W_{k+1} \geq \dim(H) + \dim(W_{k+1}) - r = r - 1 + k + 1 - r = k$, and since $V_k \subseteq H \cap W_{k+1}$ and has dimension at most k, this is possible. □

We recall some facts about affine algebraic varieties over an algebraically closed field K. If X is an affine algebraic set over K, its coordinate ring $K[X]$ is the same as the set of regular functions from X to K. If $I \subseteq K[x_1, \ldots, x_n]$, a polynomial ring, is the radical ideal that defines XS, so that $X = \mathcal{V}(I)$, then $K[X] \cong K[x_1, \ldots, x_n]/I$. X is a variety if and only if I is prime, and also if and only if $K[X]$ is an integral domain. There is an antiequivalence of categories between affine algebraic sets (which arise as Zariski closed subsets of $\mathring{A}^n_K$ and regular morphism reduced finitely generated K-algebras. The algebraic set X corresponds to the ring $K[X]$. A regular morphism of algebraic varieties $X \to Y$ is called *dominant* if the image of X is Zariski dense in Y. This is equivalent to saying that the corresponding map of coordinate rings $K[Y] \to K[X]$ is an injective homomorphism of domains.

In our discussion of dimension in the sequel we need a fact relating the dimension of the domain of a dominant morphism to the dimension of the image and the dimension of a "typical" fiber. We treat this result formally below, but we first need some important facts about flatness. Part (a) is a special case of the Theorem on Generic Freeness proved in a stronger form in the notes for the Lectures from March 16–18, p. 134. We give the proof of part (b).

Lemma. *Let A, R, and S be Noetherian rings.*

(a) *(Generic freeness) Let A be a domain. If M is a finitely generated module over a finitely generated A-algebra R, then there exists $a \in A - \{0\}$ such that M_a is free over A_a.* $\square$

(b) *If $(R,\, \mathfrak{m},\, K) \to (S,\, \mathfrak{n},\, L)$ is a flat local homomorphism of local rings, then* $\dim(S) = \dim(R) + \dim(S/\mathfrak{m}S)$.

Proof. For part (b), let J be nilradical of R. Then $R/J \to S/JS$ is again a flat local homomorphism, the dimensions don't change, since we are killing ideals of nilpotents, S/mS is the same as $(S/JS)/(m/J)S/(JS)$, since $J \subseteq m$. Thus, we may assume that R is reduced. We use induction on $\dim(R)$. If $\dim(R) = 0$, then since R is reduced, we have $R = K$, and $S/mS \cong S$. The result is now obvious. If $\dim(R) = 1$, we can use prime avoidance to choose and element $x \in \mathfrak{m}$ not in any minimal prime of R, and since R is reduced, $x \notin \mathrm{Ass}(R)$. Hence, x is not a zerodivisor on R. Since S is R-flat, x is not a zerodivisor in S. It follows that $R/xR \to S/xS$ is flat, and $(S/xR)/(\mathfrak{m}/xR)(S/xS) \cong S/\mathfrak{m}S$. We have $\dim(R/xR) = \dim(R) - 1$, $\dim(S/xS) = \dim(S) - 1$, and the induction hypothesis yields that $\dim(S) - 1 = \dim(R - 1) + \dim(S/\mathfrak{m}S)$, and the desired conclusion follows at once. $\square$

The following result gives some properties of dominant maps of algebraic varieties. Throughout, K is an algebraically closed field.

Lemma. *Let $g : X \to Y$ be a dominant map of algebraic varieties, so that we have an injection of domains $K[Y] \hookrightarrow K[X]$. Then:*

(a) *The transcendence degree of $K(X)$ over $K(Y)$ is $\delta = \dim(X) - \dim(Y)$.*

(b) *There is a dense open subset U of Y such that for every $u \in U$, the dimension of the fiber $g^{-1}(u)$, thought of as a closed algebraic set in X, is $\delta = \dim(X) - \dim(Y)$.*

(c) *If $\dim(Y) = \dim(X)$ then $K(X)$ is a finite algebraic extension of $K(Y)$. Assume also that $K(X)$ is separable over $K(Y)$. Then there is a dense open set $U \subseteq Y$ such that for all $u \in U$, the fiber $g^{-1}(u)$ is a finite set of cardinality $d = [K(X) : K(Y)]$.*

Proof. Given any three fields $K \subseteq \mathcal{F} \subseteq \mathcal{G}$ the transcendence degree of $\mathcal{G}$ over K is the sum of the transcendence degree of $\mathcal{F}$ over K and the transcendence degree of $\mathcal{G}$ over $\mathcal{F}$. Part (a) follows from applying this to $K \subseteq K(Y) \subseteq K(X)$ along with the theorem that the dimension of a variety over K is the transcendence degree of its function field over K.

To prove part (b), let $R = K[Y] \subseteq K[X] = S$. Then S is a domain finitely generated over the domain R, and by the Noether normalization theorem for domains, we may localize at one nonzero element $f \in R$ so that S_f is a module-finite extension of a polynomial ring over R. The number of variables must be δ, the transcendence degree. Let U be the open set corresponding to $D(f)$ in Y. Thus, after replacing R and S by R_f and S_f, it suffices to show that if S is a module-finite domain extension of $R[x_1,\, \ldots,\, x_\delta]$, then all fibers over maximal ideals m of R have dimension δ. Since S/mS is module-finite over $(R/m)[x_1,\, \ldots,\, x_\delta]$ the dimension is at most δ. Since S has prime ideal Q lying over

$mR[x_1, \dots, x_\delta]$ by the lying over theorem, and we have $S/mS \twoheadrightarrow S/Q$, while S/Q is a module-finite extension domain of $(R/m)]x_1, \dots, x_\delta]$, we also have that the dimension is at least δ.

It remains to consider part (c). We continue the notations from the proof of (b). The first statement is immediate from (a) and the fact that $S = K[X]$ is finitely generated over K and, hence, over $R = K[Y]$. We may localize at $f \in R - \{0\}$ and so assume that S is module-finite over R. Then $K(Y) \otimes_R S = K(X)$. Choose a primitive element θ for $K(X)$ over $K(Y)$: by multiplying by a suitable nonzero element in R, we may assume that θ is in S. Let G be the minimal monic polynomial of θ over the fraction field of R. By our hypothesis on the field extension, G will be separable over R. By inverting one more element of $R - \{0\}$ we may assume that the coefficients of G are in R. Note that $S/R[\theta]$, as an R-module, is torsion. Therefore we may invert yet another element of R and assume without loss of generality that $S = R[\theta]$, and then $S \cong R[x]/G$.

Consider the roots of G in a suitably large extension field of the fraction field of R. The product of the squares of their differences (the discriminant of G) is a symmetric polynomial over $\mathbb{Z}$ in the roots of G, and therefore is expressible as a polynomial D over $\mathbb{Z}$ in the coefficients of G, which, up to sign, are the elementary symmetric functions of the roots. The discriminant is therefore a nonzero element of R. We localize at the discriminant as well, and so we may assume that it is a unit of R. Note that each localization has the effect of restricting out attention to a smaller dense open subset of Y.

The points of the fiber over a m, a maximal ideal of R, correspond to the maximal ideals of $(R/m)[x]/\overline{G}$, where $\overline{G}$ is simply the image of G modulo m. But $R/m = K$ and the discriminant of $\overline{G}$ is simply the image of the discriminant of G (one substitutes the images of the coefficients of G into D), and so is not zero. It follows that the roots of G are mutually distinct, and so the number of points in the finite fiber is precisely the degree of G, which is the same as the degree of G and is equal to $[K(Y) : K(X)]$. □

Part (b) of the preceding remark shows that for a dominant of map of varieities $X \to Y$, the dimension of X is the same as the sum of the dimension of Y and the dimension of a "typical" fiber over a point of Y, in the sense that this is true for all points of a dense Zariski open subset of Y contained in the image of X.

We are now ready to show the irreducibility of the algebraic sets corresponding to the ideals we are claiming to be prime.

Proposition. *With notation as in the Theorem, if σ is standard, $V = V(I_\sigma(X) + J_{s_k}(X))$ is irreducible.*

Proof. Consider $r \times (t-1)$ matrices B such that the first k entries of the first row are 0. These may be thought of as the points of $\mathbb{A}_K^{r(t-1)-k}$. Let C_j be a $j \times (s_j - s_{j-1})$ matrix over K, $1 \le j \le t-1$. (Recall that $s_0 = 0$ and $s_{t-1} = s$.) Consider the matrix

$$A = B|_1 C_1 \# B|_2 C_2 \# \cdots \# B|_{t-1} C_{t-1}.$$

The first k columns are in the span of the columns of $B|_k$ and so all have a 0 as their initial entry. Moreover, the columns of $A|_{s_j}$ are in the span of the columns of $B|_j$ for every j, and so the rank of $A|_{s_j}$ is at most j for every j. That is, A is a point of V. The choices for C_j are parametrized in bijective fashion by the points of $\mathbb{A}_K^{j(s_j-s_{j-1})}$ for all j. Therefore, we have a map $\mathbb{A}_K^N \to V$, where

$$N = r(t-1) - k + \sum_{j=1}^{t-1} j(s_j - s_{j-1}).$$

To show that V is irreducible, it suffices to show that this map is onto.

Consider any matrix A representing a point of V. Let V_j be the span of the columns of $A|_{s_j}$. Then the V_j satisfy the conditions of the Lemma, and we may choose W_j as in the lemma: the linear functional is projection on the first coordinate. Choose B so that its first column spans W_1, its first two columns span W_2, and, in general, its first j columns span W_j. It is a straightforward induction to prove that this can be done.

Now the columns of $A|_{s_j}$ are in the span of the columns of $B|_j$ for all j: in particular, this is true for the last $s_j - s_{j-1}$ columns, which says precisely that the matrix formed from those columns has the form $B|_j C_j$, as required. $\square$

We can now compute the dimension of V, keeping the above notation. We can consider the open set $U \subseteq V$ where the matrix formed by the columns indexed by the $s_{j-1}+1$, $1 \le j \le t-1$, has rank $t-1$: call this matrix B. Note that U is non-empty because we can use part of the standard basis $e_2, \ldots, e_t$ for K^r for the columns of A indexed by the numbers $s_{j-1}+1$, $1 \le j \le t-1$, and take the rest of the columns of A to be 0.

For each j, the submatrix D_j of A consisting of the columns indexed by $s_{j-1}+1, \ldots, s_j$ can be written uniquely as a linear combination of the columns of $B|_j$. The coefficients needed comprise the columns of a $j \times (s_j - s_{j-1})$ matrix C_j. Note that the first column of C_j is the last column vector in the standard basis for K^j: this corresponds to the fact that the first column of D_j is the same as the column of A indexed by $s_{j-1}+1$ and is the j th column of B. It is therefore the last column of $B|_j$. The entries of C_j other than the first column are arbitrary scalars and therefore C_j may be thought of as varying in an affine space $A^{j(s_j-s_{j-1}-1)}$, and this is also true, therefore, of D_j. It follows that the dimension of V should be

$$r(t-1) - k + 1(s_1 - 1) + 2(s_2 - s_1 - 1) + \cdots + (t-1)(s_{t-1} - s_{t-2} - 1)$$

which we can rewrite as

$$r(t-1) - k - (s_1 + s_2 + \cdots + s_{t-2}) + (t-1)s - \binom{t}{2}$$

.

We can make this more precise as follows. Let $W \subseteq \mathbb{A}_K^{r(t-1)}$ be the non-empty open set consisting of matrices of rank $t-1$, and let $f : U \to W$ be the map that sends the matrix A to the matrix $B = f(A)$ consisting of the columns of A with indices $s_{j-1}+1$, $1 \leq j \leq t-1$. For fixed B, consider the fiber of f over B. Let V_j be the vector space spanned by the first j columns of B. Then the fiber may be described as consisting of all matrices A such that each column of A indexed by $s_{j-1}+1$, $1 \leq j \leq t-1$, is the jth column of B and each column of A with index h, $s_{j-1}+1 < h \leq s_j$ is in the vector space V_j. It follows that the fiber is isomorphic with

$$\prod_{j=1}^{t-1} V_j^{s_j - s_{j-1} - 1},$$

so that each fiber has dimension $d = \sum_{j=1}^{t-1} j(s_j - s_{j-1} - 1)$, and so the dimension of U (and, likewise, of V) is the sum of the dimensions of W and d, as required. We have now proved:

Theorem. *With notation as above, if σ is standard then*

$$\dim\big(V(I_\sigma(X) + J_{s_k}(X))\big) = (r+s)(t-1) - k - (\sum_{j=1}^{t-2} s_j) - \binom{t}{2}. \quad \square$$

We can now complete the proof that all the ideals of the form $I = I_\sigma(X) + J_a(X)$ are radical. Because of our result on irreducibility, this also shows that the ones where $a = s_k$ are prime. As usual we may assume $a < s$ or else we can work with the matrix obtained by deleting the first row of X instead. Let $x = x_{1,a+1}$. We use the two lemmas that are the basis for the method of principal radical systems. If we specialize x to 1 and all other entries of the matrix to 0 we see that we have a point A where all generators of I vanish but x does not. Thus, $I + (x) = I_\sigma + J_{a+1}(X)$ is strictly larger than I, and therefore radical by the induction hypothesis. If $a = s_k$ for some k we are done, since we know that $\mathrm{Rad}\,(I)$ is then prime. Otherwise we have that $s_k < a < s_{k+1}$ for some k. In this case, from the lemma on killing minors we have that $xI_k(X|_a) \subseteq I$. Let σ' be the t-tuple that agrees with σ except that we change the $k+1$st entry s_k to a. By the induction hypothesis, $I_{\sigma'}(X) + J_a(X)$ is radical and, therefore, prime: call it P, and $I \subseteq P$. But $xP \subseteq I$, and so I is radical. $\square$

Our next objective is to prove the Cohen-Macaulayness assertions in the statement of the second the Theorem on p. 215 (the seventh page of the notes for this lecture). The argument is entirely similar to what we did earlier in studying the ideal generated by the 2×2 minors of a matrix of indeterminates.

We use reverse induction, assuming the result that larger ideals of the form $I_\sigma + J_{s_k}(X)$ are Cohen-Macaulay.

Suppose that a specific prime of the form $I_\sigma + J_{s_k}(X)$ is given. Call the ideal P. To show that $K[X]/P$ is Cohen-Macaulay, it suffices to show that the depth of $K[X]/P$ on the ideal m generated by all the $x_{i,j}$ in $K[X]$ is $d = \dim(K[X]/P)$. REF EARLIER Let $x = x_{1,s_k+1}$. Since we already know that $K[X]/P$ is a domain, we have that x is a not a zerodivisor, and so $K[X]/P$ is Cohen-Macaulay if and only if $K[X]/(P + xK[x])$ is, and this may be described as $K[X]/(I_\sigma(X) + J_{s_k+1}(X))$.

There are two cases. If $s_k + 1 = s_{k+1}$, then $I + xK[X]$ is a larger prime ideal of our family, and so killing it gives a Cohen-Macaulay ring by the induction hypothesis. If $s_k + 1 < s_{k+1}$ then $I + (x)$ is radical. By the lemma on killing minors, each of the variables $x_{1,b}$ for $s_k + 1 < b < s_{k+1}$ kills $I_k(X|_{s_k+1})$. Let σ' be the result of changing s_k in σ to $s_k + 1$, while leaving all other entries fixed. Let $Q_1 = I_{\sigma'} + J_{s_k+1}(X)$ and $Q_2 = I_\sigma(X) + J_{s_{k+1}}(X)$. Both of these ideals are prime, and we know that they have Cohen-Macaulay quotients by the induction hypothesis. This is also true for $Q_3 = Q_1 + Q_2 = I_{\sigma'}(X) + J_{s_{k+1}}(X)$.

Note that $V(P + (x)) = V(Q_1) \cup V(Q_2)$ by the lemma on killing minors: since all of the ideals are radical, we have that $P = Q_1 \cap Q_2$.

Moreover, $K[X]/Q_1$ has dimension $d - 1$: among the numbers used in calculating the dimension, s_k has increased by one while all others, including k, have not changed. Similarly, $K[X]/Q_2$ has dimension mat$d - 1$: here, only k has changed, increasing by 1. Finally, $K[X]/Q_3$ has dimension $d - 2$, since in this case k has increased by 1 and s_k has increased by one. Since these are Cohen-Macaulay, in the short exact sequence

$$0 \to K[X]/(P + (x)) \to K[X/Q_1 \oplus K[X]/Q_2 \to K[X]/Q_3 \to 0$$

the depths of the middle and right hand terms on m are $d - 1$ and $d - 2$ respectively, and so the depth of $K[X]/(P + (x))$ is $d - 1$, as required. □

Corollary. *For any field K and $r \times s$ matrix of indeterminates X, if $! \le t \le r \le s$ then $R = K[X]/I_t(X)$ is a Cohen-Macaulay normal domain.*

Proof. We have already established that R is a Cohen-Macaulay domain. What is left to prove is normality. We use induction on t. If $t = 1$, the quotient is a field and there is nothing to prove. Hence, we may assume $t \ge 2$. The Cohen-Macaulay condition implies that all associated primes of ideals generated by regular sequences $f_1, \ldots, f_h$ have height h. In particular, since this is true when $h = 1$, we need only show that the localization of R at any height one prime P is Noetherian discrete valuation ring. P cannot contain all the indeterminates, and, by symmetry we, may assume that $x_{11} \notin P$. Then R_P is also a local ring at a height one prime of the ring $R[1/x_{11}]$. Thus, it suffices to show that $R[1/x_{11}]$ is normal. Multiply the first row of the matrix X by $1/x_{11}$. The upper left entry is 1. Now perform elementary column operations to make the other entries of the first row 0, and then elementary row operations to make the other entries of the first column zero. These operations do not affect the ideal generated by the size t minors. The new matrix is the direct sum of a 1×1 block, $\bigl(1\bigr)$, and an $(r-1) \times (s-1)$ matrix X' whose typical entry is $x'_{ij} = x_{ij} - (x_{i1}x_{1j}/x_{11})$, $2 \le i \le r$, $2 \le j \le s$. It is easy to see that the

$K[X][1/x_{11}] = K[X'][x_{ij} : i = 1 \text{ or } j = 1][1/x_{11}]$, which implies that the entries of X' and the indeterminates in the first row and first column of X are algebraically independent. It is also easy to check that the ideal generated by the t size minors of X becomes the ideal generated by the $t-1$ size minors of X'. It follows that $R[1/x_{11}]$ is a localization of a polynomial ring over $K[X']/I_{t-1}(X')$, and it follows from the induction hypothesis that $K[X']/I_{t-1}(X')$ is normal. $\square$