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

Mel Hochster

Math 615, Winter 2020: Lectures of Mon., March 16 – Wed., March 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 $K[x_1, \dots, x_n]$ 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 $f \in D[x_1, \dots, x_n]$. 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 $D[x_1, \dots, x_n]$ 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 $\alpha = (a_1, \dots, a_n)$ 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

$$c_\alpha (x_n^N)^{a_1}(x_n^{N^2})^{a_2}\cdots(x_n^{N^{n-1}})^{a_{n-1}}x_n^{a_n} = c_\alpha x_n^{a_n+a_1N+a_2N^2+\cdots+a_{n-1}N^{n-1}}.$$

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

$$a_n + a_1N + a_2N^2 + \cdots + a_{n-1}N^{n-1}$$

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

Theorem (Noether normalization over a domain). *Let 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. $\square$

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. $\square$

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. $\square$

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 $F_1, \dots, F_d$ for A. We also know that for $1 \le i \le d-1$,

$$(F_1, \dots, F_i)R \cap A = (F_1, \dots, F_i)A.$$

We want to prove that $F_1, \dots, F_d$ is a regular sequence. Suppose not, and suppose that

$$(\dagger) \quad GF_{i+1} = G_1F_1 + \cdots + G_iF_i$$

where $G_1, \dots, G_i$, $G \in A$ and $G \notin (F_1, \dots, F_i)A$, where $i \le d-1$. We want to show that we can construct an example with the same properties in prime characteristic $p > 0$.

Since $F_1, \dots, F_d$ is a homogeneous system of parameters for A, every u_j has a power in the ideal generated by $F_1, \dots, F_d$. Hence, for every j we can choose $m_j \ge 1$ 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 $u_1, \dots, u_s$ with coefficients in K, say $F_k = P_k(u_1, \dots, u_s)$, $G_k = Q_k(u_1, \dots, u_s)$ for $1 \le k \le d$, $G = Q(u_1, \dots, u_s)$, and $w_{j,k} = H_{j,k}(u_1, \dots, u_s)$. 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 $x_1, \dots, x_n$), 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 $R_D = D[x_1, \dots, x_n]$, and let $A_D = D[u_1, \dots, u_s] \subseteq R_D$. 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 $\mathrm{Rad}\big((F_1, \dots, F_d)A_D\big)$ 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.