00000000000000000000000000000000000000000000000000000000000000000000000000000000■

Math 615: Lecture of February 23, 2007

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 $K[F_1, \ldots, F_d]$, we know that $F_1, \ldots, F_d$ are algebraically independent over K and, hence, over the smaller ring D. This yields

$$(1) \quad 0 \to D[F_1, \ldots, F_d] \to A_D \to A_D/D[F_1, \ldots, F_d] \to 0$$

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. $\square$

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 February 16 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 February 16.

Remarks. It might seem more natural to prove the Theorem stated in the mdidle of p. 3 of the Lecture Notes of February 16 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 $X = \left(x_{i,j}\right)$ is a 2×3 matrix of indeterminates that sends the entries of X to the corresponding entries of γX for all $\gamma \in G$. We have already noted 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: see the third Example on p. 3 of the Lecture Notes of January 31. 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:

$$\begin{array}{ccc} H(\mathbb{C},\, \Delta) & \xrightarrow{\quad\iota\quad} & H(\mathbb{C},\, \Delta) \otimes_{\mathbb{C}[\Delta]} \mathbb{C}[X] \\ \uparrow & & \uparrow \\ H(\mathbb{Q},\, \Delta) & \longrightarrow & H(\mathbb{Q},\, \Delta) \otimes_{\mathbb{Q}[\Delta_1,\, \Delta_2,\, \Delta_3]} \mathbb{Q}[X] \end{array} .$$

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, including one definition of the functor Ext. A detailed treatment of Ext is given in the Lecture Notes from Math 615, Winter 2004. There is a discussion of homotopic maps of complexes in the Lectures of February 2 and February 4: it is used to prove the independence of Ext from the choice of projective resolution in the definition below. Ext itself is defined in the Lecture of March 22 from the same set of Lecture Notes.

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).

There are other definitions: one may use an injective resolution of N instead, for example, and there are formulations of the theory where neither projectives nor injectives are used. $\mathrm{Ext}^i(M, N)$ is independent of the choice of the projective resolution up to canonical (choice-free) isomorphism. If M is held fixed, $\mathrm{Ext}^i_R(M, N)$ is a covariant functor of N. If N is held fixed, it is a contravariant functor of M. The functor $\mathrm{Ext}^0_R(M, N)$ may be identified canonically with $\mathrm{Hom}_R(M, N)$. The elements of $\mathrm{Ext}^1_R(M, N)$ are in bijective correspondence with isomorphism classes of short exact sequence $0 \to N \to W \to M \to 0$: the reason for the name "Ext" is that $\mathrm{Ext}^1_R(M, N)$ classifies such extensions.

There are two long exact sequences associated with Ext. If $0 \to N_1 \to N_2 \to N_3 \to 0$ is a short exact sequence of R-modules, then there is a long exact sequence

$$0 \to \mathrm{Hom}_R(M, N_1) \to \mathrm{Hom}_R(M, N_2) \to \mathrm{Hom}_R(M, N_3) \to \mathrm{Ext}^1_R(M, N_1) \to \cdots$$

$$\to \mathrm{Ext}^i_R(M, N_1) \to \mathrm{Ext}^i_R(M, N_2) \to \mathrm{Ext}^i_R(M, N_3) \to \mathrm{Ext}^{i+1}_R(M, N_1) \to \cdots .$$

Similarly, if $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact there is a long exact sequence

$$0 \to \mathrm{Hom}_R(M_3, N) \to \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1, N) \to \mathrm{Ext}^1_R(M_3, N) \to \cdots$$

$$\to \mathrm{Ext}^i_R(M_3, N) \to \mathrm{Ext}^i_R(M_2, N) \to \mathrm{Ext}^i_R(M_1, N) \to \mathrm{Ext}^{i+1}_R(M_3, N) \to \cdots .$$

The module $\operatorname{Ext}^i_R(M,\, N)$ is killed both by $\operatorname{Ann}_R M$ and $\operatorname{Ann}_R N$. When R is Noetherian and M, N are finitely generated, one can calculate the modules $\operatorname{Ext}^i_R(M,\, N)$ using a free resolution of M by finitely generated free R-modules, and it follows that all of the modules $\operatorname{Ext}^i_R(M,\, N)$ are finitely generated R-modules in this case.

If R is Noetherian, $I = (f_1, \ldots, f_s)$ is an ideal of R, and M is any R-module, the i th *local cohomology module* of M with support in I is defined as

$$\varinjlim{}_t \operatorname{Ext}^i(R/I_t,\, M)$$

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

$$0 \longrightarrow S^2 \xrightarrow{\beta} S^3 \xrightarrow{\alpha} S \longrightarrow S/I \longrightarrow 0$$

is such a resolution, where $\alpha = \begin{pmatrix}\Delta_1 & -\Delta_2 & \Delta_3\end{pmatrix}$ 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. $\square$