

Math 615: Lecture of February 16, 2007

The additive group $G = (K, +)$ of the field K may be identified with the group of upper triangular 2×2 unipotent matrices

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in K \right\},$$

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 as 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 eigenvector 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. \square

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 $R \rightarrow R^G$ 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 $M \rightarrow aM$ 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. \square

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 $R \rightarrow A$ 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 $a = f_1 r_1 + \cdots + f_k r_k$ 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 $I_j R$ is eventually stable, and so for some k , $I_k R = I_{k+h} R$ 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, \dots, F_h . Let $B = K[F_1, \dots, F_h] \subseteq A$. 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 $F = \sum_{j=1}^h G_j F_j$, 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. \square

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 isomorphic with V . We may let G act on V using the G -module structure of G , and this action extends to the polynomial ring S . The map $S \rightarrow R$ 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 $S \rightarrow R$. 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 $S \rightarrow R$, we also have a surjection $S^G \rightarrow R^G$. S^G is finitely generated over K by the graded case already considered, and so R^G is finitely generated over K . \square

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 $R = K[r_1, \dots, r_k]$. Suppose that $|G| = n$, say $G = \{\gamma_1, \dots, \gamma_n\}$. For each r_i , consider the elements $\gamma_1(r_i), \dots, \gamma_n(r_i)$. The elementary symmetric functions of these elements are invariant, and give coefficients for an equation of integral dependence of r_i , namely $\prod_{j=1}^n (z - \gamma_j(r_i)) = 0$. Hence, if R_0 is generated over K by the k sets of elementary symmetric functions of elements $\gamma_1(r_i), \dots, \gamma_n(r_i)$, $1 \leq i \leq k$, 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 . \square

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 $R = K[x_1, \dots, x_n]$ 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 .

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 rationnelles 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 $K[x_1, \dots, x_n]$. 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.

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, \dots, F_d be a homogeneous system of parameters of A such that for every i , $1 \leq i \leq d-1$, $(F_1, \dots, F_i)R \cap A = (F_1, \dots, F_i)A$. 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 $(F_1, \dots, F_i)A$ 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, \dots, F_d be a homogeneous system of parameters for A . Suppose that one has a relation:*

$$u_{i+1}F_{i+1} = u_1F_1 + \dots + u_iF_i$$

for some i . Then there exists an element $c \in A - \{0\}$ such that for all nonnegative integers $e \gg 0$,

$$(*) \quad cu_{i+1}^{p^e} \in (F_1^{p^e}, \dots, F_i^{p^e})A.$$

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

$$(**) \quad cu_{i+1}^q \in (F_1^q, \dots, F_i^q)A.$$

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 $(u^q : u \in J)A$, i.e., the ideal generated by all q th powers of elements of J . If J has generators u_i , then $J^{[q]}$ has generators u_i^q , since

$$(r_{i_1}u_{i_1} + \dots + r_{i_h}u_{i_h})^q = r_{i_1}^q u_{i_1}^q + \dots + r_{i_h}^q u_{i_h}^q,$$

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, \dots, 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 adjoining sufficiently many q th roots of elements in A). From the equation

$$(\#) \quad cu_{i+1}^q = F_1^q u_1 + \dots + F_i^q u_i$$

one gets

$$(\#\#) \quad c^{1/q}u_{i+1} = F_1u_1^{1/q} + \cdots + F_iu_i^{1/q}.$$

As $q \rightarrow \infty$, $1/q$ 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, \dots, F_i) , although in a somewhat larger ring than A .

Proof of the Theorem on colon-capturing. A is module-finite over $B = K[F_1, \dots, F_d]$. Let u_1, \dots, u_h be a maximal sequence of elements of A that are linearly independent over B , so that $G = Bu_1 + \cdots + Bu_h$ is a free B -module of rank h . Here, h will be the same as the degree of the extension of fraction fields, $[\text{frac}(A) : \text{frac}(B)]$. Consequently, A/G is a torsion-module over the domain B : we can see this as follows. If $u \in A - G$, it must have a nonzero multiple in G : otherwise u_1, \dots, u_h, u 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

$$F_{i+1}u_{i+1} = F_1u_1 + \cdots + F_iu_i,$$

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, \dots, F_{i+1}^q with coefficients in the free B -module G . Since F_1^q, \dots, F_{i+1}^q is a regular sequence on B , it is a regular sequence on G , and we can conclude that

$$cu_{i+1}^q \in (F_1^q, \dots, F_i^q)G \subseteq (F_1^q, \dots, F_i^q)A,$$

for all $q = p^e$, as required. \square

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 property 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. \square

It remains to prove the Lemma.