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

Mel Hochster

Math 615, Winter 2020: Lecture of Monday, 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 $x_1, \dots, x_d$ 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 $(x_1, \dots, x_d)S$.

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 $f_1,\, \dots\,, f_n$ 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 $c_1,\, \dots\,, c_n \in K^n$ 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. $\square$

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 $\theta_i(v) \neq 0$. $\square$

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 $x_i \mapsto \gamma_i x_i$, $1 \le i \le s$. 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 $x_1, \ldots, x_n$ 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 $k_{1,j}, \ldots, k_{s,j} \in \mathbb{Z}$ such that for all $\gamma = (\gamma_1, \ldots, \gamma_s) \in G$, γ sends

$$x_j \mapsto \gamma_1^{k_{1,j}} \cdots \gamma_s^{k_{s,j}} x_j.$$

Thus, the action of G on $R = K[x_1, \ldots, x_n]$ 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 $\gamma = (\gamma_1, \ldots, \gamma_s) \in G$, 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.* $\square$

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 $K[x_1, \ldots, x_r, y_1, \ldots, y_s]$, where $x_1, \ldots, x_r, y_1, \ldots, y_s$ 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 degree 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

$$R^G = K[x_i y_j : 1 \le i \le r, 1 \le j \le s].$$

Consider an $r \times s$ matrix of new indeterminates $Z = \bigl(z_{i,j}\bigr)$. There is a K-algebra surjection

$$K[Z] \twoheadrightarrow K[x_i y_j : 1 \le i \le r, 1 \le j \le s] = R^G$$

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 $\overline{z}_{1,1} \ne 0$. 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 $1 \le i \le r$ and and $y_j \mapsto \overline{z}_{1,j}$ for $1 \le j \le s$. 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. $\square$

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.* $\square$

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.