Math 615: Lecture of February 7, 2007

Remark. Let $R \to S$ be a homomorphism of Noetherian rings, $I$ an ideal of $R$, and $M$ a finitely generated $S$-module such that $IM \neq M$. Let $x_1, \ldots, x_k \in I$ be a regular sequence on $M$. Let $J = (x_1, \ldots, x_k)R$. Then $\text{depth}_I M / JM = \text{depth}_M M - k$, and $\text{depth}_{I/J} M / JM = \text{depth}_I M - k$, where in the second equality we have replaced $R$ by $R/J$ and $S$ by $S/JS$. The point is that if we extend $x_1, \ldots, x_k$ to a maximal regular sequence $x_1, \ldots, x_n$ in $I$ on $M$, then $x_{k+1}, \ldots, x_n$ is very easily seen to be a maximal regular sequence in $I$ on $M/JM$, and its image in $R/J$ is a maximal regular sequence in $I/J$ on $M/JM$.

Remark. We next want to see that, with the same hypothesis as in the first sentence of the previous remark, we have that $\text{depth}_I M = \text{depth}_{IS} M$. Let $\theta : R \to S$ be the map, and let $x_1, \ldots, x_n$ be a maximal regular sequence in $I$ on $M$. Clearly, $\theta(x_1), \theta(x_2), \ldots, \theta(x_n)$ is a regular sequence on $M$ in $IS$ because $x_i$ acts on $M$ exactly the way that $\theta(x_i)$ acts on $M$. We need only see that it is maximal. Again, since the $x_i$ act on $M$ exactly as the $\theta(x_i)$ act on $M$, we have that $M / (x_1, \ldots, x_n)M = M / (\theta(x_1), \theta(x_2), \ldots, \theta(x_n))M$.

Since $x_1, \ldots, x_n$ is a maximal regular sequence on $M$, there exists an element $u \in M / (x_1, \ldots, x_n)M - \{0\}$ that is killed by $I$. Since the annihilator of $u$ is an ideal of $S$, we must have that $u$ is killed by $IS$ as well, which shows that $\theta(x_1), \theta(x_2), \ldots, \theta(x_n)$ is a maximal regular sequence in $IS$ on $M$, as required. □

Remark. When $(R, m, K)$ is local, $\text{depth}(M)$, with no specification of an ideal, is understood to be $\text{depth}_m M$.

Remark. When $I$ is an ideal of $R$, $\text{depth}_I R$ is sometimes referred to as the depth of $I$ as an ideal. However, the phrase “as an ideal” is frequently omitted. This terminology is flawed, since the two depths may be different. For example, if $R = K[[x, y]]$ and $I = (x, y)R$, the depth of $I$ as an ideal is 2, since $x, y$ is a regular sequence. However, if $I$ is regarded as an $R$-module, the depth of $I$ on $m = (x, y)R$ is only one: $I/xI$ has depth 0, since the image of $x$ is killed by $m = I$, while $x \notin mI$. However, the situation is rarely confusing, because when $I$ is an ideal, “the depth of $I$” is almost always used for $\text{depth}_I R$.

Linear systems of parameters for standard graded algebras

We shall refer to a finitely generated $\mathbb{N}$-graded algebra $R$ over $R_0 = K$, a field, such that $R_1$, the vector space of linear forms, generates $R$ as a standard graded $K$-algebra. The following fact gives a very strong form of avoidance of ideals, not just prime ideals, and will enable us to prove the existence of regular sequences consisting of linear forms.
Proposition. Let $K$ be an infinite field, $V \subseteq W$ be vector spaces, and let $V_1, \ldots, V_h$ be vector subspaces of $W$ such that $V \subseteq \bigcup_{i=1}^h V_i$. Then $V \subseteq V_i$ for some $i$.

Proof. If not, for each $i$ choose $v_i \in V - V_i$. We may replace $V$ by the span of the $v_i$ and so assume it is finite-dimensional of dimension $d$. We may replace $V_i$ by $V_i \cap V$, so that we may assume every $V_i \subseteq V$. The result is clear when $d = 1$. When $d = 2$, we may assume that $V = K^2$, and the vectors $(1, c), c \in K - \{0\}$ lie on infinitely many distinct lines. For $d > 2$ we use induction. Since each subspace of $V \cong K^d$ of dimension $d - 1$ is covered by the $V_i$, each is contained in some $V_i$, and, hence, equal to some $V_i$. Therefore it suffices to see that there are infinitely many subspaces of dimension $d - 1$. Write $V = K^2 \oplus W$ where $W \cong K^{d-2}$. The line $L$ in $K^2$ yields a subspace $L \oplus W$ of dimension $d - 1$, and if $L \neq L'$ then $L \oplus W$ and $L' \oplus W$ are distinct subspaces. □

Theorem. Let $R$ be a standard graded $K$-algebra, and let $M$ be a $\mathbb{Z}$-graded finitely generated $R$-module. Let $m = \bigoplus_{d=1}^\infty [R]_d$ denote the homogeneous maximal ideal of $R$.

(a) $R$ has a homogeneous system of parameters consisting of linear forms.

(b) The depth of $M$ on $m$ is at least $h$ if and only if there exists a regular sequence on $M$ consisting of linear forms.

(c) In particular, the depth of $R$ on $m$ is at least $h$ if and only if there is a regular sequence on $R$ of length $h$ consisting of linear forms.

Proof. We construct the required sequence of linear forms for (a) and (b) recursively as follows. If the union of minimal primes of $R$ (respectively, the associated primes of $M$) contains $V = [R]_1$, then by the Lemma above, one of them contains $V$, and since $V$ generates $m$, we have that $m$ is a minimal prime of $R$ (respectively, an associated prime of $M$). In the case of (a), $R$ has dimension 0. In the case of (b), the depth of $M$ on $m$ is 0. In either case, the empty sequence satisfies the condition. If not, we can choose a linear form $F_1$ that is not in the union of these primes. This gives the first element of a system of parameters in (a), and the first element of a regular sequence in part (b). We can construct the required sequence recursively by passing to $R/F_1 R$ for (a) and to $M/F_1 M$ for (b). Part (c) is simply the case of (b) where $M = R$. □

Change of field

We want to make several comments about the effect of change of field on various questions.

Discussion: change of field and Gröbner bases. Let $R = K[x_1, \ldots, x_n]$, let $F$ be a finitely generated free $R$-module with ordered basis $e_1, \ldots, e_s$, let $M \subseteq F$ be a submodule, and fix a monomial order on $F$. Let $K \subseteq L$ be a field extension. We use $L$ as a subscript to indicate the result of applying $L \otimes_K -$. Thus, $R_L \cong L[x_1, \ldots, x_n]$, $F_L$ is a finitely generated free $R_L$-module with ordered basis $1 \otimes e_1, \ldots, 1 \otimes e_s$, $M_L \subseteq F_L$, and the monomials in $F_L$ are
the images of the monomials in $F$ under the obvious injection $F \to F_L$ that sends $f \mapsto 1 \otimes f$ for all $f \in F$. We identify $F$ with its image. The monomial order on $F$ then immediately gives a corresponding monomial order on $F_L$ because the two sets of monomials have been identified.

In this situation, let $g_1, \ldots, g_r$ denote a Gröbner basis for $M$. Then $g_1, \ldots, g_r$ is a Gröbner basis for $M_L$ as well. We can apply the Buchberger criterion to see this: as we apply it, all the divisions can be carried out over $K$, and so we have standard expressions with remainder 0, as required, independent of whether we think over $K$ or over $L$. This implies that $\text{in}(M_L)$ contains the same monomials as $\text{in}(M)$, and we have $\text{in}(M_L) = \text{in}(M)_L$.

In the graded case, the Hilbert functions of $M$ and $M_L$ are the same. We know that $R$ and $R_L$ are both Cohen-Macaulay or not alike: this is problem 4(d). in Problem Set #2.

There are also many properties of rings which, if they hold for $R_L$, hold for $R$. If $R_L$ is (1) reduced, or (2) a domain, or (3) normal, so is $R$. (1) and (2) hold simply because $R \subseteq R_L$. The third may be proved as follows: suppose that $a/b$ is integral over $R$, where $a \in R$ and $b$ is a nonzerodivisor over $R$. Because $R_L$ is flat over $R$, $b$ is a nonzerodivisor on $R_L$, and $a/b$ is certainly integral over $R_L$. It follows that $a/b \in R_L$, and so $a \in bR_L \cap R$.

When $S$ is faithfully flat over $R$, for every ideal $I$ of $R$, $IS \cap R = I$ ($R/I \to S/IS$ is still faithfully flat, which implies injective). Hence, $bR_L \cap R = bR$, and we have that $a \in bR$, which implies that $a/b \in R$.

However, $R_L$ can be a UFD even though $R$ is not. For example, if $R = \mathbb{R}[X, Y](X^2 + Y^2 - 1)$, where $X$ and $Y$ are indeterminates, it turns out that $R$ is not a UFD (the height one prime ideal $(X, Y - 1)R$ can be shown not to be principal), but $R_C \cong \mathbb{C}[X, Y]/(X^2 + Y^2 - 1)$ is a UFD: one can use new variables $U = X + iY$, $V = X - iY$, making a linear change of coordinates over $\mathbb{C}$, and then see that $R_C \cong \mathbb{C}[U, V]/(UV - 1) \cong \mathbb{C}[U, 1/U]$.

**Generic linear combinations as regular sequences**

We want to show that if an ideal contains a regular sequence on a module $M$, one can use “generic” linear combinations of the generators of the ideal, i.e., linear combinations with indeterminate coefficients, to produce such a regular sequence. We first observe:

**Proposition.** Let $R$ be a Noetherian ring, and $S = R[z_1, \ldots, z_k] = R[z]$ a polynomial ring over $R$. Let $N \subseteq M$ be finitely generated $R$-modules. We write $M[z]$ for $R[z] \otimes_R M$.

(a) If $P$ is prime in $R$, then $PS$ is prime in $S$.

(b) If $M$ is $P$-coprimary, then $M[z]$ is $PS$-coprimary.

(c) If $N = N_1 \cap \cdots \cap N_k$ is a primary decomposition of $N$ in $M$, then we have that $N[z] = N_1[z] \cap \cdots \cap N_k[z]$ is a primary decomposition of $N[z]$ in $M[z]$.

(d) $\text{Ass}(M[z])$ over $S$ is $\{PS : P \in \text{Ass}(M)\}$. 
Proof. (a) There is an obvious surjection $R[z] \to (R/P)[z]$. The result follows because $(R/P)[z]$ is a domain, and the kernel is clearly $PR[z]$.

(b) We may localize at $R - P$, which consists of nonzerodivisors on both $M$ and $M[z]$, without affecting the issue, and so we may assume that $(R, P, K)$ is local. Then $M$ has a finite filtration whose factors are copies of $K$, and since $R[z]$ is $R$-flat, $M[z]$ has a finite filtration by copies of $K \otimes R[z] = K[z]$. Since Ass $(K[z])$ over $S$ is clearly $PR[z]$, this is also true for $M[z]$.

(c) We have that $N[z] = N_1[z] \cap \cdots \cap N_k[z]$ since flat base change preserves finite intersection. Suppose that $N_i$ is $P_i$-coprimary. By part (b), $N_i[z]$ is $P_iS$-coprimary. It remains only to see that the intersection of the $N_j[z]$, omitting $N_i[z]$, is not $N[z]$. This follows from the fact that the intersection of the $N_j$, omitting $N_i$, is not $N$, and the fact that $S$ is faithfully flat over $R$.

(d) This is immediate from the primary decomposition in part (c). □

Corollary. Let $R$ be a Noetherian ring, let $I$ be an ideal of $R$ with generators $f_1, \ldots, f_h$, and let $M$ be a finitely generated $R$-module with $IM \neq M$.

(a) If depth$_1 M \geq 1$ and $z_1, \ldots, z_h$ are indeterminates over $R$, then $g = z_1 f_1 + \cdots + z_h f_h$ is a nonzerodivisor on $M[z]$ in $IR[z]$.

(b) If depth$_1 M = n$, then for every set of indeterminates $z$ over $R$, depth$_1 R[z]M[z] = n$. Moreover, if we take $z$ to include indeterminates $z_{i,j}$ where $1 \leq i \leq n$ and $1 \leq j \leq h$ and we let $g_i = z_{i,1} f_1 + \cdots + z_{i,h} f_h$ for $1 \leq j \leq n$, then $g_1, \ldots, g_n$ is a maximal regular sequence in $IR[z]$ on $M[z]$. In particular, we may take $M = R$.

(c) Let $R$ be a finitely generated $K$-algebra. Let notation be as in part (b). Let $L = K(z)$, the fraction field of $K[z]$, where the indeterminates $z$ include $z_{i,j}$ as in part (b). Let the subscript $L$ indicate the result of applying $L \otimes_K$. Then $g_1, \ldots, g_n$ is a maximal regular sequence in $IR_L$ on $M$. In particular, if $M = R$, $g_1, \ldots, g_n$ is a maximal regular sequence in $R_L$.

Proof. (a) If $g$ is a zerodivisor, it is in Ass $(M[z])$, and so it is in $PR[z]$ for some associated prime $P$ of $M$. This implies that all coefficients occurring are in $P$, and so $I \subseteq P$, which contradicts depth$_1 M \geq 1$.

Part (b) is simply the iterated use of (a). In part (c), it is clear that the $g_1, \ldots, g_n$ will still be a regular sequence after localization, provided that we still have $IM_L \neq M_L$. This follows from the fact that $L$ is free, and, hence, faithfully flat, over $K$. □

The Zariski topology on $K^n$ over an infinite field $K$

Let $K$ be an infinite field. We consider the ring $R = K[x_1, \ldots, x_n]$ of polynomials as a ring of functions on $K^n$. We note that if a polynomial is nonzero as an element of $R$, then it yields a nonzero function. In fact, this is true if $n = 1$ because a nonzero polynomial
of degree at most \( n \) has at most \( n \) roots, and \( K \) is infinite. We may use induction on \( n \). A polynomial \( f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \) may be written as a polynomial in \( x_n \) with coefficients in \( K[x_1, \ldots, x_{n-1}] \). If it is nonzero, we can choose a nonzero coefficient \( g(x_1, \ldots, x_{n-1}) \), and by the induction hypothesis we can choose a point \((c_1, \ldots, c_{n-1}) \in K^{n-1} \) such that \( g(c_1, \ldots, c_{n-1}) \neq 0 \). Then \( F(c_1, \ldots, c_{n-1}, x_n) \) is a nonzero polynomial in \( K[x_n] \), and so by the one variable case we can choose \( c_n \) so that it does not vanish for \( x_n = c_n \).

If \( \mathcal{S} \) as any subset of \( R \), we let

\[
\mathcal{V}(\mathcal{S}) = \{(c_1, \ldots, c_n) \in K^n : \text{ for all } f \in \mathcal{S}, \ f(c_1, \ldots, c_n) = 0\},
\]

and we shall say that these sets are closed algebraic sets in \( K^n \). As in the case where \( K \) is algebraically closed, \( \mathcal{V}(\mathcal{S}) \) is the same as \( \mathcal{V}(I) \), where \( I \) is the ideal generated by \( \mathcal{S} \), and it is also the same as \( \mathcal{V}(\text{Rad}(I)) \). However, distinct radical ideals may define the same closed algebraic set.

These sets are, likewise, the closed sets of a topology on \( K^n \) called the Zariski topology. We note that the complement of any proper closed set \( \mathcal{V}(I) \) of \( K^n \) is Zariski dense in \( K^n \). That is, every nonempty Zariski open set in \( K^n \) is dense. To see this, note that we have at least one nonzero polynomial \( f \) in \( I \). If the complement of \( \mathcal{V}(I) \) were a proper closed set, it would be contained in \( \mathcal{V}(g) \) for some nonzero polynomial \( g \). But then the nonzero polynomial \( fg \) vanishes everywhere, a contradiction.

We may view \( G = \text{GL}(n, K) \) as a Zariski open set in \( K^{n^2} \). We may identify an \( n \times n \) matrix with a point of \( K^{n^2} \), and then \( G \) is the complement of the set where the determinant function vanishes. We note that, as in the case of an algebraically closed field, the open subset \( X_f \) of an algebraic set \( X \subseteq K^N \) where a polynomial \( f \) does not vanish may be viewed as closed algebraic set in \( K^{N+1} \): it is in bijective correspondence with the set

\[
\{(c_1, \ldots, c_{N+1}) \in K^{n+1} : (c_1, \ldots, c_N) \in X \text{ and } c_{N+1} = 1/f(c_1, \ldots, c_n)\},
\]

which is the closed set defined by the same polynomials in \( x_1, \ldots, x_N \) that define \( X \) along with the polynomial \( fx_{N+1} - 1 \). The inherited Zariski topologies on \( X_f \subseteq X \) and on the corresponding set in \( K^{N+1} \) are the same.

In particular, we have a Zariski topology on \( \text{GL}(n, K) \), and every nonempty open subset is dense: such a subset is open in \( K^{n^2} \), and hence dense even in \( K^{n^2} \).

We shall write \( B^U_n \) for the subgroup of upper triangular invertible matrices in \( \text{GL}(n, K) \) and \( B^L_n \) for the subgroup of lower triangular invertible matrices. The subscript \( n \) will often be omitted.

**Generic initial modules**

Let \( R = K[x_1, \ldots, x_n] \) where \( K \) is an infinite field, let \( F \) be a finitely generated free \( R \)-module with ordered basis, and fix a monomial order on \( F \). Let \( M \) be a submodule of \( F \).
Let $A \in \text{GL}(n, K)$. Then $A = (a_{i,j})$ acts on the vector space $[R]_1$ of forms of degree 1 by sending the form $c_1x_1 + \cdots + c_nx_n$ to the form $c_1'x_1 + \cdots + c_n'x_n$ where

$$A \begin{pmatrix} c_1 \\
\vdots \\
c_n \end{pmatrix} = \begin{pmatrix} c_1' \\
\vdots \\
c_n' \end{pmatrix}.$$ 

This means that the coefficients of $A(x_j)$ are given by the entries of the $i$ th column of the matrix, i.e., $Ax_j = \sum_{i=1}^n a_{i,j}x_i$. This is a left action of $G = \text{GL}(n, K)$ on the vector space of one-forms.

This action extends to an action of $\text{GL}(n, K)$ on $R$ by $K$-algebra automorphisms, where $A : f \mapsto f(A(x_1), \ldots, A(x_n))$. The action extends also to $F$ in an obvious way by letting $A(f_1e_1 + \cdots + f_se_s) = A(f_1)e_1 + \cdots + A(f_s)e_s$.

We let $A(M)$ denote the image of $M$ under the action of $F$. We want to prove:

**Theorem.** There is a Zariski open subset $U$ of $\text{GL}(n, K)$ such that for all $A \in U$, in($AM$) is the same monomial module. Moreover, if $Z = (z_{i,j})$ is an $n \times n$ matrix of indeterminates over $K$, and $L = K(z_{i,j} : i,j)$, so that $Z \in \text{GL}(n, L)$, then in($ZM_L$) gives a monomial module containing the same monomials.

**Proof.** Let $g_1, \ldots, g_r$ be a Gröbner basis for $ZM_L$ containing images for generators of $M$ under $Z$. We form a finite family of polynomials in $K[Z]$ as follows. We include all denominators of coefficients of the $g_r$, and all numerators of the coefficients of their initial terms. By the Buchberger criterion, for each $i, j$ there is a standard expression

$$G_{i,j} = \sum_{k=1}^r q_{i,j,k}g_k$$

with remainder 0. We include in our family all denominators of coefficients of the $q_{i,j,k}$ and all numerators of the initial terms of the $q_{i,j,k}g_k$. Let $f$ be the product of all the polynomials in this family. The Gröbner basis and all elements in the expressions (*) have coefficients in $K[Z]_f$. For any matrix $A \in \text{GL}(n, K)_f$, there is a $K$-homomorphism $K[Z]_f \rightarrow K$ that maps the entries of $Z$ to the corresponding entries of $A$. This map carries $g_1, \ldots, g_r$ to a Gröbner basis for $AM$: we may take the images of the expressions in (*), and these show that we have a Gröbner basis by the Buchberger criterion. The monomial initial terms of $g_1, \ldots, g_r$ therefore generate both in($ZM_L$) and every in($AM$) for $A \in \text{GL}(n, K)_f = U$. □

The common initial module that we have proved to exist is denoted $\text{Gin}(M)$, and called the *generic initial module*. Note that even when $K$ is finite, we can still consider the span in $F$ of the monomial terms in in($ZM_L$) as a generic initial module: it becomes one after a base change to any infinite field.