Math 711: Lecture of November 17, 2006

Our next objective is to give a matrix factorization of a generic form over $\mathbb{Z}$ instead of $\mathbb{Z}[\xi]$. The idea is to replace the ring $\mathbb{Z}[\xi]$ by a ring of matrices over $\mathbb{Z}$.

Discussion: block form. Let R be any associative ring with identity, and let $\mathcal{M}_n(R)$ denote the ring of $n \times n$ matrices with entries of R, which we may identify, as usual, with the ring of R-linear edomorphisms of R^n, thought of as $n \times 1$ column vectors over R. The matrix η acts on the column γ by mapping it to $\eta\gamma$. The observation we want to make is that we may identify $\mathcal{M}_{kh}(R) \cong \mathcal{M}_k(\mathcal{M}_h(R))$. The naive way to make the identification is to partition each $kh \times kh$ matrix into a $k \times k$ array of $h \times h$ blocks. More conceptually, we may think of the domain of an R-linear map $R^{kh} \to R^{kh}$ as the direct sum of k copies of R^h, i.e., as $(R^h)^{\oplus k}$, and we may think of the target of the map as $(R^h)^k$, the product of k copies of R^h. Then the map is determined by its restrictions to the k direct summands R^h of the domain, and the map from a particular summand $R^h \to (R^h)^k$ corresponds to giving k R-linear maps $R^h \to R^h$, one for each factor of the target module.

Discussion: polynomials in commuting variables over a matrix ring. . Let $X_1, \ldots, X_k$ denote indeterminates both over R and over each matrix ring over R such that the X_i commute with one another, with elements of R, and with matrices over R. Then we may identify the rings

$$\mathcal{M}_n(R[X_1, \ldots, X_k]) \cong \mathcal{M}_n(R)[X_1, \ldots, X_k].$$

Given a finite linear combination $\sum_h \eta^{(h)}\mu_h$ where each $\eta^{(h)} = \bigl(r_{ij}^{(h)}\bigr) \in \mathcal{M}_n(R)$ and each μ_h is a monomial in the X_i, we let it correspond to the matrix $\bigl(\sum_h r_{ij}^{(h)}\mu_h\bigr)$.

Let ξ be a primitive dth root of unity. Recall that its minimal polynomial is denoted $\Psi_d(t)$: suppose that $\delta = \Phi(d)$, which is the degree of Ψ_d, and that

$$\Psi_d(z) = z^\delta + c_{\delta-1}z^{\delta-1} + \cdots + c_0,$$

where the $c_j \in \mathbb{Z}$. If we take $1, \xi, \xi^2, \ldots, \xi^{\delta-1}$ as a basis for $\mathbb{Z}[\xi]$, then the matrix of multiplication by ξ on $Z[\xi]$ is

$$\theta = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & 0 & \cdots & 0 & -c_2 \\ & & & \cdots & & \\ & & & \cdots & & \\ 0 & 0 & 0 & \cdots & 1 & -c_{\delta-1} \end{pmatrix},$$

the *companion* matrix of $\Psi_d(t)$, and $\mathbb{Z}[\xi] \cong \mathbb{Z}[\theta] \subseteq \mathcal{M}_\delta(\mathbb{Z})$. Notice that each of the powers $\boldsymbol{I}_\delta, \theta, \theta^2, \ldots, \theta^{d-1}$ has an entry equal to 1, because θ^i maps the basis element 1 to the basis element θ^i, $0 \le i \le d-1$.

We then have:

Theorem. *Let $d \geq 2$ and $s \geq 1$ be integers, and let f denote the degree d linear form over $\mathbb{Z}$ in sd variables given as*

$$f = X_{1,1}X_{1,2}\cdots X_{1,d} + \cdots + X_{s,1}X_{s,2}\cdots X_{s,d}.$$

Let $\delta = \Phi(d)$. Then f has a matrix factorization $f\boldsymbol{I}_{\delta d^{s-1}} = \alpha_1 \cdots \alpha_d$ over

$$R = \mathbb{Z}[X_{i,j} : 1 \leq i \leq s,\ 1 \leq j \leq d]$$

of size δs^{d-1} such that $I(\alpha) = (X_{i,j} : 1 \leq i \leq s,\ 1 \leq j \leq d)R$.

Proof. We begin with the matrix factorization over $R[\xi]$ which has size d^{s-1} given in the Theorem on p. 5 of the Lecture Notes of November 15. We write $\underline{X}$ for the collection of variables $X_{i,j}$, $1 \leq i \leq s$, $1 \leq j \leq d$. By the Discussions above, we have an embedding of

$$\mathbb{Z}[\xi][\underline{X}] \hookrightarrow \mathcal{M}_\delta(\mathbb{Z})[\underline{X}] \cong \mathcal{M}_\delta(\mathbb{Z}[\underline{X}])$$

which will give a matrix factorization of $(f\boldsymbol{I}_\delta)\boldsymbol{I}_{d^{s-1}}$ with d factors in $\mathcal{M}_{d^{s-1}}\big(\mathcal{M}_\delta(R)\big)$. Under the identification $\mathcal{M}_{d^{s-1}}\big(\mathcal{M}_\delta(R)\big) \cong \mathcal{M}_{\delta d^{s-1}}(R)$ this yields a matrix factorization for $f\boldsymbol{I}_{\delta d^{s-1}}$ whose entries are $\mathbb{Z}$-linear forms in the variables $\underline{X}$. In the factorization given in the previous Theorem, every $X_{i,j}$ occurred, possibly with a coefficient ξ^k, $0 \leq k \leq \delta - 1$. In the new factorization $\xi^k X_{i,j}$ is replaced by a block corresponding to $\theta^k X_{i,j}$. Since θ^k has an entry equal to 1, the variable $X_{i,j}$ occurs as an entry. $\square$

Now that we have dealt with the generic case, we can immediately get a corresponding result for any finitely generated ideal in any ring.

Theorem. *Let I be a finitely generated ideal of a ring R, and let $f \in I^d$, where $d \geq 2$. Then for some integer N there exists a matrix factorization $f\boldsymbol{I}_N = \alpha_1 \cdots \alpha_d$ such that $I(\alpha) = I$. In fact, there exists such a factorization in which $\alpha_1 = \alpha_2 = \cdots = \alpha_d$, and $I(\alpha_i) = I$, $1 \leq i \leq d$.*

Proof. Since $f \in I^d$, for some choice of elements $u_{ij} \in I$ we can write

$$f = u_{1,i} \cdots u_{1,d} + \cdots + u_{s,1} \cdots u_{s,d}$$

with all of the $u_{i,j} \in I$. We may assume all of the finitely many generators of I occur among the $u_{i,j}$ by including some extra terms in which one of the factors is 0. We may then map $\mathbb{Z}[X_{i,j} : 1 \leq i \leq s, 1 \leq j \leq d] \to R$ so that $X_{i,j} \mapsto u_{i,j}$. Applying the homomorphism to the factorization for the generic form given in the preceding Theorem, we obtain a factorization of f satisfying all but one of the conditions needed: it need not satisfy the condition that

$$\alpha_1 = \alpha_2 = \cdots = \alpha_d.$$

But we may satisfy the additional condition by increasing the size by a factor of d and taking all of the matrices to be $\mathrm{cyc}(\alpha_1, \ldots, \alpha_d)$: see the discussion on p. 5 of the Lecture Notes of November 15. $\square$

The following result will play an important role in our construction of linear maximal Cohen-Macaulay modules over hypersurfaces.

Theorem. *Let (R, m, K) be a local ring, and let $f \in m^d$ be a nonzerodivisor, where $d \geq 2$. Then for some s there is a matrix factorization $f\boldsymbol{I}_s = \alpha_1 \cdots \alpha_d$ such that $I(\alpha_i) = m$ for $1 \leq i \leq d$. Let $G = G_0 = R^s$, and let G_i be the image of $\psi_i = \alpha_1\alpha_2 \cdots \alpha_i$, so that $G_i \subseteq R^s$ as well, and $G_d = fR^s$. Let $M_i = G_i/G_{i+1}$, $1 \leq i \leq d$. Then all of the modules G_i/G_d, G/G_{i+1} and M_i, $0 \leq i \leq d-1$, are maximal Cohen-Macaulay modules over $\overline{R} = R/fR$, and all of them have finite projective dimension, necessarily 1, over R. Moreover, $\nu(M_i) = s$, $0 \leq i \leq d-1$.*

Proof. Since $f\boldsymbol{I}_s = \psi_i\psi_i'$, where $\psi_i' = \alpha_{i+1} \cdots \alpha_d$, we have from the Discussion on the first page of the Lecture Notes of November 13 concerning Cohen-Macaulay modules over hypersurfaces that if $\overline{}$ indicates images after applying $\overline{R} \otimes_R \_$, then

$$\cdots \xrightarrow{\overline{\psi}_i'} \overline{R}^s \xrightarrow{\overline{\psi}_i} \overline{R}^s \xrightarrow{\overline{\psi}_i'} \overline{R}^s \xrightarrow{\overline{\psi}_i} \overline{R}^s \to 0$$

is acyclic, and that

$$\mathrm{Ker}\,\overline{\psi_i'} = \mathrm{Im}\,\overline{\psi_i} \cong \mathrm{Coker}\,\overline{\psi_i'} \cong \mathrm{Coker}\,\psi_i',$$

and the same holds with the roles of ψ_i and ψ_i' interchanged. The image of ψ_i contains fR^s, which is the image of $\psi_i\psi_i'$, i.e., $fR^s \subseteq G_i \subseteq R^s$, and $G_i/fR^s = G_i/G_d$ may be identified with $\mathrm{Im}\,\overline{\psi_i}$. Thus, every G_i/G_d is a maximal Cohen-Macaulay module over $\overline{R}$ of finite projective dimension over R. Note as well that $R^d/G_i = \mathrm{Coker}\,\psi_i$ is a maximal Cohen-Macaulay module over $\overline{R}$ of finite projective dimension over R.

We have that $G_{i+1} = \mathrm{Im}\,\psi_{i+1} = \mathrm{Im}\,\psi_i\alpha_{i+1} \subseteq \psi_i(mR^s)$, since $I(\alpha_{i+1}) = m$, and this is contained in $m\psi_i(R_s) = mG_i$. Hence, $M_i = G_i/G_{i+1}$ is minimally generated over $\overline{R}$ by s elements, and the short exact sequences

$$0 \to M_i \to R^s/G_{i+1} \to R^s/G_i \to 0$$

show that every M_i is a maximal Cohen-Macaulay over $\overline{R}$ of finite projective dimension over R as well.

A maximal Cohen-Macaulay module over $\overline{R}$ that has finite projective dimension over R must have projective dimension 1 over R, since its depth is $d-1$. $\square$

Proposition. *Let (R, m, K) be local and $f \in m^d - m^{d+1}$. Let $\mathcal{L}(f)$ denote the leading form of f, i.e., the image of f in $m^d/m^{d+1} = [\mathrm{gr}_m(R)]_d$. Suppose that N is a finitely generated R-module ($N = R$ is the most important case) and that $\mathcal{L}(f)$ is a nonzerodivisor on $\mathrm{gr}_m(N)$. Let $\overline{R} = R/fR$, which has maximal ideal $\overline{m} = m/fR$, and let $\overline{N} = N/fN$. Then*

(a) *f is a nonzerodivisor on N.*

(b) *For every integer $n \geq 0$, $fN \cap m^nN = fm^{n-d}N$.*

(c) *For every $u \in N - \{0\}$, $\mathcal{L}(fg) = \mathcal{L}(f)\mathcal{L}(u)$, and the m-adic order of fu is the sum of the m-adic orders of f and u.*

(d) $\mathrm{gr}_{\overline{m}}(\overline{N}) \cong \mathrm{gr}_m(N)/\mathcal{L}(f)\mathrm{gr}_m(N)$.

Proof. We first prove (c). If $u \neq 0$, say $u \in m^h N - m^{h+1}N$, then it follows that $fu \notin m^{d+h+1}N$, i.e., that $fu \in m^{d+h}N - m^{d+h+1}N$, or else $\mathcal{L}(f)\mathcal{L}(u) = 0$, a contradiction. This proves both that $\mathrm{ord}\,(fu) = d + h$ and that $\mathcal{L}(fu) = \mathcal{L}(f)\mathcal{L}(u)$. Part (a) follows as well, for if $fu = 0$, then $\mathcal{L}(f)\mathcal{L}(u) = 0$.

To prove (b), note that if $fu \in m^n N$, then $d + \mathrm{ord}\,(u) \geq n$, and so $\mathrm{ord}\,(u) \geq n - d$, which shows that $u \in m^{n-d}N$.

Finally, to prove (d), note that

$$\overline{m}^n\overline{N}/\overline{m}^{n+1}\overline{N} \cong (m^nN + fN)/(m^{n+1}N + fN) \cong m^nN/\big(m^nN \cap (m^{n+1}N + fN)\big).$$

Now if $u_n = u_{n+1} + fv$ with $u_n \in m^nN$ and $u_{n+1} \in m^{n+1}N$, then $fv = u_n - u_{n+1} \in m^nN$, and so $v \in m^{n-d}N$ by part (b). Then

$$\begin{aligned}\overline{m}^n\overline{N}/\overline{m}^{n+1}\overline{N} &\cong m^nN/(m^{n+1}N + fm^{n-d}N)\\ &\cong [\mathrm{gr}_m(N)]/\mathcal{L}(f)[\mathrm{gr}_m(N)]_{n-d} \cong [\mathrm{gr}_m(N)/\mathcal{L}(f)\mathrm{gr}_m(N)]_n,\end{aligned}$$

as required. $\square$

Discussion. To calculate the multiplicity of a local ring $(R,\, m,\, K)$ or of an R-module M one may work alternatively with the Hilbert function of $\mathrm{gr}_m(R)$ or the Hilbert function of $\mathrm{gr}_m(M)$: the lattter, for example, is defined as $\dim_K[\mathrm{gr}_m(M)]_n$, and is eventually a polynomial of degree $\dim\,(M) - 1$. This function is the first difference of the Hilbert function. If the Hilbert function of M has leading term $\frac{e}{r!}n^r$, where $r = \dim\,(M)$, then the leading term of the Hilbert function of $\mathrm{gr}_m(M)$ will be

$$\frac{e}{r!}rn^{r-1} = \frac{e}{(r-1)!}n^{r-1}.$$

Corollary. *Let $(R,\, m,\, K)$ be local and let $f \in m$ be such that its leading form $\mathcal{L}(f)$ has degree d.*

(a) *If $\mathcal{L}(f)$ is a nonzerodivisor in $\mathrm{gr}_m(R)$, then $e(R/fR) = de(R)$.*

(b) *If N is a finitely generated R-module and $\mathcal{L}(f)$ is a nonzerodivisor on $\mathrm{gr}_m(N)$, then $e(N) = de(N/fN)$.*

Proof. It suffices to prove (b), which is more general. In the notation of the preceding proposition. $e(\overline{N})$ may be calculated from the Hilbert function of $\mathrm{gr}_{\overline{m}}(\overline{N})$, which is $\mathrm{gr}(N)/\mathcal{L}(f)\mathrm{gr}(N)$. If the Hilbert function of $\mathrm{gr}_m(N)$ is $H(n)$, the Hilbert function for $\mathrm{gr}(N)/\mathcal{L}(f)\mathrm{gr}(N)$ will be $H(n) - H(n-d)$. If the leading term of the polynomial corresponding to $H(n)$ is $\frac{e}{(r-1)!}n^{r-1}$, the new leading term is $\frac{de}{(r-2)!}n^{r-2}$, since the polynomial $cn^{r-1} - c(n-d)^{r-1}$ has leading term $cd(r-1)n^{r-2}$ for any constant c. $\square$

In order to prove the result we want on existence of linear maximal Cohen-Macaulay modules, we need to generalize the Theorem on p. 3 to a situation in which we have tensored with a linear maximal Cohen-Macaulay module N over R.