Math 615: Lecture of February 9, 2007

Elementary matrices and unipotent matrices

We shall write $\mathcal{U}_n^{\mathrm{U}} \subseteq \mathcal{B}_n^{\mathrm{U}}$ for the subgroup consisting of upper triangular matrices such that all diagonal entries are equal to 1. This is the group of upper triangular unipotent matrices. Similarly, $\mathcal{U}_n^{\mathrm{L}} \subseteq \mathcal{B}_n^{\mathrm{L}}$ is the subgroup consisting of lower triangular matrices with all diagonal entries equal to 1, the group of lower triangular unipotent matrices. The subscript $_n$ will often be omitted.

If $i \neq j$ are integers with $1 \leq i, j \leq n$ and $c \in K$, we denote by $E_{ij}(c)$ the matrix obtained by adding c times the j th row of the $n \times n$ identity matrix to the i th row. This matrix has all diagonal entries equal to 1, and precisely one off-diagonal entry that may be nonzero: the entry in the i th row and j th column is c. The field K and the value of n should be clear from context. For any $A \in \mathrm{GL}(n, K)$, $E_{ij}A$ is the matrix obtained from A be adding c times the j th row of A to the i th row of A. If $i < j$, then $E_{ij}(c) \in \mathcal{U}^{\mathrm{U}}$, while if $i > j$, then $E_{ij}(c) \in \mathcal{U}^{\mathrm{L}}$.

Every element A of $\mathcal{B}^{\mathrm{U}}$ is the product (on either side) of the diagonal matrix whose diagonal entries are the same as those of A and an upper triangular unipotent matrix. The upper triangular unipotent matrices are generated by the $E_{ij}(c)$ for $i < j$. Note that $E_{ij}(c)$ and $E_{ij}(-c)$ are inverses. Given any upper triangular unipotent matrix, it can be "brought to" the identity matrix by a finite sequence of elementary row operations corresponding to left multiplication by matrices $E_{ij}(c)$ with $i < j$. One subtracts multiples of the last row from earlier rows to make all entries of the last column except the bottom entry equal to 0. Then one subtracts multiples of the $n-1$ st row from the earlier rows to make all entries in the $n-1$ st column except the $n-1$ st equal to 0. Once the j th column has only one nonzero entry, which is 1, in the j th spot for all $j > i$, one subtracts multiples of the i th row from the earlier rows until all entries of the i th column are 0, except for the i th entry, which is 1. One continues in this way until off-diagonal entries are 0. This means that one can choose upper triangular matrices $E_1, \ldots, E_N$ such that

$$E_N \cdots E_1 A = I.$$

But this in turn implies that

$$A = E_1^{-1} \cdots E_N^{-1},$$

as required. It follows that $\mathcal{B}^{\mathrm{U}}$ is generated by the diagonal matrices and the matrices $E_{ij}(c)$ for $i < j$.

In an exactly similar way (or simply by transposing) we have that every element A of $\mathcal{B}^{\mathrm{L}}$ is the product (on either side) of the diagonal matrix whose diagonal entries are the same as those of A and a lower triangular unipotent matrix. The lower triangular unipotent matrices are generated by the $E_{ij}(c)$ for $i > j$, and $\mathcal{B}^{\mathrm{L}}$ is generated by the diagonal matrices and the matrices $E_{ij}(c)$ for $i > j$.

Lower triangular matrices preserve the initial form

Let $R = K[x_1, \ldots, x_n]$ and let F be a finitely generated free module with ordered basis $e_1, \ldots, e_s$. We assume a monomial order on F such that if $i < j$, then $x_i e_t > x_j e_t$ for $1 \le t \le s$. This means that for any term ν,

$$(\#) \quad x_i^h \nu > x_i^{h-d} x_j^d \nu$$

for $1 \le d \le h$ and $i < j$. Ignoring the scalar, $\nu = \mu e_t$, and

$$x_i^h \nu e_t = x_i^{h-1} \nu x_i e_t > x_i^{h-1} \nu x_j e_t = x_i^{h-1} x_j \nu e_t$$

which is the case $d = 1$. But then, by induction on d, if $d > 1$ the last term is greater than $x_i^{(h-1)-(d-1)} x_j^{d-1} x_j \nu e_i$, which yields the result.

Theorem. *Let $A \in \mathcal{B}^{\mathrm{L}}$. For every nonzero element $f \in F$, $\mathrm{in}(Af) = \mathrm{in}(f)$. Hence, for every submodule $M \subseteq F$, we have that $\mathrm{in}(AM) = \mathrm{in}(M)$.*

Proof. The second statement is clear from the first. Since A can be written as a product of diagonal matrices and matrices $E_{ij}(c)$ with $i > j$, it suffices to prove the first statement for each of the two types. If A is diagonal, it is clear that the monomials occurring in terms of Af are the same as the monomials occurring in terms of f: the action is such that each term of f is multiplied by a nonzero scalar in the field, and no new terms are introduced.

Therefore we may assume that $A = E_{ji}(c)$ with $j > i$. We consider the effect of the action of A on a typical term of f. Note that A sends $x_i \mapsto x_i + cx_j$ while fixing all the other x_k. The term can be written as $x_i^h \nu$ where ν is a term not divisible by x_i. Then A maps this term to $(x_i + cx_j)^h \nu$. When we expand we get $x_i^h \nu$ and a sum of other terms, which, if nonzero, have the form $c' x_i^{h-d} x_j^d \nu$ where $c' \in K - \{0\}$ and $1 \le d \le h$. Thus, the original term occurs, and the other terms are strictly smaller, by (#) displayed above. It follows that if $x_i^h \nu$ is the initial term of f, it still occurs in Af, and all other terms occurring are strictly smaller, so that it remains the initial term. $\square$

Corollary. *If U is a Zariski dense open subset of $\mathrm{GL}(n, K)$ such that $\mathrm{in}(AM)$ is $\mathrm{Gin}(M)$ for all $A \in U$, then $\mathcal{B}^{\mathrm{L}} U$ is a Zariski dense open set with the same property.*

Proof. If $\mathrm{in}(AM) = \mathrm{Gin}(M)$ and $B \in \mathcal{B}^{\mathrm{L}}$, then we have from the preceding Theorem that $\mathrm{in}\big(B(AM)\big) = \mathrm{in}(AM) = \mathrm{Gin}(M)$, from which it follows that every matrix in $\mathcal{B}^{\mathrm{L}} U = \{BA : B \in \mathcal{B}^{\mathrm{L}},\, A \in U\}$ consists entirely of matrices that map M to a module whose initial module is $\mathrm{Gin}(M)$. Multiplication by $B \in GL(n, K)$ is an automorphism of $\mathrm{GL}(n, K)$ as an algebraic set (*not* as a group), so that for all $B \in \mathcal{B}^{\mathrm{L}}$, $BU = \{BA : A \in U\}$ is again a dense open set. Since $\mathcal{B}^{\mathrm{L}} U$ is the union of the family $\{BU : B \in \mathcal{B}^{\mathrm{L}}\}$, it is also a dense open set. $\square$

We next note:

Lemma. $\mathcal{B}^{\mathrm{L}}\mathcal{U}^{\mathrm{U}} = \{BA : B \in \mathcal{B}^{\mathrm{L}},\ A \in \mathcal{U}^{\mathrm{U}}\}$ *is a Zariski dense open set in* $\mathrm{GL}(n, K)$.

Proof. For $1 \leq k \leq n$, let D_k be the polynomial function on $GL(n, K)$ given by the determinant of the $k \times k$ submatrix in the upper left corner. Let D be the product $D_1 D_2 \cdots D_{n-1}$. We claim that $\mathcal{B}^{\mathrm{L}}\mathcal{U}^{\mathrm{U}} = \mathrm{GL}(n, K)_D$, the set of invertible $n \times n$ matrices such that the nested minors in the upper left corner do not vanish. Evidently, $\mathcal{U}^{\mathrm{U}} \subseteq \mathrm{GL}(n, K)_D$. Next note that if $A \in \mathrm{GL}(n, K)_D$ and B is an invertible diagonal matrix, then $BA \in \mathrm{GL}(n, K)_D$ (the relevant minors are each multiplied by a nonzero scalar) and $E_{ij}(c)B \in \mathrm{GL}(n, K)_D$ for all $i > j$ and $c \in K$ (adding a multiple of an earlier row to later row does not change any of the relevant minors). Hence, $\mathcal{B}^{\mathrm{L}}\mathcal{U}^{\mathrm{U}} \subseteq \mathrm{GL}(n, K)_D$.

It remains to prove the opposite inclusion. Now consider any matrix $A \in \mathrm{GL}(n, K)_D$. By the hypothesis on the nonvanishing of D, we have that D_1 does not vanish, i.e., the entry in the upper left hand corner is not 0. Hence, we can subtract multiples of the first row from lower rows to obtain a matrix in which the first column is 0 below the first entry. In the course of this process, at each stage we are multiplying by a lower triangular elementary matrix. We can proceed by, indiuction on j, to multiply by lower triangular elementary matrices unitl we reach a matrix such that all entries below the main diagonal in the first j columns are 0. At every stage, we continue to have a matrix in $\mathrm{GL}(n, K)_D$. Suppose this has been done for all columns preceding the j th column. The hypothesis that D does not vanish implies that D_j does not vanish, and since the $j \times j$ submatrix in the upper left corner is now upper triangular, this implies that the j, j entry on the diagonal is nonzero. We can therefore subtract multiples of the j th row from lower rows until the j th column contains only 0 entries below the main diagonal. In this way, we eventually reach an upper triangular matrix. We have multiplied the original matrix A on the left by a lower triangular unipotent matrix B in the process, thereby obtaining an upper triangular matrix C. Since $BA = C$, we have $A = B^{-1}C$, as required. □

Corollary. *Let* $R = K[x_1, \ldots, x_n]$ *be a polynomial ring over an infinite field* K*, let* F *be a finitely generated free* R*-module with ordered basis* $e_1, \ldots, e_s$*, and suppose that we have a monomial order on* F *such that for all* t *and* $i < j$*,* $x_i e_t > x_j e_t$*. Let* $M \subseteq F$ *be a submodule. Let* $U \subseteq \mathrm{GL}(n, K)$ *be such that* $\mathcal{B}^{\mathrm{L}}U \subseteq U$ *and* $\mathrm{in}(AM) = \mathrm{Gin}(M)$ *for all* $A \in U$*. Then* U *has nonempty intersection with* $\mathcal{U}^{\mathrm{U}}$.

Proof. Since U and $\mathcal{B}^{\mathrm{L}}\mathcal{U}^{\mathrm{U}}$ are Zariski dense open sets, their intersection is nonempty. Choose $A \in U$ such that $A = BC$ with $B \in \mathcal{B}^{\mathrm{L}}$ and $C \in \mathcal{U}^{\mathrm{U}}$. Then $C = B^{-1}A \in U$, as required. □

Ideals stable under the action of the group of invertible diagonal matrices

We want to show that when K is infinite, an ideal I of the polynomial ring $R = K[x_1, \ldots, x_n]$ over a field K is stable under the action of $\mathcal{D}_n$, i.e., mapped into itself by every element of $\mathcal{D}_n$, if and only if it is a monomial ideal.

We shall prove some much stronger results. We first want to prove a result on the invertibility of Van der Monde matrices.

Discussion: Van der Monde matrices. Let $u_1, \ldots, u_h$ be elements of a commutative ring. Let Q be the $h \times h$ matrix $\bigl(u_i^{j-1}\bigr)$, which is called a *Van der Monde* matrix. We want to show that if the elements $u_i - u_j$ are all invertible, then so is Q. We give two proofs.

(a) We shall show that the determinant of Q is $\prod_{j>i}(u_j - u_i)$. Hence, Q is invertible if $u_j - u_i$ is a unit for $j > i$. It suffices to prove the first statement when the u_i are indeterminates over $\mathbb{Z}$. Call the determinant D. If we set $u_j = u_i$, then D vanishes because two rows become equal. Thus, $u_j - u_i$ divides D in $\mathbb{Z}[u_1, \ldots, u_h]$. Since the polynomial ring is a UFD and these are relatively prime in pairs, the product P of the $u_j - u_i$ divides D. But they both have degree $1 + 2 + \cdots + h - 1$. Hence, $D = cP$ for some integer c. The monomial $u_2 u_3^2 \cdots u_h^{h-1}$ obtained from the main diagonal of matrix in taking the determinant occurs with coefficient 1 in both P and D, so that $c = 1$. $\square$

(b) We can also show the invertibility of Q as follows: if the determinant is not a unit, it is contained in a maximal ideal. We can kill the maximal ideal. We may therefore assume that the ring is a field K, and the u_i are mutually distinct elements of this field. If the matrix is not invertible, there a nontrivial relation on the columns with coefficients $c_0, \ldots, c_{n-1}$ in the field. This implies that the nonzero polynomial

$$c_{h-1}x^{h-1} + \cdots + c_1 x + c_0$$

has h distinct roots, $u_1, \ldots, u_h$, in the field K, a contradiction. $\square$

Next note the following. Suppose that R is an $\mathbb{N}$- or $\mathbb{Z}$-graded algebra and that $u \in R_0$ is a unit. The there is an automorphism $\eta_u : R \to R$ such that if $f \in [R]_d$, then $\eta_u(f) = u^d f$.

Proposition. *Let R be an $\mathbb{N}$- or $\mathbb{Z}$-graded algebra such that R_0 contains an infinite field or, more generally, such that R_0 contains infinitely many elements u_i that are units and such that for all $i \neq j$, the element $u_i - u_j$ is a unit. Let $I \subseteq R$ be any ideal that is stable under all of the automorphism η_{u_i}, with notation as just above. Then I is a homogeneous ideal of R.*

Proof. Let $f_{t+1} + \cdots + f_{t+h} = f$ be an element of I, where the interval $[t+1, \ldots, t+h]$ includes all degrees in which the element has a nonzero homogeneous component, and f_j denotes the homogeneous component in degree j. Choose invertible elements $u_1, \ldots, u_h$ in R_0 such that $u_i - u_j$ is invertible for $i \neq j$. By letting η_{u_i} act we obtain an equation

$$(*_i) \quad u_i^{t+1} f_{t+1} + \cdots + u_i^{t+j} f_{t+j} + \cdots + u_i^{t+h} f_{t+h} = \eta_{u_i}(f) \in I$$

We can multiply this equation by u_i^{-t-1} and let $g_i = u_i^{-t-1}\eta_{u_i}(f) \in I$ to obtain

$$(**_i) \quad f_{t+1} + \cdots + u_i^{j-1} f_{t+j} + \cdots + u_i^{h-1} f_{t+h} = g_i$$

for $1 \leq i \leq h$. In matrix form, these equations can be written as

$$Q \begin{pmatrix} f_{t+1} \\ \vdots \\ f_{t+h} \end{pmatrix} = \begin{pmatrix} g_1 \\ \vdots \\ g_h \end{pmatrix},$$

where Q is the Van der Monde matrix discussed above, and so is invertible over R. We then have

$$\begin{pmatrix} f_{t+1} \\ \vdots \\ f_{t+h} \end{pmatrix} = Q^{-1} \begin{pmatrix} g_1 \\ \vdots \\ g_h \end{pmatrix},$$

and since Q^{-1} has entries in R and the $g_j \in I$, it follows that all of the homogeneous components of f are in I, as required. $\square$

Corollary. *Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over an infinite field K, and let I be an ideal of R that is stable under the action of the diagonal matrices $\mathcal{D}_n \subseteq \mathrm{GL}(n, K)$. Then I is a monomial ideal of R.*

Proof. Let S_k be the polynomial ring in the remaining variables with x_k omitted for $1 \leq k \leq n$, so that $R = S_k[x_k]$. Then R is $\mathbb{N}$-graded thinking of it as a polynomial ring in one variable over S_k, with $[R]_d = S_k x_k^d$ for every $d \in \mathbb{N}$, and $K \subseteq R_0 = S_k$. If $u \in K - \{0\}$, the automorphism η_u conincides with the action of the diagonal matrix with u on the diagonal in the k, k spot and all other entries equal to 1 on R, and so I is stable with respect to this action. Hence, I is homogeneous with respect to each of the x_k gradings. Given an element f of I, it is a sum of x_n-homogeneous componets all of which are in I: these have the form $g_{n-1}x_n^d$ where $g_{n-1} \in K[x_1, \ldots, x_{n-1}]$. Each of these is in turn a sum of x_{n-1}-homogeneous components, all of which are in I. These have the form $g_{n-2}x_{n-1}^{d_{n-1}}x_n^{d_n}$ where $g_{n-2} \in K[x_1, \ldots, x_{n-2}]$. Continuing in this way, we see that every monomial term of f is in I, as required. $\square$

Borel-fixed ideals

We shall show soon that in the graded case, generic initial monomial ideals are stable under the action of $\mathcal{B}_n^{\mathrm{U}}$. In this section we want to charactize the ideals of the polynomial ring $R = K[x_1, \ldots, x_n]$ that are stable under the action of $\mathcal{B}_n^{\mathrm{U}}$.

We first prove an elementary fact about the behavior of binomial coefficients modulo a prime integer p that we shall need to handle the characteristic $p > 0$ case.

In the Lemma below, the binomial coefficients $\binom{k}{h}$, where $h, k \in \mathbb{N}$, are defined to be 0 if $h > k$. Otherwise, they have their usual meaning, $\dfrac{k!}{h!(k-h)!}$. Note that $\binom{k}{h}$ is always nonzero if $0 \leq h \leq k$: in particular, if $h = 0$ its value is 1, even if $k = 0$.

Lemma. *Let h and k be nonnegative integers and let p be a positive prime integer. Let*

$$h = h_d p^d + h_{d-1} p^{d-1} + \cdots + h_0$$

and

$$k = k_d p^d + k_{d-1} p^{d-1} + \cdots + k_0$$

be expansions of h and k respectively in base p, so that $0 \le h_i \le p-1$ and $0 \le k_i \le p-1$ for all i. (The length d of the expansion is permitted to be longer than needed, so that, for example, h_d, or several of the initial h_i, may be 0, and the same holds for k.) Then

$$\binom{k}{h} \equiv \binom{k_d}{h_d}\binom{k_{d-1}}{h_{d-1}}\cdots\binom{k_1}{h_1}\binom{k_0}{h_0} \mod p.$$

Hence, $\binom{k}{h} \not\equiv 0 \mod p$ *if and only if* $h_i \le k_i$ *for all* i.

Proof. Let z be an indeterminate over $\mathbb{Z}_p = \mathbb{Z}/pZ$. Then

$$(1+z)^k = \big((1+z)^{p^d}\big)^{k_d}\big((1+z)^{p^{d-1}}\big)^{k_{d-1}}\cdots\big((1+z)^p\big)^{k_1}(1+z)^{k_0},$$

and since we are in prime characteristic $p > 0$ we may rewrite this as

$$(1+z^{p^d})^{k_d}(1+z^{p^{d-1}})^{k_{d-1}}\cdots(1+z^p)^{k_1}(1+z)^{k_0}.$$

If we expand each factor by the binomial theorem and then multiply out, using the generalized distributive law, we obtain the sum of $(k_d+1)(k_{d-1}+1)\cdots(k_0+1)$ terms, one for every choice of integers $h_d, \ldots, h_0$ with $0 \le h_i \le k_i$, namely:

$$\binom{k_d}{h_d}\binom{k_{d-1}}{h_{d-1}}\cdots\binom{k_1}{h_1}\binom{k_0}{h_0}(z^{p^d})^{h_d}(z^{p^{d-1}})^{h_{d-1}}\cdots(z^p)^{h_1}z^{h_0} =$$

$$\binom{k_d}{h_d}\binom{k_{d-1}}{h_{d-1}}\cdots\binom{k_1}{h_1}\binom{k_0}{h_0}z^{h_dp^d+h_{d-1}p^{d-1}+\cdots+h_1p+h_0}.$$

Because the exponents are distinct expansions of nonnegative integers in base p, they are all distinct, and there are no cancellations of terms. These coefficients are all nonzero, because p does not occur as factor in the formula for the binomial coefficient $\binom{k_i}{h_i}$ when $0 \le h_i \le k_i \le p-1$. There is no nononzero term involving z^h if the expansion of h in base p is such that $h_i > k_i$ for some i, and the formula given remains correct in this case because $\binom{k_i}{h_i} = 0$ when $h_i > k_i$. The final statement is now clear. □

For each integer p in the set $\{0, 2, 3, 5, \ldots\}$ consisting of 0 and the positive prime integers, if $h, k \in \mathbb{N}$ we define $h \le_p k$ to mean $\binom{k}{h}$ does not vanish modulo p. If $p = 0$ this is the usual total order on $\mathbb{N}$, but if $p > 0$ it is a partial ordering because of the characterization in the last statement of the Lemma just above.

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring in n variables over a field. We define an ideal of R to be *Borel-fixed* if it is stable under the action of $\mathcal{B}_n^{\mathrm{U}}$, the Borel subgroup of $\mathrm{GL}(n, K)$ consisting of upper triangular matrices. Such an ideal is stable under the action of $\mathcal{D}_n$, and so it must be a monomial ideal. We have the following:

Proposition. *Let notation be as in the paragraph above, and let $I \subseteq R$. Then I is Borel-fixed if and only if it is a monomial ideal and has a set of monomial generators μ with the following property:*

$(\#)$ *if $\mu = x_j^k \nu$ where $x_j \not| \, \nu$, then $x_i^h x_j^{k-h} \nu \in I$ for all h such $h \leq_p k$.*

If I is Borel-fixed, condition $(\#)$ is satisfied by every monomial $\mu \in I$.

Proof. I is stable under the action $\mathcal{D}$ if and only if it is monomial, and a monomial ideal I is Borel-fixed if and only if every $E_{ij}(c)$, $c \in K - \{0\}$ and $i < j$, maps I into itself, since the diagonal matrices together with the $E_{ij}(c)$ for $i < j$ generate $\mathcal{B}^{\mathrm{U}}$. It is sufficient that every μ in a set of monomial generators for I map into I, and it is necessary that every $\mu \in I$ map into I. But given μ, its image under the map that sends $x_j \mapsto cx_i + x_j$ while the other variables are fixed is

$$(cx_i + x_j)^k \nu = \sum_{0 \leq h \leq_p k} \binom{k}{h} c^k x_i^h x_j^{k-h} \nu,$$

since the integers h satisfying $0 \leq h \leq_p k$ are precisely the ones that yield a nonzero binomial coefficient. The stated result is now immediate. $\square$