ALGEBRA III
SEPTEMBER 9, 2004

GABRIEL C. DRUMMOND-COLE

Monomial ideals are easiest: $I = \langle m_i | i \in A\rangle \subset k[x_1, \ldots, x_n] = S$. Monomials are $m = \underline{x}^{\underline{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. We can look at the staircase diagram that comes from α.

So we want to look at the dimension of $R = k[x_1, \ldots, x_n]/I = \oplus_{i=0}^{\infty} R_i$ a k-vectorspace. Note that $R_i R_j \subset R_{i+j}$.

Now, $dim_k(R) =$ and $dim_k(R_i)$ is the number of monomials of degree i in S not in I_i.

Now say J is a more general ideal. We're going to find a monomial ideal I such that all monomials not in I form a basis for S/J as a k-vector space. This will prove the Hilbert basis theorem. It will also eventually allow us to decide whether an element of S lives in J. If J is homogeneous, I'll also be able to find the dimensions of the graded pieces. If J is a homogeneous ideal $\langle f_1, \ldots, f_n\rangle$, then S/J is a graded vector space $\oplus_{i=0}^{\infty} V_j$. We have a very important function $H : p \to dim)k(S/J)_p$. It turns out that this agrees with a polynomial except at finitely many values.

Now if J were a monomial ideal, then counting this dimension would be easy. So how do you find this monomial ideal? You essentially want to pick monomials out of the polynomials you have. So you need some sort of ordering.

Now you need your monomial ideal to contain a monomial from each generator polynomial of J.

Definition 1. *Given an order on the variables, a monomial order on $S = k[x_1, \ldots, x_n]$ is a relation $\succ$ on $\underline{x}^{\underline{\alpha}}$ such that*

(1) *$\succ$ is a total ordering*
(2) *$\succ$ is compatible with $\cdot$, so that $\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}}$ implies $\underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\gamma}}\underline{x}^{\underline{\beta}}(\succ \underline{x}^{\underline{\gamma}}$*
(3) *$\succ$ is a well-ordering (redundant with the end of the previous line)*

Exercise 1. *Show that any selection function to give the monomial ideal I must be a monomial order.*

Exercise 2. *Show that there is only one monomial order on $k[x]$, the order by degree.*

Typically a monomial order will refine the degree. Now say you are in $k[x_1, \ldots, x_n]$. Here are some orders:

- lex: Here, $\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}}$ if the leftmost nonzero entry of $\underline{\alpha} - \underline{\beta}$ is positive.
- Grlex: Grade first by degree, i.e., by $\alpha \succ \beta$ if $|\alpha| > |\beta|$ and then if $|\alpha| = |\beta|$ you grade by lex.

- This is a bad order, but is the best possible for doing computations. You can eliminate variables. revlex: $\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}}$ if either $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta$ is negative.

Exercise 3. *There is one order refining degree in two variables.*

So compare x^3y^6 with x^3y^4z, then x^3y^6 is greater in glex. This is also largest in revlex.

On the other hand, for xz and y^2 we have xz larger in glex and y^2 larger in revlex.

There are other orders you can build, which have some geometric interpretation. You look at some weighted functional related to a polytope in some way.

Definition 2. *If $f \in k[x_1, \dots, x_n]$ and $\succ$ is a monomial ordering, then the initial $m_\succ(f)$ is the largest monomial in f with respect to $\succ$.*

Exercise 4. (1) *If $m_{lex}(f) \in k[x_s, \dots, x_n]$, then $f \in k[x_s, \dots, x_n]$. If f is homogeneous then the same is true for m_{Grlex}.*
(2) *If $m_{revlex}(f) \in (x_s, \dots, x_n)$, then $f \in (x_s, \dots, x_n)$. Note that this is an ideal whereas in the first case it was a subring.*

Lemma 1. *Dickson Lemma*
Any set of monomials has only finitely many minimal elements in the partial order given by divisibility. Equivalently, every monomial ideal is finitely generated (by a subcollection of any set of monomial generators)

Now take your favorite ideal $J \subset S$ and a monomial ordering $\succ$. Now take from each polynomial in J the initial monomial to get the initial ideal of J, $m_\succ(J) = \langle m_\succ(f) | f \in J \rangle$. With the Dickson lemma this will give us the Hilbert basis theorem. That is, $m_\succ(J)$ will be a monomial ideal. Then a subcollection $\langle m_\succ(g_1), \dots, m_\succ(g_m) \rangle$ will generate $m_\succ(J)$ and we can get that $\langle g_1, \dots, g_m \rangle$ generates J. Then J is finitely generated. If you want to be really picky, this works not just over a field, but over any Noetherian ring. Now such a set $\{g_1, \dots, g_m\}$ is called a Gröbner basis.

This shouldn't really be called a Gröbner basis because Gröbner didn't really work with these. His student did. Other people were already working with things like these, in, say, power series rings.

This is essentially Gordon's proof of Hilbert's basis theorem. The standard proof was by induction and was nonconstructive. Hilbert put the German mathematicians looking for these things out of business by saying that these were always finitely generated. But he gave no way to find the generators. Gordon gave you a way to find it.

You use this stuff to prove that $k[x_1, \dots, x_n]^{\sigma_n} = k[y_1, \dots, y_n]$ by $y_i \to \sigma_i$, where these are the symmetric polynomials of degree i.

Now I'm going to give you an algorithm. A lot of these are no good from a computer scientist standpoint. If you work in Grlex, the degree of the Gröbner basis will be doubly exponential in the number of variables, whereas with revlex the degree will be roughly comparable with the number of variables.

By the way, this also solves the problem of ideal membership. I give you a finite polynomial basis and I want to know if another polynomial, say 1 for instance, is in their span. You look instead at the initials. It is a combination if and only if the initial term is in the initial ideal.

Now let's prove Dickson's lemma.
We'll proceed by induction on the number of variables. If $n = 1$ then the ideal is $\langle x_1^{\alpha} | \alpha \in A \subset \mathbb{N}\rangle = \langle x_1^{\alpha_{min}} | \alpha_{min} = \min\{\alpha | \alpha \in A\}\rangle$ So if $n = 1$ then the ideal is principally generated.

For the induction step, I'm going to use $\underline{x}$ to refer to the monomial factor in the first $n-1$ variables. Now, we want to look at $(I : x_n^{\infty})$ by which we mean $\langle \underline{x^{\alpha}} | \exists m_{\alpha}, \underline{x^{\alpha}} x_n^{m_{\alpha}} \in I\rangle$. This is an ideal $J \subset k[x_1, \dots, x_{n-1}]$ which is finitely generated (by $\{\underline{x^{\alpha_1}}, \dots, \underline{x^{\alpha_s}}\}$ by induction. So take first $\underline{x^{\alpha_i}} x_n^{m_i}$ For each $k < \max\{m_i\}$ let $J_k = (I : x_n^k) = \langle \underline{x^{\alpha}} | \underline{x^{\alpha}} x_n^k \in I\rangle \subset k[x_1, \dots, x_{n-1}]$. This is finitely generated by $\{\underline{x^{\alpha_{k1}}}, \dots, \underline{x^{\alpha_{ks}}}\}$. Then my Gröbner basis will be $\{\underline{x^{\alpha_i}} x_n^{m_i}, \underline{x^{\alpha_{kj}}} x_n^k\}$. So you just show that these generate I, which is fairly straightforward.

The only thing missing is that you can always get a subcollection. Say $I = \langle \underline{x^{\alpha}}, \alpha \in A\rangle$. We pick a Gröbner basis $\{\underline{x^{\beta_i}}\}$; each of these must be a multiple of some $\underline{x^{\alpha_i}}$. Then this collection of corresponding $\underline{x^{\alpha_i}}$ generates I as well.

This triviality is called Macaulay's theorem:

Theorem 1. *A basis of S/I is formed by all monomials not in $m_{\succ}(I)$.*