Math 615: Lecture of January 8, 2007

Monomial Ideals and Submodules

Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. When a free R-module F is given, it will typically be assumed to be finitely generated with an ordered free basis $b_1, \ldots, b_n$. The ordered free basis provides an isomorphism with R^n under which $\sum_{i=1}^n r_i b_i$ corresponds to $(r_1, \ldots, r_n)$. Therefore, for the most part, in working with a free module with ordered basis, we might as well assume that it is R^n with the standard basis $e_1, \ldots, e_n$, where e_i has 1 in the ith spot and 0 in the other spots. However, especially when we are working with more than one free module, it may be inconvenient to identify all of the modules with various R^{n_i}.

By a *monomial* μ in R, we mean an element of the form $x_1^{a_1} \cdots x_n^{a_n}$ where the $a_i \in \mathbb{N}$, the nonnegative integers. If $\alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n$, we write x^α for $x_1^{a_1} \cdots x_n^{a_n}$. Thus, there is a bijection betwen monomials of R and elements of $\mathbb{N}^n$. We write $\mathcal{M}$ for the set of monomials of R.

More generally, given a finitely generated free module F with ordered basis, by a *monomial* in F we mean an element of the form μb_i, where $\mu \in M$ and b_i is in the ordered basis. In particular, when $F = R^s$ with the standard basis, we mean an element of the form μe_i with $\mu \in \mathcal{M}$.

The monomials of F form a K-vector space basis for F. Every element $f \in F$ is uniquely expressible as a K-linear combination of mutually distinct monomials (for 0, the set of monomials occurring is the empty set). We refer to the monomials that occur as the *monomials of* f. We shall refer to the product of a nonzero element of K with a monomial as a *term*. Thus, every element of F is uniquely expressible as a sum of terms involving mutually distinct monomials: these terms are referred to as the *terms of* f. In particular, this terminolgy applies in the case where $F = R$.

Proposition. *Let $R = K[x_1, \ldots, x_n]$ be a polynomial ring over K. Let $F \cong R^s$ be a free module with ordered basis. The following three conditions on a submodule M of F (respectively, an ideal I of R) are equivalent:*

(1) *M (respectively, I) is generated by monomials.*

(2) *M (respectively, I) is the K-span of monomials.*

(3) *If $f \in M$ (respectively, I), the monomials of f are in M (respectively, I).*

Moreover, if M (respectively, I) is generated by monomials ν_λ (the index set may be infinite), then $f \in M$ if and only if every monomial in f is the product of a monomial $\mu \in \mathcal{M}$ and some ν_λ.

Proof. It suffices to consider the module case. Suppose that $\mathcal{G}$ is a family of monomials in F. The submodule generated by $\mathcal{G}$ must contain all the elements $\{\mu\nu : \mu \in \mathcal{M}, \nu \in \mathcal{G}\}$.

The K-span of this set of monomials is closed under multiplication by any element of R, by the distributuve law. It follows that (1) $\Rightarrow$ (2). This implies the final statement. Moreover, (2) $\Rightarrow$ (1) and (2) $\Leftrightarrow$ (3) are obvious. $\square$

Of course, it is *not true* that an arbitrary set of monomials spans a submodule: $\mathcal{G}$ spans a submodule if and only if whenever $\nu \in \mathcal{G}$ and $\mu \in \mathcal{M}$, we have that $\mu\nu \in \mathcal{G}$.

Consider a K-vector space with basis $\mathcal{B}$, and let $\mathcal{S}$ be the set of K-vector subspaces that are spanned by a subset of $\mathcal{B}$. Then there is an order-preserving bijection between $\mathcal{S}$ and the set of subsets of $\mathcal{B}$. This bijection preserves intersection, even infinite intersection, and takes sums, even infinite sums, to unions. Thus, for such a family of vector spaces, intersection distributes over sum (even when the sum is infinite) and union distributes over intersection (even if the intersection is infinite).

Since monomial ideals (respectively, monomial submodules) have K-bases consisting of monomials, it follows that for monomial ideals and submodules, intersection distributes over sums, including infinite sums, and sum distributes over intersections, even infinite intersections.

Let $\alpha = (a_1, \ldots, a_n)$ and let $\beta = (b_1, \ldots, b_n)$. Let $c_i = \min\{a_i, b_i\}$ for each i and let $d_i = \max\{a_i, b_i\}$ for each i. Let $\gamma = (c_1, \ldots, c_n)$ and $\delta = (d_1, \ldots, d_n)$. We define $\mathrm{GCD}(x^\alpha, x^\beta) = x^\gamma$, and $\mathrm{LCM}(x^\alpha, x^\beta) = x^\delta$. These definitions agree with the usual UFD notions of greatest common divisor and least common multiple.

In particular, $x^\alpha R \cap x^\beta R = x^\delta R$ where $x^\delta = \mathrm{LCM}(x^\alpha, x^\beta)$. Now suppose that I is generated by monomials x^{α_i} where i varies in some index set, and that J is generated by monomials x^{β_j}, where j varies in some index set. Thus, I is the sum of the ideals $x^{\alpha_i}R$ and J is the sum of the ideals $x^{\beta_j}R$. Since intersection distributes over sum for monomial ideals, it follows that $I \cap J$ is the sum of the ideals $x^{\gamma_{ij}}R$, where $\gamma_{ij} = \mathrm{LCM}(\alpha_i, \beta_j)$, since $x^{\gamma_{ij}}R = x^{\alpha_i}R \cap x^{\beta_j}R$ for all choices of i and j.

Now let F be a finitely generated free module with ordered basis $B_1, \ldots, B_s$. We can extend these definitions to pairs of monomials of F that involve the same basis element, so that $\mathrm{GCD}(\mu_1 b_i, \mu_2 b_i) = \mathrm{GCD}(\mu_1, \mu_2)b_i$ and $\mathrm{LCM}(\mu_1 b_i, \mu_2 b_i) = \mathrm{LCM}(\mu_1, \mu_2)b_i$

Lemma. *If $\{a_n\}_{n\in\mathbb{N}}$ is an infinite sequence of nonnegative integers, then it has an infinite subsequence that is either constant or strictly increasing. In particular, it has an infinite subsequence that is non-decreasing.*

Proof. If the sequence is bounded above, then only finitely many integers occur, and so at least one of them must occur infinitely many times. If the sequence is not bounded, let $n_1 = 1$ and, recursively, let n_{i+1} be the least integer strictly larger than n_i such that $a_{n_{i+1}} > a_{n_i}$. (If there is no such integer, then the sequence is bounded above.) Clearly, $\{a_{n_i}\}_i$ is strictly inreasing. $\square$

The Lemma above is quite easy, but it has an interesting consequence. Let F be a finitely generated free module with ordered basis over $R = K[x_1, \ldots, x_n]$. The set of

monomials of F is partiallly ordered by $\nu_1 \geq \nu_2$ means that $\nu_2 = \mu\nu_1$ for some $\mu \in \mathcal{M}$, i.e., ν_2 is a multiple (necessarily by a monomial) of μ_1. Then:

Proposition. *Let R and F be as above. Then there is no infinite subset of F consisting of mutually incomparable monomials. Equivalently, given any infinite sequence of monomials in F, one of them divides another. In particular, this holds when $F = R$.*

Proof. Suppose that $\nu_1, \nu_2, \nu_3, \ldots$ is an infinite sequence of monomials in F. Then some e_i must occur in infinitely many terms, and so we may pass to an infinite subsequence in which each term has the form $\mu_n e_i$. It therefore suffices to prove the result for an infinite sequence $\mu_1, \mu_2, \mu_3, \ldots$ of monomials in R. Consider the exponents $a_1, a_2, a_3, \ldots$ occurring on the variable x_1 in this sequence. Then we may pass to an infinite subsequence such that these exponents are non-decreasing, by the Lemma above. By the same reasoning we may pass to a still smaller infinite subsequence such that the exponents $b_1, b_2, b_3, \ldots$ on x_2 are *also* non-decreasing. By a straightforward induction, we may repeat this step for each variable, and the n th subsequence obtained will have the property that for all of the variables x_i, where $1 \leq i \leq n$, the sequence of exponents on x_i is non-decreasing. But this means that every monomial in the subsequence divides all monomials that come after it in the subsequence. $\square$

Corollary. *Let R and F be as above. Then every monomial submodule M of F is finitely generated by the set of minimal monomials in M under the partial ordering by divisibility. In particular, this holds for monomial ideals in R.*

Proof. Given any monomial in F, there are only finitely monomials in F that are smaller in the partial ordering, and so given any monomial in M, among the monomials in M that divide it there must be a minimal one. Therefore, M is generated by the minimal monomials in M. Since these are mutually incomparable, the preceding Proposition shows that the set of minimal monomials in M is finite. $\square$

The set of minimal monomials in a monomial submodule (or ideal) is also referred to as the *set of minimal monomial generators*.

Gröbner bases reduce a multitude of problems about ideals of R and about arbitrary submodules of a free module F to the monomial case! In particular we shall use them to give a very simple proof of the Hilbert basis theorem. In order to define Gröbner basis, we need to introduce the idea of a monomial order.

Monomial orders

Let $R = K[x_1, \ldots, x_n]$ and let $\mathcal{M}$ be the set of all monomials in R. A *monomial order* on $\mathcal{M}$ is a *total* ordering $>$ of $\mathcal{M}$ such that

(1) If $\mu, \mu_1, \mu_2 \in \mathcal{M}$ and $\mu_1 > \mu_2$ then $\mu\mu_1 > \mu\mu_2$.

(2) The element 1 is the least element in $\mathcal{M}$.

The second property implies that a monomial order refines the partial ordering by divisibility: since $1 \leq \mu_2$ for all $\mu_2 \in \mathcal{M}$, we have that $\mu_1 \leq \mu_1\mu_2$ for all μ_1, $\mu_2 \in \mathcal{M}$ By renumbering the variables, we may assume that $x_1 > x_2 > \cdots > x_n$, and we shall always assume this about any monomial order that we introduce.

By a *monomial order* on a finitely generated free module F with ordered basis $b_1, \ldots, b_s$ we mean a total ordering of the monomials in F such that

(1) If $\mu \in \mathcal{M}$ and ν_1, ν_2 are monomials in F with $\nu_1 > \nu_2$, then $\mu\nu_1 > \mu\nu_2$.

(2) For every i, the element b_i is least among the elements of the form μb_i for μ in $\mathcal{M}$.

Property (2) implies that if $\nu \in F$ is a monomial and $\mu \neq 1$ is in $\mathcal{M}$, then $\nu < \mu\nu$. Evidently, this agrees with the first definition when $F = R$ with the ordered basis consisting of 1.

Given a monomial order $>$ on $\mathcal{M}$ we can construct a monomial order on F by requiring that $\mu_1 b_i > \mu_2 b_j$ precisely when $\mu_1 > \mu_2$ or $\mu_1 = \mu_2$ and $i < j$ (so that $b_1 > b_2 > \cdots b_s$). Unless otherwise specified, we shall always do this in working with monomial orders on free modules.

To see that monomial orders on R exist, we give the example of *lexicographic* order, frequently referred to simply as *lex* order. If $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$, the definition is simply that $x^\alpha > x^\beta$ precisely if there exists an integer j, where $1 \leq j \leq n$, such that $a_i = b_i$ for $i < j$ while $a_j > b_j$. It is very easy to see that this satisfies (1) and (2) above. Note that it is true that $x_1 > \cdots > x_n$ as well.

Suppose that x_1, x_2, x_3 $\ldots$, x_{26} are the letters of the Roman alphabet, A, B, C, $\ldots$, Z. Suppose that given a monomial we write it out as a string of letters with letters occurring in alphabetical order, so that $x_1^3 x_2 x_3^2 x_4^5$ would be written out as $AAABCCDDDDD$. The order we have specified is the same order as these "words" would occur in a dictionary or lexicon. This is the reason for the term "lexicographic order."

We shall soon see that if R has two or more variables, there are uncountably many monomial orders! However, we really only need to make use of two or three of them.