Lecture Notes for Math 627B
Modern Algebra
Groebner Bases

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
wwww-rohan.sdsu.edu/ ~ mosulliv

February 20, 2013

1 Monomial Orderings

Definition 1.1. A *monomial ordering* $<$ (also called a *term ordering*) is a an ordering of $\mathbb{N}_0^n$ such that

(1) $<$ is a total ordering: for any $\alpha, \beta \in \mathbb{N}_0^n$, either $\alpha < \beta$, or $\alpha = \beta$ or $\alpha > \beta$.

(2) $<$ respects addition: $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$.

(3) $<$ is a well ordering: any nonempty subset of $\mathbb{N}_0^n$ has a least element.

Given a term ordering, for $f \in k[x_1, \ldots, x_n]$ we will write $\mathrm{LT}(f)$ for the leading term, $\mathrm{LM}(f)$ for the leading monomial, $\mathrm{LC}(f)$ for the leading coefficient, and $\mathrm{LE}(f)$ for the leading exponent (the exponent of the leading term). IVA calls $\mathrm{LE}(f)$ the multidegree and uses $\mathrm{mdeg}(f)$.

Here is a summary of a results concerning monomial orderings from Robbiano (*Theory of graded structures*, 1986, and *Term orderings on the polynomial ring* , 1985).

(1) Any term ordering on $\mathbb{N}_0^n$ extends in a unique way to a term ordering on $\mathbb{Z}^n$.

(2) Any term ordering on $\mathbb{Z}^n$ extends in a unique way to a term ordering on $\mathbb{Q}^n$.

(3) Any term ordering on $\mathbb{Q}^n$ extends is such that $(\mathbb{Q}^n)^+$ (the set of elements larger than $(0,\ldots,0)$) is convex, and $(\mathbb{Q}^n)^-$ (the set of elements smaller than $(0,\ldots,0)$) is also convex.

(4) This implies that the ordering is continuous. That means $\forall\alpha \in \mathbb{Q}^n$ if ther exists a neighborhood U_α such that $U_\alpha - \{\alpha\} \subseteq (\mathbb{Q}^n)^+$ then $\alpha \in (\mathbb{Q}^n)^+$ (and similarly for $-$).

(5) Thus, every ordering on $\mathbb{Q}^n$ extends to a continuous order on $\mathbb{R}^n$.

I will just explain the first step above (the second is similar, the rest are harder). Suppose that $<$ is an ordering on $\mathbb{N}_0^n$. Let $\alpha, \beta \in \mathbb{Z}^n$ (so α and β may have negative terms). There is some $\gamma \in \mathbb{N}_0^n$ such that $\alpha + \gamma$ and $\beta + \gamma$ both have positive components (Check this!). We will say that $\alpha < \beta$ if $\alpha + \gamma < \beta + \gamma$. Since there are many choices for γ, we have to check consistency: $\alpha + \gamma < \beta + \gamma$ iff $\alpha + \gamma' < \beta + \gamma'$ for all γ' large enough so that $\alpha + \gamma'$ and $\beta + \gamma'$ are in $\mathbb{N}_0^n$. (Check this!)

Theorem 1.2. *Every term ordering on $\mathbb{N}_0^n$ is given by some sequence $u_1, u_2, \ldots, u_s \in \mathbb{R}^n$, in the following sense. $\alpha < \beta$ iff there is some t such that $\alpha \cdot u_i = \beta \cdot u_i$ for $i < t$ and $\alpha \cdot u_t < \beta \cdot u_t$.*

The $\cdot$ means the dot product. In other words, $\alpha < \beta$ if $\alpha \cdot u_1 < \beta \cdot u_1$ and $\alpha > \beta$ if $\alpha \cdot u_1 > \beta \cdot u_1$. If this test is inconclusive, that is $\alpha \cdot u_1 = \beta \cdot u_1$, then use u_2 to compare. Continue on till you get a definitive answer.

If there are n vectors $u_1, \ldots u_n$ and they are linearly independent, then any unequal α and β will be distinguished by one of these tests (Check!). It is possible for fewer than n vectors to determine a total ordering. This is because α and β have integer entries. Find an example with $n = 2$.

2 Groebner Bases

Fix a monomial ordering.

Theorem 2.1 (Dickson)**.** *Every monomial ideal has a finite generating set. More precisely, for $A \subseteq \mathbb{N}_0^n$ there is a finite $A' \subseteq A$ such that*

$$\langle x^\alpha : \alpha \in A \rangle = \langle x^\alpha : \alpha \in A' \rangle$$

Furthermore, we may take A' so that $x^\alpha \nmid x^\beta$ for all $\alpha, \beta \in A'$.

The last sentence of the theorem should be fairly clear. If x^α divides x^β then any monomial divisible by x^β is also divisible by x^α so we may remove β from A' and still have a generating set. Removing all such unnecessary exponents gives the result.

Every monomial ideal has a finite generating set.

Theorem 2.2 (Groebner Basis)**.** *Any ideal I in $k[x_1, \ldots, x_n]$ is finitely generated. There is a subset $G = \{g_1, \ldots, g_t\} \subseteq I$ such that $I = \langle g_1, \ldots, g_t \rangle$.*

Proof. Let $x^{\alpha_1}, \ldots, x^{\alpha_t}$ generate $\langle \mathrm{LT}(I) \rangle$. By Diskson's lemma the x_i^α are leading terms of elements of I, say $x^{\alpha_i} = \mathrm{LT}(g_i)$. Now let $f \in I$. Dividing f by G we get $f = a_1 g_1 + \cdots + a_t g_t + r$ and the remainder r has no terms divisible by any of the x^{α_i} (terms are only placed in the remainder when they are not divisible by any leading term of a g_i). Now $f - \sum a_i g_i = r \in I$. If $r \neq 0$ then $\mathrm{LT}(r) \in \langle \mathrm{LT}\, I) \rangle$ so $\mathrm{LT}(r)$ is divisible by some x^{α_i}. This gives a contradicition. Thus $r = 0$. □

There are several corollary results that we can derive with a careful look at the proof.

Definition 2.3. Given a term order on $k[x_1, \ldots, x_n]$ and ideal I let $\Delta(I) = \mathbb{N}_0^n - \mathrm{LT}(I)$. We will call $\Delta(I)$ the *footprint* of I.

Proposition 2.4. *Given $f \in I$ there is a unique $g \in I$ and unique $r = \sum_{\alpha \in \Delta(I)} r_\alpha x^\alpha$ such that $f = g + r$. Furthermore, for any Groebner basis, G (and any ordering of G), r is the remainder when f is divided by G.*

Proof. We can divide any $f \in k[x_1, \ldots, x_n]$ by a Groebner basis $G = \{g_1, \ldots, g_t\}$ and get $f = \sum a_i g_i + r$ with remainder r having terms with exponents in $\Delta(I)$. Let $g = \sum a_i g_i$. We have shown existence of g, r; must show uniqueness. Suppose $f = g + r$ and $f = g' + r'$. Then $g + r - (g' + r') = 0$ so $g - g' = r' - r$. I claim $g = g'$ and $r = r'$. If not $g - g' \in I$, so $\mathrm{LE}(g - g') \notin \Delta(I)$. On the other hand $\mathrm{LE}(r - r') \in \Delta(I)$ since all terms of r and r' have exponents in $\Delta(I)$. This gives a contradiction.

We have also shown that r is the remainder when f is divided by G, for any Groebner basis G. □

Note: this is all based on a fixed term order!.

Definition 2.5. A Groebner basis G for I is *minimal* when each $g \in G$ is monic and $\{\mathrm{LT}(g) : g \in G\}$ satisfies the second sentence of Theorem 2.1, $LT(g) \nmid \mathrm{LT}(g')$ for all $g, g' \in G$. A Groebner basis is *reduced* when in addition no term of $g \in G$ is divisible by $\mathrm{LT}(g')$ for $g' \in G - \{g\}$.

Proposition 2.6. *A nonzero ideal I has a unique reduced Groebner basis.*

Proof. For existence, let $G = \{g_1, \dots, g_t\}$ be a minimal Groebner basis. Divide g_1 by $g_2, \dots g_t$. We get $g_1 = \sum_{i-2}^{t} a_i g_i + r_1$. Furthermore $r_1 \in I$ and r_1 has the same leading term as g_1. Replace g_1 with r_1 and we still have a minimal Groeber basis, but no term of r_1 is divisible by $\mathrm{LT}(g_i)$ for $i = 2, \dots, t$. Proceed similarly with g_i for $i = 2, \dots, t$. $\square$

These important results generalize the Division Theorem (we get a unique remainder, and element of I). We have also solved the ideal description problem in a satisfying way: there is a *unique* Groebner basis. We have an easy test for ideal membership, divide by the Groebner basis and see if the results is 0.

The next and key question is how to compute a Groebner basis, akin to the question for $k[x]$: how do we compute the gcd of two polynomials in one variable? The answer in one indeterminate is the Euclidean algorithm. It is not so simple with several indeterminates.

3 S-polynomials

Definition 3.1. Let $\alpha, \beta \in \mathbb{N}_0^n$. For $i = 1, \dots, n$, let $\gamma_i = \max(\alpha_i, \beta_i)$. We will call γ the $\mathrm{LCM}(\alpha, \beta)$. We will also call x^γ the $\mathrm{LCM}(x^\alpha, x^\beta)$.

It should be clear that $\mathrm{LCM}(x^\alpha, x^\beta)$ is the smallest monomial that is a multiple of both x^α and x^β. Using LCM for α and β is a small abuse of terminology that may be useful at some point.

Definition 3.2. Let $f, g \in k[x_1, \dots, x_n]$. The syzygy polynomial of f and g (also called the S-polynomial is

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} f - \frac{x^\gamma}{\mathrm{LT}(g)} g$$

where $\gamma = \mathrm{LCM}(\mathrm{LE}(f), \mathrm{LE}(g))$.

In other words if the leading term of f is x^α (we may as well take it to be monic) and the leading term of g is x^β, then $\dfrac{x^\gamma}{\mathrm{LT}(f)} f$ and $\dfrac{x^\gamma}{\mathrm{LT}(g)} g$ both have leading term x^γ, which is the smallest monomial divisible by both $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$. The S-poly results from taking the smallest multiples of f and g that will give cancellation of leading terms. Thus $\mathrm{LM}(S(f,g)) < \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g))$. Of course if $f, g \in I$ then $S(f,g) \in I$.

Let $F = \{f_1, \ldots, f_s\}$ and let $I = \langle F \rangle$ be the ideal generated by F. We would like to have (1) a test to see if F is a Groebner basis for I and (2) an algorithm to compute a Groebner basis for I if F is not one.

The algorithm is essentially this: for various $f_1, f_2 \in F$ compute $S(f_1, f_2)$ then divide the result by F and get a remainder r with no terms divisible by leading terms of polynomials in F. Since $S(f_1, f_2) \in I$ and we divided by $F \subseteq I$ we must have $r \in I$. In particular $\mathrm{LT}(r)$ is not divisible by $\mathrm{LT}(f)$ for all $f \in F$. If $r \neq 0$, we add r to our set F and repeat the process: choose two elements of $F \cup \{r\}$, compute their S-poly, divide by $F \cup \{r\}$ to get a remainder, if it is nonzero throw it into our set of polynomials and continue.

Note: $\overline{h}^F$ means the remainder when h is divided by F where F is an ordered set of polynomials, $F = f_1, \ldots, f_t$. The symbol $h \to_F r$ means that $h = \sum a_i f_i + r$ and $\mathrm{LE}(f) \geq \mathrm{LE}(a_i f_i)$ for all i with $a_i \neq 0$. We'll discuss this in class.

Theorem 3.3 (S-poly). *Let $G = \{g_1, \ldots, g_t\}$ be a generating set for I. G is a Groebner basis for I iff $\overline{S(g_i, g_j)}^G = 0$ for all i, j.*

Futhermore the algorithm described above terminates with a Groebner basis for I after a finite number of steps.

These results take some work to prove. We will use them now, and I will prove later after covering some of the general theory of rings and modules.