

# Math 499 Lecture Notes

Amanda Knecht

February 9, 2005

## 1 Monomial Ordering

**Notation:** Let  $\alpha = (\alpha_1, \dots, \alpha_n)$  for  $\alpha_i$  nonnegative integers and  $x = (x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ .

We write  $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ . We also can define the absolute value  $|\alpha| = \sum_{i=1}^n \alpha_i$ .

**Definition.** A *monomial ordering* on  $\mathbb{C}[x_1, \dots, x_n]$  is any relation  $>$  on  $\mathbb{Z}_{\geq 0}^n$  satisfying:

- (i)  $>$  is a total (or linear) ordering on  $\mathbb{Z}_{\geq 0}^n$ .
- (ii) If  $\alpha > \beta$  and  $\gamma \in \mathbb{Z}_{\geq 0}^n$ , then  $\alpha + \gamma > \beta + \gamma$ .
- (iii)  $>$  is a well-ordering on  $\mathbb{Z}_{\geq 0}^n$ . (i.e. every nonempty subset of  $\mathbb{Z}_{\geq 0}^n$  has a smallest element under  $>$ )

**Definition. (Lexicographic Order)** Let  $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$ . We say that  $\alpha >_{lex} \beta$  if, in the vector difference  $\alpha - \beta \in \mathbb{Z}^n$ , the left-most nonzero entry is positive. We write  $x^\alpha >_{lex} x^\beta$  if  $\alpha >_{lex} \beta$ .

**Examples:**

(a)  $t^5 x^2 y^3 >_{lex} t x^5 y^5$  because  $(5, 2, 3) - (1, 5, 5) = (4, -3, -2)$ .

(b)  $t x^2 y^3 >_{lex} t x y$  because  $(1, 2, 3) - (1, 1, 1) = (0, 1, 2)$ .

In practice, if we are given two or three variables, we will call them  $x, y$  or  $x, y, t$ , respectively, and use alphabetical order  $t > x > y$  in order to define the lexicographic order. There are two other orderings which could come into play this semester, so we will define them now.

**Definition. (Graded Lex Order)** Let  $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ . We say  $\alpha >_{grlex} \beta$  if either

- 1.  $|\alpha| > |\beta|$
- 2. or  $|\alpha| = |\beta|$  and  $\alpha >_{lex} \beta$ .

Simply stated, grlex orders by total degree first and then uses lex order to break ties in total degree.

**Examples:**

(a)  $t x^2 y^3 >_{grlex} t^4 x$  because  $|(1, 2, 3)| = 6 > |(4, 1, 0)| = 5$

(b)  $t x^2 y^3 >_{grlex} t x y^4$  because  $|(1, 2, 3)| = 6 = |(1, 1, 4)|$  and  $t x^2 y^3 >_{lex} t x y^4$

**Definition. (Graded Reverse Lex Order)** Let  $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ .

We say  $\alpha >_{grelex} \beta$  if either

- 1.  $|\alpha| > |\beta|$

2. or  $|\alpha| = |\beta|$  and in  $\alpha - \beta$  the right-most nonzero entry is negative.

As with grlex, grevlex orders by total degree, but now to break ties we look at the right-most nonzero entry instead of the left-most.

**Examples:**

- (a)  $txy >_{\text{grevlex}} tx$
- (b)  $tx^2 >_{\text{grevlex}} txy$

Now, let's see how to put the terms of a polynomial in  $\mathbb{C}[x_1, \dots, x_n]$  in decreasing order with respect to these orderings. For an example, let's set  $f = 4x^2y^4 - 6ty + 3t^2xy - ty^5$ .

- With respect to lex order, we would write

$$f = 3t^2xy - ty^5 - 6ty + 4x^2y^4.$$

- With respect to grlex order, we would write

$$f = -ty^5 + 4x^2y^4 + 3t^2xy - 6ty.$$

- With respect to grevlex order, we would write

$$f = 4x^2y^4 - ty^5 + 3t^2xy - 6ty.$$

In order to generalize this example to all polynomials in  $n$  variables we develop the following terminology.

**Definition.** Let  $f = \sum_{\alpha} a_{\alpha}x^{\alpha}$  be a nonzero polynomial in  $\mathbb{C}[x_1, \dots, x_n]$  and let  $>$  be a monomial order.

(i) The **multidegree** of  $f$  is defined

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0).$$

(ii) The **leading coefficient** of  $f$  is

$$LC(f) = a_{\text{multideg}(f)} \in k.$$

(iii) The **leading monomial** of  $f$  is

$$LM(f) = x^{\text{multideg}(f)}.$$

(iv) The **leading term** of  $f$  is

$$LT(f) = LC(f) \cdot LM(f).$$

So, in our example from before where  $f = 4x^2y^4 - 6ty + 3t^2xy - ty^5$  we have:

- With respect to lex order:

$$\text{multideg}(f) = (2, 1, 1), LC(f) = 3, LM(f) = t^2xy, LT(f) = 3t^2xy$$

- With respect to grlex order:

$$\text{multideg}(f) = (1, 0, 5), LC(f) = -1, LM(f) = ty^5, LT(f) = -ty^5$$

- With respect to grevlex order,

$$\text{multideg}(f) = (0, 2, 4), LC(f) = 4, LM(f) = x^2y^4, LT(f) = 4x^2y^4$$

**Lemma.** Let  $f, g \in \mathbb{C}[x_1, \dots, x_n]$  be nonzero polynomials. Then:

(i)  $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$ .

(ii) If  $f + g \neq 0$ , then  $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$ . Equality holds if  $\text{multideg}(f) \neq \text{multideg}(g)$ .

Now that we have established what we mean by a leading term with respect to a given monomial ordering, we can speak of a **division algorithm** in the ring  $\mathbb{C}[x_1, \dots, x_n]$ .

**Proposition.** Fix a monomial order  $>$  on  $\mathbb{Z}_{\geq 0}^n$  and let  $F = (f_1, \dots, f_s)$  be an ordered  $s$ -tuple of polynomials in  $\mathbb{C}[x_1, \dots, x_n]$ .

Then every  $f \in \mathbb{C}[x_1, \dots, x_n]$  can be written as  $f = a_1 f_1 + \dots + a_s f_s + r$ , where  $a_i, r \in \mathbb{C}[x_1, \dots, x_n]$ , and either  $r = 0$  or  $r$  is a linear combination, with coefficients in  $k$ , of monomials, none of which is divisible by any  $\text{LT}(f_i)$ . Furthermore, if  $a_i f_i \neq 0$  then  $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$ .

## 2 Monomial Ideals

**Definition.** An **ideal**,  $I$ , of the polynomial ring  $\mathbb{C}[x_1, \dots, x_n]$  is a subset of  $\mathbb{C}[x_1, \dots, x_n]$  such that:

1. If  $a, b \in I$ , then  $a + b \in I$ .
2. If  $a \in I$  and  $f \in \mathbb{C}[x_1, \dots, x_n]$ , then  $af \in I$ . [namely, 0 and  $-a$  are in  $I$ ]

**Notation:**

For an ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$ , we let  $V(I) = \{p \in \mathbb{C}^n \mid f(p) = 0 \text{ for all } f \in I\}$ .

**Definition.** An ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$  is a **monomial ideal** if there is a subset  $A \subset \mathbb{Z}_{\geq 0}^n$  (can be infinite) such that  $I$  consists of all polynomials which are finite sums of the form  $\sum_{\alpha \in A} h_{\alpha} x^{\alpha}$ , where  $h_{\alpha} \in \mathbb{C}[x_1, \dots, x_n]$ .

We write  $I = \langle x^{\alpha} \mid \alpha \in A \rangle$ .

**Some properties of monomial ideals:**

- Let  $I = \langle x^{\alpha} \mid \alpha \in A \rangle$ . Then the monomial  $x^{\beta} \in I$  if and only if some  $\alpha \in A$ ,  $x^{\alpha}$  divides  $x^{\beta}$ . Note: In this case we can write  $x^{\beta} = x^{\alpha} \cdot x^{\gamma}$  for some  $\gamma \in \mathbb{Z}_{\geq 0}^n$ . This equivalent to  $\beta = \alpha + \gamma$ .
- Let  $I$  be a monomial ideal and  $f$  a polynomial in  $\mathbb{C}[x_1, \dots, x_n]$ . Then  $f \in I \Leftrightarrow$  every term of  $f$  lies in  $I \Leftrightarrow f$  is a  $\mathbb{C}$ -linear combination of monomials in  $I$ .
- Two monomial ideals are the same if and only if they contain the same monomials.
- **(Dickson's Lemma)** A monomial ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$  has a finite basis.

Now suppose that we start with a regular polynomial ideal and want a monomial ideal. The most obvious ones to consider is defined below.

**Definition.** Let  $I \subset \mathbb{C}[x_1, \dots, x_n]$  be a nonzero ideal.

(i) The ideal of leading terms of elements of  $I$  is defined

$$\text{LT}(I) = \{cx^{\alpha} \mid \text{there exists } f \in I \text{ with } \text{LT}(f) = cx^{\alpha}\}$$

(ii) We denote the ideal generated by the elements of  $LT(I)$ ,  $\langle LT(I) \rangle$ .

**Note:** If we let  $I = \langle f_1, \dots, f_n \rangle$ , then the ideals  $\langle LT(f_1), \dots, LT(f_n) \rangle$  and  $\langle LT(I) \rangle$  may be different. By definition  $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$  for each  $i$ , and thus  $\langle LT(f_1), \dots, LT(f_n) \rangle \subseteq \langle LT(I) \rangle$ . But, we can see that equality is not guaranteed with the following example.

Let  $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$ . Let our monomial order be graded lexicographical order. Then  $\langle LT(f_1), LT(f_2) \rangle = \langle x^3, x^2y \rangle$ . Because we have the identity

$$x(x^2y - 2y^2 + x) - y(x^3 - 2xy) = x^2,$$

we know that  $x^2 \in \langle LT(I) \rangle$ . But,  $x^2 \notin \langle x^3, x^2y \rangle$ .

**Proposition.** For a nonzero ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$ ,  $\langle LT(I) \rangle$  is a monomial ideal.

Dickson's Lemma then tells us that for any nonzero ideal  $I \subset \mathbb{C}[x_1, \dots, x_n]$ , there are polynomials  $g_1, \dots, g_s \in I$  such that  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$ . This fact and the division algorithm prove the existence of a finite generating set for every polynomial ideal.

### 3 Groebner Basis

**Theorem (Hilbert Basis Theorem).** Every ideal  $I \in \mathbb{C}[x_1, \dots, x_n]$  has a finite generating set. That is,  $I = \langle g_1, \dots, g_s \rangle$  for some  $g_1, \dots, g_s \in I$ .

We can choose the  $g_i \in I$  such that they are exactly the polynomials with the property  $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$ . We give such ideals a special name.

**Definition.** Fix a monomial order. A finite subset  $G = \{g_1, \dots, g_s\}$  of an ideal  $I$  is said to be a **Groebner basis** if  $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$ .

From what we have seen above, we find that every nonzero ideal has a Groebner basis. In fact, any Groebner basis for an ideal  $I$  is actually a basis for  $I$ . We can use Maple and other computer algebra programs to compute the Groebner basis of an ideal, but before we can use the computers to compute Groebner bases, we should first learn how to compute them by hand.

**Definition.** Let  $f, g \in \mathbb{C}[x_1, \dots, x_n]$  be nonzero polynomials.

(i) If  $\text{multideg}(f) = \alpha$  and  $\text{multideg}(g) = \beta$ , then let  $\gamma = (\gamma_1, \dots, \gamma_n)$  where  $\gamma_i = \max(\alpha_i, \beta_i)$  for each  $i$ . We call  $\mathbf{x}^\gamma$  the **least common multiple** of  $LM(f)$  and  $LM(g)$  and write  $\mathbf{x}^\gamma = \text{LCM}(LM(f), LM(g))$ .

(ii) The **S-polynomial** of  $f$  and  $g$  is the combination

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

(The S-polynomial is designed to cancel leading terms).

**Theorem.** Let  $I$  be a polynomial ideal. Then a basis  $G = \{g_1, \dots, g_s\}$  for  $I$  is a Groebner basis of  $I$  if and only if for all  $i \neq j$ , the remainder on division of  $S(g_i, g_j)$  by  $G$  (in some fixed order) is 0.

Suppose we are given an ideal  $I$  and a basis  $G = \{g_1, \dots, g_s\}$ . First compute  $S(g_1, g_2)$ , and if  $S(g_1, g_2)$  is not an element of  $\langle g_1, \dots, g_s \rangle$ , then add it to the ideal  $\langle g_1, \dots, g_s \rangle$ . Now you have the ideal  $\langle g_1, \dots, g_s, S(g_1, g_2) \rangle = \langle g_1, \dots, g_{s+1} \rangle$ . Next take the S-polynomials of  $g_i$ ,  $i = 1..s$ , and  $g_{s+1}$ . Check to see if each leading term is in our new leading term ideal, and if not, add the S-polynomials to the ideal. Keep going until you have found a Groebner basis. This process will terminate and is formally known as Buchberger's Algorithm.

One of the uses of Groebner bases is to find the implicit form of a rational curve when you are given the parametric form.

**Theorem (Rational Implicitization).** Let  $F : \mathbb{C} - V(g_1g_2) \rightarrow \mathbb{C}^2$  be the function determined by the polynomial parametrization  $x = \frac{f_1(t)}{g_1(t)}$ ,  $y = \frac{f_2(t)}{g_2(t)}$ , so  $F(t) = \left(\frac{f_1(t)}{g_1(t)}, \frac{f_2(t)}{g_2(t)}\right)$ . Let  $I$  be the ideal  $\langle f_1 - g_1x, f_2 - g_2y, 1 - g_1g_2s \rangle \subset \mathbb{C}[s, t, x, y]$  and let  $I' = I \cap \mathbb{C}[x, y]$ . Then  $V(I')$  is the smallest variety in  $\mathbb{C}^2$  containing  $F(\mathbb{C} - V(g_1g_2))$ .

Note: If  $g_1 = g_2 = 1$ , then you do not need to introduce the new variable  $s$ .

**Theorem (The Elimination Theorem).** Let  $I \subset \mathbb{C}[s, t, x, y]$  be an ideal and let  $G$  be the Groebner basis of  $I$  with respect to lex order where  $s > t > x > y$ . Then the set  $G' = G \cap \mathbb{C}[x, y]$  is a Groebner basis for  $I' = I \cap \mathbb{C}[x, y]$ .

This Implicitization Theorem tells us that in order to get the implicit form of a curve from its parametric form, all you have to do is find the polynomials in only  $x$ 's and  $y$ 's in a certain ideal. Finding those polynomials is not easy if you are just given a random ideal. This is why we use Groebner Bases. The Elimination Theorem tells us that we can just pull out the polynomial in the Groebner basis which only contains  $x$  and  $y$  to find our implicit polynomial.

## 4 Groebner Basis Example

Suppose we are given the curve,  $C$ , parameterized by  $x = t^2, y = t^3$ . We want to find a polynomial  $f \in \mathbb{C}[x, y]$  such that  $C = C(f)$ .

1. Define the ideal  $I = \langle f_1 - g_1x, f_2 - g_2y, 1 - g_1g_2s \rangle \subset \mathbb{C}[s, t, x, y]$ .

In this example we are given  $f_1 = t^2, f_2 = t^3, g_1 = 1, g_2 = 1$ , so we do not have to introduce the variable  $s$ . The ideal is defined,

$$I = \langle t^2 - x, t^3 - y \rangle \subset \mathbb{C}[t, x, y].$$

Define new polynomials in the ring  $\mathbb{C}[t, x, y]$ ,

$$h_1 = t^2 - x, h_2 = t^3 - y.$$

Thus,  $I = \langle h_1, h_2 \rangle$ .

2. Find the Groebner Basis of  $I$  using Buchberger's Algorithm.

Compute our first S-polynomial using lexicographical ordering and  $t > x > y$ .

$LM(h_1) = t^2, LM(h_2) = t^3$ , so  $\gamma = (3, 0, 0)$  and  $\mathbf{x}^\gamma = t^3$ .

$$S(h_1, h_2) = \frac{t^3}{t^2}(t^2 - x) - \frac{t^3}{t^3}(t^3 - y) = -tx + y.$$

Consider the ideal  $\langle LT(f_1), LT(f_2) \rangle = \{f \in \mathbb{C}[t, x, y] \mid f = gt^2 + ht^3 \text{ for some } g, h \in \mathbb{C}[t, x, y]\} = \langle t^2 \rangle$ .  $LT(S(h_1, h_2)) = -tx \notin \langle t^2 \rangle$  because there does not exist a polynomial  $g \in \mathbb{C}[t, x, y]$  such that  $gt^2 = -tx$ . Thus, we must add  $h_3 = S(h_1, h_2)$  to the ideal  $\langle h_1, h_2 \rangle$  to get a new ideal  $I_3 = \langle h_1, h_2, h_3 \rangle$ . You can save a lot of time by being smart about things. For example, in  $I_3$  we have  $h_2 = t(h_1) - h_3$ . So, we can just throw out  $h_2$  and let  $I_3 = \langle h_1, h_3 \rangle$ .

Now that we must compute another S-polynomial.

$$S(h_1, h_3) = \frac{t^2x}{t^2}(t^2 - x) - \frac{t^2x}{-tx}(-tx + y) = ty - x^2.$$

$LT(S(h_1, h_3)) = ty \notin \langle t^2, -tx \rangle$  so we add an  $h_4 = S(h_1, h_3) = ty - x^2$  to the ideal. We now are considering the ideal  $I_4 = \langle h_1, h_3, h_4 \rangle$  and need to compute two more S-polynomials.

$$S(h_1, h_4) = -tx^2 + xy.$$

$$S(h_3, h_4) = -x^3 + y^2.$$

$LT(S(h_1, h_4)) \in \langle t^2, -tx, -ty \rangle$  so it does not affect the ideal. But  $LT(S(h_3, h_4)) = -x^3 \notin \langle t^2, -tx, ty \rangle$ , so we add an  $h_5 = S(h_3, h_4) = -x^3 + y^2$  to the ideal. We now have the ideal  $I_5 = \langle h_1, h_3, h_4, h_5 \rangle$  and must take three more S polynomials!

$$S(h_1, h_5) = t^2y^2 - x^4.$$

$$S(h_3, h_5) = t^2y^2 - x^2y.$$

$$S(h_4, h_5) = -ty^3 - x^5.$$

All of these polynomials have leading terms in the ideal  $\langle t^2, -tx, ty, -x^3 \rangle$ , so we have found our desired ideal  $\langle t^2 - x, t^3 - y, -tx + y, ty - x^2, -x^3 + y^2 \rangle$ . Thus our Groebner basis is

$$G = \{t^2 - x, -tx + y, ty - x^2, -x^3 + y^2\}.$$

3. Take the intersection  $G \cap \mathbb{C}[x, y]$ .

The intersection of  $I$  with the polynomial ring in two variables  $\mathbb{C}[x, y]$  is generated by the elements in  $G \cap \mathbb{C}[x, y] = \{y^2 - x^3\}$ . Thus,  $I' = \langle y^2 - x^3 \rangle$ , and we have found that  $C = C(y^2 - x^3)$ .