Math 143

Bernd Sturmfels

Davis Foote[*]

University of California, Berkeley

August 27th, 2015 – December 10th, 2015

Contents

[*]djfoote@berkeley.edu

1 Geometry, Algebra, and Algorithms

1.1 *Ideals*

Lecture 1
September 1st, 2015

1.1.1 DEFINITION. A subset I of $R = K[x_1, \dots, x_n]$ is an **ideal** if

(1) $0 \in I$

(2) $f, g \in I \Rightarrow f + g \in I$

(3) $f \in I, h \in R \Rightarrow h \cdot f \in I$

1.1.2 DEFINITION. The **ideal generated** by polynomials $f_1, \dots, f_s \in R$ is

$$\langle f_1, \dots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i : h_i \in R \right\}$$

1.1.3 PROPOSITION. *If $f_1, \dots, f_s$ and $g_1, \dots, g_t$ generate the same ideal I, they have the same variety $V(I)$.*

1.1.4 LEMMA. *Conversely, if $V \subseteq K^n$ is any variety, then $I(V) = \{f \in R : f(a) = 0 \text{ for all } a \in V\}$*

1.1.5 EXAMPLE. Let $V = \{(t, t^2, t^3) \in \mathbb{R}^3\}$, the "twisted cubic curve." Then $I(V) = \langle y - z^2, z - x^3 \rangle$. So any polynomial which vanishes at V is a polynomial combination of $y - z^2$ and $z - x^3$.

1.1.6 LEMMA. *If $f_1, \dots, f_s \in R$, then $\langle f_1, \dots, f_s \rangle \subseteq I(V(f_1, \dots, f_s))$, but equality need not hold.*

Proof. Suppose $f = \sum_{i=1}^{s} h_i f_i$. Since each f_i vanishes on $V(f_1, \dots, f_s)$, so does f. This means $f \in I(V(f_1, \dots, f_s))$. $\square$

1.2 *Polynomials in One Variable*

1.2.1 DEFINITION. Let $f = a_0 x^m + a_1 x^{m-1} + \dots + a_m \in K[x]$ with $a_0 \neq 0$. The **leading term** of f is $LT(f) = a_0 x^m$.

1.2.2 FACT. $\deg(f) \leq \deg(g) \Leftrightarrow LT(f)$ divides $LT(g)$

1.2.3 PROPOSITION (Division Algorithm). *Fix $g \in K[x] \setminus \{0\}$. Every $f \in K[x]$ can be written uniquely as $f = q \cdot g + r$, where $q, r \in K[x]$ and ($r = 0$ or $\deg(r) < \deg(g)$).*

TODO: Typeset this later ALGORITHM Input: g, f Output: q, r as in * q := 0, r:= f while $r \neq 0$ and $LT(g)$ divides $LT(r)$ do $q := q + \frac{LT(r)}{LT(g)}$ $r := r - \frac{LT(r)}{LT(g)} \cdot g$

1.2.4 COROLLARY. *Every $f \in K[x] \setminus \{0\}$ has at most* $\deg(f)$ *many roots.*

Proof. Induction on $m = \deg(f)$. True for $m = 0, 1$. For $m \geq 2$, if f has no roots in K, done. Otherwise, let $a \in K$ be a root, and write $f = q \cdot (x - a) + r$ where r is a constant. We have $f(a) = r = 0 \Rightarrow q$ divides r and $\deg(q) < m$, so it satisfies the conclusion. □

1.2.5 COROLLARY. *Every ideal in $K[x]$ has the form $\langle f \rangle$ for some $f \in K[x]$. Here f is unique up to a multiplicative scalar.*

1.2.6 PROPOSITION. *Let $f, g \in K[x]$. Then*

(1) The greatest common divisor $GCD(f, g)$ is unique

(2) $GCD(f, g)$ generates the ideal $\langle f, g \rangle$

(3) There is an algorithm for finding $GCD(f, g)$

1.2.7 EXAMPLE. Decide whether $x^2 - y$ lies in $\langle x^3 + x^2 - 4x + 4, x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \rangle$.

First, compute the GCD of these three polynomials. It is $x - 2$. So the above ideal is equal to $\langle x - 2 \rangle$.

$x^2 - 4 = (x + 2)(x - 2) \in \langle x - 2 \rangle$

To find which linear combination of the above polynomials equals $x^2 - 4$, use the extended Eauclidean algorithm.

2 Grobner Bases

2.1 *Introduction*

Problems concerning ideals in $R = K[x_1, \ldots, x_n]$:

- Description: Does every ideal $I \subseteq R$ have a finite generating set?
- Membership: Given $I \subseteq R$ and $f \in R$, how to test whether $f \in I$
- Solving Equations: Describe $V(f_1, \ldots, f_s)$
- Implicitization: Compute the image in K^n of a polynomial parameterization $(x_i = g_i(f_1, \ldots, f_m))_{1 \leq i \leq n}$

2.2 *Orderings on Monomials*

We are concerned with $R = K[x_1, \dots, x_n]$. What is the leading term of a polynomial in R?

2.2.1 REMARK. We can define a bijection between monomials $x^a = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ in R to vectors a in $\mathbb{Z}^n_{\geq}$.

2.2.2 DEFINITION. A **monomial ordering** on R is a total ordering $>$ on $\mathbb{Z}$ such that

(1) If $a > b$ and $c \in \mathbb{Z}^n_{\geq 0}$ than $a + c > b + c$.

(2) $>$ is a well-ordering, i.e. every non-empty subset has a least element.

2.2.3 LEMMA. *A monomial ordering $>$ is a well-ordering if and only if every strictly decreasing sequence $a(1) > a(2) > a(3) > \cdots$ in $\mathbb{Z}^n_{\geq 0}$ eventually terminates.*

Proof. ($\Rightarrow$) Suppose $>$ is not a well-ordering. Pick $S \subset \mathbb{Z}^n_{\geq 0}$ with no least element. Pick $a(1) \in S$. We can find $a(1) > a(2)$ in S, and $a(2) > a(3)$, etc.

($\Leftarrow$) If $a(1) > a(2) > a(3) > \cdots$ is an infinite sequence then $S = \{a(1), a(2), a(3), \dots\}$ has no least element.

□

For each of the following orderings, we refer to a and b vectors of exponents as described in Remark 2.1.

2.2.4 DEFINITION (Lexicographic ordering). $a >_{\text{lex}} b$ if the leftmost nonzero entry in $a - b$ is positive. Referred to as "lex."

2.2.5 DEFINITION (Graded lexicographic ordering). $a >_{\text{grlex}} b$ if $|a| > |b|$. If $|a| = |b|$, ties are broken lexicographically. This ordering respects total degree. Referred to as "grlex."

2.2.6 DEFINITION (Graded reverse lexicographic ordering). $a >_{\text{grevlex}} b$ if $|a| > |b|$. If $|a| = |b|$, $a >_{\text{grevlex}} b$ if the rightmost nonzero entry in $a - b$ is negative. Referred to as "grevlex."

2.2.7 EXAMPLE. Consider quadratic monomials in $n = 4$ variables. Refer to the variables as a, b, c, d.

In grlex, $a^2 > ab > ac > ad > b^2 > bc > bd > c^2 > cd > d^2$.

In grevlex, $a^2 > ab > b^2 > ac > bc > c^2 > ad > bd > cd > d^2$.

2.2.8 DEFINITION. Fix a monomial order $>$ and let $f = \sum_a c_a x^a \in R$.

- The **multidegree** of f is $\max\{a \in \mathbb{Z}^n_{\geq 0} : c_a \neq 0\}$.
- The **leading coefficient** is $L(f) = C_{\text{multideg}(f)} \in K^* = K \setminus \{0\}$.
- The **leading monomial** is $LM(f) = x^{\text{multideg}(f)}$
- The **leading term** is $LT(f) = L(f) \cdot LM(f)$

2.2.9 EXERCISE. Which order (lex, grlex, grevlex) was used in writing

(a) $7x^2y^4z - 2xy^6 + x^2y$

(b) $xy^3z + xy^2z^2 + x^2z^3$

(c) $x^4y^5z + 2x^3y^2z - 4xy^2z^4$

2.3 *A Division Algorithm in R*

Goal: Divide f by $\{f_1, \dots, f_s\}$, i.e. write $f = a_1f_1 + \cdots + a_sf_s + r$. The sum of all a_if_i is called the quotient, and r is called the remainder. We also want r to be small.

2.3.1 EXAMPLE. $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$, $f_2 = y^2 - 1$. $f = (x+y)f_1 + 1 \cdot f_2 + (x + y + 1)$.

None of the terms in r is divisible by $LM(f_1)$ or by $LM(f_2)$. However, the remainder is generally not unique: $f = xf_1 + (x+1)f_2 + (2x+1)$.

Hence $\langle f_1, f_2 \rangle \ni r - r' = y - x$. What is $V(f_1, f_2)$? $\{(1,1), (-1,-1)\}$.

2.3.2 THEOREM (Division Algorithm). *Fix a monomial ordering $>$ on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \dots, f_s)$ be an ordered tuple of polynomials in R. Then every other polynomial $f \in R$ can be written as $f = a_1f_1 + \cdots + a_sf_s + r$ where $a_1, r \in R$ and*

- *the remainder r is a K-linear combination of monomials, none of which is divisible by any of the leading terms of $f_1, \dots, f_s$. (Intuitively, the remainder is small.)*
- *multideg$(f) \geq$ multideg(a_if_i) for all a_i with $a_i \neq 0$*

Proof. We present an algorithm to compute such a decomposition.

TODO: typeset this later
Input: $f_1, \dots, f_s, f$
Output: $a_1, \dots, a_s, r$ such that the above hold.

$(a_1, a_2, \dots, a_2) := (0, 0, \dots, 0)$
$p := f$
while $p \neq 0$ do:

$i := 1$
divisionOccurred := false
while $i \leq s$ and (divisionOccurred=false) do:
if $LT(f_i)$ divides $LT(p)$ then:
$a_i := a_i + \frac{LT(p)}{LT(f_i)}$
$p := p - (\frac{LT(p)}{LT(f_i)}) \cdot f_i$
divisionOccurred=true
else:
$i := i + 1$
if divisionOccurred=false then:
$r := r + LT(p)$
$p := p - LT(p)$

The invariant on the outer while loop is $f = a_1 f_1 + \ldots + a_s f_s + p + r$. Intuitively, p is the part of f which hasn't been decomposed yet. Therefore when the loop is exited and p is 0, we have the desired decomposition.

The algorithm is guaranteed to terminate because $LT(p)$ is guaranteed to decrease in each iteration. □

2.3.3 FACT. The ordering of $F = (f_1, \ldots, f_s)$ matters.

2.3.4 EXAMPLE. Let $f_1 = xy + 1$, $f_2 = y^2 - 1$. Dividing $f = xy^2 - x$ by $F = (f_1, f_2)$ gives the result $f = y \cdot f_1 + 0 \cdot f_2 + (-x - y)$. On the other hand, dividing f by $F = (f_2, f_1)$ gives the result $f = x \cdot f_2 + 0 \cdot f_1 + 0$.

2.3.5 PROBLEM. How can we solve the ideal membership problem using such a division algorithm? If the remainder is 0, then we know the input f is in the ideal generated by $F = (f_1, \ldots, f_s)$. However, as seen in the above example, we can run the algorithm and get a result with nonzero remainder even when f is in the ideal.

2.3.6 EXAMPLE. For fixed F, the map $f \mapsto r$ is K-linear.

2.4 *Monomial Ideals and Dickson's Lemma*

Lecture 2
September 8th, 2015

2.4.1 DEFINITION. An ideal I in $R = K[x_1, \ldots, x_n]$ is a **monomial ideal** if it is generated by a (possibly infinite) set of monomials $x^a = x_1^{a_1} \cdots x_n^{a_n}$, i.e.

$$I = \langle x^a : a \in A \rangle$$

where $a \subset \mathbb{Z}^n$.

2.4.2 LEMMA. *A monomial x^b lies in I_b if and only if there exists some $a \in A$ such that x^a divides x^b.*

TODO: Include graphic from textbook

2.4.3 LEMMA. *Let I be a monomial ideal, $f \in R$. Then the following are equivalent:*

(1) $f \in I$

(2) Every term of f is in I.

(3) f is a K-linear combination of monomials in I.

2.4.4 THEOREM (Dickson's Lemma). *Every monomial ideal $I = \langle x^a : a \in A\rangle$ is finitely generated. More precisely, there exists $a_1, \ldots, a_s \in A$ such that $I = \langle x^{a_1}, \ldots, x^{a_s})\rangle$.*

TODO: Complete this proof.

Proof. Proved by induction on n. For $n = 1$, the set $A \subset \mathbb{Z}_{\geq 0}$ has a smallest element b such that for all $a \in A$, $a \geq b$. Thus $I = \langle x^b\rangle$.

Suppose the lemma is true for some $n - 1$. □

2.4.5 COROLLARY. *Let $>$ be a total ordering on $\mathbb{Z}^n_{\geq 0}$ satisfying ($a > b$ and $c \in \mathbb{Z}^n_{\geq 0}$ implies $a + c > b + c$). Then $>$ is a well-ordering if and only if $a \geq 0$ according to the ordering for all $a \in \mathbb{Z}^n_{\geq 0}$.*

2.5 *The Hilbert Basis Theorem and Groebner Bases*

2.5.1 DEFINITION. Fix a monomial ordering on $R = K[x_1, \ldots, x_n]$. Let $I \subset R$ be a nonzero ideal. The **leading ideal** $\langle LT(I)\rangle$ is the ideal generated by $LT(I) = \{LT(f) : f \in I\}$.

2.5.2 EXAMPLE. Using lex ordering with $x > y > z$, let $I = \langle x + y + z, x + 2y + 3z\rangle$. $\langle LT(I)\rangle = \langle x, y\rangle$.

2.5.3 EXAMPLE. Using lex ordering, let $I = \langle g_1, g_2, g_3\rangle = \langle xy^2 - xy + x, xy - z^2, x - yz^2\rangle$. Give an example of $g \in I$ such that $LT(g) \notin \langle LT(g_1), LT(g_2), LT(g_3)\rangle$.

$g_2 - yg_3 = y^2z^4 - z^2$.

2.5.4 PROPOSITION. *(1) $\langle LT(I)\rangle$ is a monomial ideal.*

(2) There are $g_1, g_2, \ldots, g_s \in I$ such that $\langle LT(I)\rangle = \langle LT(g_1), LT(g_2), \ldots, LT(g_s)\rangle$.

Proof. (1) $\langle LT(I)\rangle$ is also generated by $S = \{LM(g) : g \in I \setminus \{0\}\}$ because $LT(g)$ and $LM(g)$ differ by a constant.

(2) S is a set of monomials, so by Dickson's lemma, $\langle LT(I)\rangle$ is finitely generated by a subset of S.

□

2.5.5 theorem (Hilbert Basis Theorem). *Every ideal in $R = K[x_1, \dots, x_n]$ is finitely generated.*

TODO: What about the case where $r \neq 0$ and $r \notin I$?

Proof. Choose $g_1, \dots, g_s \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Claim: $I = \langle g_1, \dots, g_s \rangle$.

Clearly $\langle g_1, \dots, g_s \rangle \subset I$. For the reverse inclusion, consider some $f \in I$. Apply the division algorithm to get a representation of f as

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

where no term in r is divisible by any of the leading terms of the g_i's.

If $r = 0$, we have obtained a representation of f as a combination of the g_i's, so we are done. If instead $r \neq 0$ and $r \in I$, then $LT(r) \in \langle LT(I) \rangle$ so there exists some i such that $LT(g_i)$ divides $LT(r)$, which is a contradiction to the division algorithm. □

2.5.6 definition. A finite subset $G = \{g_1, \dots, g_s\}$ of an ideal I is a **Groebner basis** if

$$LT(I) = \langle LT(g_1), \dots, LT(g_s) \rangle$$

Note how this differs from a basis in linear algebra: there is no statement of minimality. If S is a Groebner basis for I, then $S \cup S'$ is still a Groebner basis for I.

2.5.7 corollary. *Fix a monomial order on R. Every ideal $I \subset R$ has a Groebner basis. Any such Groebner basis generates I*

In practice, these are computed using a computer, which requires as input an ideal and a monomial ordering.

2.5.8 theorem. *Let $I_1 \subset I_2 \subset I_3 \subset \cdots$ be an ascending chain of ideals in R. Then this terminates, i.e. there exists a positive integer k such that $I_k = I_{k+1} = I_{k+2} = \cdots$.*

TODO: Complete this proof.

Proof. The set $\bigcup_{g=0}^{\infty} I_j$ is an ideal. By the Hilbert Basis Theorem, I is finitely generated and $I = \langle f_1, \dots, f_s \rangle$. So there exists some k such that $f_1, \dots, f_s \in I_k$. □

2.5.9 PROPOSITION. *If $I \subset R$ is an ideal, then $\mathbf{V}(I)$ is an affine variety in K^n. In fact $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$ for any finite generating set $\{f_1, \ldots, f_s\}$ of I.*

2.5.10 THEOREM (Eisenbud-Evans Theorem). *Every affine variety in K^n is the zero set of only n polynomials.*

2.6 *Properties of Groebner Bases*

2.6.1 PROPOSITION. *Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for an ideal $I \subset K[x_1, \ldots, x_n] = R$, and $f \in R$. There is a unique $r \in R$ such that*

(1) No term of r is divisible by any of $LT(g_1), \ldots, LT(G_s)$

(2) There is $g \in I$ such that $f = g + r$.

In particular, r is the remainder on division of f by G, independently of the ordering of G.

Proof. The division algorithm gives existence

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

For uniqueness, suppose $f = g + r = g' + r'$ both satisfying (1) and (2). Then $r - r' = g - g' \in I$, so $LT(r - r') \in LT(I) = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Since this is a monomial ideal, it must be that some term of $r - r'$ is divisible by $LT(g_i$ for some i. This is impossible if $r - r'$ is nonzero, so $r = r'$ and $g = g'$. □

2.6.2 DEFINITION. The **remainder** of f upon division into an ordered list $F = (f_1, \ldots, f_s)$ is written as $\overline{f}^F$. This value is independent of the ordering of F if F is a Groebner basis.

2.6.3 COROLLARY. *$f \in I$ if and only if $\overline{f}^G$.*

2.6.4 DEFINITION. Let $f, g \in R$ and $x^c = LCM(LM(f), LM(g))$. The **S-polynomial** of f and g is

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

2.6.5 EXAMPLE. Suppose $f = x^3y^2 - x^2y^3 + x$ and $g = 3x^4y + y^2$.

$$S(f, g) = x \cdot f - \frac{1}{3} y \cdot g = -x^3y^3 + x^2 - \frac{1}{3} y^3$$

2.6.6 THEOREM (Buchberger's Criterion). *A basis $G = \{g_1, \ldots, g_s\}$ for an ideal $I \subset R$ is a Groebner basis if and only if for all $i \neq j$, $\overline{S(g_i, g_j)}^G = 0$.*

The proof is this theorem will not be presented (available on pages 85-87 in the text).

2.6.7 exercise. Show that $\{y - x^2, z - x^3\}$ is not a Groebner basis for lex order with $x > y > z$.

Solution. $S(y - x^2, z - x^3) = xy - z$. This already is the remainder upon division by the set, and it's nonzero. Therefore this is not a Groebner basis. $\square$

2.7 *Buchberger's Algorithm*

We would like to be able to add nonzero remainders $\overline{S(f_i, g_j)}^F$ to the given basis.

2.7.1 theorem (Buchberger's Algorithm). *Let $I = \langle f_1, \ldots, f_s \rangle \neq \{0\}$. Then a Groebner basis for I can be constructed according to Algorithm 1.*

Algorithm 1 Buchberger's Algorithm

Input: $F = (f_1, \ldots, f_s)$ and a monomial ordering.
Output: A Groebner basis $G = (g_1, \ldots, g_t)$ for I with $F \subset G$.

procedure
    $G := F$
    $G' := G$
    while $G \neq G'$ **do**
        for each pair $p, q \in G$, $p \neq q$ **do**
            $S := \overline{S(p,q)}^{G'}$
            if $S \neq 0$ **then** $G := G \cup \{S\}$

TODO: Replace "while" with "repeat... until"

Proof. We have $\langle F \rangle = I$ hence $\langle G \rangle = I$ throughout. The algorithm terminates when Buchberger's criterion is satisfied. When this happens, G is a Groebner basis. It remains to prove that the algorithm terminates.

After each iteration of the main loop, we have $\langle LT(G') \rangle \subsetneq \langle LT(G) \rangle$ because the new S-polynomial remainders have leading monomials not in $\langle LT(G) \rangle$. By the ACC (Theorem 7 in Section 2.5), this must terminate. $\square$

TODO: What is the ACC?

2.7.2 definition. A **minimal Groebner basis** for I is a Groebner basis for I such that

(1) $LC(p) = 1$ for $p \in G$.

(2) For all $p \in G$, $LT(p) \notin \langle LT(G)\{p\}\rangle$

We can construct a minimal Groebner basis from the output of Buchberger's algorithm by successive removal.

2.7.3 DEFINITION. G is a **reduced Groebner basis** if the following strengthening of (2) above holds:

(2') For all $p \in G$, no monomial of p lies in $\langle LT(G)\{p\}\rangle$.

2.7.4 PROPOSITION. *Given a fixed monomial ordering, every nonzero ideal has a unique reduced Groebner basis.*

It's helpful when learning these new ideas to think back to univariate polynomials and linear polynomials and consider the implications to these easy-to-understand examples.

For linear polynomials, finding a Groebner basis is equivalent is identical to Gaussian elimination. A minimal Groebner basis requires removing all redundant rows from the result. A reduced Groebner basis here involves subtracting rows back up so that no two rows have a nonzero element in the same column.

2.8 *First Applications of Groebner Bases*

Ideal Membership

How do we test whether f lies in $I = \langle f_1, \ldots, f_s\rangle$? We can do this by computing a Groebner basis $G = \{g_1, \ldots, g_s\}$ for I. Then $f \in I$ if and only if $\overline{f}^G = 0$

Solving Polynomial Equations

Use lexicographic Groebner bases to triangularize.

2.8.1 EXAMPLE. $I = \langle x^2 + y^2 - 4, xy - 1\rangle$. Calculate a Groebner basis in the lex order with $y > x$. The unique reduced Groebner basis is $\{x^4 - 4x^2 + 1, y + x^3 - 4x\}$. Solving for x in the first of those polynomials, we see that $x = \pm\frac{\sqrt{6}}{2} \pm \frac{\sqrt{2}}{2}$. Recovering y from the original polynomials yields the solutions to the system.

Implicitization

Suppose we want to implicitize a surface in 3-space, $C : x = f(s,t); y = g(s,t); z = h(s,t)$.

(1) Compute a Groebner basis $\mathcal{G}$ for the ideal given by

$$\langle x - f(s,t), y - g(s,t), z - h(s,t) \rangle$$

with respect to the lex order with $s > t > x > y > z$.

(2) Select $\mathcal{G} \cap K[x,y,z] = \{\varphi(x,y,z)\}$.

2.8.2 example. $C : x = s^2 + t^2; y = s^3 + t^3; z = s^4 + t^4$. In this case,

$$\varphi = x^6 - 4x^3y^2 - 4y^4 + 12xy^2z - 3x^2z^2 - 2z^3$$

Note that we have no guarantee here that $\mathrm{im}(f,g,h) = \mathbf{V}(\varphi)$. This is a more delicate question that we will address later.