Math 143

Bernd Sturmfels

Davis Foote[*]

University of California, Berkeley

August 27^{th}, 2015 – December 10^{th}, 2015

Contents

1 Geometry, Algebra, and Algorithms

1.1 *Ideals*

Lecture 1
September 1^{st}, 2015

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

[*]djfoote@berkeley.edu

1.2 definition. The **ideal generated** by polynomials $f_1, \ldots, f_s \in R$ is

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

1.3 proposition. *If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ generate the same ideal I, they have the same variety $V(I)$.*

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

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 $z - x^3$.

1.6 lemma. *If $f_1, \ldots, f_s \in R$, then $\langle f_1, \ldots, f_s \rangle \subseteq I(V(f_1, \ldots, f_s))$, but equality need not hold.*

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

1.2 *Polynomials in One Variable*

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

1.8 fact. $\deg(f) \leq \deg(g) \Leftrightarrow LT(f)$ divides $LT(g)$

1.9 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 $q := q + \frac{LT(r)}{LT(g)}$ $r := r - \frac{LT(r)}{LT(g)} \cdot g$

1.10 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. □

1.11 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.*

1.12 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 $GCD(f, g)$

1.13 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

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 $(x_i = g_i(f_1, \ldots, f_m))_{1 \le i \le n}$

2.1 *Orderings on Monomials*

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

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 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.

2.3 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 $S = \{a(1), a(2), a(3), \ldots\}$ has no least element.

$\square$

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

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

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."

2.6 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."

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

2.8 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 $LT(f) = L(f) \cdot LM(f)$

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

2.2 *A Division Algorithm in R*

Goal: Divide f by $\{f_1, \ldots, f_s\}$, i.e. write $f = a_1 f_1 + \cdots + a_s f_s + r$. The sum of all $a_i f_i$ is called the quotient, and r is called the remainder. We also want r to be small.

2.10 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 $V(f_1, f_2)$? $\{(1,1), (-1,-1)\}$.

2.11 THEOREM (Division Algorithm). *Fix a monomial ordering $>$ on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \ldots, f_s)$ be an ordered tuple of polynomials in R. Then every other polynomial $f \in R$ can be written as $f = a_1 f_1 + \cdots + a_s f_s + r$ 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 $f_1, \ldots, f_s$. (Intuitively, the remainder is small.)*
- *$multideg(f) \geq multideg(a_i f_i)$ for all a_i with $a_i \neq 0$*

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

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

$(a_1, a_2, \ldots, a_2) := (0, 0, \ldots, 0)$
$p := f$
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. $\square$

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

2.13 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 $f = x \cdot f_2 + 0 \cdot f_1 + 0$.

2.14 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.

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