PURE Math Residents' Program
Gröbner Bases and Applications
Week 1 Lectures

John B. Little

Department of Mathematics and Computer Science
College of the Holy Cross

June 2012

Overview

Our work this summer will be concerned mostly with polynomials in several variables, and

- techniques for solving systems of polynomial equations
- understanding geometric objects defined by polynomial equations
- algorithmic and computational techniques for working with polynomials
- applications to some interesting questions from *celestial mechanics* (central configurations)

Polynomials

A polynomial in two variables x, y is just a *finite* sum of terms of the form $cx^a y^b$, where

- c is a constant coefficient, for us always coming from some *field* of constants (e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.)
- a, b are integers ≥ 0 (we sometimes write $a, b \in \mathbb{Z}_{\geq 0}$)

For example,

$$p(x, y) = 5x^3y^4 - \frac{3}{2}xy^2 - 3$$

is a polynomial in x, y with coefficients in $\mathbb{Q}$.

Multiindex notation

- If there are more than two or three variables, then we might want to *number* them as $x_1, x_2, \ldots, x_n$.

Multiindex notation

- If there are more than two or three variables, then we might want to *number* them as $x_1, x_2, \ldots, x_n$.
- A *monomial* is a product $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_i \in \mathbb{Z}_{\geq 0}$ for all i.

Multiindex notation

- If there are more than two or three variables, then we might want to *number* them as $x_1, x_2, \ldots, x_n$.
- A *monomial* is a product $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_i \in \mathbb{Z}_{\geq 0}$ for all i.
- Abbreviate as x^α where $\alpha \in \mathbb{Z}_{\geq 0}$ is the vector of exponents

Multiindex notation

- If there are more than two or three variables, then we might want to *number* them as $x_1, x_2, \ldots, x_n$.
- A *monomial* is a product $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_i \in \mathbb{Z}_{\geq 0}$ for all i.
- Abbreviate as x^α where $\alpha \in \mathbb{Z}_{\geq 0}$ is the vector of exponents
- Examples: $x_1^3 x_2^2 x_3^4$ corresponds to $\alpha = (3, 2, 4)$ and $x_1^7 x_3$ corresponds to $\alpha = (7, 0, 1)$ if those are the only variables

Multiindex notation

- If there are more than two or three variables, then we might want to *number* them as $x_1, x_2, \ldots, x_n$.
- A *monomial* is a product $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where $\alpha_i \in \mathbb{Z}_{\geq 0}$ for all i.
- Abbreviate as x^α where $\alpha \in \mathbb{Z}_{\geq 0}$ is the vector of exponents
- Examples: $x_1^3 x_2^2 x_3^4$ corresponds to $\alpha = (3, 2, 4)$ and $x_1^7 x_3$ corresponds to $\alpha = (7, 0, 1)$ if those are the only variables
- A general polynomial can be compactly written as $\sum_\alpha c_\alpha x^\alpha$, where $c_\alpha = 0$ for all but finitely many of the $\alpha \in \mathbb{Z}_{\geq 0}$.

Polynomial algebra

In high school algebra, calculus, etc. you probably remember working with expressions of this form. Recall that we can combine them

- by addition, for instance:

$$(3x^2y + 2x + 3) + (-2x^2y + y + 4) = x^2y + 2x + y + 7$$

Polynomial algebra

In high school algebra, calculus, etc. you probably remember working with expressions of this form. Recall that we can combine them

- by addition, for instance:

$$(3x^2y + 2x + 3) + (-2x^2y + y + 4) = x^2y + 2x + y + 7$$

- by multiplication, for instance:

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

Polynomial algebra

In high school algebra, calculus, etc. you probably remember working with expressions of this form. Recall that we can combine them

- by addition, for instance:

$$(3x^2y + 2x + 3) + (-2x^2y + y + 4) = x^2y + 2x + y + 7$$

- by multiplication, for instance:

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

- Note that both of these come down to rules:
  1. $cx^\alpha + dx^\alpha = (c + d)x^\alpha$, and
  2. $x^\alpha x^\beta = x^{\alpha+\beta}$ where $\alpha + \beta$ means add the exponent vectors coordinate-wise in $\mathbb{Z}_{\geq 0}$
  3. Multiplication distributes over addition as in arithmetic with ordinary rational or real numbers

Some notation

Definition 1

The set of all polynomials in the variables $x_1, \ldots, x_n$ with coefficients in the field k is denoted

$$k[x_1, \ldots, x_n]$$

So, for example we can say

$$p(x, y) = 5x^3y^4 - \frac{3}{2}xy^2 - 3 \in \mathbb{Q}[x, y]$$

Ring properties for polynomials

It is not difficult to show that the addition and multiplication operations on $k[x_1, \ldots, x_n]$ have the following properties:

1. For all $f, g, h \in k[x_1, \ldots, x_n]$, $(f + g) + h = f + (g + h)$ (addition is associative)
2. There is a zero polynomial $0 \in k[x_1, \ldots, x_n]$ such that $f + 0 = 0 + f = f$ for all $f \in k[x_1, \ldots, x_n]$
3. For each $f \in k[x_1, \ldots, x_n]$, there is a $-f \in k[x_1, \ldots, x_n]$ such that $f + (-f) = (-f) + f = 0$ (the zero polynomial from 3)
4. For all $f, g \in k[x_1, \ldots, x_n]$, $f + g = g + f$ (addition is commutative)

(Together properties 1-4 say that $k[x_1, \ldots, x_n]$ is an *abelian group* under addition.)

Ring properties for polynomials, cont.

5. For all $f, g, h \in k[x_1, \ldots, x_n]$, $(fg)h = f(gh)$ (multiplication is associative)
6. There is a polynomial $1 \in k[x_1, \ldots, x_n]$ such that $f \cdot 1 = 1 \cdot f = f$ for all $f \in k[x_1, \ldots, x_n]$
7. For all $f, g \in k[x_1, \ldots, x_n]$, $fg = gf$ (multiplication is commutative)
8. For all $f, g, h \in k[x_1, \ldots, x_n]$, $f(g + h) = fg + fh$ and $(f + g)h = fh + gh$ (multiplication distributes over addition)

Together 1-8 say that $k[x_1, \ldots, x_n]$ is an *commutative ring with (multiplicative) identity*.
Note: A *field* is an algebraic structure in which all of these properties hold, *and* in which every nonzero element has a multiplicative inverse. $k[x_1, \ldots, x_n]$ is *not a field*. (For example, is there a polynomial f such that $x_1 \cdot f = 1$? Why or why not?)

Polynomial functions

- Up to now the $f \in k[x_1, \ldots, x_n]$ are essentially formal expressions, but

Polynomial functions

- Up to now the $f \in k[x_1, \ldots, x_n]$ are essentially formal expressions, but
- Each such f also defines a *function* $f : k^n \to k$

Polynomial functions

- Up to now the $f \in k[x_1, \ldots, x_n]$ are essentially formal expressions, but
- Each such f also defines a *function* $f : k^n \to k$
- defined by evaluation $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$

Polynomial functions

- Up to now the $f \in k[x_1, \ldots, x_n]$ are essentially formal expressions, but
- Each such f also defines a *function* $f : k^n \to k$
- defined by evaluation $(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n)$
- For example $f(x, y) = x^2y - 3x \in \mathbb{R}[x, y]$ defines a function from $\mathbb{R}^2$ to $\mathbb{R}$ with $f(0, 0) = 0$, $f(1, 1) = -2$, etc.

Polynomial functions, continued

- Can two different polynomials define the same polynomial function?

Polynomial functions, continued

- Can two different polynomials define the same polynomial function?
- Answer is *yes*, if k is a *finite field*(!)

Polynomial functions, continued

- Can two different polynomials define the same polynomial function?
- Answer is *yes*, if k is a *finite field*(!)
- For instance, $k = \mathbb{Z}_p$ is a field if p is prime. With $n = 1$, the polynomials $f(x) = x^p$ and $g(x) = x$ actually define the same function since $a^p = a$ for all $a \in \mathbb{Z}_p$.

Polynomial functions, continued

- Can two different polynomials define the same polynomial function?
- Answer is *yes*, if k is a *finite field*(!)
- For instance, $k = \mathbb{Z}_p$ is a field if p is prime. With $n = 1$, the polynomials $f(x) = x^p$ and $g(x) = x$ actually define the same function since $a^p = a$ for all $a \in \mathbb{Z}_p$.
- *But*, if k is infinite (e.g. $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.) then $f, g \in k[x_1, \ldots, x_n]$ define the same polynomial function if and only if $f = g$. (Note: the $\Leftarrow$ implication is always true)

Proof of the $\Rightarrow$ implication

- We argue by induction on n, the number of variables.

Proof of the $\Rightarrow$ implication

- We argue by induction on n, the number of variables.
- When $n = 1$, recall from high school algebra that a nonzero polynomial of degree n in one variable has at most n roots.

Proof of the $\Rightarrow$ implication

- We argue by induction on n, the number of variables.
- When $n = 1$, recall from high school algebra that a nonzero polynomial of degree n in one variable has at most n roots.
- So if $f(a) = g(a)$ for all $a \in k$, the polynomial $f - g$ is zero at all $a \in k$. This implies $f - g$ is the zero polynomial, so $f = g$.

Proof of the $\Rightarrow$ implication

- We argue by induction on n, the number of variables.
- When $n = 1$, recall from high school algebra that a nonzero polynomial of degree n in one variable has at most n roots.
- So if $f(a) = g(a)$ for all $a \in k$, the polynomial $f - g$ is zero at all $a \in k$. This implies $f - g$ is the zero polynomial, so $f = g$.
- Now assume the result is true for polynomials in $n - 1$ variables, and consider $f, g \in k[x_1, \ldots, x_n]$ defining the same polynomial function.

Proof, concluded

- Write $f = f_k(x_1, \ldots, x_{n-1})x_n^k + \cdots + f_0(x_1, \ldots, x_{n-1})$ and similarly for g.

Proof, concluded

- Write $f = f_k(x_1, \ldots, x_{n-1})x_n^k + \cdots + f_0(x_1, \ldots, x_{n-1})$ and similarly for g.
- By assumption, for all $f(a_1, \ldots, a_{n-1}) \in k^{n-1}$, $f(a_1, \ldots, a_{n-1}, x_n) = g(a_1, \ldots, a_{n-1}, x_n)$ define the same function of x_n.

Proof, concluded

- Write $f = f_k(x_1, \ldots, x_{n-1})x_n^k + \cdots + f_0(x_1, \ldots, x_{n-1})$ and similarly for g.
- By assumption, for all $f(a_1, \ldots, a_{n-1}) \in k^{n-1}$, $f(a_1, \ldots, a_{n-1}, x_n) = g(a_1, \ldots, a_{n-1}, x_n)$ define the same function of x_n.
- By the base case, this implies that $f_i(a_1, \ldots, a_{n-1}) = g_i(a_1, \ldots, a_{n-1})$ for all i and all $(a_1, \ldots, a_{n-1})$.

Proof, concluded

- Write $f = f_k(x_1, \ldots, x_{n-1})x_n^k + \cdots + f_0(x_1, \ldots, x_{n-1})$ and similarly for g.
- By assumption, for all $f(a_1, \ldots, a_{n-1}) \in k^{n-1}$, $f(a_1, \ldots, a_{n-1}, x_n) = g(a_1, \ldots, a_{n-1}, x_n)$ define the same function of x_n.
- By the base case, this implies that $f_i(a_1, \ldots, a_{n-1}) = g_i(a_1, \ldots, a_{n-1})$ for all i and all $(a_1, \ldots, a_{n-1})$.
- But then, the induction hypothesis implies $f_i = g_i$ all i, and hence $f = g$. QED

Geometric objects from polynomials

We can use polynomials $f \in k[x_1, \ldots, x_n]$ to define geometric objects as subsets of k^n as follows.

Definition 2

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Then $V(f_1, \ldots, f_s)$ (called the *variety* defined by the f_i) is the subset of k^n given as the common zero locus of all the f_i:

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \mid f_i(a_1, \ldots, a_n) = 0, i = 1, \ldots, s\}$$

Examples

To draw pictures, we will almost always take $k = \mathbb{R}$

- $V(y - g(x))$ is the usual *graph* of the polynomial function $g(x)$

Examples

To draw pictures, we will almost always take $k = \mathbb{R}$

- $V(y - g(x))$ is the usual *graph* of the polynomial function $g(x)$
- $V\left(\frac{x^2}{9} - \frac{y^2}{4} - 1\right)$ is a hyperbola in the plane

Examples

To draw pictures, we will almost always take $k = \mathbb{R}$

- $V(y - g(x))$ is the usual *graph* of the polynomial function $g(x)$
- $V\left(\frac{x^2}{9} - \frac{y^2}{4} - 1\right)$ is a hyperbola in the plane
- $V\left(x^2 + y^2 - 1, x - y + \frac{1}{2}\right)$ consists of the two intersection points of the circle defined by $x^2 + y^2 - 1 = 0$ and the line defined by $x - y + \frac{1}{2} = 0$. [Sage demo]

Examples

To draw pictures, we will almost always take $k = \mathbb{R}$

- $V(y - g(x))$ is the usual *graph* of the polynomial function $g(x)$
- $V\left(\frac{x^2}{9} - \frac{y^2}{4} - 1\right)$ is a hyperbola in the plane
- $V\left(x^2 + y^2 - 1, x - y + \frac{1}{2}\right)$ consists of the two intersection points of the circle defined by $x^2 + y^2 - 1 = 0$ and the line defined by $x - y + \frac{1}{2} = 0$. [Sage demo]
- $V(y - x^2, z - x^3)$ is the *twisted cubic curve* in $\mathbb{R}^3$. [Sage demo]

Some observations

- Since $V(f_1, \ldots, f_s)$ is the set of solutions of the simultaneous system of equations $f_1 = 0, \ldots, f_s = 0$, we have
$$V(f_1, \ldots, f_s) = V(f_1) \cap \cdots \cap V(f_s)$$

Some observations

- Since $V(f_1, \ldots, f_s)$ is the set of solutions of the simultaneous system of equations $f_1 = 0, \ldots, f_s = 0$, we have
$$V(f_1, \ldots, f_s) = V(f_1) \cap \cdots \cap V(f_s)$$
- Since our polynomial functions take values in a field, a product $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$ if and only if $f(a_1, \ldots, a_n) = 0$ or $g(a_1, \ldots, a_n) = 0$. So,
$$V(fg) = V(f) \cup V(g)$$

Some observations

- Since $V(f_1, \ldots, f_s)$ is the set of solutions of the simultaneous system of equations $f_1 = 0, \ldots, f_s = 0$, we have
$$V(f_1, \ldots, f_s) = V(f_1) \cap \cdots \cap V(f_s)$$
- Since our polynomial functions take values in a field, a product $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$ if and only if $f(a_1, \ldots, a_n) = 0$ or $g(a_1, \ldots, a_n) = 0$. So,
$$V(fg) = V(f) \cup V(g)$$
- In fact if $V = V(f_1, \ldots, f_s)$ and $W = V(g_1, \ldots, g_t)$ are varieties, then so are $V \cap W$ and $V \cup W$:

Some observations

- Since $V(f_1, \ldots, f_s)$ is the set of solutions of the simultaneous system of equations $f_1 = 0, \ldots, f_s = 0$, we have
$$V(f_1, \ldots, f_s) = V(f_1) \cap \cdots \cap V(f_s)$$
- Since our polynomial functions take values in a field, a product $f(a_1, \ldots, a_n)g(a_1, \ldots, a_n) = 0$ if and only if $f(a_1, \ldots, a_n) = 0$ or $g(a_1, \ldots, a_n) = 0$. So,
$$V(fg) = V(f) \cup V(g)$$
- In fact if $V = V(f_1, \ldots, f_s)$ and $W = V(g_1, \ldots, g_t)$ are varieties, then so are $V \cap W$ and $V \cup W$:
- $V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t)$ and $V \cup W = V(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t)$.

Parametrizations

Some varieties can also be described as the images of *parametrization mappings*

$$\begin{aligned} F : k^m &\rightarrow k^n, \\ (t_1, \ldots, t_m) &\mapsto (F_1(t_1, \ldots, t_m), \ldots, F_n(t_1, \ldots, t_m)) \end{aligned}$$

- For instance, the circle $V(x^2 + y^2 - 1)$ can be parametrized by $F(t) = (\cos(t), \sin(t))$ (not polynomial functions, of course!)
- The twisted cubic $V(y - x^2, z - x^3)$ is the image of $F(t) = (t, t^2, t^3)$

To Ideals

The set of defining equations $f_1 = 0, \ldots, f_s = 0$ defining a variety $V = V(f_1, \ldots, f_s)$ is *never unique*.

- First notice that if $g, \ldots, g_s$ are any polynomials at all and $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$, then $f = g_1 f_1 + \cdots + g_s f_s$ satisfies

$$f(a_1, \ldots, a_n) = g_1(a_1, \ldots, a_n) \cdot 0 + \cdots + g_1(a_1, \ldots, a_n) \cdot 0 = 0$$

To Ideals

The set of defining equations $f_1 = 0, \ldots, f_s = 0$ defining a variety $V = V(f_1, \ldots, f_s)$ is *never unique*.

- First notice that if $g, \ldots, g_s$ are any polynomials at all and $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$, then $f = g_1 f_1 + \cdots + g_s f_s$ satisfies

$$f(a_1, \ldots, a_n) = g_1(a_1, \ldots, a_n) \cdot 0 + \cdots + g_1(a_1, \ldots, a_n) \cdot 0 = 0$$

- Hence f *also vanishes at every point of* $V = V(f_1, \ldots, f_s)$, and

To Ideals

The set of defining equations $f_1 = 0, \ldots, f_s = 0$ defining a variety $V = V(f_1, \ldots, f_s)$ is *never unique*.

- First notice that if $g, \ldots, g_s$ are any polynomials at all and $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$, then $f = g_1 f_1 + \cdots + g_s f_s$ satisfies

$$f(a_1, \ldots, a_n) = g_1(a_1, \ldots, a_n) \cdot 0 + \cdots + g_1(a_1, \ldots, a_n) \cdot 0 = 0$$

- Hence f *also vanishes at every point of* $V = V(f_1, \ldots, f_s)$, and
- It follows that $V(f_1, \ldots, f_s, f) = V(f_1, \ldots, f_s)$

More motivation

- The polynomial f is above superfluous

More motivation

- The polynomial f is above superfluous
- If we turn this around though, we see a way for detecting extra, unneeded equations in some cases: If $V = V(f_1, \ldots, f_s)$ and $f_s = g_1 f_1 + \ldots + g_{s-1} f_{s-1}$ for some polynomials $g_1, \ldots, g_{s-1}$, then $V = V(f_1, \ldots, f_{s-1})$ also.

More motivation

- The polynomial f is above superfluous
- If we turn this around though, we see a way for detecting extra, unneeded equations in some cases: If $V = V(f_1, \ldots, f_s)$ and $f_s = g_1 f_1 + \ldots + g_{s-1} f_{s-1}$ for some polynomials $g_1, \ldots, g_{s-1}$, then $V = V(f_1, \ldots, f_{s-1})$ also.
- Finding polynomials $f = g_1 f_1 + \ldots + g_s f_s$ with "special" features like *factorizations* can also be useful.

More motivation

- The polynomial f is above superfluous
- If we turn this around though, we see a way for detecting extra, unneeded equations in some cases: If $V = V(f_1, \ldots, f_s)$ and $f_s = g_1 f_1 + \ldots + g_{s-1} f_{s-1}$ for some polynomials $g_1, \ldots, g_{s-1}$, then $V = V(f_1, \ldots, f_{s-1})$ also.
- Finding polynomials $f = g_1 f_1 + \ldots + g_s f_s$ with "special" features like *factorizations* can also be useful.
- Example: Consider $W = V\left(x^2 + y^2 + z^2 - 1, x^2 + y^2 - \frac{1}{4}\right)$ in $\mathbb{R}^3$. Notice:

$$\begin{aligned}(1)(x^2 + y^2 + z^2 - 1) \quad + \quad (-1)(x^2 + y^2 - \frac{1}{4}) &= z^2 - \frac{3}{4} \\ &= (z - \sqrt{3}/2)(z + \sqrt{3}/2)\end{aligned}$$

What does this tell us about the variety W?

Ideal generated by $f_1, \ldots, f_s$

Definition 3

Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. The *ideal generated by the* $f_1, \ldots, f_s$ is the subset of $k[x_1, \ldots, x_n]$ defined by

$$\langle f_1, \ldots, f_s \rangle = \{g_1 f_1 + \cdots + g_s f_s \mid g_i \in k[x_1, \ldots, x_n]\}$$

For instance the example on the last slide shows

$$z^2 - \frac{3}{4} \in \left\langle x^2 + y^2 + z^2 - 1, x^2 + y^2 - \frac{1}{4} \right\rangle.$$

Ideals

Note that $I = \langle f_1, \ldots, f_s \rangle$ has the following properties:

a. If $f, g \in I$, then $f + g \in I$
b. If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $h \cdot f \in I$

Definition 4

A nonempty subset I of a $k[x_1, \ldots, x_n]$ is said to be *an ideal* if

a. $f, g \in I$ implies $f + g \in I$, and
b. $f \in I$ and $h \in k[x_1, \ldots, x_n]$ implies $h \cdot f \in I$.

Given any $f_1, \ldots, f_s$, $\langle f_1, \ldots, f_s \rangle$ satifies this definition. But are there other ideals too in $k[x_1, \ldots, x_s]$ (ones with n finite generating set?

Other examples of ideals

The answer is not so clear at first, because of examples like these:

- Let $S \subset k^n$ be any subset and define

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ all } a = (a_1, \ldots, a_n) \in S\}$$

  Easy to check this satisfies the definition. (Why?)

Other examples of ideals

The answer is not so clear at first, because of examples like these:

- Let $S \subset k^n$ be any subset and define

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ all } a = (a_1, \ldots, a_n) \in S\}$$

  Easy to check this satisfies the definition. (Why?)

- Let I be an ideal in $k[x_1, \ldots, x_n]$ and let $\sqrt{I}$ *(the radical of I)* be

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^k \in I \text{ for some } k \geq 1\}.$$

Other examples of ideals

The answer is not so clear at first, because of examples like these:

- Let $S \subset k^n$ be any subset and define

  $$I(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ all } a = (a_1, \ldots, a_n) \in S\}$$

  Easy to check this satisfies the definition. (Why?)
- Let I be an ideal in $k[x_1, \ldots, x_n]$ and let $\sqrt{I}$ *(the radical of I)* be

  $$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid f^k \in I \text{ for some } k \geq 1\}.$$

Theorem 5

Let I be an ideal in $k[x_1, \ldots, x_n]$. Then $\sqrt{I}$ is an ideal.

Proof of the theorem

- For part b of the definition, if $f \in \sqrt{I}$, then $f^k \in I$ for some integer $k \geq 1$. If h is an arbitrary polynomial, $(hf)^k = h^k f^k \in I$, since $f^k \in I$. Hence $hf \in \sqrt{I}$.

Proof of the theorem

- For part b of the definition, if $f \in \sqrt{I}$, then $f^k \in I$ for some integer $k \geq 1$. If h is an arbitrary polynomial, $(hf)^k = h^k f^k \in I$, since $f^k \in I$. Hence $hf \in \sqrt{I}$.
- For part a, if $f, g \in \sqrt{I}$, then $f^k \in I$ and $g^m \in I$ for some k, m (not necessarily the same). By looking at the binomial expansion

$$(f+g)^{k+m-1} = \sum_{\ell=0}^{k+m-1} \binom{k+m-1}{\ell} f^\ell g^{k+m-1-\ell}$$

we can see that each term contains either f^ℓ for $\ell \geq k$ or g^p for $p \geq m$. Hence $(f+g)^{k+m-1} \in I$, which says $f + g \in \sqrt{I}$. QED

An observation

Theorem 6

Let $V = V(f_1, \ldots, f_s)$ *be a variety, and let* $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$. *Then* $V = V(g_1, \ldots, g_t)$ *also.*

- In other words, varieties are “really” defined by ideals, not particular sets of equations – we’ll write $V(I)$.

An observation

Theorem 6

Let $V = V(f_1, \ldots, f_s)$ *be a variety, and let* $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$. *Then* $V = V(g_1, \ldots, g_t)$ *also.*

- In other words, varieties are "really" defined by ideals, not particular sets of equations – we'll write $V(I)$.
- Proof: $V \subset V(g_1, \ldots, g_t)$ is more or less clear since each $g_i = h_{i1} f_1 + \cdots + h_{is} f_s$ for some polynomials h_{ij}.

An observation

Theorem 6

Let $V = V(f_1, \ldots, f_s)$ *be a variety, and let* $\langle g_1, \ldots, g_t \rangle = \langle f_1, \ldots, f_s \rangle$. *Then* $V = V(g_1, \ldots, g_t)$ *also.*

- In other words, varieties are "really" defined by ideals, not particular sets of equations – we'll write $V(I)$.
- Proof: $V \subset V(g_1, \ldots, g_t)$ is more or less clear since each $g_i = h_{i1}f_1 + \cdots + h_{is}f_s$ for some polynomials h_{ij}.
- The reverse inclusion follows in the same way since each $f_j = p_{j1}g_1 + \cdots p_{jt}g_t$ for some polynomials p_{ji}. QED

An example

- Consider $V = V(x^2 + y^2 - 1, x^2 - x + y^2 - 3/4)$.

An example

- Consider $V = V(x^2 + y^2 - 1, x^2 - x + y^2 - 3/4)$.
- We have

$$x - 1/4 = (1)(x^2 + y^2 - 1) + (-1)(x^2 - x + y^2 - 3/4)$$

An example

- Consider $V = V(x^2 + y^2 - 1, x^2 - x + y^2 - 3/4)$.
- We have

$$x - 1/4 = (1)(x^2 + y^2 - 1) + (-1)(x^2 - x + y^2 - 3/4)$$

- Hence

$$\langle x^2 + y^2 - 1, x - 1/4 \rangle = \langle x^2 + y^2 - 1, x^2 - x + y^2 - 3/4 \rangle$$

(why?)

An example

- Consider $V = V(x^2 + y^2 - 1, x^2 - x + y^2 - 3/4)$.
- We have

$$x - 1/4 = (1)(x^2 + y^2 - 1) + (-1)(x^2 - x + y^2 - 3/4)$$

- Hence

$$\langle x^2 + y^2 - 1, x - 1/4 \rangle = \langle x^2 + y^2 - 1, x^2 - x + y^2 - 3/4 \rangle$$

  (why?)
- The theorem implies that

$$V = V(x^2 + y^2 - 1, x - 1/4).$$

An example

- Consider $V = V(x^2 + y^2 - 1, x^2 - x + y^2 - 3/4)$.
- We have

$$x - 1/4 = (1)(x^2 + y^2 - 1) + (-1)(x^2 - x + y^2 - 3/4)$$

- Hence

$$\langle x^2 + y^2 - 1, x - 1/4 \rangle = \langle x^2 + y^2 - 1, x^2 - x + y^2 - 3/4 \rangle$$

  (why?)
- The theorem implies that

$$V = V(x^2 + y^2 - 1, x - 1/4).$$

- The same sort of thing happens for all pairs of circles in $\mathbb{R}^2$. The variety is also defined by one of the circles and a linear polynomial in x, y. (What happens if the circles don't intersect?)

$I(V(I))$

- Suppose we start with an ideal and look at the variety $V(I)$. Is $I(V(I)) = I$?

$I(V(I))$

- Suppose we start with an ideal and look at the variety $V(I)$. Is $I(V(I)) = I$?
- One inclusion is always true. Which one?

$I(V(I))$

- Suppose we start with an ideal and look at the variety $V(I)$. Is $I(V(I)) = I$?
- One inclusion is always true. Which one?
- Answer to first question: *not always!* Example: Let $I = \langle x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the y-axis in the plane, and it's not too hard to show $I(V(I)) = \langle x \rangle \neq I$.

$I(V(I))$

- Suppose we start with an ideal and look at the variety $V(I)$. Is $I(V(I)) = I$?
- One inclusion is always true. Which one?
- Answer to first question: *not always!* Example: Let $I = \langle x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the y-axis in the plane, and it's not too hard to show $I(V(I)) = \langle x \rangle \neq I$.
- In fact, it follows directly that $\sqrt{I} \subset I(V(I))$: If $f \in \sqrt{I}$, then $f^k \in I$ for some $k \geq 1$. At any point a in $V(I)$, $(f^k)(a) = (f(a))^k = 0$, which implies $f(a) = 0$. Therefore, $f \in I(V(I))$.

$I(V(I))$, continued.

- On the other hand, here is another example where $I(V(I)) = I$ is true. As above $I \subset I(V(I))$ always holds.

$I(V(I))$, continued.

- On the other hand, here is another example where $I(V(I)) = I$ is true. As above $I \subset I(V(I))$ always holds.
- Say $I = \langle y - x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the usual parabola.

$I(V(I))$, continued.

- On the other hand, here is another example where $I(V(I)) = I$ is true. As above $I \subset I(V(I))$ always holds.
- Say $I = \langle y - x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the usual parabola.
- Given any $f(x, y)$ we can substitute $f(x, y) = f(x, (y - x^2) + x^2)$ expand out and collect terms to obtain:

$$f(x, y) = q(x, y)(y - x^2) + r(x)$$

$I(V(I))$, continued.

- On the other hand, here is another example where $I(V(I)) = I$ is true. As above $I \subset I(V(I))$ always holds.
- Say $I = \langle y - x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the usual parabola.
- Given any $f(x, y)$ we can substitute $f(x, y) = f(x, (y - x^2) + x^2)$ expand out and collect terms to obtain:

$$f(x, y) = q(x, y)(y - x^2) + r(x)$$

- If $f \in I(V(I))$ (that is if f vanishes at every point of the parabola $y - x^2$), then we must have $r(x) = 0$ for all $x \in \mathbb{R}$.

$I(V(I))$, continued.

- On the other hand, here is another example where $I(V(I)) = I$ is true. As above $I \subset I(V(I))$ always holds.
- Say $I = \langle y - x^2 \rangle$ in $\mathbb{R}[x, y]$. Then $V(I)$ is the usual parabola.
- Given any $f(x, y)$ we can substitute $f(x, y) = f(x, (y - x^2) + x^2)$ expand out and collect terms to obtain:

$$f(x, y) = q(x, y)(y - x^2) + r(x)$$

- If $f \in I(V(I))$ (that is if f vanishes at every point of the parabola $y - x^2$), then we must have $r(x) = 0$ for all $x \in \mathbb{R}$.
- But that implies $r(x)$ is the zero polynomial, so $f \in \langle y - x^2 \rangle$. This shows $I(V(I)) \subset I$ in this case, so they are equal.

Division in $k[x]$

There is a basic operation in the polynomial ring in one variable over a field that has extremely strong implications for ideals in this case. This is the *polynomial division algorithm*. You probably saw this in high school algebra at some point. [Recall idea with an example on the board] The precise results of what we're doing here can be stated like this:

Theorem 7

Let $f(x), g(x)$ be polynomials in $k[x]$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

1. $f(x) = q(x)g(x) + r(x)$, *and*
2. *either* $r(x) = 0$ *or* $\deg r(x) < \deg g(x)$.

Division algorithm

Hand process to produce quotient $q(x)$ and remainder $r(x)$ can be described using *pseudocode* like this:

```
Input: f,g
Output: q,r
q := 0; r := f
while r <> 0 and LT(g) divides LT(r) do
   q := q + LT(r)/LT(g)
   r := r - (LT(r)/LT(g))g
```

(Here $LT(f)$ denotes the “leading term” or term of highest degree in a polynomial f.)

Idea of proof

Proof.

The full details of the proof are given in the text. The key idea is that the equation $f = qg + r$ holds after the initial assignments, and if it holds at the start of one pass through the while loop, then it also holds and the end of the pass because we have just "rearranged the terms" like this:

$$f = (q + LT(r)/LT(g))g + r - (LT(r)/LT(g))g$$

Hence it will also be true at the conclusion of the while loop. The loop terminates because the degree of r is reduced by at least one on each pass through the while loop. On termination, $r(x) = 0$ or $\deg r(x) < \deg g(x)$ because if not, then $LT(g)$ would still divide $LT(g)$. □

Theorem 8

Let I be an ideal in $k[x]$. Then $I = \langle g(x) \rangle$ for some $g(x) \in I$.

In other words, every ideal in $k[x]$ is *principal* (generated by a single polynomial. Abstract algebra: $k[x]$ is a PID.

Proof.

If $I = \{0\}$, then take $g(x) = 0$. Otherwise, let $g(x)$ be a nonzero polynomial in I of *minimal degree*. We claim that $I = \langle f(x) \rangle$. The $\supset$ inclusion is clear. To show $\subset$: let $f(x) \in I$ be an arbitrary polynomial. Using the division algorithm, write $f(x) = q(x)g(x) + r(x)$. If $r(x) \neq 0$, then $\deg r(x) < \deg g(x)$. But $r(x) = f(x) - q(x)g(x) \in I$. This is a contradiction to the way we chose $g(x)$. Hence $r(x) = 0$, so $f(x) = q(x)g(x) \in \langle g(x) \rangle$. It follows that $I = \langle g(x) \rangle$. □

Ideal membership test

- If we know the generator polynomial $g(x)$, we can also test for membership in the ideal $I = \langle g(x) \rangle$ using division:

Ideal membership test

- If we know the generator polynomial $g(x)$, we can also test for membership in the ideal $I = \langle g(x) \rangle$ using division:
- Given $f(x)$, compute $f(x) = q(x)g(x) + r(x)$ by division

Ideal membership test

- If we know the generator polynomial $g(x)$, we can also test for membership in the ideal $I = \langle g(x) \rangle$ using division:
- Given $f(x)$, compute $f(x) = q(x)g(x) + r(x)$ by division
- Then by uniqueness, $f(x) \in I \Leftrightarrow r(x) = 0$

Ideal membership test

- If we know the generator polynomial $g(x)$, we can also test for membership in the ideal $I = \langle g(x) \rangle$ using division:
- Given $f(x)$, compute $f(x) = q(x)g(x) + r(x)$ by division
- Then by uniqueness, $f(x) \in I \Leftrightarrow r(x) = 0$
- Example: Let $g(x) = x^2 - 5x + 6$, and $f(x) = x^3 + 25x + 30$.

Ideal membership test

- If we know the generator polynomial $g(x)$, we can also test for membership in the ideal $I = \langle g(x) \rangle$ using division:
- Given $f(x)$, compute $f(x) = q(x)g(x) + r(x)$ by division
- Then by uniqueness, $f(x) \in I \Leftrightarrow r(x) = 0$
- Example: Let $g(x) = x^2 - 5x + 6$, and $f(x) = x^3 + 25x + 30$.
- $f(x) = (x+5)(x^2 - 5x + 6) + 0 \Rightarrow f(x) \in \langle g(x) \rangle$.

Polynomial gcd's

- An example: Consider $I = \langle x^4 - 16, x^2 - 2x - 8 \rangle$ in $\mathbb{Q}[x]$. By the theorem, there must be some single polynomial $g(x)$ such that $\langle g(x) \rangle = I$.

Polynomial gcd's

- An example: Consider $I = \langle x^4 - 16, x^2 - 2x - 8\rangle$ in $\mathbb{Q}[x]$. By the theorem, there must be some single polynomial $g(x)$ such that $\langle g(x)\rangle = I$.
- Note that $g(x)$ must divide each of $x^4 - 16 = (x-2)(x+2)(x^2+4)$ and $x^2 - 2x - 8 = (x+2)(x-4)$.

Polynomial gcd's

- An example: Consider $I = \langle x^4 - 16, x^2 - 2x - 8\rangle$ in $\mathbb{Q}[x]$. By the theorem, there must be some single polynomial $g(x)$ such that $\langle g(x)\rangle = I$.
- Note that $g(x)$ must divide each of $x^4 - 16 = (x-2)(x+2)(x^2+4)$ and $x^2 - 2x - 8 = (x+2)(x-4)$.
- Hence we can see that $g(x) = x + 2$, the gcd of the two polynomials.

Polynomial gcd's

- An example: Consider $I = \langle x^4 - 16, x^2 - 2x - 8 \rangle$ in $\mathbb{Q}[x]$. By the theorem, there must be some single polynomial $g(x)$ such that $\langle g(x) \rangle = I$.
- Note that $g(x)$ must divide each of $x^4 - 16 = (x - 2)(x + 2)(x^2 + 4)$ and $x^2 - 2x - 8 = (x + 2)(x - 4)$.
- Hence we can see that $g(x) = x + 2$, the gcd of the two polynomials.
- In general $g(x) = \text{gcd}(f(x), h(x))$ can be defined as the monic generator of the ideal $\langle f(x), h(x) \rangle$ using the theorem, or it can be characterized by its properties (see Definition 5 in Chapter 1, §5 in IVA).

Polynomial gcd's

- An example: Consider $I = \langle x^4 - 16, x^2 - 2x - 8\rangle$ in $\mathbb{Q}[x]$. By the theorem, there must be some single polynomial $g(x)$ such that $\langle g(x)\rangle = I$.
- Note that $g(x)$ must divide each of $x^4 - 16 = (x-2)(x+2)(x^2+4)$ and $x^2 - 2x - 8 = (x+2)(x-4)$.
- Hence we can see that $g(x) = x + 2$, the gcd of the two polynomials.
- In general $g(x) = \gcd(f(x), h(x))$ can be defined as the monic generator of the ideal $\langle f(x), h(x)\rangle$ using the theorem, or it can be characterized by its properties (see Definition 5 in Chapter 1, §5 in IVA).
- "Ideally," we would like a way to compute $\gcd(f(x), h(x))$ without factoring.

The method here goes all the way back to the *Elements* of Euclid (although he discussed the corresponding procedure for integers, not polynomials). In the following, `remainder` means compute the remainder using the division algorithm above:

```
Input:   f,g
Output: h
h := f; s := g
while s <> 0 do
   rem := remainder(h,s)
   h := s
   s := rem
```

Euclidean algorithm, step-by-step

If we give separate names to the remainders obtained at each step, we get something like:

$$\begin{aligned} f &= q_1 g + r_1 \\ g &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_k r_{k-1} + r_k \end{aligned}$$

The algorithm terminates the first time a zero remainder r_k is found. (This must happen after a finite number of steps since the degrees of the remainders form a strictly decreasing sequence.)

An example

We will carry this out for $f = x^4 - 16$, $g = x^2 - 2x - 8$ as above:

$$\begin{aligned} x^4 - 16 &= (x^2 + 2x + 12)(x^2 - 2x - 8) + 40x + 80 \\ x^2 - 2x - 8 &= \left(\frac{1}{40}x - \frac{1}{10}\right)(40x + 80) + 0 \end{aligned}$$

Note that the loop terminates here since $s = 0$. The gcd is the *final nonzero remainder* – that is $40x + 80$, or $x + 2$ if we require a monic polynomial. This agrees with our earlier results obtained by factorization.

Another example

Now say $f = x^5 + x + 1$, $g = x^4 + x^2 + 1$. What is $\gcd(f, g)$?

$$\begin{aligned}
x^5 + x + 1 &= x(x^4 + x + 1) + (-x^2 + 1) \\
x^4 + x + 1 &= (-x^2 - 1)(-x^2 + 1) + (x + 2) \\
-x^2 + 1 &= (-x + 2)(x + 2) + (-3) \\
x + 2 &= (x/3 + 2/3)(3) + 0
\end{aligned}$$

Up to a constant multiple, the final nonzero remainder is 1. We say the polynomials f, g are *relatively prime* in this case.

Leading terms

- Since division is so useful for revealing properties of ideals in $k[x]$, can ask whether there is a generalization to $k[x_1, \ldots, x_n]$.

Leading terms

- Since division is so useful for revealing properties of ideals in $k[x]$, can ask whether there is a generalization to $k[x_1, \ldots, x_n]$.
- You may have seen a naive version ("pseudo-division") in two variables

Leading terms

- Since division is so useful for revealing properties of ideals in $k[x]$, can ask whether there is a generalization to $k[x_1, \ldots, x_n]$.
- You may have seen a naive version ("pseudo-division") in two variables
- For instance, say $g(x, y) = y^n + g_1(x)y^{n-1} + \cdots + g_n(x)$

Leading terms

- Since division is so useful for revealing properties of ideals in $k[x]$, can ask whether there is a generalization to $k[x_1, \ldots, x_n]$.
- You may have seen a naive version ("pseudo-division") in two variables
- For instance, say $g(x, y) = y^n + g_1(x)y^{n-1} + \cdots + g_n(x)$
- We can divide g into any $f(x, y)$ as for polynomials in y alone, but doing arithmetic in $k[x]$ for the coefficients.

Leading terms

- Since division is so useful for revealing properties of ideals in $k[x]$, can ask whether there is a generalization to $k[x_1, \ldots, x_n]$.
- You may have seen a naive version ("pseudo-division") in two variables
- For instance, say $g(x, y) = y^n + g_1(x)y^{n-1} + \cdots + g_n(x)$
- We can divide g into any $f(x, y)$ as for polynomials in y alone, but doing arithmetic in $k[x]$ for the coefficients.
- Do an [example on board]

But, ...

- Not a complete analog of division in $k[x]$ for several reasons:

But, ...

- Not a complete analog of division in $k[x]$ for several reasons:
- The variable y plays a special role and note that leading coefficient of g must be 1 as above, or else we start introducing denominators (remainder is of degree $< n$ in y with coefficients rational functions in x, or zero)

But, ...

- Not a complete analog of division in $k[x]$ for several reasons:
- The variable y plays a special role and note that leading coefficient of g must be 1 as above, or else we start introducing denominators (remainder is of degree $< n$ in y with coefficients rational functions in x, or zero)
- More seriously, not every ideal in $k[x_1, \ldots, x_n]$ has form $\langle g(x) \rangle$ if $n \geq 2$.

But, ...

- Not a complete analog of division in $k[x]$ for several reasons:
- The variable y plays a special role and note that leading coefficient of g must be 1 as above, or else we start introducing denominators (remainder is of degree $< n$ in y with coefficients rational functions in x, or zero)
- More seriously, not every ideal in $k[x_1, \ldots, x_n]$ has form $\langle g(x) \rangle$ if $n \geq 2$.
- Example: $I = \langle x, y \rangle \subset k[x, y]$

But, ...

- Not a complete analog of division in $k[x]$ for several reasons:
- The variable y plays a special role and note that leading coefficient of g must be 1 as above, or else we start introducing denominators (remainder is of degree $< n$ in y with coefficients rational functions in x, or zero)
- More seriously, not every ideal in $k[x_1, \ldots, x_n]$ has form $\langle g(x) \rangle$ if $n \geq 2$.
- Example: $I = \langle x, y \rangle \subset k[x, y]$
- Why is there no $g(x, y)$ such that $\langle g(x, y) \rangle = \langle x, y \rangle$?

Leading terms

- If we want to try to generalize division, we need a way to select a *leading term* from each polynomial

Leading terms

- If we want to try to generalize division, we need a way to select a *leading term* from each polynomial
- But that is not so clear in general! For instance, which should be the leading term in

$$f(x, y) = x^3y^3 + x^5 + xy^4?$$

Leading terms

- If we want to try to generalize division, we need a way to select a *leading term* from each polynomial
- But that is not so clear in general! For instance, which should be the leading term in

$$f(x, y) = x^3y^3 + x^5 + xy^4?$$

- (Surprising?) answer: There are many possible ways, and *each of the three terms could be the leading term*, depending on how we order monomials!

Leading terms

- If we want to try to generalize division, we need a way to select a *leading term* from each polynomial
- But that is not so clear in general! For instance, which should be the leading term in

$$f(x, y) = x^3y^3 + x^5 + xy^4?$$

- (Surprising?) answer: There are many possible ways, and *each of the three terms could be the leading term*, depending on how we order monomials!
- What properties do we want?

Desired properties

- We should be able to put the terms in any nonzero polynomial into a unique (say decreasing) order

Desired properties

- We should be able to put the terms in any nonzero polynomial into a unique (say decreasing) order
- Then the leading term will the *largest* term (leading term of 0 is undefined)

Desired properties

- We should be able to put the terms in any nonzero polynomial into a unique (say decreasing) order
- Then the leading term will the *largest* term (leading term of 0 is undefined)
- If we multiply $f = \sum_\alpha c_\alpha x^\alpha$ by a monomial x^γ, then the terms in $x^\gamma f = \sum_\alpha c_\alpha x^{\alpha+\gamma}$ should not “switch around” – that is,
$$x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma}.$$

Desired properties

- We should be able to put the terms in any nonzero polynomial into a unique (say decreasing) order
- Then the leading term will the *largest* term (leading term of 0 is undefined)
- If we multiply $f = \sum_\alpha c_\alpha x^\alpha$ by a monomial x^γ, then the terms in $x^\gamma f = \sum_\alpha c_\alpha x^{\alpha+\gamma}$ should not "switch around" – that is,
$$x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma}.$$
- (Not so obvious at first, maybe): There should be no *infinite* descending chains starting from a fixed $x^{\alpha(1)}$:
$$x^{\alpha(1)} > x^{\alpha(2)} > \cdots > x^{\alpha(n)} > \cdots$$
(otherwise processes like division could go on forever(!))

Monomial orders

Definition 9

A *monomial order* is a relation $>$ on the set of monomials x^α in $k[x_1, \ldots, x_n]$ (or on the $\alpha \in \mathbb{Z}^n_{\geq 0}$ such that

i. $>$ is a total order relation (that is, for every pair of monomials x^α and x^β, exactly one of the statements: $x^\alpha > x^\beta$, $x^\alpha = x^\beta$, or $x^\beta > x^\alpha$ is true)

ii. For all α, β, γ, if $x^\alpha > x^\beta$, then $x^{\alpha+\gamma} > x^{\beta+\gamma}$

iii. $>$ is a well-ordering (every nonempty set of monomials has a smallest element, or equivalently, there are no infinite descending chains of monomials starting from any x^α)

Monomial orders on $k[x]$

- Consider the pair of monomials $1, x$. Since $1 \neq x$, then property i in the definition implies either $x > 1$, or $1 > x$.

Monomial orders on $k[x]$

- Consider the pair of monomials $1, x$. Since $1 \neq x$, then property i in the definition implies either $x > 1$, or $1 > x$.
- If $1 > x$, then by property ii in the definition, $x > x^2$, $x^2 > x^3$, etc. So we get an infinite descending chain starting from 1(!)

Monomial orders on $k[x]$

- Consider the pair of monomials $1, x$. Since $1 \neq x$, then property i in the definition implies either $x > 1$, or $1 > x$.
- If $1 > x$, then by property ii in the definition, $x > x^2$, $x^2 > x^3$, etc. So we get an infinite descending chain starting from 1(!)
- Hence, the *only* monomial order on $k[x]$ has $x > 1$, and then $\cdots x^3 > x^2 > x > 1$ is just the usual degree ordering

Monomial orders on $k[x]$

- Consider the pair of monomials $1, x$. Since $1 \neq x$, then property i in the definition implies either $x > 1$, or $1 > x$.
- If $1 > x$, then by property ii in the definition, $x > x^2$, $x^2 > x^3$, etc. So we get an infinite descending chain starting from 1(!)
- Hence, the *only* monomial order on $k[x]$ has $x > 1$, and then $\cdots x^3 > x^2 > x > 1$ is just the usual degree ordering
- Note that this is just the order used in division in $k[x]$(!)

Monomial orders on $k[x]$

- Consider the pair of monomials $1, x$. Since $1 \neq x$, then property i in the definition implies either $x > 1$, or $1 > x$.
- If $1 > x$, then by property ii in the definition, $x > x^2$, $x^2 > x^3$, etc. So we get an infinite descending chain starting from 1(!)
- Hence, the *only* monomial order on $k[x]$ has $x > 1$, and then $\cdots x^3 > x^2 > x > 1$ is just the usual degree ordering
- Note that this is just the order used in division in $k[x]$(!)
- Leading term in a nonzero polynomial in $k[x]$ is the term of highest degree

The lexicographic order

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

The lexicographic order

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

Definition 10

We say $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

The lexicographic order

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

Definition 10

We say $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

- Example: In $k[x, y, z]$, let $x^\alpha = x^3y^4z$ and $x^\beta = x^2yz^8$.

The lexicographic order

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

Definition 10

We say $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

- Example: In $k[x, y, z]$, let $x^\alpha = x^3y^4z$ and $x^\beta = x^2yz^8$.
- Then $\alpha = (3, 4, 1)$, $\beta = (2, 1, 8)$, $\alpha - \beta = (1, 3, -7)$

- In $k[x_1, \ldots, x_n]$, let's start out by assuming $x_1 > x_2 > \cdots > x_n$. Then we get a first example of a monomial order by the following:

Definition 10

We say $x^\alpha >_{lex} x^\beta$ if the leftmost nonzero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

- Example: In $k[x, y, z]$, let $x^\alpha = x^3y^4z$ and $x^\beta = x^2yz^8$.
- Then $\alpha = (3, 4, 1)$, $\beta = (2, 1, 8)$, $\alpha - \beta = (1, 3, -7)$
- So $x^3y^4z >_{lex} x^2yz^8$ (with $x > y > z$).

Another *lex* example

- Consider the polynomial $f(x,y) = x^3y^3 + x^5 + xy^4$ from before

Another *lex* example

- Consider the polynomial $f(x, y) = x^3y^3 + x^5 + xy^4$ from before
- Which is the *lex* leading term (taking $x > y$)?

Another *lex* example

- Consider the polynomial $f(x, y) = x^3y^3 + x^5 + xy^4$ from before
- Which is the *lex* leading term (taking $x > y$)?
- The exponent vectors are $(3, 3), (5, 0), (1, 4)$.

Another *lex* example

- Consider the polynomial $f(x, y) = x^3y^3 + x^5 + xy^4$ from before
- Which is the *lex* leading term (taking $x > y$)?
- The exponent vectors are $(3, 3), (5, 0), (1, 4)$.
- In *lex* order, we have $(5, 0) >_{lex} (3, 3) >_{lex} (1, 4)$

Another *lex* example

- Consider the polynomial $f(x, y) = x^3y^3 + x^5 + xy^4$ from before
- Which is the *lex* leading term (taking $x > y$)?
- The exponent vectors are $(3, 3), (5, 0), (1, 4)$.
- In *lex* order, we have $(5, 0) >_{lex} (3, 3) >_{lex} (1, 4)$
- Note: *lex* order is analogous to dictionary order for words(!)

Showing *lex* satisfies the definition

- Property i follows from properties of integers

Showing *lex* satisfies the definition

- Property i follows from properties of integers
- Property ii is easy since $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$

Showing *lex* satisfies the definition

- Property i follows from properties of integers
- Property ii is easy since $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$
- Property iii is the "interesting" and subtle one here

Showing *lex* satisfies the definition

- Property i follows from properties of integers
- Property ii is easy since $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$
- Property iii is the “interesting” and subtle one here
- Idea is that the usual order on $\mathbb{Z}_{\geq 0}$ is a well-order.

Showing *lex* satisfies the definition

- Property i follows from properties of integers
- Property ii is easy since $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$
- Property iii is the “interesting” and subtle one here
- Idea is that the usual order on $\mathbb{Z}_{\geq 0}$ is a well-order.
- So in any descending chain of monomials in the *lex* order, eventually the exponent of x_1 must “stabilize,” then the exponent of x_2 must “stabilize,” etc. But the way this works is a bit subtle – arbitrarily long chains exist:

Showing *lex* satisfies the definition

- Property i follows from properties of integers
- Property ii is easy since $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$
- Property iii is the "interesting" and subtle one here
- Idea is that the usual order on $\mathbb{Z}_{\geq 0}$ is a well-order.
- So in any descending chain of monomials in the *lex* order, eventually the exponent of x_1 must "stabilize," then the exponent of x_2 must "stabilize," etc. But the way this works is a bit subtle – arbitrarily long chains exist:
- Example $x^3y > x^2y^2 > xy^5 > xy^4 > xy^3 > xy^2 > xy$

Graded lex order

- For $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $|\alpha| = \alpha_1 + \cdots + \alpha_n$

Graded lex order

- For $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $|\alpha| = \alpha_1 + \cdots + \alpha_n$

Definition 11

We say $x^\alpha >_{grlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and $x^\alpha >_{lex} x^\beta$.

Graded lex order

- For $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $|\alpha| = \alpha_1 + \cdots + \alpha_n$

Definition 11

We say $x^\alpha >_{grlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and $x^\alpha >_{lex} x^\beta$.

- Easy to see satisfies definition; *grlex* compares by total degree first, then "break ties" with $>_{lex}$

Graded lex order

- For $\alpha \in \mathbb{Z}^n_{\geq 0}$, let $|\alpha| = \alpha_1 + \cdots + \alpha_n$

Definition 11

We say $x^\alpha >_{grlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and $x^\alpha >_{lex} x^\beta$.

- Easy to see satisfies definition; *grlex* compares by total degree first, then "break ties" with $>_{lex}$
- Examples: $x^3y^2z >_{grlex} x^4z$ since $|(3,2,1)| = 6 > 5 = |(4,0,1)|$. $x^3y^2z >_{grlex} x^3yz^2$ since $|(3,2,1)| = 6 = |(3,1,2)|$ but $(3,2,1) - (3,1,2) = (0,1,-1)$.
- *grlex* leading term of $f(x,y) = x^3y^3 + x^5 + xy^4$?

Graded reverse lex order

Definition 12

We say $x^\alpha >_{grevlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and in $\alpha - \beta$ the rightmost nonzero entry is *negative*.

- Example: $x^3y^2z >_{grevlex} x^4z$ as for *grlex*

Graded reverse lex order

Definition 12

We say $x^\alpha >_{grevlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and in $\alpha - \beta$ the rightmost nonzero entry is *negative*.

- Example: $x^3y^2z >_{grevlex} x^4z$ as for *grlex*
- Example: $x^4yz >_{grevlex} x^3y^2z$ since total degrees are both 6, but $(4,1,1) - (3,2,1) = (1,-1,0)$

Graded reverse lex order

Definition 12

We say $x^\alpha >_{grevlex} x^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = |\beta|$ and in $\alpha - \beta$ the rightmost nonzero entry is *negative*.

- Example: $x^3y^2z >_{grevlex} x^4z$ as for *grlex*
- Example: $x^4yz >_{grevlex} x^3y^2z$ since total degrees are both 6, but $(4,1,1) - (3,2,1) = (1,-1,0)$
- Note that $f(x,y,z) = x^2y^2z^2 + xy^4z + x^5$ has three different leading terms depending on which of the orders *lex, grlex, grevlex* we use

Why different monomial orders?

- Best answer is that, when we introduce Gröbner bases next week, we'll see that a monomial order is built into the definition

Why different monomial orders?

- Best answer is that, when we introduce Gröbner bases next week, we'll see that a monomial order is built into the definition
- GB's with respect to different monomial orders do different (and all useful) things!

Why different monomial orders?

- Best answer is that, when we introduce Gröbner bases next week, we'll see that a monomial order is built into the definition
- GB's with respect to different monomial orders do different (and all useful) things!
- *lex* order GB's systematically eliminate variables (good for direct approach to solving systems of equations, but computationally "expensive")

Why different monomial orders?

- Best answer is that, when we introduce Gröbner bases next week, we'll see that a monomial order is built into the definition
- GB's with respect to different monomial orders do different (and all useful) things!
- *lex* order GB's systematically eliminate variables (good for direct approach to solving systems of equations, but computationally "expensive")
- GB's with respect to graded orders (including *grlex, grevlex*, are usually less "expensive" computationally

Why different monomial orders?

- Best answer is that, when we introduce Gröbner bases next week, we'll see that a monomial order is built into the definition
- GB's with respect to different monomial orders do different (and all useful) things!
- *lex* order GB's systematically eliminate variables (good for direct approach to solving systems of equations, but computationally "expensive")
- GB's with respect to graded orders (including *grlex, grevlex*, are usually less "expensive" computationally
- There are also *conversion algorithms* to go from a GB with respect to one order to a GB with respect to another order – may "get into" some of that in projects(!)