Computational Algebraic Geometry

Groebner Bases

Kaie Kubjas

kaie.kubjas@aalto.fi

January 18, 2021

Overview

Last time:

- Ideals
  - Ideal generated by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$
  - Finitely generated ideal
  - Vanishing ideal of an affine variety
    - $\langle f_1, \ldots, f_s \rangle \subseteq I(V(f_1, \ldots, f_s))$
    - $V \subseteq W \Leftrightarrow I(V) \supseteq I(W)$
- Polynomials in one variable
  - Division algorithm
  - A degree m polynomial has at most m roots
  - Every ideal in $k[x]$ can be written in the form $\langle f \rangle$
  - Greatest common divisor

Today:

- Motivation for Groebner bases
- Orders of the monomials
- Division algorithm for polynomials in n variables

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \ldots, f_s \rangle$.
- Use the division algorithm to write $f = qh + r$ where $\deg(r) < \deg(h)$.
- The polynomial f is in the ideal if and only if $r = 0$.

Example

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$
- $x^3 + 4x^2 + 3x - 7$ is not in the ideal

Quiz: Does $x \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

Groebner bases introduction

Introduction

We will study the method of Groebner bases which will allow us to solve problems about polynomial ideals in algorithmic and computational fashion.

- The ideal description problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set?
- The ideal membership problem: Given $f \in k[x_1, \ldots, x_n]$ and ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$.
- The problem of solving polynomial equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

- The implicitization problem: If V is given by a rational parametric representation, find a system of polynomial equations that defines V.

Introduction

We will study the method of Groebner bases which will allow us to solve problems about polynomial ideals in algorithmic and computational fashion.

- The ideal description problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set?
- The ideal membership problem: Given $f \in k[x_1, \ldots, x_n]$ and ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$.
- The problem of solving polynomial equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

- The implicitization problem: If V is given by a rational parametric representation, find a system of polynomial equations that defines V.

Introduction

We will study the method of Groebner bases which will allow us to solve problems about polynomial ideals in algorithmic and computational fashion.

- The ideal description problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set?
- The ideal membership problem: Given $f \in k[x_1, \ldots, x_n]$ and ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$.
- The problem of solving polynomial equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

- The implicitization problem: If V is given by a rational parametric representation, find a system of polynomial equations that defines V.

Introduction

We will study the method of Groebner bases which will allow us to solve problems about polynomial ideals in algorithmic and computational fashion.

- The ideal description problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set?
- The ideal membership problem: Given $f \in k[x_1, \ldots, x_n]$ and ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$.
- The problem of solving polynomial equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

- The implicitization problem: If V is given by a rational parametric representation, find a system of polynomial equations that defines V.

Introduction

We will study the method of Groebner bases which will allow us to solve problems about polynomial ideals in algorithmic and computational fashion.

- The ideal description problem: Does every ideal $I \subset k[x_1, \ldots, x_n]$ have a finite generating set?
- The ideal membership problem: Given $f \in k[x_1, \ldots, x_n]$ and ideal $I = \langle f_1, \ldots, f_s \rangle$, determine if $f \in I$.
- The problem of solving polynomial equations: Find all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0.$$

- The implicitization problem: If V is given by a rational parametric representation, find a system of polynomial equations that defines V.

Ideal description and membership problems

Example

- When $n = 1$, we solved the ideal description problem. Given $I \subset k[x]$, we showed that $I = \langle g \rangle$ for some $g \in k[x]$.
- The solution to the ideal membership problem follows from the division algorithm: given $f \in k[x]$, to check whether $f \in I = \langle g \rangle$, we divide f by g:

$$f = qg + r.$$

Then $f \in I$ if and only if $r = 0$.

Ideal description and membership problems

Example

- When $n = 1$, we solved the ideal description problem. Given $I \subset k[x]$, we showed that $I = \langle g \rangle$ for some $g \in k[x]$.
- The solution to the ideal membership problem follows from the division algorithm: given $f \in k[x]$, to check whether $f \in I = \langle g \rangle$, we divide f by g:

$$f = qg + r.$$

Then $f \in I$ if and only if $r = 0$.

Solving polynomial equations

Example

Solve the system of polynomial equations

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0, \\ x_1 + x_2 - 1 &= 0, \\ x_1 + x_3 - 3 &= 0. \end{aligned}$$

Gaussian elimination gives the reduced row echelon form:

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence

$$x_1 = -t + 3, x_2 = t - 2, x_3 = t.$$

Solving polynomial equations

Example

Solve the system of polynomial equations

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0, \\ x_1 + x_2 - 1 &= 0, \\ x_1 + x_3 - 3 &= 0. \end{aligned}$$

Gaussian elimination gives the reduced row echelon form:

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence

$$x_1 = -t + 3, x_2 = t - 2, x_3 = t.$$

Solving polynomial equations

Example

Solve the system of polynomial equations

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0, \\ x_1 + x_2 - 1 &= 0, \\ x_1 + x_3 - 3 &= 0. \end{aligned}$$

Gaussian elimination gives the reduced row echelon form:

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Hence

$$x_1 = -t + 3, x_2 = t - 2, x_3 = t.$$

Implicitization problem

Consider the affine linear subspace V in k^4 parametrized by

$$\begin{aligned} x_1 &= t_1 + t_2 + 1, \\ x_2 &= t_1 - t_2 + 3, \\ x_3 &= 2t_1 - 1, \\ x_4 &= t_1 + 2t_2 - 3. \end{aligned}$$

Order the variables $t_1, t_2, x_1, x_2, x_3, x_4$. The corresponding matrix of coefficients is:

$$\left(\begin{array}{cccccc|c} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{array}\right).$$

Implicitization problem

Consider the affine linear subspace V in k^4 parametrized by

$$\begin{aligned} x_1 &= t_1 + t_2 + 1, \\ x_2 &= t_1 - t_2 + 3, \\ x_3 &= 2t_1 - 1, \\ x_4 &= t_1 + 2t_2 - 3. \end{aligned}$$

Order the variables $t_1, t_2, x_1, x_2, x_3, x_4$. The corresponding matrix of coefficients is:

$$\left(\begin{array}{cccccc|c} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{array}\right).$$

Implicitization problem

Gaussian elimination gives the matrix:

$$\left(\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{array}\right).$$

The last two rows of this matrix correspond to the equations:

$$x_1 - (1/4)x_3 - (1/2)x_4 - 3 = 0,$$
$$x_2 - (3/4)x_3 + (1/2)x_4 - 3 = 0.$$

These two equations define V in k^4.

Implicitization problem

Gaussian elimination gives the matrix:

$$\left(\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{array}\right).$$

The last two rows of this matrix correspond to the equations:

$$x_1 - (1/4)x_3 - (1/2)x_4 - 3 = 0,$$
$$x_2 - (3/4)x_3 + (1/2)x_4 - 3 = 0.$$

These two equations define V in k^4.

Implicitization problem

Gaussian elimination gives the matrix:

$$\left(\begin{array}{cccccc|c} 1 & 0 & 0 & 0 & -1/2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1/4 & -1/2 & 1 \\ 0 & 0 & 1 & 0 & -1/4 & -1/2 & 3 \\ 0 & 0 & 0 & 1 & -3/4 & 1/2 & 3 \end{array}\right).$$

The last two rows of this matrix correspond to the equations:

$$\begin{aligned} x_1 - (1/4)x_3 - (1/2)x_4 - 3 &= 0, \\ x_2 - (3/4)x_3 + (1/2)x_4 - 3 &= 0. \end{aligned}$$

These two equations define V in k^4.

Orders on monomials

Orders on monomials

In dividing $f(x) = x^5 - 3x^2 + 1$ by $g(x) = x^2 - 4x + 7$:

- write the terms in decreasing order
- subtract $x^3 g(x)$ from f to cancel the leading term
- repeat the process
- the degree order of the monomials

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$$

Gaussian elimination:

- work with the entries to the left first
- order of the variables

$$x_1 > x_2 > \cdots > x_n$$

Orders on monomials

In dividing $f(x) = x^5 - 3x^2 + 1$ by $g(x) = x^2 - 4x + 7$:

- write the terms in decreasing order
- subtract $x^3 g(x)$ from f to cancel the leading term
- repeat the process
- the degree order of the monomials

$$\cdots > x^{m+1} > x^m > \cdots > x^2 > x > 1$$

Gaussian elimination:

- work with the entries to the left first
- order of the variables

$$x_1 > x_2 > \cdots > x_n$$

Orders on monomials

- to extend polynomial division and Gaussian elimination to arbitrary polynomials, one needs an order on the terms in polynomials in $k[x_1, \ldots, x_n]$
- a 1-to-1 correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$
- would like to compare every pair of monomials $\Rightarrow$ total order
- a monomial times a polynomial should keep the relative order of terms $\Rightarrow$ if $x^\alpha > x^\beta$ and x^γ is any monomial, then we require $x^\alpha x^\gamma > x^\beta x^\gamma$

Orders on monomials

- to extend polynomial division and Gaussian elimination to arbitrary polynomials, one needs an order on the terms in polynomials in $k[x_1, \ldots, x_n]$
- a 1-to-1 correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$
- would like to compare every pair of monomials $\Rightarrow$ total order
- a monomial times a polynomial should keep the relative order of terms $\Rightarrow$ if $x^\alpha > x^\beta$ and x^γ is any monomial, then we require $x^\alpha x^\gamma > x^\beta x^\gamma$

Orders on monomials

- to extend polynomial division and Gaussian elimination to arbitrary polynomials, one needs an order on the terms in polynomials in $k[x_1, \ldots, x_n]$
- a 1-to-1 correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$
- would like to compare every pair of monomials $\Rightarrow$ total order
- a monomial times a polynomial should keep the relative order of terms $\Rightarrow$ if $x^\alpha > x^\beta$ and x^γ is any monomial, then we require $x^\alpha x^\gamma > x^\beta x^\gamma$

Orders on monomials

- to extend polynomial division and Gaussian elimination to arbitrary polynomials, one needs an order on the terms in polynomials in $k[x_1, \ldots, x_n]$
- a 1-to-1 correspondence between the monomials in $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$
- would like to compare every pair of monomials $\Rightarrow$ total order
- a monomial times a polynomial should keep the relative order of terms $\Rightarrow$ if $x^\alpha > x^\beta$ and x^γ is any monomial, then we require $x^\alpha x^\gamma > x^\beta x^\gamma$

Total order

Definition

Let X and Y be sets. A **binary relation** R on X and Y is a subset of $X \times Y$. The statement $(x, y) \in R$ is denoted xRy.

If $X = Y$, then we say that R is a binary relation on X.

Definition

Let X be a set. A binary relation $\geq$ is a **total order** on X if it satisfies for all a, b and c in X:

- (Antisymmetry) If $a \geq b$ and $b \geq a$, then $a = b$,
- (Transitivity) If $a \geq b$ and $b \geq c$, then $a \geq c$, and
- (Connexity) $a \geq b$ or $b \geq a$.

A total order is also called a **linear order**.

Total order

Definition

Let X and Y be sets. A **binary relation** R on X and Y is a subset of $X \times Y$. The statement $(x, y) \in R$ is denoted xRy.

If $X = Y$, then we say that R is a binary relation on X.

Definition

Let X be a set. A binary relation $\geq$ is a **total order** on X if it satisfies for all a, b and c in X:

- (Antisymmetry) If $a \geq b$ and $b \geq a$, then $a = b$,
- (Transitivity) If $a \geq b$ and $b \geq c$, then $a \geq c$, and
- (Connexity) $a \geq b$ or $b \geq a$.

A total order is also called a **linear order**.

Strict total order

Each total order $\geq$ defines a **strict total order** $>$ in the following way: $a > b$ if $a \geq b$ and $a \neq b$.

It satisfies the following properties:

- (Transitivity) If $a > b$ and $b > c$, then $a > c$, and
- (Trichotomy) Exactly one of $a > b$, $b > a$ and $a = b$ is true.

Conversely, a transitive trichotomous binary relation $>$ defines a total order $\geq$ in the following way: $a \geq b$ if $a > b$ or $a = b$.

Strict total order

Each total order $\geq$ defines a **strict total order** $>$ in the following way: $a > b$ if $a \geq b$ and $a \neq b$.

It satisfies the following properties:

- (Transitivity) If $a > b$ and $b > c$, then $a > c$, and
- (Trichotomy) Exactly one of $a > b$, $b > a$ and $a = b$ is true.

Conversely, a transitive trichotomous binary relation $>$ defines a total order $\geq$ in the following way: $a \geq b$ if $a > b$ or $a = b$.

Strict total order

Each total order $\geq$ defines a **strict total order** $>$ in the following way: $a > b$ if $a \geq b$ and $a \neq b$.

It satisfies the following properties:

- (Transitivity) If $a > b$ and $b > c$, then $a > c$, and
- (Trichotomy) Exactly one of $a > b$, $b > a$ and $a = b$ is true.

Conversely, a transitive trichotomous binary relation $>$ defines a total order $\geq$ in the following way: $a \geq b$ if $a > b$ or $a = b$.

Monomial order

Definition

A **monomial order** $\geq$ on $k[x_1, \ldots, x_n]$ is an relation $\geq$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

1. $\geq$ is a total order on $\mathbb{Z}^n_{\geq 0}$.
2. If $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \geq \beta + \gamma$.
3. $\geq$ is a well-order on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $\geq$.

We will call the strict total order defined by a monomial order also a monomial order.

Monomial order

Definition

A **monomial order** $\geq$ on $k[x_1, \ldots, x_n]$ is an relation $\geq$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

1. $\geq$ is a total order on $\mathbb{Z}^n_{\geq 0}$.
2. If $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \geq \beta + \gamma$.
3. $\geq$ is a well-order on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $\geq$.

We will call the strict total order defined by a monomial order also a monomial order.

Monomial order

Definition

A **monomial order** $\geq$ on $k[x_1, \ldots, x_n]$ is an relation $\geq$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

1. $\geq$ is a total order on $\mathbb{Z}^n_{\geq 0}$.
2. If $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \geq \beta + \gamma$.
3. $\geq$ is a well-order on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $\geq$.

We will call the strict total order defined by a monomial order also a monomial order.

Monomial order

Definition

A **monomial order** $\geq$ on $k[x_1, \ldots, x_n]$ is an relation $\geq$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

1. $\geq$ is a total order on $\mathbb{Z}^n_{\geq 0}$.
2. If $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \geq \beta + \gamma$.
3. $\geq$ is a well-order on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $\geq$.

We will call the strict total order defined by a monomial order also a monomial order.

Monomial order

Definition

A **monomial order** $\geq$ on $k[x_1, \ldots, x_n]$ is an relation $\geq$ on $\mathbb{Z}^n_{\geq 0}$ satisfying:

1. $\geq$ is a total order on $\mathbb{Z}^n_{\geq 0}$.
2. If $\alpha \geq \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma \geq \beta + \gamma$.
3. $\geq$ is a well-order on $\mathbb{Z}^n_{\geq 0}$. This means that every nonempty subset of $\mathbb{Z}^n_{\geq 0}$ has a smallest element under $\geq$.

We will call the strict total order defined by a monomial order also a monomial order.

Monomial order

Example

The usual numerical order

$$\cdots > m+1 > m > \cdots > 3 > 2 > 1 > 0$$

on the elements $\mathbb{Z}_{\geq 0}$ is a monomial order.

Monomial order

Lemma

An order relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well-order if and only if every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

This lemma will be used to show that various algorithms must terminate because some term strictly decreases at each step of the algorithm.

Proof: "$\Rightarrow$" Assume that $>$ is a well-order. Let us consider the set $\{\alpha(1), \alpha(2), \alpha(3), \dots\}$. This set has a minimal element. This minimal element has to be the last element of the decreasing sequence. Hence the sequence terminates.

"$\Leftarrow$" Assume that $>$ is not a well-order. There exists a nonempty set that does not have a minimal element. Let $\alpha(1)$ be an element in the set. We can choose $\alpha(2)$ in the set s.t. $\alpha(1) > \alpha(2)$. Since the set has no minimal element, we can continue to construct a decreasing sequence that does not terminate. $\boxtimes$

Monomial order

Lemma

An order relation $>$ on $\mathbb{Z}^n_{\geq 0}$ is a well-order if and only if every strictly decreasing sequence in $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

This lemma will be used to show that various algorithms must terminate because some term strictly decreases at each step of the algorithm.

Lexicographic order

Definition

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Quiz

Compare w.r.t the lexicographic order:

1. $(1, 2, 0)$ *and* $(0, 3, 4)$
2. $(3, 2, 4)$ *and* $(3, 2, 1)$

Lexicographic order

Definition

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Quiz

Compare w.r.t the lexicographic order:

1. $(1, 2, 0)$ *and* $(0, 3, 4)$
2. $(3, 2, 4)$ *and* $(3, 2, 1)$

Lexicographic order

Definition

Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Example

1. $(1, 2, 0) >_{lex} (0, 3, 4)$ since $\alpha - \beta = (1, -1, -4)$
2. $(3, 2, 4) >_{lex} (3, 2, 1)$ since $\alpha - \beta = (0, 0, 3)$
3. the variables $x_1, \ldots, x_n$ are ordered in the usual way:

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \cdots >_{lex} (0, \ldots, 0, 1)$$

4. analogous to the order of words in dictionaries

Lexicographic order

Proposition

The lex order on $\mathbb{Z}^n_{\geq 0}$ is a monomial order.

- there are many lex orders, corresponding to which 1-to-1 correspondence between the monomials $k[x_1, \ldots, x_n]$ and $\mathbb{Z}^n_{\geq 0}$ is chosen
- this corresponds to how the variables are ordered
- so far used lex order with $x_1 > x_2 > \ldots > x_n$
- there are $n!$ lex orders
- in lex order a variable dominates any monomial involving only smaller variables

Proof: ① It is a total order by definition and that numerical order on $\mathbb{Z}_{\geq 0}$ is a monomial order.

② Assume $\alpha > \beta$. It implies that the leftmost nonzero entry of $\alpha - \beta$ is positive. Then $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$ and $\alpha + \gamma > \beta + \gamma$.

③ Consider a non-empty subset of $\mathbb{Z}^n_{\geq 0}$. Since the numerical order is a well-order, we can choose the minimal value among the first coordinate of all the elements in this set. Among all the elements of this set that have the first coordinate with the minimal value, we can pick minimal value for the second coordinate. We can repeat the procedure for all coordinates to obtain the minimal element in the set. Hence $>_{lex}$ is a well-ordering. ∎

Graded lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Quiz

Compare w.r.t the graded lexicographic order:

1. $(1, 2, 3)$ *and* $(3, 2, 0)$
2. $(1, 1, 5)$ *and* $(1, 2, 4)$

Graded lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Quiz

Compare w.r.t the graded lexicographic order:

1. $(1, 2, 3)$ *and* $(3, 2, 0)$
2. $(1, 1, 5)$ *and* $(1, 2, 4)$

Graded lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Example

- $(1,2,3) >_{grlex} (3,2,0)$ since $|(1,2,3)| = 6 > |(3,2,0)| = 5$
- $(1,2,4) >_{grlex} (1,1,5)$ since $|(1,2,4)| = |(1,1,5)|$ and $(1,2,4) >_{lex} (1,1,5)$
- the variables are ordered according to the lex order

Graded reverse lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and}$$

the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

Quiz

Compare w.r.t the graded reverse lexicographic order:

1. $(4, 2, 3)$ *and* $(4, 7, 1)$
2. $(1, 5, 2)$ *and* $(4, 1, 3)$

Graded reverse lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and}$$

the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

Quiz

Compare w.r.t the graded reverse lexicographic order:

1. $(4, 2, 3)$ *and* $(4, 7, 1)$
2. $(1, 5, 2)$ *and* $(4, 1, 3)$

Graded reverse lexicographic order

Definition

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and}$$

the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

Example

- $(4,7,1) >_{grevlex} (4,2,3)$ since $|(4,7,1)| = 12 > |(4,2,3)| = 9$
- $(1,5,2) >_{grevlex} (4,1,3)$ since $|(1,5,2)| = |(4,1,3)|$ and $(1,5,2) - (4,1,3) = (-3,4,-1)$
- gives the same order on the variables

Quiz

Order the terms of $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *with respect to lex, grlex and grevlex orders.*

Quiz

Order the terms of $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *with respect to lex, grlex and grevlex orders.*

- *Wrt the lex order*

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2.$$

- *Wrt the grlex order*

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2.$$

- *Wrt grevlex order*

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

Terminology

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

1. The **multidegree** of f is

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

2. The **leading coefficient** of f is

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

3. The **leading monomial** of f is

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

Terminology

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

1. The **multidegree** of f is

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

2. The **leading coefficient** of f is

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

3. The **leading monomial** of f is

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

Terminology

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

1. The **multidegree** of f is

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

2. The **leading coefficient** of f is

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

3. The **leading monomial** of f is

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

Terminology

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, \ldots, x_n]$ and let $>$ be a monomial order.

1. The **multidegree** of f is

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

2. The **leading coefficient** of f is

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

3. The **leading monomial** of f is

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

Terminology

Definition

4. The **leading term** of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Quiz

Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $>$ be the lex order. Find its multidegree, leading coefficient, leading monomial and leading term.

Terminology

Definition

4. The **leading term** of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Quiz

Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ *and let* $>$ *be the lex order. Find its multidegree, leading coefficient, leading monomial and leading term.*

Terminology

Definition

4. The **leading term** of f is

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Quiz

Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $>$ be the lex order. Find its multidegree, leading coefficient, leading monomial and leading term.

- $multideg(f) = (3, 0, 0)$
- $LC(f) = -5$
- $LM(f) = x^3$
- $LT(f) = -5x^3$

Properties of multidegree

Lemma

Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials. Then

1. $multideg(fg) = multideg(f) + multideg(g)$.
2. *if $f + g \neq 0$, then $multideg(f + g) \leq \max(multideg(f), multideg(g))$. If in addition $multideg(f) \neq multideg(g)$, then equality occurs.*

A division algorithm in $k[x_1, \ldots, x_n]$

A division algorithm

- **Goal:** divide $f \in k[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$
- **Result:** $f = a_1 f_1 + \cdots + a_s f_s + r$

Example

Divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$.
Result: $x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1(y^2-1) + x + y + 1$

A division algorithm

- **Goal:** divide $f \in k[x_1, \ldots, x_n]$ by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$
- **Result:** $f = a_1 f_1 + \cdots + a_s f_s + r$

Example

Divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$.
Result: $x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1(y^2-1) + x + y + 1$

$a_1 : x + y$

$a_2 : 1$

$xy - 1$

$y^2 - 1$

$$x^2y + xy^2 + y^2$$
$$x^2y - x$$

$$xy^2 + x + y^2$$
$$xy^2 - y$$

$$x + y^2 + y \longrightarrow x$$

$$y^2 + y$$
$$y^2 - 1$$

$$y + 1 \longrightarrow x + y$$

$$1 \longrightarrow x + y + 1$$

$$x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1 \cdot (y^2-1) + x + y + 1$$

A division algorithm

Theorem

Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every f can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where $a_i, r \in k[x_1, \ldots, x_n]$, and either $r = 0$ or r is a linear combination of monomials with coefficients in k, none of which is divisible by any of $LT(f_1), \ldots, LT(f_s)$. We will call r a ***remainder*** *of f on division by F. Furthermore, if $a_i f_i \neq 0$, then we have*

$$multideg(f) \geq multideg(a_i f_i).$$

A division algorithm

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$
$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
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
            $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
            $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i)) \cdot f_i$
            divisionoccurred := true
        ELSE
            $i := i + 1$
    IF divisionoccurred := false THEN
        $r := r + \mathrm{LT}(p)$
        $p := p - \mathrm{LT}(p)$

<u>Proof:</u> ① To prove that the algorithm works, first we show that

$f = a_1 \cdot f_1 + \dots + a_s \cdot f_s + p + r$ at each step of the algorithm. This is true when we initialize $a_1, \dots, a_s, p, r$. At each step either a_i and p get redefined (as in the 1-var case) or p and r get redefined. In both cases, the identity is still satisfied.

② The algorithm ends when $p = 0$.
Then $f = a_1 f_1 + \dots + a_s f_s + \cancel{p} + r$.

③ The algorithm terminates, because at each step p gets redefined either as

$$p - \left(\frac{LT(p)}{LT(f_i)}\right) \cdot LT(f_i) \quad \text{or} \quad p - LT(p).$$

In both cases the multidegree of p drops. By earlier lemma, every decreasing sequence terminates.

(4) r is zero or no term of r is divisible by any of $LT(f_i)$, because at initialization r is zero and terms are added precisely when they are not divisible by any of $LT(f_i)$. $\blacksquare$

Order of the polynomials

The order of the s-tuple of polynomials $f_1, \ldots, f_s$ matters:

1. Divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy - 1$ using lex order with $x > y$:
   $x^2y + xy^2 + y^2 = (x+1)(y^2-1) + x(xy-1) + 2x + 1$
2. Divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$ using lex order with $x > y$:
   $x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1(y^2-1) + x + y + 1$

Order of the polynomials

The order of the s-tuple of polynomials $f_1, \ldots, f_s$ matters:

1. Divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy - 1$ using lex order with $x > y$:
   $x^2y + xy^2 + y^2 = (x+1)(y^2-1) + x(xy-1) + 2x + 1$
2. Divide $f = x^2y + xy^2 + y^2$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$ using lex order with $x > y$:
   $x^2y + xy^2 + y^2 = (x+y)(xy-1) + 1(y^2-1) + x + y + 1$

Ideal membership problem

- the division algorithm in $k[x]$ solves the ideal membership problem
- if after division of f by $F = (f_1, \ldots, f_s)$ we obain a remainder $r = 0$, then

$$f = a_1 f_1 + \ldots + a_s f_s \text{ and } f \in \langle f_1, \ldots, f_s \rangle$$

- $r = 0$ is a sufficient by not a necessary condition for being in the ideal

Ideal membership problem

- the division algorithm in $k[x]$ solves the ideal membership problem
- if after division of f by $F = (f_1, \ldots, f_s)$ we obain a remainder $r = 0$, then

$$f = a_1 f_1 + \ldots + a_s f_s \text{ and } f \in \langle f_1, \ldots, f_s \rangle$$

- $r = 0$ is a sufficient by not a necessary condition for being in the ideal

Ideal membership problem

- the division algorithm in $k[x]$ solves the ideal membership problem
- if after division of f by $F = (f_1, \ldots, f_s)$ we obain a remainder $r = 0$, then

$$f = a_1 f_1 + \ldots + a_s f_s \text{ and } f \in \langle f_1, \ldots, f_s \rangle$$

- $r = 0$ is a sufficient by not a necessary condition for being in the ideal

Ideal membership problem

- the division algorithm in $k[x]$ solves the ideal membership problem
- if after division of f by $F = (f_1, \ldots, f_s)$ we obain a remainder $r = 0$, then

$$f = a_1 f_1 + \ldots + a_s f_s \text{ and } f \in \langle f_1, \ldots, f_s \rangle$$

- $r = 0$ is a sufficient by not a necessary condition for being in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

A division algorithm

- $f_1 = xy + 1, f_2 = y^2 - 1 \in k[x, y]$ with the lex order
- divide f by $F = (f_1, f_2)$
- **result:** $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$
- divide f by $F = (f_2, f_1)$
- **result:** $xy^2 - x = x(y^2 - 1) + 0(xy + 1) + 0$
- the second calculation shows that $f \in \langle f_1, f_2 \rangle$
- the first calculation shows that even if $f \in \langle f_1, f_2 \rangle$ it is possible to obtain a nonzero remainder
- pass to the ideal I generated by $f_1, \ldots, f_s$
- want a good generating set for I
- Groebner bases: condition $r = 0$ is equivalent to membership in the ideal

Conclusion

Today:

- Motivation for Gröbner bases
- Orders of the monomials
- Division algorithm for polynomials in n variables

Next time:

- Monomial ideals
- Hilbert basis theorem
- Groebner bases