Computational Algebraic Geometry

Geometry, Algebra and Algorithms

Kaie Kubjas

kaie.kubjas@aalto.fi

January 13, 2021

Overview

Last time:

- Monomials and polynomials
- Polynomials as functions - link between algebra and geometry
- Affine varieties
- Rational parametric description and implicit representation

Overview

Last time:

- Monomials and polynomials
- Polynomials as functions - link between algebra and geometry
- Affine varieties
- Rational parametric description and implicit representation

Today:

- 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
- Polynomials in one variable
  - Division algorithm
  - A degree m polynomial has at most m roots
  - Greatest common divisor
  - Every ideal in $k[x]$ can be generated by one polynomial

Ideals

Ideals

Definition

A subset $I \subset k[x_1, \ldots, x_n]$ is an **ideal** if it satisfies:

1. $0 \in I$.
2. If $f, g, \in I$, then $f + g \in I$.
3. If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

Ideals

Definition

A subset $I \subset k[x_1, \ldots, x_n]$ is an **ideal** if it satisfies:

1. $0 \in I$.
2. If $f, g, \in I$, then $f + g \in I$.
3. If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

- the goal today is to introduce some naturally occuring ideals and to see how ideals relate to affine varieties

Ideals

Definition

A subset $I \subset k[x_1, \ldots, x_n]$ is an **ideal** if it satisfies:

1. $0 \in I$.
2. If $f, g, \in I$, then $f + g \in I$.
3. If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

- the goal today is to introduce some naturally occuring ideals and to see how ideals relate to affine varieties
- the real importance of ideals is that they will give us a language for computing with affine varieties

Ideals

Definition

Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Ideals

Definition

Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$

Lemma

If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle$ is an ideal of $k[x_1, \ldots, x_n]$. We will call $\langle f_1, \ldots, f_s \rangle$ the ***ideal generated*** *by $f_1, \ldots, f_s$.*

Proof: We want to show that $\langle f_1, \dots, f_s \rangle$ is an ideal.

1) $0 \in \langle f_1, \dots, f_s \rangle$ because

$$0 = \sum_{i=1}^{s} 0 \cdot f_i$$

2) Let $g, h \in \langle f_1, \dots, f_s \rangle$. Hence

$$g = \sum_{i=1}^{s} g_i f_i \,, \quad g_i \in k[x_1, \dots, x_n]$$

$$h = \sum_{i=1}^{s} h_i f_i \,, \quad h_i \in k[x_1, \dots, x_n]$$

$$g + h = \sum_{i=1}^{s} (g_i + h_i) \cdot f_i \in \langle f_1, \dots, f_s \rangle$$

3) Let $g \in \langle f_1, \dots, f_s \rangle$, $h \in k[x_1, \dots, x_n]$.

$$h \cdot g = \sum_{i=1}^{s} (h \cdot g_i) \cdot f_i \in \langle f_1, \dots, f_s \rangle.$$

Thus $\langle f_1, \dots, f_s \rangle$ is an ideal. $\blacksquare$

Interpretation in terms of polynomial equations

Given $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, we get the system of equations

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{aligned}$$

Interpretation in terms of polynomial equations

Given $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, we get the system of equations

$$f_1 = 0,$$
$$\vdots$$
$$f_s = 0.$$

If we multiply the first equation by $h_1 \in k[x_1, \ldots, x_n]$, the second by $h_2 \in k[x_1, \ldots, x_n]$ etc and then add the resulting equations, we get

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0.$$

Interpretation in terms of polynomial equations

Given $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, we get the system of equations

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{aligned}$$

If we multiply the first equation by $h_1 \in k[x_1, \ldots, x_n]$, the second by $h_2 \in k[x_1, \ldots, x_n]$ etc and then add the resulting equations, we get

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0.$$

- The left-hand side is an element of the ideal $\langle f_1, \ldots, f_s \rangle$.

Interpretation in terms of polynomial equations

Given $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, we get the system of equations

$$\begin{aligned} f_1 &= 0, \\ &\vdots \\ f_s &= 0. \end{aligned}$$

If we multiply the first equation by $h_1 \in k[x_1, \ldots, x_n]$, the second by $h_2 \in k[x_1, \ldots, x_n]$ etc and then add the resulting equations, we get

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0.$$

- The left-hand side is an element of the ideal $\langle f_1, \ldots, f_s \rangle$.
- We can think of $\langle f_1, \ldots, f_s \rangle$ as consisting of all "polynomial consequences" of the equations $f_1 = f_2 = \ldots = f_s = 0$.

Ideals example

Consider the example

$$x = 1 + t$$
$$y = 1 + t^2.$$

Ideals example

Consider the example

$$x = 1 + t$$
$$y = 1 + t^2.$$

In the previous lecture we learned that eliminating t gives

$$y = x^2 - 2x + 2.$$

Ideals example

Consider the example

$$x = 1 + t$$
$$y = 1 + t^2.$$

In the previous lecture we learned that eliminating t gives

$$y = x^2 - 2x + 2.$$

In fact $x^2 - 2x + 2 - y$ is in the ideal $\langle x - 1 - t, y - 1 - t^2 \rangle$:

$$(x - 1 - 1t)(x - 1 + t) + (-1)(y - 1 - t^2) = x^2 - 2x + 2 - y$$

Ideals

Definition

We say that an ideal I is **finitely generated** if there exist $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ such that $I = \langle f_1, \dots, f_s \rangle$, and we say that $f_1, \dots, f_s$ forms a basis of I.

Ideals

Definition

We say that an ideal I is **finitely generated** if there exist $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$, and we say that $f_1, \ldots, f_s$ forms a basis of I.

- We will learn that every ideal of $k[x_1, \ldots, x_n]$ is finitely generated.

Ideals

Definition

We say that an ideal I is **finitely generated** if there exist $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$, and we say that $f_1, \ldots, f_s$ forms a basis of I.

- We will learn that every ideal of $k[x_1, \ldots, x_n]$ is finitely generated.
- A given ideal may have many different bases.

Ideals

Definition

We say that an ideal I is **finitely generated** if there exist $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that $I = \langle f_1, \ldots, f_s \rangle$, and we say that $f_1, \ldots, f_s$ forms a basis of I.

- We will learn that every ideal of $k[x_1, \ldots, x_n]$ is finitely generated.
- A given ideal may have many different bases.
- An especially useful type of basis is Groebner basis.

Analogy with linear algebra

- the definition of an ideal is similar to the definition of a subspace

Analogy with linear algebra

- the definition of an ideal is similar to the definition of a subspace
- both have to be closed under addition and multiplication (for a subspace multiply with scalars whereas for an ideal we multiply by polynomials)

Analogy with linear algebra

- the definition of an ideal is similar to the definition of a subspace
- both have to be closed under addition and multiplication (for a subspace multiply with scalars whereas for an ideal we multiply by polynomials)
- the ideal generated by polynomials $f_1, \dots, f_s$ is similar to the span of a finite number of vectors $v_1, \dots, v_s$

Analogy with linear algebra

- the definition of an ideal is similar to the definition of a subspace
- both have to be closed under addition and multiplication (for a subspace multiply with scalars whereas for an ideal we multiply by polynomials)
- the ideal generated by polynomials $f_1, \ldots, f_s$ is similar to the span of a finite number of vectors $v_1, \ldots, v_s$
- in both cases one takes linear combinations, using field coefficients for the subspace and polynomial coefficients for the ideal

Ideals

Proposition

If $f_1, \dots, f_s$ and $g_1, \dots, g_t$ are bases of the same ideal in $k[x_1, \dots, x_n]$, so that $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$, then we have $\mathbb{V}(f_1, \dots, f_s) = \mathbb{V}(g_1, \dots, g_t)$.

Ideals

Proposition

If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $k[x_1, \ldots, x_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then we have $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t)$.

Example

- consider the variety $\mathbb{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$

Ideals

Proposition

If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $k[x_1, \ldots, x_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then we have $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t)$.

Example

- consider the variety $\mathbb{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$
- $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$

Ideals

Proposition

If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $k[x_1, \ldots, x_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then we have $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t)$.

Example

- consider the variety $\mathbb{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3)$
- $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$
- hence $\mathbb{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbb{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$

Proof: Assume that

$$\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle.$$

Let $(a_1, \dots, a_n) \in \mathbb{V}(f_1, \dots, f_s)$.

Hence $f_i(a_1, \dots, a_n) = 0$.

Since $g_j \in \langle f_1, \dots, f_s \rangle$, we can write $g_j = \sum_{i=1}^{s} h_i f_i$. Hence

$$g_j(a_1, \dots, a_n) = \sum_{i=1}^{s} (h_i f_i)(a_1, \dots, a_n) = 0.$$

Hence $(a_1, \dots, a_n) \in \mathbb{V}(g_1, \dots, g_t)$.

This proves "$\mathbb{V}(f_1, \dots, f_s) \subseteq \mathbb{V}(g_1, \dots, g_t)$". $\blacksquare$

The ideal of an affine variety

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V\}.$$

The ideal of an affine variety

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}.$$

Lemma

If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \ldots, x_n]$ is an ideal. We call $I(V)$ the (vanishing) ideal of V.

The ideal of an affine variety

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}.$$

Lemma

If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \ldots, x_n]$ is an ideal. We call $I(V)$ the (vanishing) ideal of V.

Quiz: Find $I(\{0, 0\})$ and $I(k^n)$ when k is infinite.

The ideal of an affine variety

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V\}.$$

Lemma

If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \dots, x_n]$ is an ideal. We call $I(V)$ the (vanishing) ideal of V.

Quiz: Find $I(\{0,0\})$ and $I(k^n)$ when k is infinite.

- $I(\{0,0\}) = \langle x, y \rangle$

The ideal of an affine variety

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V\}.$$

Lemma

If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \dots, x_n]$ is an ideal. We call $I(V)$ the (vanishing) ideal of V.

Quiz: Find $I(\{0, 0\})$ and $I(k^n)$ when k is infinite.

- $I(\{0, 0\}) = \langle x, y \rangle$
- $I(k^n) = \{0\}$ when k is infinite

Definition

Let $V \subset k^n$ be an affine variety. Then we set

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V\}.$$

Lemma

If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \ldots, x_n]$ is an ideal. We call $I(V)$ the (vanishing) ideal of V.

Quiz: Find $I(\{0, 0\})$ and $I(k^n)$ when k is infinite.

- $I(\{0, 0\}) = \langle x, y \rangle$
- $I(k^n) = \{0\}$ when k is infinite
- $V = \mathbb{V}(y - x^2, z - x^3) \Rightarrow I(V) = \langle y - x^2, z - x^3 \rangle$

The ideal of an affine variety

polynomials $f_1, \ldots, f_s \to$ variety $\mathbb{V}(f_1, \ldots, f_s) \to$ ideal $I(\mathbb{V}(f_1, \ldots, f_s))$

The ideal of an affine variety

polynomials $f_1, \dots, f_s \to$ variety $\mathbb{V}(f_1, \dots, f_s) \to$ ideal $I(\mathbb{V}(f_1, \dots, f_s))$

- $I(\mathbb{V}(f_1, \dots, f_s)) = \langle f_1, \dots, f_s \rangle$?

The ideal of an affine variety

polynomials $f_1, \ldots, f_s \to$ variety $\mathbb{V}(f_1, \ldots, f_s) \to$ ideal $I(\mathbb{V}(f_1, \ldots, f_s))$

- $I(\mathbb{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$?
- the answer is not always yes

The ideal of an affine variety

polynomials $f_1, \ldots, f_s \to$ variety $\mathbb{V}(f_1, \ldots, f_s) \to$ ideal $I(\mathbb{V}(f_1, \ldots, f_s))$

- $I(\mathbb{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$?
- the answer is not always yes

Lemma

If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle \subset I(\mathbb{V}(f_1, \ldots, f_s))$, although equality need not occur.

The ideal of an affine variety

polynomials $f_1, \ldots, f_s \to$ variety $\mathbb{V}(f_1, \ldots, f_s) \to$ ideal $I(\mathbb{V}(f_1, \ldots, f_s))$

- $I(\mathbb{V}(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$?
- the answer is not always yes

Lemma

If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle \subset I(\mathbb{V}(f_1, \ldots, f_s))$, although equality need not occur.

Proposition

Let V and W be affine varieties in k^n. Then

1. *$V \subset W$ if and only if $I(V) \supset I(W)$*
2. *$V = W$ if and only if $I(V) = I(W)$*

Proof: ① "$\subseteq$" Assume $V \subseteq W$. Take $f \in I(W)$.
Then for all $(a_1, \dots, a_n) \in W$, we have $f(a_1, \dots, a_n) = 0$. Since $V \subseteq W$, also $f(a_1, \dots, a_n) = 0$ $\forall (a_1, \dots, a_n) \in V$. Hence $f \in I(V)$.

"$\supseteq$" Assume $I(W) \subseteq I(V)$. Let $(a_1, \dots, a_n) \in V$.
Then $\forall f \in I(V)$, we have $f(a_1, \dots, a_n) = 0$. Hence $f(a_1, \dots, a_n) = 0$ for all $f \in I(W)$. This means that $(a_1, \dots, a_n) \in W$.

② This follows from $V = W$ being equivalent to $V \subseteq W$ and $W \subseteq V$. ∎

Polynomials in one variable

Polynomials in one variable

Definition

Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$

where $a_i \in k$ and $a_0 \neq 0$. Then we say that $a_0 x^m$ is the **leading term** of f, written $LT(f) = a_0 x^m$.

Polynomials in one variable

Definition

Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$

where $a_i \in k$ and $a_0 \neq 0$. Then we say that $a_0 x^m$ is the **leading term** of f, written $LT(f) = a_0 x^m$.

Quiz

What is the leading term of $f = 2x^3 - 4x + 3$*?*

Division algorithm

Proposition

Let g be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as

$$f = qg + r,$$

where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, q and r are unique, and there is an algorithm for finding q and r.

Division algorithm

Proposition

Let g be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as

$$f = qg + r,$$

where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, q and r are unique, and there is an algorithm for finding q and r.

Proof.

Input: g, f
Output: q, r
$q := 0, r := f$
WHILE $r \neq 0$ AND $LT(g)$ divides $LT(r)$ DO
$\quad q := q + LT(r)/LT(g)$
$\quad r := r - (LT(r)/LT(g))g$ $\square$

Example:

$f = x^3 + 2x^2 + x + 1 \qquad g = 2x + 1$

* $q := 0 \qquad r := x^3 + 2x^2 + x + 1$
* $q_{new} := 0 + \dfrac{x^3}{2x} = \dfrac{1}{2}x^2$

$$r_{new} := x^3 + 2x^2 + x + 1 - \frac{x^3}{2x} \cdot (2x+1) =$$

$$= \frac{3}{2}x^2 + x + 1$$

Proof: 1) We will show that at each step $f = q \cdot g + r$. It clearly holds at the first step.

At each next step

$$\left(q + \frac{LT(r)}{LT(g)}\right) g + r - \frac{LT(r)}{LT(g)} \cdot g =$$

$$= q \cdot g + r = f.$$

2) The algorithm terminates: At each step the degree of r decreases, because

$r - \dfrac{LT(r)}{LT(g)} \cdot g$ is either zero or smaller than the degree of r.

3) Uniqueness: Suppose $f = q \cdot g + r =$

$= q' \cdot g + r'$. Then

$$r - r' = q' \cdot g - q \cdot g$$

Then $\deg(r - r') = \deg(q' \cdot g - q \cdot g)$

$= \deg((q' - q) \cdot g) = \deg(q' - q) + \deg(g)$

$\geq \deg(g)$. This contradicts

that $\deg(r) < \deg(g)$. Hence

$r = r'$ and $q = q'$. $\blacksquare$

Division algorithm

Corollary

If k is a field and $f \in k[x]$ is a nonzero polynomial, then f has at most $\deg(f)$ roots in k.

Proof: We will use induction.

<u>Basis</u>: If f is a constant, then it has no roots.

<u>Step</u>: Assume that the statement holds for polynomials of degree $m-1$. Let f be a polynomial of degree m. If f has no roots, then we are done. Otherwise f has a root a. We will divide f by $x-a$: $f = q \cdot (x-a) + r$. Evaluating both sides at a gives

$$\overset{0}{\overset{\shortparallel}{f(a)}} = r \Rightarrow \text{Hence } r=0 \text{ and}$$

$f = q \cdot (x-a)$. Now q has degree $m-1$ and by the ind. hypothesis has at most $m-1$ roots. Any root b of f different from a is a root of q, because $0 = f(b) = q(b)(b-a)$. Since k

is a field, we have $q(b) = 0$.

This completes the proof. $\boxtimes$

Division algorithm

Corollary

If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.

Proof: If $I = \{0\}$, then we are done. Otherwise take f to be a lowest degree element in I. We claim that $I = \langle f \rangle$. The inclusion $\langle f \rangle \subseteq I$ is obvious. Take $g \in I$. Then $g = q \cdot f + r$ by the division algorithm, where $\deg(r) < \deg(f)$ or $r = 0$. Then $r = g - q \cdot f \in I$. If $r \neq 0$, then $\deg(r) < \deg(f)$, which is a contradiction to f being a lowest degree element in I. Hence $r = 0$ and $g = q \cdot f \in \langle f \rangle$.

Uniqueness: Suppose $\langle f \rangle = \langle f' \rangle$. Hence $f = h' \cdot f'$ and $\deg(f) =$

$\deg(h') + \deg(f') \geq \deg(f')$.

Similarly $\deg(f') \geqslant \deg(f)$.

Hence $\deg(f) = \deg(f')$ and

f and f' differ up to

multiplication by a constant. $\blacksquare$

Division algorithm

Corollary

If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.

- an ideal generate by one element is called a **principal ideal**

Division algorithm

Corollary

If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.

- an ideal generate by one element is called a **principal ideal**
- $k[x]$ is a principal ideal domain

Division algorithm

Corollary

If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f \rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k.

- an ideal generate by one element is called a **principal ideal**
- $k[x]$ is a principal ideal domain
- how do we find a generator of the ideal $\langle x^4 - 1, x^6 - 1 \rangle$?

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f, g \in k[x]$ is a polynomial h such that:

1. h divides f and g.
2. If p is another polynomial which divides f and g, then p divides h. When h has these properties, we write $h = GCD(f, g)$.

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f, g \in k[x]$ is a polynomial h such that:

1. h divides f and g.
2. If p is another polynomial which divides f and g, then p divides h. When h has these properties, we write $h = GCD(f, g)$.

Proposition

Let $f, g \in k[x]$. Then:

1. *$GCD(f, g)$ exists and is unique up to multiplication by a nonzero constant in k.*

Definition

A **greatest common divisor** of polynomials $f, g \in k[x]$ is a polynomial h such that:

1. h divides f and g.
2. If p is another polynomial which divides f and g, then p divides h. When h has these properties, we write $h = GCD(f, g)$.

Proposition

Let $f, g \in k[x]$. Then:

1. *$GCD(f, g)$ exists and is unique up to multiplication by a nonzero constant in k.*
2. *$GCD(f, g)$ is a generator of the ideal $\langle f, g \rangle$.*

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f, g \in k[x]$ is a polynomial h such that:

1. h divides f and g.
2. If p is another polynomial which divides f and g, then p divides h. When h has these properties, we write $h = GCD(f, g)$.

Proposition

Let $f, g \in k[x]$. Then:

1. *$GCD(f, g)$ exists and is unique up to multiplication by a nonzero constant in k.*
2. *$GCD(f, g)$ is a generator of the ideal $\langle f, g \rangle$.*
3. *There is an algorithm for finding $GCD(f, g)$.*

<u>Proof</u>: ①/② There exists h s.t. $\langle f,g\rangle = \langle h\rangle$.

We will show that $GCD(f,g) = h$.

The pol. h divides both f and g, because $f,g \in \langle h\rangle$. Suppose p is another pol. that divides f and g. We can write $f = Ap$ and $g = B\cdot p$ for $A,B \in k[x]$.

Because $h \in \langle f,g\rangle$, we can write $h = C\cdot f + D\cdot g$ for some $C,D \in k[x]$.

Hence $h = C\cdot A\cdot p + D\cdot B\cdot p = (CA + DB)\cdot p$.

Thus p divides h and h is $GCD(f,g)$.

<u>Uniqueness</u> follows from the def. because h and h' would have to divide each other.

③ Notation: Let $f,g \in k[x]$, $g \neq 0$.

We write $f = q\cdot g + r$ as in the division algorithm. We denote remainder $(f,g) := r$.

Euclidean algorithm:

Input : f, g
Output : h

$h := f$

$s := g$

WHILE $s \neq 0$ DO

$\quad rem := \text{remainder}(h, s)$ $\left[\begin{array}{l} h = q \cdot s + r \\ \text{remainder is } r \end{array}\right]$

$\quad h_{new} := s$

$\quad s_{new} := rem$

---

* The algorithm terminates, since the degree of s decreases at each step.

* $GCD(f, g) = GCD(g, \underbrace{r}_{f - q \cdot g})$,

because $\langle f, g \rangle = \langle g, f - q \cdot g \rangle$.

Similarly

$$GCD(f, g) = GCD(g, r) = GCD(r, r') =$$
$$= GCD(r', r'') = \dots,$$

where $r, r', r'', \dots$ are remainders obtained by the consecutive steps of the Euclidean algorithm. The last two remainders are the output h and 0. Since $GCD(h, 0) = h$, we have $GCD(f, g) = GCD(h, 0) = h$. $\blacksquare$

Quiz

Compute the GCD of $x^4 - 1$ *and* $x^6 - 1$.

The greatest common divisor

Quiz

Compute the GCD of $x^4 - 1$ and $x^6 - 1$.

Example

$$
\begin{aligned}
x^4 - 1 &= 0(x^6 - 1) + x^4 - 1, \\
x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1, \\
x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0 \\
&\Rightarrow GCD(x^4 - 1, x^6 - 1) = x^2 - 1
\end{aligned}
$$

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f_1, \ldots, f_s \in k[x]$ is a polynomial h such that:

1. h divides $f_1, \ldots, f_s$.
2. If p is another polynomial which divides $f_1, \ldots, f_s$, then p divides h. When h has these properties, we write $h = GCD(f_1, \ldots, f_s)$.

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f_1, \dots, f_s \in k[x]$ is a polynomial h such that:

1. h divides $f_1, \dots, f_s$.
2. If p is another polynomial which divides $f_1, \dots, f_s$, then p divides h. When h has these properties, we write $h = GCD(f_1, \dots, f_s)$.

Proposition

Let $f_1, \dots, f_s \in k[x]$, where $s \geq 2$. Then:

1. *$GCD(f_1, \dots, f_s)$ exists and is unique up to multiplication by a nonzero constant in k.*

Definition

A **greatest common divisor** of polynomials $f_1, \ldots, f_s \in k[x]$ is a polynomial h such that:

1. h divides $f_1, \ldots, f_s$.
2. If p is another polynomial which divides $f_1, \ldots, f_s$, then p divides h. When h has these properties, we write $h = GCD(f_1, \ldots, f_s)$.

Proposition

Let $f_1, \ldots, f_s \in k[x]$, where $s \geq 2$. Then:

1. *$GCD(f_1, \ldots, f_s)$ exists and is unique up to multiplication by a nonzero constant in k.*
2. *$GCD(f_1, \ldots, f_s)$ is a generator of the ideal $\langle f_1, \ldots, f_s \rangle$.*

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f_1, \ldots, f_s \in k[x]$ is a polynomial h such that:

1. h divides $f_1, \ldots, f_s$.
2. If p is another polynomial which divides $f_1, \ldots, f_s$, then p divides h. When h has these properties, we write $h = GCD(f_1, \ldots, f_s)$.

Proposition

Let $f_1, \ldots, f_s \in k[x]$, where $s \geq 2$. Then:

1. *$GCD(f_1, \ldots, f_s)$ exists and is unique up to multiplication by a nonzero constant in k.*
2. *$GCD(f_1, \ldots, f_s)$ is a generator of the ideal $\langle f_1, \ldots, f_s \rangle$.*
3. *If $s \geq 3$, then $GCD(f_1, \ldots, f_s) = GCD(f_1, GCD(f_2, \ldots, f_s))$.*

The greatest common divisor

Definition

A **greatest common divisor** of polynomials $f_1, \ldots, f_s \in k[x]$ is a polynomial h such that:

1. h divides $f_1, \ldots, f_s$.
2. If p is another polynomial which divides $f_1, \ldots, f_s$, then p divides h. When h has these properties, we write $h = GCD(f_1, \ldots, f_s)$.

Proposition

Let $f_1, \ldots, f_s \in k[x]$, where $s \geq 2$. Then:

1. *$GCD(f_1, \ldots, f_s)$ exists and is unique up to multiplication by a nonzero constant in k.*
2. *$GCD(f_1, \ldots, f_s)$ is a generator of the ideal $\langle f_1, \ldots, f_s \rangle$.*
3. *If $s \geq 3$, then $GCD(f_1, \ldots, f_s) = GCD(f_1, GCD(f_2, \ldots, f_s))$.*
4. *There is an algorithm for finding $GCD(f_1, \ldots, f_s)$.*

The greatest common divisor

Quiz

Compute the GCD of $x^3 - 3x + 2$, $x^4 - 1$ *and* $x^6 - 1$.

The greatest common divisor

Quiz

Compute the GCD of $x^3 - 3x + 2, x^4 - 1$ *and* $x^6 - 1$.

Example

$$\begin{aligned} & GCD(x^3 - 3x + 2, x^4 - 1, x^6 - 1) \\ = & GCD(x^3 - 3x + 2, GCD(x^4 - 1, x^6 - 1)) \\ = & GCD(x^3 - 3x + 2, x^2 - 1) = x - 1 \end{aligned}$$

It follows that

$$\langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle = \langle x - 1 \rangle$$

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \ldots, f_s \rangle$?

Ideal membership problem

- Is there an algorithm for deciding whether a given polynomial $f \in k[x]$ lies in the ideal $\langle f_1, \dots, f_s \rangle$?
- Using GCDs find a generator h of $\langle f_1, \dots, f_s \rangle$.

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 $\deg(r) < \deg(h)$.

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 $r = 0$.

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

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?

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

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?

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

- $x^3 + 4x^2 + 3x - 7 \in \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 \in \langle x - 1 \rangle$?
- $x^3 + 4x^2 + 3x - 7 = (x^2 + 5x + 8)(x - 1) + 1$

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

Conclusion

Today:

- 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
- Polynomials in one variable
  - Division algorithm
  - A degree m polynomial has at most m roots
  - Greatest common divisor
  - Every ideal in $k[x]$ can be generated by one polynomial

Next time:

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