Computational Algebraic Geometry

The Algebra-Geometry Dictionary

Kaie Kubjas

kaie.kubjas@aalto.fi

February 10, 2021

Overview

Last time:

- Three ideal operations: Sums, products, intersections
- Generating sets of the ideals obtained by these operations
- Geometric operations corresponding to the algebraic operations
- Zariski closure
- Finished the proof of the Closure Theorem

Today:

- Quotients of ideals
- Irreducible varieties and prime ideals
- Decomposition of a variety into irreducibles

Zariski closure and quotients of ideals

Zariski closure

Proposition

If $S \subseteq k^n$, the affine variety $\mathbb{V}(\mathbb{I}(S))$ is the smallest variety that contains S.

Definition

The Zariski closure of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subseteq k^n$, the Zariski closure of S is denoted $\overline{S}$ and is equal to $\mathbb{V}(\mathbb{I}(S))$.

Zariski closure

Proposition

If $S \subseteq k^n$, the affine variety $\mathbb{V}(\mathbb{I}(S))$ is the smallest variety that contains S.

Definition

The Zariski closure of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subseteq k^n$, the Zariski closure of S is denoted $\overline{S}$ and is equal to $\mathbb{V}(\mathbb{I}(S))$.

Recall the difference of two varieties need not be a variety:

- $K = \langle xz, yz \rangle, I = \langle z \rangle$
- $\mathbb{V}(K) - \mathbb{V}(I)$ is the z-axis with the origin moved
- the z-axis is the smallest variety containing $\mathbb{V}(K) - \mathbb{V}(I)$

Zariski closure

Proposition

If $S \subseteq k^n$, the affine variety $\mathbb{V}(\mathbb{I}(S))$ is the smallest variety that contains S.

Definition

The Zariski closure of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subseteq k^n$, the Zariski closure of S is denoted $\overline{S}$ and is equal to $\mathbb{V}(\mathbb{I}(S))$.

Recall the difference of two varieties need not be a variety:

- $K = \langle xz, yz \rangle, I = \langle z \rangle$
- $\mathbb{V}(K) - \mathbb{V}(I)$ is the z-axis with the origin moved
- the z-axis is the smallest variety containing $\mathbb{V}(K) - \mathbb{V}(I)$

Proposition

If V and W are varieties with $V \subseteq W$, then $W = V \cup (\overline{W - V})$.

Ideal quotient

Definition

If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set

$$\{f \in k[x_1, \ldots, x_n] : fg \in I \text{ for all } g \in J\}$$

and is called the ideal quotient (or colon ideal) of I by J.

Ideal quotient

Definition

If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set

$$\{f \in k[x_1, \ldots, x_n] : fg \in I \text{ for all } g \in J\}$$

and is called the ideal quotient (or colon ideal) of I by J.

Example

$$\begin{aligned}
\langle xz, yz \rangle : \langle z \rangle &= \{f \in k[x, y, z] : fz \in \langle xz, yz \rangle\} \\
&= \{f \in k[x, y, z] : fz = Axz + Byz\} \\
&= \{f \in k[x, y, z] : f = Ax + By\} = \langle x, y \rangle
\end{aligned}$$

Ideal quotient

Definition

If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set

$$\{f \in k[x_1, \ldots, x_n] : fg \in I \text{ for all } g \in J\}$$

and is called the ideal quotient (or colon ideal) of I by J.

Example

$$\begin{aligned}\langle xz, yz\rangle : \langle z\rangle &= \{f \in k[x,y,z] : fz \in \langle xz, yz\rangle\}\\ &= \{f \in k[x,y,z] : fz = Axz + Byz\}\\ &= \{f \in k[x,y,z] : f = Ax + By\} = \langle x, y\rangle\end{aligned}$$

Proposition

If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is an ideal in $k[x_1, \ldots, x_n]$ and $I : J$ contains I.

Ideal quotient

Theorem

Let I and J be ideals in $k[x_1, \ldots, x_n]$. Then

$$\mathbb{V}(I : J) \supseteq \overline{\mathbb{V}(I) - \mathbb{V}(J)}.$$

If, in addition if k is algebraically closed and I is a radical ideal, then

$$\mathbb{V}(I : J) = \overline{\mathbb{V}(I) - \mathbb{V}(J)}.$$

Example

Let $I = \langle xy^2 \rangle$ and $J = \langle y \rangle$. What is $I : J$? What is $\overline{\mathbb{V}(I) - \mathbb{V}(J)}$?

Ideal quotient

Theorem

Let I and J be ideals in $k[x_1, \ldots, x_n]$. Then

$$\mathbb{V}(I : J) \supseteq \overline{\mathbb{V}(I) - \mathbb{V}(J)}.$$

If, in addition if k is algebraically closed and I is a radical ideal, then

$$\mathbb{V}(I : J) = \overline{\mathbb{V}(I) - \mathbb{V}(J)}.$$

Example

Let $I = \langle xy^2 \rangle$ and $J = \langle y \rangle$. What is $I : J$? What is $\overline{\mathbb{V}(I) - \mathbb{V}(J)}$? Then $I : J = \langle xy \rangle$, $\mathbb{V}(I : J)$ is the union of x-axis and y-axis and $\overline{\mathbb{V}(I) - \mathbb{V}(J)}$ is the y-axis.

Proof: We will show that $I:J \subseteq I(\mathbb{V}(I) - \mathbb{V}(J))$. Let $f \in I:J$. Let $x \in \mathbb{V}(I) - \mathbb{V}(J)$. Then $f \cdot g \in I$ for all $g \in J$. Since $x \in \mathbb{V}(I)$, we have $f(x) \cdot g(x) = 0$ for all $g \in J$. Since $x \notin \mathbb{V}(J)$, then $\exists g \in J$ s.t. $g(x) \neq 0$. Hence $f(x) = 0$. Hence $f \in I(\mathbb{V}(I) - \mathbb{V}(J))$. Thus $I:J \subseteq I(\mathbb{V}(I) - \mathbb{V}(J))$ and $\mathbb{V}(I:J) \supseteq \mathbb{V}(I(\mathbb{V}(I) - \mathbb{V}(J)))$. ∎

Corollary

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

$$\mathbb{I}(V) : \mathbb{I}(W) = \mathbb{I}(V - W).$$

Example

- Let V be the union of x-axis and y-axis.
- Let W be the x-axis.
- Then $\mathbb{I}(V) = \langle xy \rangle$, $\mathbb{I}(W) = \langle y \rangle$ and $\mathbb{I}(V) : \mathbb{I}(W) = \langle x \rangle$.
- $V - W$ is the y-axis without the point $(0, 0)$.
- $\mathbb{I}(V - W) = \langle x \rangle$

Ideal quotient

Proposition

Let I, J, and K be ideals in $k[x_1, \dots, x_n]$. Then:

1. $I : k[x_1, \dots, x_n] = I$.
2. $IJ \subseteq K$ if and only if $I \subseteq K : J$.
3. $J \subseteq I$ if and only if $I : J = k[x_1, \dots, x_n]$.

Ideal quotient

Proposition

Let I, J, and K be ideals in $k[x_1, \dots, x_n]$. Then:

1. $I : k[x_1, \dots, x_n] = I$.
2. $IJ \subseteq K$ if and only if $I \subseteq K : J$.
3. $J \subseteq I$ if and only if $I : J = k[x_1, \dots, x_n]$.

Proposition

Let I, I_i, J, J_i, and K be ideals in $k[x_1, \dots, x_n]$ for $1 \leq i \leq r$. Then

$$(\cap_{i=1}^r I_i) : J = \cap_{i=1}^r (I_i : J),$$

$$I : (\sum_{i=1}^r J_i) = \cap_{i=1}^r (I : J_i),$$

$$(I : J) : K = I : JK.$$

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$
- compute a basis for $I : \langle g_i \rangle$

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \dots, x_n]$. If $\{h_1, \dots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \dots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle = \langle g_1 \rangle + \dots + \langle g_s \rangle$
- compute a basis for $I : \langle g_i \rangle$
- compute a basis for $\langle f_1, \dots, f_r \rangle \cap \langle g_i \rangle$

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$
- compute a basis for $I : \langle g_i \rangle$
- compute a basis for $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$ by finding a Groebner basis of $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ wrt a lex order in which t precedes all the x_i

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$
- compute a basis for $I : \langle g_i \rangle$
- compute a basis for $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$ by finding a Groebner basis of $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ wrt a lex order in which t precedes all the x_i
- use the division algorithm to get a basis for $I : \langle g_i \rangle$

Ideal quotient

Theorem

Let I be an ideal and g an element of $k[x_1, \ldots, x_n]$. If $\{h_1, \ldots, h_p\}$ is a basis of the ideal $I \cap \langle g \rangle$, then $\{h_1/g, \ldots, h_p/g\}$ is a basis of $I : \langle g \rangle$.

An algorithm for computing a basis of an ideal quotient:

- $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle = \langle g_1 \rangle + \cdots + \langle g_s \rangle$
- compute a basis for $I : \langle g_i \rangle$
- compute a basis for $\langle f_1, \ldots, f_r \rangle \cap \langle g_i \rangle$ by finding a Groebner basis of $\langle tf_1, \ldots, tf_r, (1-t)g_i \rangle$ wrt a lex order in which t precedes all the x_i
- use the division algorithm to get a basis for $I : \langle g_i \rangle$
- compute a basis of $I : J$ by applying the intersection algorithm $s - 1$ times, computing first a basis for $I : \langle g_1, g_2 \rangle = (I : \langle g_1 \rangle) \cap (I : \langle g_2 \rangle)$ etc

Irreducible varieties and prime ideals

Irreducible varieties

- Recall that the union of two varieties is a variety
- $\mathbb{V}(xz, yz)$ is the union of a plane and a line
- The line and the plane are more fundamental than $\mathbb{V}(xz, yz)$, since they are indecomposable

Irreducible varieties

- Recall that the union of two varieties is a variety
- $\mathbb{V}(xz, yz)$ is the union of a plane and a line
- The line and the plane are more fundamental than $\mathbb{V}(xz, yz)$, since they are indecomposable

Definition

An affine variety $V \subseteq k^n$ is irreducible if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

- Recall that the union of two varieties is a variety
- $\mathbb{V}(xz, yz)$ is the union of a plane and a line
- The line and the plane are more fundamental than $\mathbb{V}(xz, yz)$, since they are indecomposable

Definition

An affine variety $V \subseteq k^n$ is irreducible if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

Example

$\mathbb{V}(xz, yz)$ is not an irreducible variety.

Irreducible varieties

- For the definition to be reasonable, a point, a line and a plane should be irreducible (homework).
- The twisted cubic $\mathbb{V}(y - x^2, z - x^3)$ is irreducible. How to prove this?
- When is an algebraic variety irreducible? The key is to consider the corresponding algebraic notion.

Irreducible varieties

- For the definition to be reasonable, a point, a line and a plane should be irreducible (homework).
- The twisted cubic $\mathbb{V}(y - x^2, z - x^3)$ is irreducible. How to prove this?
- When is an algebraic variety irreducible? The key is to consider the corresponding algebraic notion.

Definition

An ideal $I \subseteq k[x_1, \ldots, x_n]$ is prime if whenever $f, g \in k[x_1, \ldots, x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Irreducible varieties

- For the definition to be reasonable, a point, a line and a plane should be irreducible (homework).
- The twisted cubic $\mathbb{V}(y - x^2, z - x^3)$ is irreducible. How to prove this?
- When is an algebraic variety irreducible? The key is to consider the corresponding algebraic notion.

Definition

An ideal $I \subseteq k[x_1, \ldots, x_n]$ is prime if whenever $f, g \in k[x_1, \ldots, x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Proposition

Let $V \subseteq k^n$ be an affine variety. Then V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal.

Proof: "$\Rightarrow$" Assume that V is irreducible and let f, g be such that $f \cdot g \in \mathbb{I}(V)$. Define $V_1 = V \cap \mathbb{V}(f)$ and $V_2 = V \cap \mathbb{V}(g)$. Then $f \cdot g \in \mathbb{I}(V)$ implies that $V = V_1 \cup V_2$. Since V is irreducible, either $V = V_1$ or $V = V_2$. If $V = V_1 = V \cap \mathbb{V}(f)$, which implies that f vanishes on V and hence $f \in \mathbb{I}(V)$. Otherwise if $V = V_2$, similarly $g \in \mathbb{I}(V)$.

"$\Leftarrow$" Assume that $\mathbb{I}(V)$ is prime and let $V = V_1 \cup V_2$. Suppose that $V \neq V_1$. We claim that $V = V_2$. Note $\mathbb{I}(V) \subsetneq \mathbb{I}(V_1)$ and $\mathbb{I}(V) \subseteq \mathbb{I}(V_2)$. Pick $f \in \mathbb{I}(V_1) - \mathbb{I}(V)$. Let $g \in \mathbb{I}(V_2)$. Since $V = V_1 \cup V_2$, then $f \cdot g \in \mathbb{I}(V)$. Since $\mathbb{I}(V)$ is prime, then either f or g lies in $\mathbb{I}(V)$. Since $f \notin \mathbb{I}(V)$, we must have that $g \in \mathbb{I}(V)$. This proves $\mathbb{I}(V_2) = \mathbb{I}(V)$. Hence $V_2 = V$. Thus V is irreducible. ■

Irreducible varieties

Note that every prime ideal is radical.

Corollary

When k is algebraically closed, then functions I and V induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, \ldots, x_n]$.

Irreducible varieties

Note that every prime ideal is radical.

Corollary

When k is algebraically closed, then functions I and V induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, \ldots, x_n]$.

Example

The ideal of the twisted cubic is prime:

- suppose $fg \in \mathbb{I}(V)$
- $f(t, t^2, t^3)g(t, t^2, t^3) = 0$ for all t
- $f(t, t^2, t^3)$ or $g(t, t^2, t^3)$ is the zero polynomial
- f or g lies in $\mathbb{I}(V)$
- $\mathbb{I}(V)$ is a prime ideal
- twisted cubic is an irreducible variety in $\mathbb{R}^3$

The idea how we showed that the twisted cubic is an irreducible variety can be generalized:

Proposition

If k is an infinite field and $V \subseteq k^n$ is a variety defined parametrically

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned}$$

where $f_1, \ldots, f_n$ are polynomials in $k[t_1, \ldots, t_m]$, then V is irreducible.

Irreducible varieties

Proposition

If k is an infinite field and $V \subseteq k^n$ is a variety defined by the rational parametrization

$$x_1 = \frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)},$$
$$\vdots$$
$$x_n = \frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)},$$

where $f_1,\ldots,f_n,g_1,\ldots,g_n \in k[t_1,\ldots,t_m]$, then V is irreducible.

Maximal ideals

- the simplest variety $\{(a_1, \ldots, a_n)\}$
- parametrization $f_i(t_1, \ldots, t_m) = a_i$
- hence a point is irreducible
- Quiz: What is the ideal of the point? Is the ideal prime?

Maximal ideals

- the simplest variety $\{(a_1, \dots, a_n)\}$
- parametrization $f_i(t_1, \dots, t_m) = a_i$
- hence a point is irreducible
- Quiz: What is the ideal of the point? Is the ideal prime?
- $\mathbb{I}(\{a_1, \dots, a_n\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$
- the ideal of a point is prime
- it is also maximal: the only ideal that strictly contains it is $k[x_1, \dots, x_n]$

Maximal ideals

- the simplest variety $\{(a_1, \ldots, a_n)\}$
- parametrization $f_i(t_1, \ldots, t_m) = a_i$
- hence a point is irreducible
- Quiz: What is the ideal of the point? Is the ideal prime?
- $\mathbb{I}(\{a_1, \ldots, a_n\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$
- the ideal of a point is prime
- it is also maximal: the only ideal that strictly contains it is $k[x_1, \ldots, x_n]$

Definition

An ideal $I \subseteq k[x_1, \ldots, x_n]$ is said to be maximal if $I \neq k[x_1, \ldots, x_n]$ and any ideal J containing I is such that either $J = I$ or $J = k[x_1, \ldots, x_n]$.

Maximal ideals

Definition

If k is any field, an ideal $I \subseteq k[x_1, \ldots, x_n]$ is called proper if I is not equal to $k[x_1, \ldots, x_n]$.

Maximal ideals

Definition

If k is any field, an ideal $I \subseteq k[x_1, \ldots, x_n]$ is called proper if I is not equal to $k[x_1, \ldots, x_n]$.

Proposition

If k is any field, an ideal $I \subseteq k[x_1, \ldots, x_n]$ of the form

$$I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

where $a_1, \ldots, a_n \in k$, is maximal.

Proof: Let J be an ideal strictly containing I. Let $f \in J - I$. We can use the division algorithm to write $f = A_1(x_1 - a_1) + \dots + A_n(x_n - a_n) + b$, where b is a constant.

Since $f \in J$, $x_i - a_i \in I \subseteq J$ $\forall i \in \{1, \dots, n\}$, then $b \in J$. Then $\frac{1}{b} \cdot b = 1 \in J$ and hence $J = k[x_1, \dots, x_n]$. Thus I is maximal. $\blacksquare$

Maximal ideals

Definition

If k is any field, an ideal $I \subseteq k[x_1, \dots, x_n]$ is called proper if I is not equal to $k[x_1, \dots, x_n]$.

Proposition

If k is any field, an ideal $I \subseteq k[x_1, \dots, x_n]$ of the form

$$I = \langle x_1 - a_1, \dots, x_n - a_n \rangle,$$

where $a_1, \dots, a_n \in k$, is maximal.

- every point $(a_1, \dots, a_n) \in k^n$ corresponds to the maximal ideal $\langle x_1 - a_1, \dots, x_n - a_n \rangle$
- the converse does not hold if k is not algebraically closed
- $\langle x^2 + 1 \rangle$ is maximal in $\mathbb{R}[x]$

Maximal ideals

Proposition

If k is any field, a maximal ideal in $k[x_1, \ldots, x_n]$ is prime.

Proof: Let I be a max ideal and $f \cdot g \in I$. Assume that $f \notin I$. Consider the ideal $I + \langle f \rangle$. This ideal strictly contains I and hence it has to be equal to $k[x_1, \ldots, x_n]$. Hence $1 = h + c \cdot f$, where $h \in I$ and $c \in k[x_1, \ldots, x_n]$. Multiplying both sides by g gives that $g = \underbrace{h}_{\in I} \cdot g + c \cdot \underbrace{f \cdot g}_{\in I} \in I$. Thus I is prime. $\blacksquare$

Maximal ideals

Proposition

If k is any field, a maximal ideal in $k[x_1, \dots, x_n]$ is prime.

Theorem

If k is an algebraically closed field, then every maximal ideal of $k[x_1, \dots, x_n]$ is of the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some $a_1, \dots, a_n \in k$.

Proof: Let I be max ideal. Since $I \neq k[x_1, \dots, x_n]$, then $\mathbb{V}(I) \neq \emptyset$ by the Weak Nullstellensatz.
Hence $\exists\ (a_1, \dots, a_n) \in \mathbb{V}(I)$. Then $\underbrace{\mathbb{I}((a_1, \dots, a_n))}_{= \langle x_1 - a_1, \dots, x_n - a_n \rangle} \supseteq \mathbb{I}(\mathbb{V}(I)) \supseteq I$.

Thus $I \subseteq \langle x_1 - a_1, \dots, x_n - a_n \rangle$. Since I is max, the inclusion is in fact an equality. $\blacksquare$

Maximal ideals

Proposition

If k is any field, a maximal ideal in $k[x_1, \dots, x_n]$ is prime.

Theorem

If k is an algebraically closed field, then every maximal ideal of $k[x_1, \dots, x_n]$ is of the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some $a_1, \dots, a_n \in k$.

Corollary

If k is an algebraically closed field, then there is a one-to-one correspondence between points of k^n and maximal ideals of $k[x_1, \dots, x_n]$.

Decomposition of a variety into irreducibles

Decomposition of a variety into irreducibles

Proposition (The Descending Chain Condition)

Any descending chain of varieties

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$$

in k^n must stabilize. That is, there exists a positive integer N such that $V_N = V_{N+1} = \cdots$.

Decomposition of a variety into irreducibles

Proposition (The Descending Chain Condition)

Any descending chain of varieties

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$$

in k^n must stabilize. That is, there exists a positive integer N such that $V_N = V_{N+1} = \cdots$.

Theorem

Let $V \subseteq k^n$ be an affine variety. Then V can be written as a finite union

$$V = V_1 \cup \cdots \cup V_m,$$

where each V_i is an irreducible variety.

Proof: Assume that V cannot be written as a finite union of irreducible varieties. Then there exist affine varieties V_1 and V_1' s.t. $V = V_1 \cup V_1'$ and $V_1 \neq V$ cannot be written as a finite union of irreducible varieties. Similarly, we can write $V_1 = V_2 \cup V_2'$ where $V_2 \neq V_1$ cannot be written as a finite union of irr varieties etc. Then we get an infinite sequence

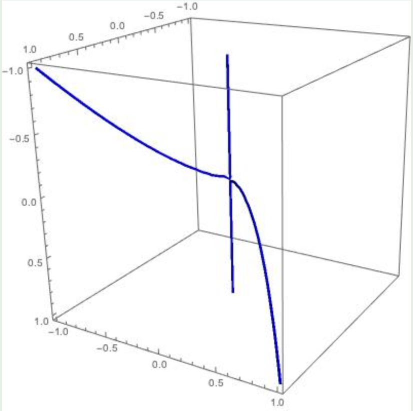
$$V \supset V_1 \supset V_2 \supset \dots$$

This contradicts the DCC. $\blacksquare$

Decomposition of a variety into irreducibles

Example

$$V = \mathbb{V}(xz - y^2, x^3 - yz)$$



Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz \rangle : \langle x, y \rangle$

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle$
- $(I : x) \cap (I : y)$

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz \rangle : \langle x, y \rangle$
- $(I : x) \cap (I : y)$
- $I \cap \langle x \rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3 \rangle$

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle$
- $(I : x) \cap (I : y)$
- $I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle$
- $I : x = \langle \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x}\rangle =$ $\langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I + \langle x^2y - z^2\rangle$

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle$
- $(I : x) \cap (I : y)$
- $I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle$
- $I : x = \langle \frac{x^2z-xy^2}{x}, \frac{x^4-xyz}{x}, \frac{x^3y-xz^2}{x}\rangle =$
  $\langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I + \langle x^2y - z^2\rangle$
- $I : y = I + \langle x^2y - z^2\rangle$

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle$
- $(I : x) \cap (I : y)$
- $I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle$
- $I : x = \langle \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x}\rangle =$
  $\langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I + \langle x^2y - z^2\rangle$
- $I : y = I + \langle x^2y - z^2\rangle$
- $I : \langle x, y\rangle = \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle$

Decomposition of a variety into irreducibles

Example

$V = \mathbb{V}(xz - y^2, x^3 - yz)$:

- z-axis $\mathbb{V}(x, y)$ is contained in V
- what about $V - \mathbb{V}(x, y)$?
- consider $\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle$
- $(I : x) \cap (I : y)$
- $I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle$
- $I : x = \langle \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x}\rangle =$ $\langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I + \langle x^2y - z^2\rangle$
- $I : y = I + \langle x^2y - z^2\rangle$
- $I : \langle x, y\rangle = \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle$
- $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ is an irreducible curve parametrized by (t^3, t^4, t^5)

Decomposition of a variety into irreducibles

Definition

Let $V \subseteq k^n$ be an affine variety. A decomposition

$$V = V_1 \cup \ldots \cup V_m,$$

where each V_i is an irreducible variety, is called a minimal decomposition if $V_i \not\subset V_j$ for $i \neq j$.

Decomposition of a variety into irreducibles

Definition

Let $V \subseteq k^n$ be an affine variety. A decomposition

$$V = V_1 \cup \ldots \cup V_m,$$

where each V_i is an irreducible variety, is called a minimal decomposition if $V_i \not\subset V_j$ for $i \neq j$.

Theorem

Let $V \subseteq k^n$ be an affine variety. Then V has a minimal decomposition

$$V = V_1 \cup \cdots \cup V_m.$$

Furthermore, this decomposition is unique up to the order in which $V_1, \ldots, V_m$ are written.

The uniqueness part is wrong if one does not assume finiteness of the decomposition.

Minimal decomposition

Theorem

If k is algebraically closed, then every radical ideal in $k[x_1, \ldots, x_n]$ can be written uniquely as a finite intersection of prime ideals, $I = P_1 \cap \cdots \cap P_r$, where $P_i \not\subset P_j$ for $i \neq j$. We often call such a presentation of a radical ideal a minimal decomposition.

Minimal decomposition

Theorem

If k is algebraically closed, then every radical ideal in $k[x_1, \ldots, x_n]$ can be written uniquely as a finite intersection of prime ideals, $I = P_1 \cap \cdots \cap P_r$, where $P_i \not\subset P_j$ for $i \neq j$. We often call such a presentation of a radical ideal a minimal decomposition.

Theorem

If k is algebraically closed and I is a proper radical ideal such that

$$I = \cap_{i=1}^{r} P_i$$

is its minimal decomposition as an intersection of prime ideals, then the P_i's are precisely the proper prime ideals that occur in the set $\{I : f : f \in k[x_1, \ldots, x_n]\}$.

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$
- want to remove $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$
- want to remove $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I : (x^2y - z^2) = \langle x, y \rangle$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$
- want to remove $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I : (x^2y - z^2) = \langle x, y \rangle$
- $I = (I : (x^2y - z^2)) \cap (I : x)$

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$
- want to remove $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I : (x^2y - z^2) = \langle x, y \rangle$
- $I = (I : (x^2y - z^2)) \cap (I : x)$
- it remains to show that $I : (x^2y - z^2)$ and $(I : x)$ are prime

Minimal decomposition

Example

- $I = \langle xz - y^2, x^3 - yz \rangle$
- Assume that I is a radical ideal
- Can we write I as an intersection of prime ideals?
- $\mathbb{V}(I) = \mathbb{V}(x, y) \cup \mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- we know $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$
- $I = \langle x, y \rangle \cap (I : x)$
- want to remove $\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2)$
- $I : (x^2y - z^2) = \langle x, y \rangle$
- $I = (I : (x^2y - z^2)) \cap (I : x)$
- it remains to show that $I : (x^2y - z^2)$ and $(I : x)$ are prime
- $I : x = \mathbb{I}(\mathbb{V}(xz - y^2, x^3 - yz, x^2y - z^2))$

Conclusion

Today:

- Quotients of ideals
- Irreducible varieties and prime ideals
- Decomposition of a variety into irreducibles

Next time: Applications in robotics