Computational Algebraic Geometry
The Algebra-Geometry Dictionary

Kaie Kubjas

kaie.kubjas@aalto.fi

February 8, 2021

Overview

Last time:

- Nullstellensätze
- Radical ideals
- Ideal and variety correspondence

Today:

- Sums of ideals
- Products of ideals
- Intersections of ideals
- Zariski closure
- Quotients of ideals (postponed to next time)

Algebraic operations on ideals

The following are algebraic operations on ideals:

- Sums of ideals
- Products of ideals
- Intersections of ideals
- Quotients of ideals

We are particularly interested in the following two questions related to these different operations:

- Given generators of a pair of ideals, can one compute generators of the ideals obtained by these operations?
- What geometric operations correspond to these algebraic operations?

Sums, products and intersections of ideals

Sum of Ideas

Definition

If I and J are ideals of the ring $k[x_1, \ldots, x_n]$, then the sum of I and J, denoted $I + J$, is the set

$$I + J = \{f + g : f \in I \text{ and } g \in J\}.$$

Sum of Ideas

Definition

If I and J are ideals of the ring $k[x_1, \dots, x_n]$, then the sum of I and J, denoted $I + J$, is the set

$$I + J = \{f + g : f \in I \text{ and } g \in J\}.$$

Proposition

If I and J are ideals in $k[x_1, \dots, x_n]$, then $I + J$ is also an ideal in $k[x_1, \dots, x_n]$. In fact, $I + J$ is the smallest ideal containing I and J. Furthermore, if $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$, then $I + J = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle$.

Proof: ① $I+J$ is an ideal:

* $0 = 0+0 \in I+J$
* Let $f_1, f_2 \in I+J$. Then $\exists g_1, g_2 \in I$ and $\exists h_1, h_2 \in J$ s.t. $f_1 = g_1 + h_1$ and $f_2 = g_2 + h_2$.
  Then $f_1 + f_2 = (g_1+h_1) + (g_2+h_2) = \underbrace{(g_1+g_2)}_{\substack{\cap \\ I}} + \underbrace{(h_1+h_2)}_{\substack{\cap \\ J}} \in I+J$.
* Let $f \in I+J$ and $\ell \in k[x_1, \dots, x_n]$. Then $\exists g \in I$ and $\exists h \in J$ s.t. $f = g+h$. Then $\ell \cdot f = \ell \cdot (g+h) =$
  $= \underbrace{\ell \cdot g}_{\substack{\cap \\ I}} + \underbrace{\ell \cdot h}_{\substack{\cap \\ J}} \in I+J$.

② $I+J$ is the smallest ideal containing I and J:

If H is an ideal that contains I and J, then it must contain all $f \in I$ and $g \in J$. Since H is an ideal, it must contain all sums $f+g$, where $f \in I$ and $g \in J$. Hence $I+J \subseteq H$ and every ideal containing I and J must contain $I+J$.

③ Generating set:

If $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$, then $\langle f_1, \dots, f_r, g_1, \dots, g_s \rangle$ is an ideal containing both I and J. Hence $I+J$ is contained in $\langle f_1, \dots, f_r, g_1, \dots, g_s \rangle$. The reverse inclusion follows since $f_i \in I$ and $g_j \in J$ and I and J are both contained in $I+J$. $\blacksquare$

Sum of Ideas

Definition

If I and J are ideals of the ring $k[x_1, \dots, x_n]$, then the sum of I and J, denoted $I + J$, is the set

$$I + J = \{f + g : f \in I \text{ and } g \in J\}.$$

Proposition

If I and J are ideals in $k[x_1, \dots, x_n]$, then $I + J$ is also an ideal in $k[x_1, \dots, x_n]$. In fact, $I + J$ is the smallest ideal containing I and J. Furthermore, if $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$, then $I + J = \langle f_1, \dots, f_r, g_1, \dots, g_s \rangle$.

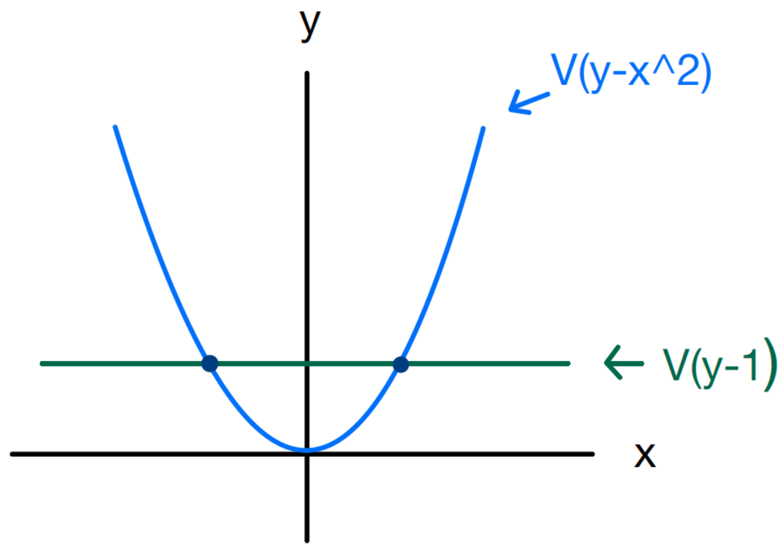
Corollary

If $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, then

$$\langle f_1, \dots, f_r \rangle = \langle f_1 \rangle + \cdots + \langle f_r \rangle.$$

Sum of ideals

$\mathbb{V}(y-x^2, y-1)$



Theorem

If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J)$.

Proof: "$\subseteq$" If $x \in \mathbb{V}(I+J)$, then $x \in \mathbb{V}(I)$, since $I \subseteq I+J$. Similarly $x \in \mathbb{V}(J)$. Hence $x \in \mathbb{V}(I) \cap \mathbb{V}(J)$.

"$\supseteq$" Let $x \in \mathbb{V}(I) \cap \mathbb{V}(J)$. Let $h \in I+J$. Then $\exists f \in I$, $g \in J$ s.t. $h = f+g$. Then $h(x) = \underbrace{f(x)}_{0} + \underbrace{g(x)}_{0} = 0$.

Hence $x \in \mathbb{V}(I+J)$. $\blacksquare$

Products of Ideals

Definition

If I and J are two ideals in $k[x_1, \dots, x_n]$, then their product, denoted $I \cdot J$, is defined to be the ideal generated by all polynomials $f \cdot g$ where $f \in I$ and $g \in J$.

Thus, the product $I \cdot J$ of I and J is the set

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r : f_1, \dots, f_r \in I, g_1, \dots, g_r \in J, r > 0\}$$

Products of Ideals

Definition

If I and J are two ideals in $k[x_1, \ldots, x_n]$, then their product, denoted $I \cdot J$, is defined to be the ideal generated by all polynomials $f \cdot g$ where $f \in I$ and $g \in J$.

Thus, the product $I \cdot J$ of I and J is the set

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r : f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r > 0\}$$

Proposition

If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I \cdot J$ is also an ideal in $k[x_1, \ldots, x_n]$. Furthermore, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $I \cdot J = \langle f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle$.

Proof: * $I \cdot J$ is an ideal - EXERCISE

* Generating set: "$\supseteq$" The products $f_i \cdot g_j$ are contained in $I \cdot J$ by definition.

"$\subseteq$" Consider an element of $I \cdot J$. It is sum of terms of the form $f \cdot g$, where $f \in I$ and $g \in J$.

We can write $f = \sum_{i=1}^{r} a_i \cdot f_i$ and $g = \sum_{j=1}^{s} b_j g_j$, where $a_i, b_j \in k[x_1, \dots, x_n]$.

Hence $f \cdot g = \sum_{i,j} \underbrace{(a_i b_j)}_{\in k[x_1, \dots, x_n]} f_i \cdot g_j$. Hence $f \cdot g \in \langle f_i \cdot g_j \rangle$.

The same is true for any sum of polynomials where each term has the form $f \cdot g$. This proves the claim. $\blacksquare$

Products of Ideals

Definition

If I and J are two ideals in $k[x_1, \ldots, x_n]$, then their product, denoted $I \cdot J$, is defined to be the ideal generated by all polynomials $f \cdot g$ where $f \in I$ and $g \in J$.

Thus, the product $I \cdot J$ of I and J is the set

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r : f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J, r > 0\}$$

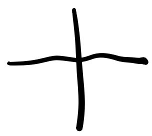
Proposition

If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I \cdot J$ is also an ideal in $k[x_1, \ldots, x_n]$. Furthermore, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $I \cdot J = \langle f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s \rangle$.

Theorem

If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

$I = \langle x \rangle$, $J = \langle y \rangle$, $I \cdot J = \langle xy \rangle$

$\mathbb{V}(I \cdot J) =$  $\mathbb{V}(I) =$  $\mathbb{V}(J) =$ 

Proof: "$\subseteq$" Let $x \in \mathbb{V}(I \cdot J)$. Then $g(x) \cdot h(x) = 0$ for all $g \in I$ and $h \in J$. If $g(x) = 0$ for all $g \in I$, then $x \in \mathbb{V}(I)$. Otherwise there exists some $g \in I$ s.t. $g(x) \neq 0$. Then it must be that $h(x) = 0$ for all $h \in J$. Then $x \in \mathbb{V}(J)$. Hence $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$.

"$\supseteq$" Let $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$. Either $g(x) = 0$ $\forall g \in I$ or $h(x) = 0$ $\forall h \in J$. Hence $g(x) \cdot h(x) = 0$ $\forall g \in I, h \in J$. Thus $f(x) = 0$ $\forall f \in I \cdot J$ and $x \in \mathbb{V}(I \cdot J)$. $\blacksquare$

Intersections of Ideals

Definition

The intersection $I \cap J$ of two ideals I and J in $k[x_1, \ldots, x_n]$ is the set of polynomials which belong to both I and J.

Intersections of Ideals

Definition

The intersection $I \cap J$ of two ideals I and J in $k[x_1, \ldots, x_n]$ is the set of polynomials which belong to both I and J.

Proposition

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

Intersections of Ideals

Definition

The intersection $I \cap J$ of two ideals I and J in $k[x_1, \dots, x_n]$ is the set of polynomials which belong to both I and J.

Proposition

If I and J are ideals in $k[x_1, \dots, x_n]$, then $I \cap J$ is also an ideal.

- $IJ \subseteq I \cap J$ $\quad f \in I \cdot J \quad \sum_{i=1}^{r} f_i g_i, \; f_i \in I, \; g_i \in J$
- Quiz: Let $I = J = \langle x, y \rangle$. Find generating sets for IJ and $I \cap J$.

Intersections of Ideals

Definition

The intersection $I \cap J$ of two ideals I and J in $k[x_1, \ldots, x_n]$ is the set of polynomials which belong to both I and J.

Proposition

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

- $IJ \subseteq I \cap J$
- Quiz: Let $I = J = \langle x, y \rangle$. Find generating sets for IJ and $I \cap J$.
- $IJ = \langle x^2, xy, y^2 \rangle$ and $I \cap J = \langle x, y \rangle$
- How to compute a set of generators for the intersection?

Intersections of Ideals

- $I \subseteq k[x_1, \ldots, x_n]$ ideal
- $f(t) \in k[t]$ polynomial in a single variable
- $fI \subseteq k[x_1, \ldots, x_n, t]$ ideal generated by $\{fh : h \in I\}$

Intersections of Ideals

- $I \subseteq k[x_1, \ldots, x_n]$ ideal
- $f(t) \in k[t]$ polynomial in a single variable
- $fI \subseteq k[x_1, \ldots, x_n, t]$ ideal generated by $\{fh : h \in I\}$

Lemma

1. *If I is generated as an ideal in $k[x_1, \ldots, x_n]$ by $p_1(x), \ldots, p_r(x)$, then $f(t)I$ is generated as an ideal in $k[x_1, \ldots, x_n, t]$ by $f(t)p_1(x), \ldots, f(t)p_r(x)$.*
2. *If $g(x, t) \in f(t)I$ and a is any element of the field k, then $g(x, a) \in I$.*

Proof: 1) Any polynomial $g(x,t) \in f(t) \cdot I$ can be expressed as a sum of terms of the form $h(x,t) \cdot f(t) \cdot p(x)$ for $h(x,t) \in k[x_1, \dots, x_n, t]$ and $p \in I$. Since $p \in I$ and I is generated by $p_1, \dots, p_r$, then $p(x) = \sum_{i=1}^{r} q_i(x) \cdot p_i(x)$, when $q_i \in k[x_1, \dots, x_n]$.

$$\text{Then } h(x,t) \cdot f(t) \cdot p(x) = \sum_{i=1}^{r} \underbrace{h(x,t) \cdot q_i(x)}_{\in\, k[x_1,\dots,x_n,t]} \cdot f(t) \cdot p_i(x) \in$$

$$\in \langle f(t) \cdot p_1(x), \dots, f(t) \cdot p_r(x) \rangle.$$

Since $g(x,t)$ is a sum of such terms, then it belongs to the ideal as well.

2) If $g(x,t) \in f(t) \cdot I$, then

$$g(x,t) = \sum_{i=1}^{r} h(x,t) \cdot f(t) \cdot p_i(x).$$

$$\text{Then } g(x,a) = \sum_{i=1}^{r} \underbrace{h(x,a) \cdot f(a)}_{\in\, k[x_1,\dots,x_n]} \cdot p_i(x) \in I. \quad \blacksquare$$

Intersections of Ideals

- $I \subseteq k[x_1, \ldots, x_n]$ ideal
- $f(t) \in k[t]$ polynomial in a single variable
- $fI \subseteq k[x_1, \ldots, x_n, t]$ ideal generated by $\{fh : h \in I\}$

Lemma

1. *If I is generated as an ideal in $k[x_1, \ldots, x_n]$ by $p_1(x), \ldots, p_r(x)$, then $f(t)I$ is generated as an ideal in $k[x_1, \ldots, x_n, t]$ by $f(t)p_1(x), \ldots, f(t)p_r(x)$.*
2. *If $g(x, t) \in f(t)I$ and a is any element of the field k, then $g(x, a) \in I$.*

Theorem

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

$$I \cap J = (tI + (1 - t)J) \cap k[x_1, \ldots, x_n].$$

Proof:

* $tI + (1-t)\cdot J$ is an ideal.

"$\subseteq$" Let $f \in I \cap J$. Then $t\cdot f \in t\cdot I$ and $(1-t)\cdot f \in (1-t)\cdot J$. Hence $f = t\cdot f + (1-t)\cdot f \in tI + (1-t)\cdot J$. Since $I, J \subseteq k[x_1, \dots, x_n]$, we have $f \in (t\cdot I + (1-t)\cdot J) \cap k[x_1, \dots, x_n]$.

"$\supseteq$" Let $f \in (tI + (1-t)J) \cap k[x_1, \dots, x_n]$. Then $f(x) = g(x,t) + h(x,t)$, where $g(x,t) \in tI$ and $h(x,t) \in (1-t)\cdot J$. First we set $t=0$: Since every element of $t\cdot I$ is a multiple of t, then $g(x,0) = 0$. Hence $f(x) = h(x,0) \in J$ by the previous lemma. Similarly, setting $t=1$ gives that $f(x) = g(x,0) \in I$. Hence $f \in I \cap J$. $\blacksquare$

Intersections of Ideals

Algorithm for computing intersections of ideals:

- $I = \langle x^2y \rangle, J = \langle xy^2 \rangle$

Intersections of Ideals

Algorithm for computing intersections of ideals:

- $I = \langle x^2y \rangle, J = \langle xy^2 \rangle$
- $tI + (1-t)J = \langle tx^2y, (1-t)xy^2 \rangle = \langle tx^2y, txy^2 - xy^2 \rangle$

Intersections of Ideals

Algorithm for computing intersections of ideals:

- $I = \langle x^2 y \rangle, J = \langle xy^2 \rangle$
- $tI + (1-t)J = \langle tx^2y, (1-t)xy^2 \rangle = \langle tx^2y, txy^2 - xy^2 \rangle$
- $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ is a Groebner basis of $tI + (1-t)J$ wrt lex order with $t > x > y$

Intersections of Ideals

Algorithm for computing intersections of ideals:

- $I = \langle x^2y \rangle, J = \langle xy^2 \rangle$
- $tI + (1-t)J = \langle tx^2y, (1-t)xy^2 \rangle = \langle tx^2y, txy^2 - xy^2 \rangle$
- $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ is a Groebner basis of $tI + (1-t)J$ wrt lex order with $t > x > y$
- Quiz: What is a generating set of $I \cap J$?

Intersections of Ideals

Algorithm for computing intersections of ideals:

- $I = \langle x^2y \rangle, J = \langle xy^2 \rangle$
- $tI + (1-t)J = \langle tx^2y, (1-t)xy^2 \rangle = \langle tx^2y, txy^2 - xy^2 \rangle$
- $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ is a Groebner basis of $tI + (1-t)J$ wrt lex order with $t > x > y$
- Quiz: What is a generating set of $I \cap J$?
- Elimination Theorem: $\{x^2y^2\}$ is a Groebner basis of $tI + (1-t)J \cap \mathbb{Q}[x,y]$
- $I \cap J = \langle x^2y^2 \rangle$

Least Common Multiple

Definition

A polynomial $h \in k[x_1, \dots, x_n]$ is called a least common multiple of $f, g \in k[x_1, \dots, x_n]$ and denoted $h = \mathrm{LCM}(f, g)$ if

1. f divides h and g divides h.
2. h divides any polynomial which both f and g divide.

Least Common Multiple

Definition

A polynomial $h \in k[x_1, \ldots, x_n]$ is called a least common multiple of $f, g \in k[x_1, \ldots, x_n]$ and denoted $h = \mathrm{LCM}(f, g)$ if

1. f divides h and g divides h.
2. h divides any polynomial which both f and g divide.

Example

$\mathrm{LCM}(x^2y, xy^2) = x^2y^2$

Least Common Multiple

Definition

A polynomial $h \in k[x_1, \ldots, x_n]$ is called a least common multiple of $f, g \in k[x_1, \ldots, x_n]$ and denoted $h = \mathrm{LCM}(f, g)$ if

1. f divides h and g divides h.
2. h divides any polynomial which both f and g divide.

Example

$\mathrm{LCM}(x^2y, xy^2) = x^2y^2$

- $f, g \in k[x_1, \ldots, x_n]$
- $f = cf_1^{a_1} \cdots f_r^{a_r}, g = c'g_1^{b_1} \cdots g_s^{b_s}$ factorizations into distinct irreducible polynomials
- for $1 \leq i \leq l$, f_i is a constant multiple of g_i and for all $i, j > l$, f_i is not a constant multiple of g_j
- $\mathrm{LCM}(f, g) = f_1^{\max(a_1,b_1)} \ldots f_l^{\max(a_l,b_l)} g_{l+1}^{b_{l+1}} \cdots g_s^{b_s} \cdot f_{l+1}^{a_{l+1}} \cdots f_r^{a_r}$

Least Common Multiple

Proposition

1. *The intersection $I \cap J$ of two principal ideals $I, J \subseteq k[x_1, \ldots, x_n]$ is a principal ideal.*
2. *If $I = \langle f \rangle, J = \langle g \rangle$ and $I \cap J = \langle h \rangle$, then*

$$h = LCM(f, g).$$

Least Common Multiple

Proposition

1. *The intersection* $I \cap J$ *of two principal ideals* $I, J \subseteq k[x_1, \ldots, x_n]$ *is a principal ideal.*
2. *If* $I = \langle f \rangle, J = \langle g \rangle$ *and* $I \cap J = \langle h \rangle$*, then*
$$h = LCM(f, g).$$

Algorithm for computing the least common multiple of two polynomials:

- $f, g \in k[x_1, \ldots, x_n]$
- compute $\langle f \rangle \cap \langle g \rangle$
- any generator of it is $\mathrm{LCM}(f, g)$

Greatest Common Divisor

Definition

Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a greatest common divisor of f and g, and denoted $h = \mathrm{GCD}(f, g)$, if

1. h divides f and g.
2. If p is any polynomial which divides both f and g, then p divides h.

Definition

Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a greatest common divisor of f and g, and denoted $h = \mathrm{GCD}(f, g)$, if

1. h divides f and g.
2. If p is any polynomial which divides both f and g, then p divides h.

Proposition

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

$$LCM(f, g) \cdot GCD(f, g) = fg.$$

Greatest Common Divisor

$$\mathrm{GCD}(f, g) = \frac{fg}{\mathrm{LCM}(f, g)}$$

Greatest Common Divisor

$$\mathrm{GCD}(f,g) = \frac{fg}{\mathrm{LCM}(f,g)}$$

Algorithm for computing the greatest common divisor:

1. compute $\mathrm{LCM}(f,g)$
2. divide it into fg by using the division algorithm

Greatest Common Divisor

$$\mathrm{GCD}(f,g) = \frac{fg}{\mathrm{LCM}(f,g)}$$

Algorithm for computing the greatest common divisor:

1. compute $\mathrm{LCM}(f,g)$
2. divide it into fg by using the division algorithm

Recall that f_{red} is the polynomial that satisfies $\langle f_{red}\rangle = \sqrt{\langle f\rangle}$.
Last time we stated:

$$f_{red} = \frac{f}{\mathrm{GCD}(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n})}.$$

Now we have an algorithm for computing f_{red}.

Intersections of Ideals

Theorem

If I and J are ideals in $k[x_1, \dots, x_n]$, then $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

Proof: "$\subseteq$" Since $I \cdot J \subseteq I \cap J$. Hence $\mathbb{V}(I \cap J) \subseteq \mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

"$\supseteq$" Let $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$. Then $x \in \mathbb{V}(I)$ or $x \in \mathbb{V}(J)$. Thus either $f(x) = 0$ $\forall f \in I$ or $f(x) = 0$ for all $f \in J$. Hence $f(x) = 0$ $\forall f \in I \cap J$ and $x \in \mathbb{V}(I \cap J)$. $\blacksquare$

Intersections of Ideals

Theorem

If I and J are ideals in $k[x_1, \dots, x_n]$, then $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

- the intersection of two ideals corresponds to the same variety as the product
- why bother with the intersection?
- the product of radical ideals need not be a radical ideal

Intersections of Ideals

Theorem

If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$.

- the intersection of two ideals corresponds to the same variety as the product
- why bother with the intersection?
- the product of radical ideals need not be a radical ideal

Proposition

If I, J are any ideals, then

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Zariski closure and quotients of ideals

Zariski closure

For $S \subseteq k^n$, define

$$\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in S\}.$$

This set is an ideal.

Zariski closure

For $S \subseteq k^n$, define

$$\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in S\}.$$

This set is an ideal.

Proposition

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

Proof: Let W be a variety containing S: $S \subseteq W \Rightarrow$
$I(W) \subseteq I(S) \Rightarrow \underbrace{\mathbb{V}(\mathbb{I}(W))}_{\overset{\shortparallel}{W}} \supseteq \mathbb{V}(\mathbb{I}(S))$
since W is a variety.

Hence $\mathbb{V}(\mathbb{I}(S)) \subseteq W$ and the result follows. $\blacksquare$

Zariski closure

For $S \subseteq k^n$, define

$$\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in S\}.$$

This set is an ideal.

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

For $S \subseteq k^n$, define

$$\mathbb{I}(S) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in S\}.$$

This set is an ideal.

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 $\mathbb{V}(\mathbb{I}(S))$.

Quiz: Let S be the x-axis without the point $(0, 0)$ inside $\mathbb{R}^2$. What is the Zariski closure of S?

Zariski closure

Claim: $\mathbb{I}(\overline{S}) = \mathbb{I}(S)$

- $S \subseteq \overline{S} \implies \mathbb{I}(\overline{S}) \subseteq \mathbb{I}(S)$
- $f \in \mathbb{I}(S)$ implies $S \subseteq \mathbb{V}(f)$. Since $\overline{S}$ is the smallest variety containing S, we have $S \subseteq \overline{S} \subseteq \mathbb{V}(f)$. Finally $f \in \mathbb{I}(\mathbb{V}(f)) \subseteq \mathbb{I}(\overline{S})$.

Zariski closure

Theorem

Let k be an algebraically closed field. Suppose $V = \mathbb{V}(f_1, \ldots, f_s) \subseteq k^n$ and let $\pi_l : k^n \to k^{n-l}$ be projection onto the last $n - l$ components. If I_l is the lth elimination ideal $I_l = \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n]$, then $\mathbb{V}(I_l)$ is the Zariski closure of $\pi_l(V)$.

Proof: We want to show that $\mathbb{V}(I_e) = \mathbb{V}(\mathbb{I}(\pi_e(V)))$.

"$\supseteq$" We know from earlier that $\pi_e(V) \subseteq \mathbb{V}(I_e)$. Since $\mathbb{V}(\mathbb{I}(\pi_e(V)))$ is the smallest variety containing $\pi_e(V)$, then $\mathbb{V}(\mathbb{I}(\pi_e(V))) \subseteq \mathbb{V}(I_e)$.

"$\subseteq$" Let $f \in \mathbb{I}(\pi_e(V))$, i.e. $f(a_{e+1}, \dots, a_n) = 0$ for all $(a_{e+1}, \dots, a_n) \in \pi_e(V)$. Considered as an element of $k[x_1, \dots, x_n]$, we have $f(a_1, \dots, a_n) = 0$ for all $(a_1, \dots, a_n) \in V$. By Hilbert's Nullstellensatz, $\exists m > 0$ s.t. $f^m \in \langle f_1, \dots, f_s \rangle$. This implies $f^m \in \langle f_1, \dots, f_s \rangle \cap k[x_{e+1}, \dots, x_n] = I_e$. Thus $f \in \sqrt{I_e}$. Hence $\mathbb{I}(\pi_e(V)) \subseteq \sqrt{I_e}$. It follows $\mathbb{V}(I_e) = \mathbb{V}(\sqrt{I_e}) \subseteq \mathbb{V}(\mathbb{I}(\pi_e(V)))$. $\blacksquare$

Conclusion

Today:

- 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

Next time:

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