Illustrating Hilbert's Nullstellensatz

Timothy Cho

UC Irvine, MATH 195

30 November 2023

Motivation: Why do Algebraic Geometry?

Motivation: Why do Algebraic Geometry?

- It's cool

Motivation: Why do Algebraic Geometry?

- It's cool
- Historical: shapes/patterns $\implies$ equations

Motivation: Why do Algebraic Geometry?

- It's cool
- Historical: shapes/patterns $\implies$ equations
- Algebraic geometry: shapes/patterns $\iff$ equations

Motivation: Why do Algebraic Geometry?

- It's cool
- Historical: shapes/patterns $\implies$ equations
- Algebraic geometry: shapes/patterns $\iff$ equations
- Connections: analysis, topology, commutative algebra, etc.

Roots of Polynomials

Find the real roots of $(x^2 + 4y^2 - 4)^2 \in \mathbb{R}[x, y]$.

Roots of Polynomials

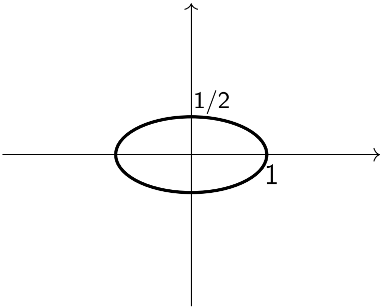
Find the real roots of $(x^2 + 4y^2 - 4)^2 \in \mathbb{R}[x, y]$.

$$(x^2 + 4y^2 - 4)^2 = 0 \implies x^2 + 4y^2 - 4 = 0 \implies x^2 + 4y^2 = 4$$

Roots of Polynomials

Find the real roots of $(x^2 + 4y^2 - 4)^2 \in \mathbb{R}[x, y]$.

$$(x^2 + 4y^2 - 4)^2 = 0 \implies x^2 + 4y^2 - 4 = 0 \implies x^2 + 4y^2 = 4$$



Algebraic Varieties

Definition

Let k be a field, and let $S \subseteq k[x_1, \ldots, x_n]$. The *algebraic variety* of S is the set

$$\mathbb{V}(S) := \{x \in k^n : f(x) = 0 \text{ for all } f \in S\}.$$

Similarly, $V \subseteq k^n$ is an *algebraic set* if $V = \mathbb{V}(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$.

Algebraic Varieties

Definition

Let k be a field, and let $S \subseteq k[x_1, \ldots, x_n]$. The *algebraic variety* of S is the set

$$\mathbb{V}(S) := \{x \in k^n : f(x) = 0 \text{ for all } f \in S\}.$$

Similarly, $V \subseteq k^n$ is an *algebraic set* if $V = \mathbb{V}(S)$ for some $S \subseteq k[x_1, \ldots, x_n]$.

Advantage: points $\iff$ pictures $\iff$ shapes
Disadvantages: hard to work with

Another Example

Let $S = \{(x^2 + y^2 - 4)(x - 1), (x^2 + y^2 - 4)(y - 1)\} \subseteq \mathbb{R}[x, y]$.
What is $\mathbb{V}(S) \subseteq \mathbb{R}^2$?

Another Example

Let $S = \{(x^2 + y^2 - 4)(x - 1), (x^2 + y^2 - 4)(y - 1)\} \subseteq \mathbb{R}[x, y]$.
What is $\mathbb{V}(S) \subseteq \mathbb{R}^2$?

$$\begin{cases} (x^2 + y^2 - 4)(x - 1) = 0 \\ (x^2 + y^2 - 4)(y - 1) = 0 \end{cases}$$

Another Example

Let $S = \{(x^2 + y^2 - 4)(x - 1), (x^2 + y^2 - 4)(y - 1)\} \subseteq \mathbb{R}[x, y]$.
What is $\mathbb{V}(S) \subseteq \mathbb{R}^2$?

$$\begin{cases} (x^2 + y^2 - 4)(x - 1) = 0 \\ (x^2 + y^2 - 4)(y - 1) = 0 \end{cases}$$

$$\implies 0 = (x^2 + y^2 - 4)(x - 1) = (x^2 + y^2 - 4)(y - 1)$$

$$\implies x^2 + y^2 = 4 \text{ or } (x, y) = (1, 1)$$

Another Example

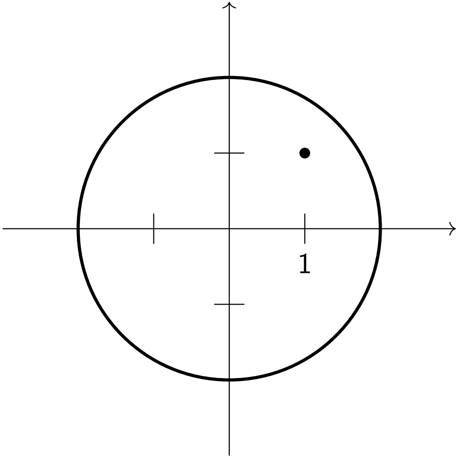


Figure: $\mathbb{V}\Big((x^2+y^2-4)(x-1),(x^2+y^2-4)(y-1)\Big)$

Ideals

Motivation: “the other way around”

Ideals

Motivation: "the other way around"

Definition

Let k be a field, and let $V \subseteq k^n$. The *ideal* of V to be the set

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

Ideals

Motivation: "the other way around"

Definition

Let k be a field, and let $V \subseteq k^n$. The *ideal* of V to be the set

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

Proposition

Let k be a field, and let $V \subseteq k^n$. Then $\mathbb{I}(V)$ is an ideal in $k[x_1, \ldots, x_n]$.

Ideals

Motivation: "the other way around"

Definition

Let k be a field, and let $V \subseteq k^n$. The *ideal* of V to be the set

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

Proposition

Let k be a field, and let $V \subseteq k^n$. Then $\mathbb{I}(V)$ is an ideal in $k[x_1, \ldots, x_n]$.

Advantage: we understand ideals!

Computing Ideals

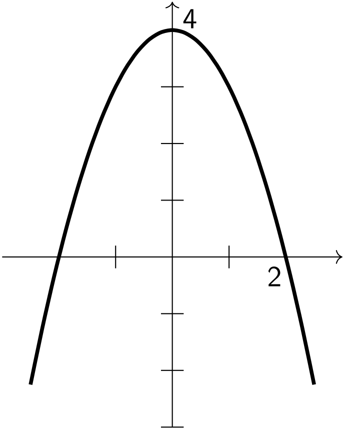


Figure: $V \subseteq \mathbb{R}^2$

What is $\mathbb{I}(V)$?

Computing Ideals

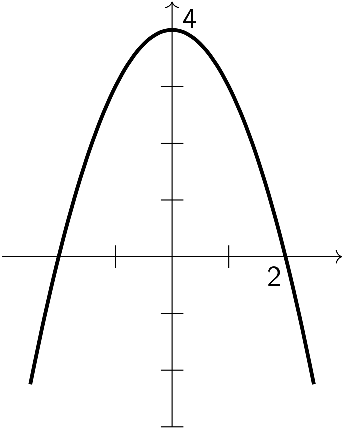


Figure: $V \subseteq \mathbb{R}^2$

What is $\mathbb{I}(V)$?

$$V = \{(x, y) \in \mathbb{R}^2 : x^2 + y - 4 = 0\}.$$

Computing Ideals

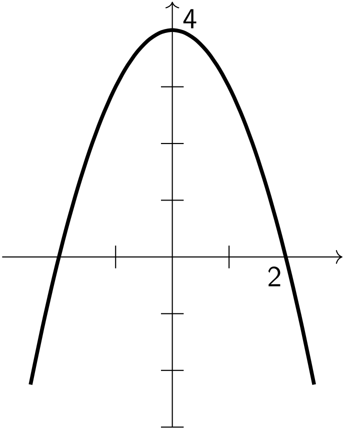


Figure: $V \subseteq \mathbb{R}^2$

What is $\mathbb{I}(V)$?

$V = \{(x, y) \in \mathbb{R}^2 : x^2 + y - 4 = 0\}$.

$f(x, y) = g(x, y)(x^2 + y - 4)$
vanishes for all $g(x, y) \in \mathbb{R}[x, y]$

Computing Ideals

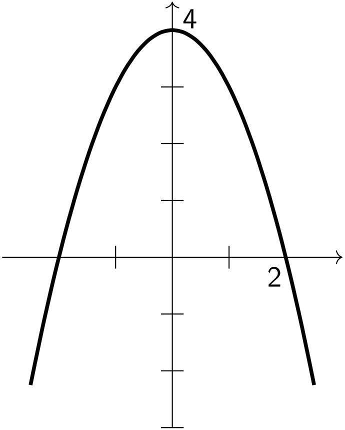


Figure: $V \subseteq \mathbb{R}^2$

What is $\mathbb{I}(V)$?

$V = \{(x, y) \in \mathbb{R}^2 : x^2 + y - 4 = 0\}$.

$f(x, y) = g(x, y)(x^2 + y - 4)$
vanishes for all $g(x, y) \in \mathbb{R}[x, y]$

$$\mathbb{I}(V) = \left\langle x^2 + y - 4 \right\rangle .$$

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$
Input	$S \subseteq k[x_1, \ldots, x_n]$	$V \subseteq k^n$

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$
Input	$S \subseteq k[x_1, \ldots, x_n]$	$V \subseteq k^n$
Output	$\mathbb{V}(S) \subseteq k^n$	$\mathbb{I}(V) \trianglelefteq k[x_1, \ldots, x_n]$

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$
Input	$S \subseteq k[x_1, \ldots, x_n]$	$V \subseteq k^n$
Output	$\mathbb{V}(S) \subseteq k^n$	$\mathbb{I}(V) \trianglelefteq k[x_1, \ldots, x_n]$
Advantages	Very visual	Easy to manipulate

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$
Input	$S \subseteq k[x_1, \ldots, x_n]$	$V \subseteq k^n$
Output	$\mathbb{V}(S) \subseteq k^n$	$\mathbb{I}(V) \trianglelefteq k[x_1, \ldots, x_n]$
Advantages	Very visual	Easy to manipulate
Disadvantages	Hard to manipulate	Not visual

$\mathbb{V}$ versus $\mathbb{I}$

Let k be a field.

Attribute	$\mathbb{V}$	$\mathbb{I}$
Input	$S \subseteq k[x_1, \ldots, x_n]$	$V \subseteq k^n$
Output	$\mathbb{V}(S) \subseteq k^n$	$\mathbb{I}(V) \trianglelefteq k[x_1, \ldots, x_n]$
Advantages	Very visual	Easy to manipulate
Disadvantages	Hard to manipulate	Not visual

In an ideal world: $\mathbb{I}$ and $\mathbb{V}$ are mutually inverse

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

Proposition

Let $V \subseteq k^n$ be an algebraic set. Then $\mathbb{V}(\mathbb{I}(V)) = V$. That is, $\mathbb{V}$ is a left-inverse to $\mathbb{I}$.

Proof.

Definition-chase. $\square$

$\mathbb{V}(\mathbb{I}(V)) = \mathbb{V}$: Example

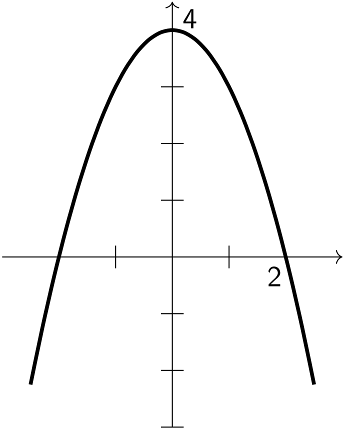


Figure: $V \subseteq \mathbb{R}^2$

Know:
$I := \mathbb{I}(V) = \langle x^2 + y - 4 \rangle$.
$\mathbb{V}(I)$: points in $\mathbb{R}^2$ that vanish on all of I

$\mathbb{V}(\mathbb{I}(V)) = \mathbb{V}$: Example

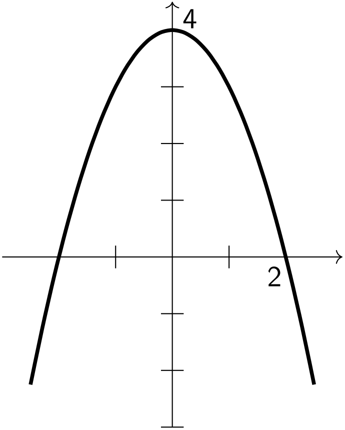


Figure: $V \subseteq \mathbb{R}^2$

Know:
$I := \mathbb{I}(V) = \langle x^2 + y - 4 \rangle$.
$\mathbb{V}(I)$: points in $\mathbb{R}^2$ that vanish on all of I — but this is just V.

$\mathbb{I}(\mathbb{V}(I)) = I$?

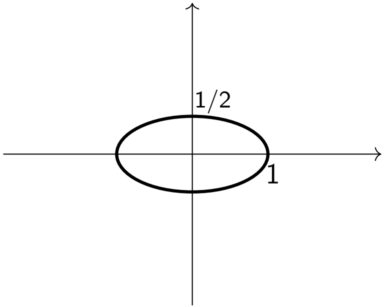


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.

$\mathbb{I}(\mathbb{V}(I)) = I$?

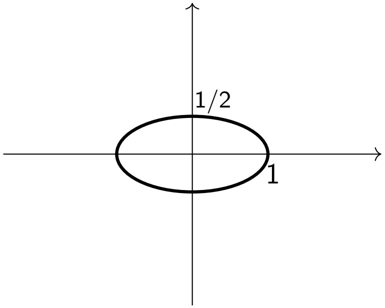


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.
$\mathbb{I}(\mathbb{V}(I))$: polynomials in $\mathbb{R}[x, y]$ that vanish on $\mathbb{V}(I)$

$$\mathbb{I}(\mathbb{V}(I)) = \langle x^2 + 4y^2 - 4 \rangle \neq I.$$

$\mathbb{I}(\mathbb{V}(I)) = I$?

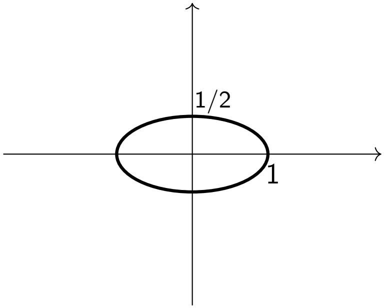


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.
$\mathbb{I}(\mathbb{V}(I))$: polynomials in $\mathbb{R}[x, y]$ that vanish on $\mathbb{V}(I)$

$$\mathbb{I}(\mathbb{V}(I)) = \langle x^2 + 4y^2 - 4 \rangle \neq I.$$

But how are $\mathbb{I}(\mathbb{V}(I))$ and I related?

Radical of an Ideal

"Set of nth roots"

Radical of an Ideal

"Set of *n*th roots"

Definition

Let $I \subseteq R$ be an ideal. Then the *radical* of I is the set

$$\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+\}.$$

Similarly, we say that an ideal I *is radical* if $I = \sqrt{I}$.

Radical of an Ideal

"Set of *n*th roots"

Definition

Let $I \subseteq R$ be an ideal. Then the *radical* of I is the set

$$\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+\}.$$

Similarly, we say that an ideal I *is radical* if $I = \sqrt{I}$.

Proposition

The radical of an ideal is an ideal.

Proposition

Prime ideals are radical.

A Rad(ical) Example

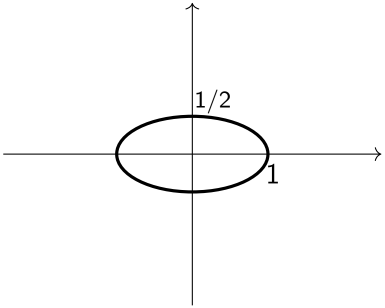


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.

$$\mathbb{I}(\mathbb{V}(I)) = \left\langle x^2 + 4y^2 - 4 \right\rangle.$$

A Rad(ical) Example

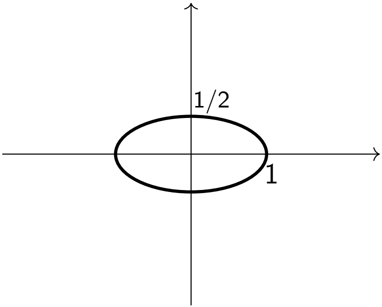


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.

$$\mathbb{I}(\mathbb{V}(I)) = \left\langle x^2 + 4y^2 - 4 \right\rangle .$$

But how are $\mathbb{I}(\mathbb{V}(I))$ and I related?

A Rad(ical) Example

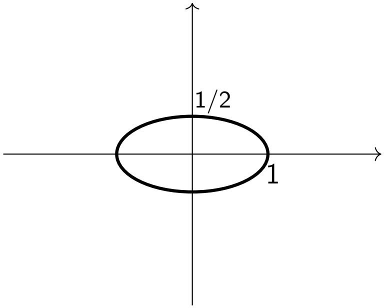


Figure: $\mathbb{V}(I)$

Let $I := \langle (x^2 + 4y^2 - 4)^2 \rangle$.

$$\mathbb{I}(\mathbb{V}(I)) = \langle x^2 + 4y^2 - 4 \rangle .$$

But how are $\mathbb{I}(\mathbb{V}(I))$ and I related?

$$\boxed{\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}}$$

The Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let k be an algebraically closed field, and let $I \trianglelefteq k[x_1, \ldots, x_n]$. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. In particular, if I is radical, then $\mathbb{I}(\mathbb{V}(I)) = I$.

The Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let k be an algebraically closed field, and let $I \trianglelefteq k[x_1, \ldots, x_n]$. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. In particular, if I is radical, then $\mathbb{I}(\mathbb{V}(I)) = I$.

Restricting to the set of radical ideals:

$$\left\{\text{algebraic sets in } k^n\right\} \longleftrightarrow \left\{\text{radical ideals of } k[x_1, \ldots, x_n]\right\}$$

The Nullstellensatz

Theorem (Hilbert's Nullstellensatz)

Let k be an algebraically closed field, and let $I \trianglelefteq k[x_1, \ldots, x_n]$. Then $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. In particular, if I is radical, then $\mathbb{I}(\mathbb{V}(I)) = I$.

Restricting to the set of radical ideals:

$$\left\{\text{algebraic sets in } k^n\right\} \longleftrightarrow \left\{\text{radical ideals of } k[x_1, \ldots, x_n]\right\}$$

The field k **must** be algebraically closed!

The Nullstellensatz, Applications

- "Fundamental theorem of algebraic geometry"

The Nullstellensatz, Applications

- "Fundamental theorem of algebraic geometry"
- Nullstellensatz: Shapes $\implies$ abstraction
- Abstraction good: equations $\iff$ shapes

The Nullstellensatz, Applications

- "Fundamental theorem of algebraic geometry"
- Nullstellensatz: Shapes $\implies$ abstraction
- Abstraction good: equations $\iff$ shapes
- Curves in weird fields: $\overline{\mathbb{F}_2}$, etc.
- Elliptic curves, number theory, FLT, etc.