Hilbert's Nullstellensatz: Computation and Proof

David Snider

Directed Reading Program
UNC Department of Mathematics

April 2022

About the Talk

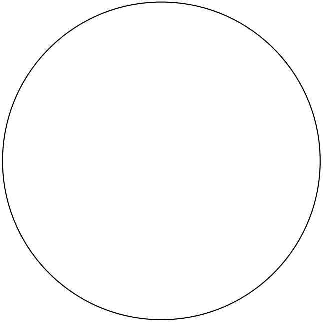
- Why Give This Talk?
  - Expose undergraduates to an area of modern research
  - Gain an appreciation for algebra's applications

About the Talk

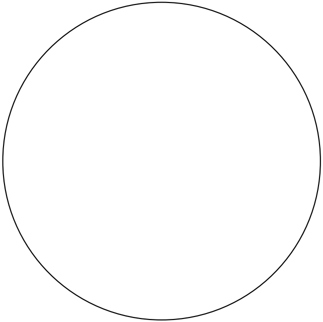
- Why Give This Talk?
  - Expose undergraduates to an area of modern research
  - Gain an appreciation for algebra's applications

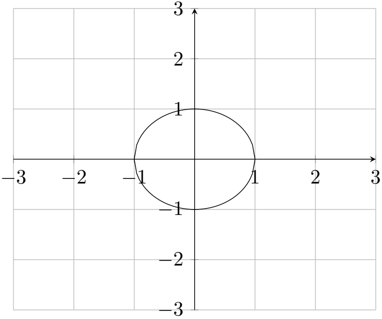
- Agenda
  - Motivation / Basic Terms (V and I)
  - Computing I(P)
  - Proof of the Nullstellensatz

Motivation

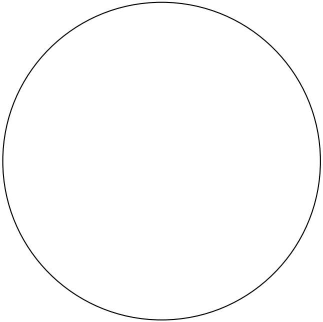


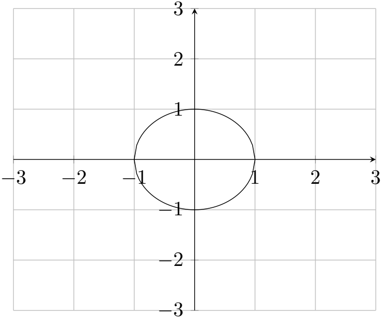
Motivation





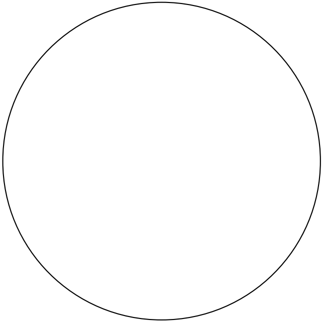
Motivation

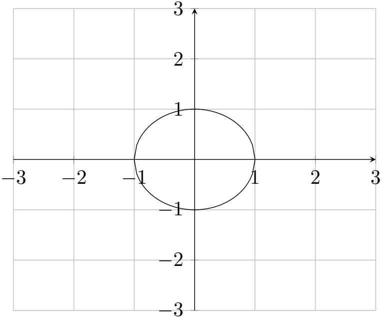




$x^2 + y^2 = 1$, or

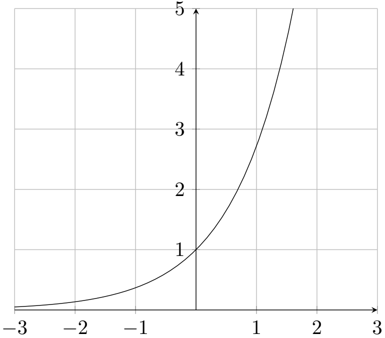
Motivation





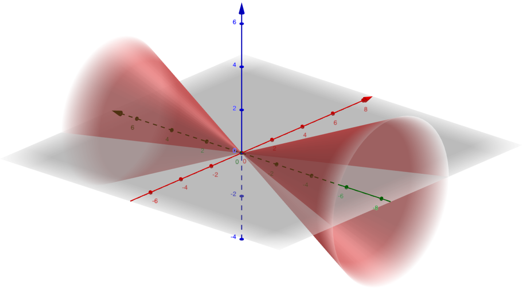
$x^2 + y^2 = 1$, or
$x^2 + y^2 - 1 = 0$

Motivation



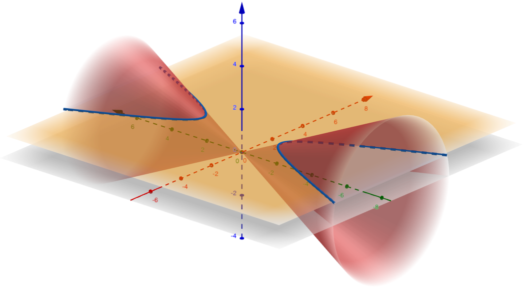
$$y - e^x = 0$$

Motivation



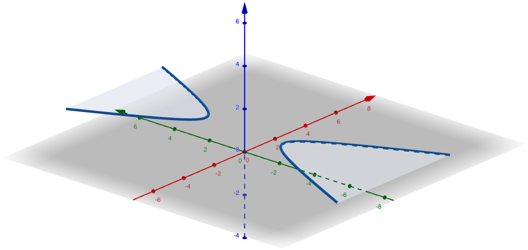
$$z^2 + x^2 - y^2 = 0$$

Motivation



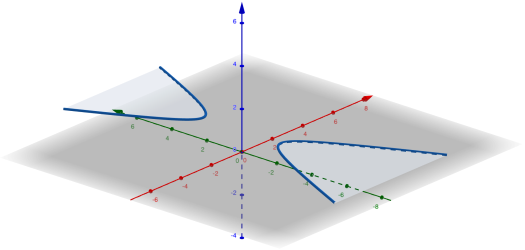
$$z^2 + x^2 - y^2 = 0$$
$$z - 1 = 0$$

Motivation



$$\{z^2 + x^2 - y^2 = 0\} \cap \{z - 1 = 0\}$$

Motivation



$$V(z^2 + x^2 - y^2, z - 1)$$

V and I

For k a field, $k[X_1, ..., X_n]$ is a ring.

V and I

For k a field, $k[X_1, ..., X_n]$ is a ring.

Eg. $p \in \mathbb{R}[X] \implies p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$, $a_i \in \mathbb{R}$

V and I

For k a field, $k[X_1, ..., X_n]$ is a ring.

Eg. $p \in \mathbb{R}[X] \implies p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$, $a_i \in \mathbb{R}$

$p \in \mathbb{R}[X, Y] \implies p(x, y) = \sum_{i,j} a_{ij} x^i y^j$ (finite sum)

V and I

In $k[X_1, ..., X_n]$, ideals are generated by a finite number of polynomials.

V and I

In $k[X_1, ..., X_n]$, ideals are generated by a finite number of polynomials.

Eg. $(x^2 + y^2 - 1) \subset \mathbb{R}[X, Y]$

V and I

In $k[X_1, ..., X_n]$, ideals are generated by a finite number of polynomials.

Eg. $(x^2 + y^2 - 1) \subset \mathbb{R}[X, Y]$

- $\{(x^2 + y^2 - 1)r : r \in \mathbb{R}[X, Y]\}$

V and I

In $k[X_1, ..., X_n]$, ideals are generated by a finite number of polynomials.

Eg. $(x^2 + y^2 - 1) \subset \mathbb{R}[X, Y]$

- $\{(x^2 + y^2 - 1)r : r \in \mathbb{R}[X, Y]\}$

Eg. $(x^2 + y^2 - 1, x - y) \subset \mathbb{R}[X, Y]$

V and I

In $k[X_1, ..., X_n]$, ideals are generated by a finite number of polynomials.

Eg. $(x^2 + y^2 - 1) \subset \mathbb{R}[X, Y]$

- $\{(x^2 + y^2 - 1)r : r \in \mathbb{R}[X, Y]\}$

Eg. $(x^2 + y^2 - 1, x - y) \subset \mathbb{R}[X, Y]$

- $\{(x^2 + y^2 - 1)r_1 + (x - y)r_2 : r_1, r_2 \in \mathbb{R}[X, Y]\}$

V and I

Definition

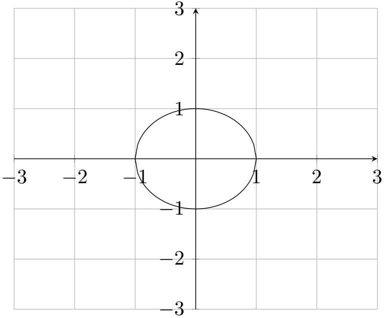
Let I be an ideal in $k[X_1, ..., X_n] =: R$.

V and I

Definition

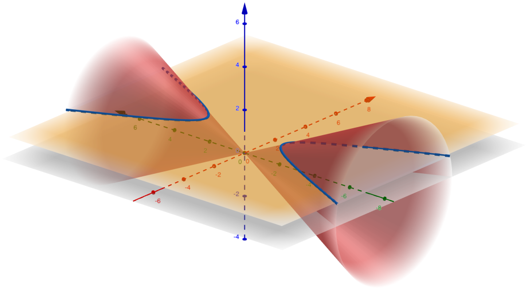
Let I be an ideal in $k[X_1, ..., X_n] =: R$.
Define $V(I) := \{x \in k^n : f(x) = 0, \forall f \in I\}$

V and I



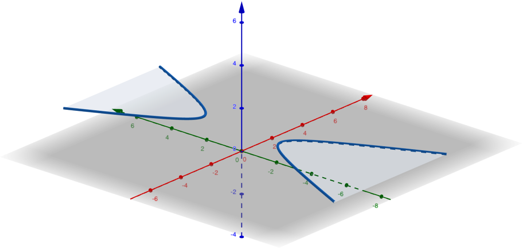
$$V(x^2 + y^2 - 1)$$

V and I



$$V(z^2 + x^2 - y^2)$$
$$V(z - 1)$$

V and I



$$V(z^2 + x^2 - y^2, z - 1)$$

V and I

Does V have an inverse?

V and I

Definition

Let $C \subset k^n$ and let $R = k[X_1, ..., X_n]$.

V and I

Definition

Let $C \subset k^n$ and let $R = k[X_1, ..., X_n]$.
Define $I(C) := \{f \in R : f(x) = 0, \forall x \in C\}$.

V and I

Definition

Let $C \subset k^n$ and let $R = k[X_1, ..., X_n]$.
Define $I(C) := \{f \in R : f(x) = 0, \forall x \in C\}$.

This is indeed an ideal.

V and I

Definition

Let $C \subset k^n$ and let $R = k[X_1, ..., X_n]$.
Define $I(C) := \{f \in R : f(x) = 0, \forall x \in C\}$.

This is indeed an ideal.
Let $f_1, f_2 \in I(C)$.
Then $\forall x \in C$, $(f_1 + f_2)(x) = 0$. So $f_1 + f_2 \in I(C)$.

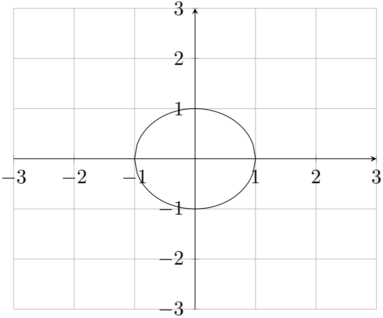
V and I

Definition

Let $C \subset k^n$ and let $R = k[X_1, ..., X_n]$.
Define $I(C) := \{f \in R : f(x) = 0, \forall x \in C\}$.

This is indeed an ideal.
Let $f_1, f_2 \in I(C)$.
Then $\forall x \in C$, $(f_1 + f_2)(x) = 0$. So $f_1 + f_2 \in I(C)$.
Let $f \in I(C)$, $r \in R$.
Then $(fr)(x) := f(x)r(x) = 0, \forall x \in I(C)$. So $fr \in I(C)$.

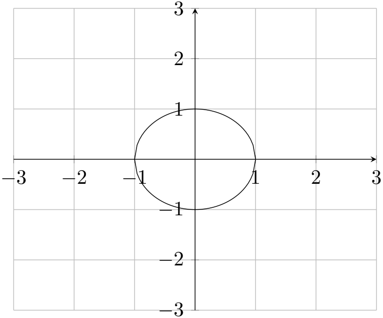
V and I



$$I(C) =$$

Let $C = \{x \in \mathbb{R}^2 : |x| = 1\}$.

V and I



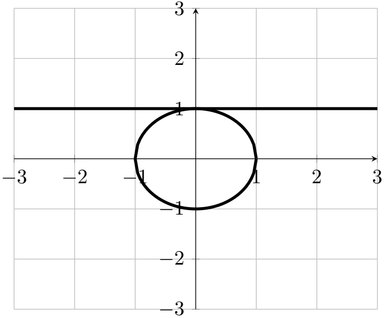
Let $C = \{x \in \mathbb{R}^2 : |x| = 1\}$.

$$I(C) = (x^2 + y^2 - 1).$$

V and I

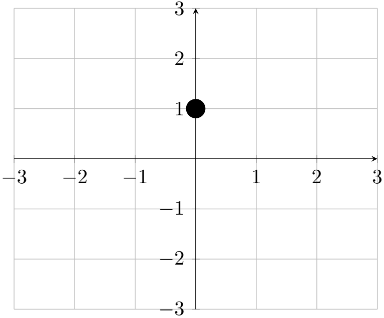
Are V and I inverses of each other?

A Computation



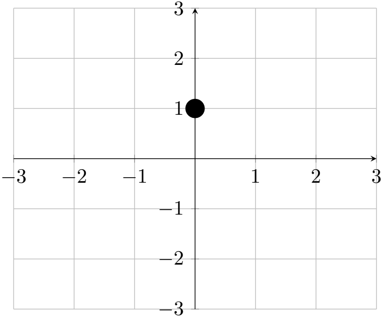
$$V(X^2 + Y^2 - 1), V(Y - 1)$$

A Computation



$$V(X^2 + Y^2 - 1, Y - 1)$$

A Computation



$$J = (X^2 + Y^2 - 1, Y - 1)$$
$$I(V(J)) = \text{?}$$

A Computation

$I(\{(0,1)\}) = ?$

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) =$

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1X + p_2(Y-1)$.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1 X + p_2(Y-1)$.
Then, $f = p_1 X + p_2(Y-1) + p_3$, where p_3 satisfies...

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1 X + p_2(Y-1)$.
Then, $f = p_1 X + p_2(Y-1) + p_3$, where p_3 satisfies...
Neither X nor $(Y-1)$ divides p_3.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1 X + p_2(Y-1)$.
Then, $f = p_1 X + p_2(Y-1) + p_3$, where p_3 satisfies...
Neither X nor $(Y-1)$ divides p_3.
$p_3 = a_0 + a_1 Y + ... + a_n Y^n$, where $(Y-1)$ does not divide p_3.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1X + p_2(Y-1)$.
Then, $f = p_1X + p_2(Y-1) + p_3$, where p_3 satisfies...
Neither X nor $(Y-1)$ divides p_3.
$p_3 = a_0 + a_1Y + ... + a_nY^n$, where $(Y-1)$ does not divide p_3.
By a MATH 578 proof, we know p_3 has a root at $y = 1$ iff $y - 1$ divides p_3.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) = 0 + 0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1 X + p_2(Y-1)$.
Then, $f = p_1 X + p_2(Y-1) + p_3$, where p_3 satisfies...
Neither X nor $(Y-1)$ divides p_3.
$p_3 = a_0 + a_1 Y + ... + a_n Y^n$, where $(Y-1)$ does not divide p_3.
By a MATH 578 proof, we know p_3 has a root at $y = 1$ iff $y - 1$ divides p_3.
So $p_3(X, 1) \neq 0$.

A Computation

$I(\{(0,1)\}) =$?
Candidate ideal: $(X, Y-1)$.
Let $f = p_1 X + p_2(Y-1)$. $f(0,1) = 0+0 = 0$. So $f \in I(\{(0,1)\})$
Let $f \notin (X, Y-1)$. Then, f cannot be written $p_1 X + p_2(Y-1)$.
Then, $f = p_1 X + p_2(Y-1) + p_3$, where p_3 satisfies...
Neither X nor $(Y-1)$ divides p_3.
$p_3 = a_0 + a_1 Y + ... + a_n Y^n$, where $(Y-1)$ does not divide p_3.
By a MATH 578 proof, we know p_3 has a root at $y=1$ iff $y-1$ divides p_3.
So $p_3(X,1) \neq 0$.
Thus, $f(0,1) = 0 + 0 + p_3(0,1) \neq 0$. So $f \notin I(\{(0,1)\})$.

A Computation

So $J = (X^2 + Y^2 - 1, Y - 1)$.
And $I(V(J)) = (X, Y - 1)$.

A Computation

So $J = (X^2 + Y^2 - 1, Y - 1)$.
And $I(V(J)) = (X, Y - 1)$.
$I(V(J)) \neq J$ by a similar proof.

A Computation

So $J = (X^2 + Y^2 - 1, Y - 1)$.
And $I(V(J)) = (X, Y - 1)$.
$I(V(J)) \neq J$ by a similar proof.

I and V are not strict inverses of each other.

A Computation

Likewise, if $J = (X^2)$,
$V(J) =$

A Computation

Likewise, if $J = (X^2)$,
$V(J) =$the y-axis.
$I(V(J)) =$

A Computation

Likewise, if $J = (X^2)$,
$V(J) =$the y-axis.
$I(V(J)) = (X)$.

A Computation

Likewise, if $J = (X^2)$,
$V(J) =$the y-axis.
$I(V(J)) = (X)$.
$X \in (X)$ but $X \notin (X^2)$.

Nullstellensatz

Let k be an algebraically closed field (such as $\mathbb{C}$).

Nullstellensatz

Let k be an algebraically closed field (such as $\mathbb{C}$).

- a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

Nullstellensatz

Let k be an algebraically closed field (such as $\mathbb{C}$).

- a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

- b) Let $J \subset A$ be an ideal, $J \neq (1)$; then $V \neq \emptyset$.
  - Weak Nullstellensatz

Nullstellensatz

Let k be an algebraically closed field (such as $\mathbb{C}$).

- a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.
- b) Let $J \subset A$ be an ideal, $J \neq (1)$; then $V \neq \emptyset$.
  - Weak Nullstellensatz
- c) For any $f \in I(V(J))$, $\exists n \in \mathbb{N}$ such that $f^n \in J$.
  - Strong Nullstellensatz

Reid, p. 63

Nullstellensatz

In an algebraically closed field,

- If a polynomial is non-constant, then it has a zero (FTA).
- If the ideal generated by a set of polynomials is not the ideal of a constant, then the vanishing set of those polynomials is nonempty (Weak NSS).

Nullstellensatz

(a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

- Given M, use $\phi : k \to k[X_1, ..., X_n] \to k[X_1, ..., X_n]/M$

Nullstellensatz

(a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

- Given M, use $\phi : k \to k[X_1, ..., X_n] \to k[X_1, ..., X_n]/M$
- Hard Fact: ϕ is an isomorphism.

Nullstellensatz

(a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

- Given M, use $\phi : k \to k[X_1, ..., X_n] \to k[X_1, ..., X_n]/M$
- Hard Fact: ϕ is an isomorphism.
- $X_i \mapsto b_i$. Let $a_i = \phi^{-1}(b_i)$. Then $X_i - a_i \in \ker f_2 = M$.

Nullstellensatz

(a) Every maximal ideal of the polynomial ring $A = k[X_1, ...X_n]$ is ... $I(\{(c_1, ..., c_n)\})$ for some $(c_1, ..., c_n) \in k^n$.

- Given M, use $\phi : k \to k[X_1, ..., X_n] \to k[X_1, ..., X_n]/M$
- Hard Fact: ϕ is an isomorphism.
- $X_i \mapsto b_i$. Let $a_i = \phi^{-1}(b_i)$. Then $X_i - a_i \in \ker f_2 = M$.
- Thus, $(X_1 - a_1, ..., X_n - a_n) \subset M$, and thus $= M$.

Nullstellensatz

(b) Let $J \subset A$ be an ideal, $J \neq (1)$; then $V \neq \emptyset$. (Weak Nullstellensatz)

- $J \neq R \implies \exists M$ maximal ideal w/ $J \subset M$.

Nullstellensatz

(b) Let $J \subset A$ be an ideal, $J \neq (1)$; then $V \neq \emptyset$. (Weak Nullstellensatz)

- $J \neq R \implies \exists M$ maximal ideal w/ $J \subset M$.
- $V(M) = \{P\}$, and $J \subset M$, so $V(J) \ni P$.

Nullstellensatz

(c) For any $J \subset A$, $I(V(J)) = \sqrt{J}$. (Strong Nullstellensatz)

- Rabinowitsch Trick
- Look it up on Wikipedia!

Thank You!

Acknowledgements:

- Hunter Dinkins, my DRP Mentor
- The DRP Committee

Citation

Miles Reid. *Undergraduate Algebraic Geometry*. Cambridge University Press, Cambridge, 1989.