# Algebraic Geometry

## An Introduction with Hilbert's Nullstellensatz

Maxwell Goldberg

Rutgers University

December 2023

# What is Algebraic Geometry

Algebraic geometry is the field of math concerned with using algebraic techniques to solve questions about geometry.

We will look at *classical* algebraic geometry, the study of solutions of multivariate polynomials.

# Setting the Stage

What operations can we do with multivariate polynomials?

- Addition, subtraction, multiplication; what about division?

# Setting the Stage

What operations can we do with multivariate polynomials?

- Addition, subtraction, multiplication; what about division?

## Definition

A **ring** is a set $R$ equipped with two operations, referred to as addition and multiplication, such that addition, subtraction, and multiplication are defined on $R$, but not necessarily division. *Note: We will be assuming all rings are commutative.*

## Remark

A ring in which division is allowed is called a field.

# Setting the Stage

What operations can we do with multivariate polynomials?

- Addition, subtraction, multiplication; what about division?

**Definition**

A **ring** is a set $R$ equipped with two operations, referred to as addition and multiplication, such that addition, subtraction, and multiplication are defined on $R$, but not necessarily division. *Note: We will be assuming all rings are commutative.*

**Remark**

A ring in which division is allowed is called a field.

**Definition**

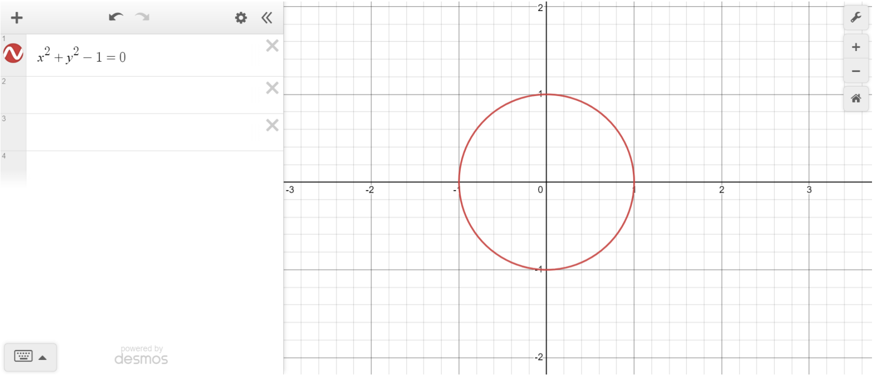
Let $R$ be a ring. Then $R[x_1, \ldots, x_n]$ polynomial ring in $n$ variables with coefficients in $R$.

# A Simple Example

Consider the solutions in $\mathbb{R}^2$ of the polynomial $f(x, y) = x^2 + y^2 - 1$.

# A Simple Example

Consider the solutions in $\mathbb{R}^2$ of the polynomial $f(x, y) = x^2 + y^2 - 1$.




- What other polynomials in $\mathbb{R}[x, y]$ *vanish* on this solution set?
- What properties can we observe about this set of polynomials?

# Varieties

## Definition

Let $k$ be a field, and let $F \subseteq k[x_1, \ldots, x_n]$. We define the variety of $F$, denoted as $V(F)$, to be the set of common zeros among polynomials in $F$. That is,

$$V(F) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in F\}.$$

In the previous example, we were examining $V(\{x^2 + y^2 - 1\})$.

# Varieties

**Definition**

Let $k$ be a field, and let $F \subseteq k[x_1, \ldots, x_n]$. We define the variety of $F$, denoted as $V(F)$, to be the set of common zeros among polynomials in $F$. That is,

$$V(F) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in F\}.$$

In the previous example, we were examining $V(\{x^2 + y^2 - 1\})$.

**Definition**

Let $k$ be a field, and let $A \subseteq k^n$. We define the ideal of $A$, denoted as $I(A)$ to be the set of functions that vanish on $A$. That is,

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

# Exploring Further

Define $C$ as the set from earlier (the circle). What properties does $I(C)$ have?

# Exploring Further

Define $C$ as the set from earlier (the circle). What properties does $I(C)$ have?

- *Closure Under Addition:* If $f, g \in I(S)$, then $f + g \in S$.
- *Absorption:* If $f \in I(S)$ and $c$ is any polynomial in $k[x_1, \ldots, x_n]$, then $cf \in I(S)$.

# Exploring Further

Define $C$ as the set from earlier (the circle). What properties does $I(C)$ have?

- *Closure Under Addition:* If $f, g \in I(S)$, then $f + g \in S$.
- *Absorption:* If $f \in I(S)$ and $c$ is any polynomial in $k[x_1, \ldots, x_n]$, then $cf \in I(S)$.

A subset of a ring satisfying the above properties is called an ideal.

## Definition

Let $F \subseteq k[x_1, \ldots, x_n]$. We define the ideal generated by $F$ as set of possible linear combinations of elements in $F$ with scalars in $k[x_1, \ldots, x_n]$.

# Properties

Let $k$ be a field. Let $A, B \subseteq k^n$ and $F, G \subseteq k[x_1, \dots, x_n]$.

# Properties

Let $k$ be a field. Let $A, B \subseteq k^n$ and $F, G \subseteq k[x_1, \ldots, x_n]$.

- If $F \subseteq G$, then $V(F) \supseteq V(G)$.

# Properties

Let $k$ be a field. Let $A, B \subseteq k^n$ and $F, G \subseteq k[x_1, \dots, x_n]$.

- If $F \subseteq G$, then $V(F) \supseteq V(G)$.
- If $A \subseteq B$, then $I(A) \supseteq I(B)$.

# Properties

Let $k$ be a field. Let $A, B \subseteq k^n$ and $F, G \subseteq k[x_1, \ldots, x_n]$.

- If $F \subseteq G$, then $V(F) \supseteq V(G)$.
- If $A \subseteq B$, then $I(A) \supseteq I(B)$.
- $V(k[x_1, \ldots, x_n]) = \varnothing$ and $V(\varnothing) = k^n$

# Properties

Let $k$ be a field. Let $A, B \subseteq k^n$ and $F, G \subseteq k[x_1, \ldots, x_n]$.

- If $F \subseteq G$, then $V(F) \supseteq V(G)$.
- If $A \subseteq B$, then $I(A) \supseteq I(B)$.
- $V(k[x_1, \ldots, x_n]) = \varnothing$ and $V(\varnothing) = k^n$
- If $F = G$, then $V(F) = V(G)$.

## Example

Consider $A = \{(-1, 0), (1, 0)\}$ and $B = \{(1, 0)\}$. Then $x - 1 \in I(B)$, but we can see that $x - 1 \notin I(A)$.

## Remark

We will not go into detail on this, but Hilbert's Basis Theorem states that every polynomial ring over a field $k$ is finitely generated. Hence, if we have an ideal $I \subseteq k[x_1, \ldots, x_n]$, then $I = (f_1, \ldots, f_m)$.

# Combining Them

Let $k$ be an algebraically closed field, and let $A \subseteq k^n$ be any variety. How does $V(I(A))$ relate to $A$?

# Combining Them

Let $k$ be an algebraically closed field, and let $A \subseteq k^n$ be any variety. How does $V(I(A))$ relate to $A$?

$$V(I(A)) = A$$

# Combining Them

Let $k$ be an algebraically closed field, and let $A \subseteq k^n$ be any variety. How does $V(I(A))$ relate to $A$?

$$V(I(A)) = A$$

Now, let $F \subseteq k[x_1, \ldots, x_n]$. How does $I(V(F))$ relate to $F$?

# Combining Them

Let $k$ be an algebraically closed field, and let $A \subseteq k^n$ be any variety. How does $V(I(A))$ relate to $A$?

$$V(I(A)) = A$$

Now, let $F \subseteq k[x_1, \ldots, x_n]$. How does $I(V(F))$ relate to $F$?

$$I(V(F)) \supseteq F$$

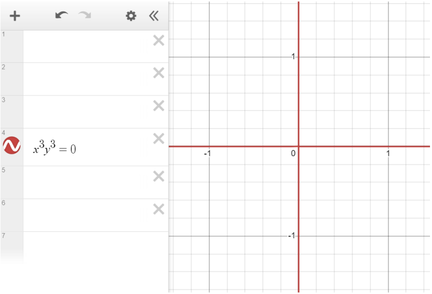
Why is this?

# Ideals of Varieties of Ideals

Consider $F = \left(x^3 y^3\right)$. What is $V(F)$?

# Ideals of Varieties of Ideals

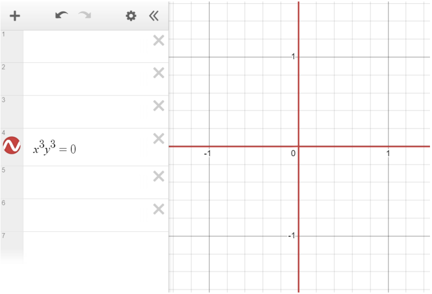
Consider $F = (x^3y^3)$. What is $V(F)$?




Now, what is $I(V(F))$?

# Ideals of Varieties of Ideals

Consider $F = (x^3y^3)$. What is $V(F)$?




Now, what is $I(V(F))$? It is everything vanishing on the set pictured above. Namely, $I(V(F)) = (xy)$.

We work more generally now. If $f^m \in I(A)$ for some variety $A$, then $f^m(a) = 0$ for each $a \in A$. So, it follows that $f(a) = 0$ for each $a \in A$, so $f \in I(A)$ as well.

# Radical Ideals

## Definition

Let $R$ be a ring, and let $I \subseteq R$ be an ideal. Then the radical of $I$, denoted as $\operatorname{Rad}(I)$ or $\sqrt{I}$, is the of all elements in $r \in R$ such that $r^m \in I$ for some $m \in \mathbb{N}$. That is,

$$\sqrt{I} = \{f \in R \mid \text{there exists } m \in \mathbb{N} \text{ such that } f^m \in I\}.$$

$I$ is called a radical ideal if $I = \sqrt{I}$.

Is it true in general that $I(V(F)) = \sqrt{F}$ for some ideal $F \subseteq k[x_1 \ldots, x_n]$?

**Hilbert's Nullstellensatz**

Let $k$ be an algebraically closed field, and let $F \subseteq k[x_1, \dots, x_n]$ be an ideal. Then $I(V(F)) = \sqrt{F}$.

The proof of this uses the *Rabinowitsch trick* along with the Weak Nullstellensatz, which we will take as given.

**Weak Nullstellensatz**

Let $k$ be an algebraically closed field, and let $F \subseteq k[x_1 \dots, x_n]$ be an ideal such that $V(F) = \varnothing$. Then $F = k[x_1, \dots, x_n]$.

# Proof of the Nullstellensatz

*Proof:* Let $F$ be an ideal in $k[x_1, \ldots, x_n]$. We have already seen a sketch of why $\sqrt{F} \subseteq V(I(F))$. The hard part is the reverse direction.

# Proof of the Nullstellensatz

*Proof:* Let $F$ be an ideal in $k[x_1, \ldots, x_n]$. We have already seen a sketch of why $\sqrt{F} \subseteq V(I(F))$. The hard part is the reverse direction.

Let $f \in I(V(F))$. We wish to show that $f \in \sqrt{F}$, we means we must show some power of $f$ is in $F$. Note that $F = (f_1, \ldots, f_m)$ by Hilbert's Basis Theorem. We now *add another variable* $x_{n+1}$ and consider $J = (f_1, \ldots, f_m, x_{n+1}f - 1) \subseteq k[x_1, \ldots, x_n, x_{n+1}]$.

# Proof of the Nullstellensatz

*Proof:* Let $F$ be an ideal in $k[x_1, \ldots, x_n]$. We have already seen a sketch of why $\sqrt{F} \subseteq V(I(F))$. The hard part is the reverse direction.

Let $f \in I(V(F))$. We wish to show that $f \in \sqrt{F}$, we means we must show some power of $f$ is in $F$. Note that $F = (f_1, \ldots, f_m)$ by Hilbert's Basis Theorem. We now *add another variable* $x_{n+1}$ and consider $J = (f_1, \ldots, f_m, x_{n+1}f - 1) \subseteq k[x_1, \ldots, x_n, x_{n+1}]$.

We claim $V(J) = \varnothing$. This is true because when all of the $f_i$'s vanish, so does $f$, but then $x_{n+1}f - 1$ is equal to $-1$ at these points and does not vanish. Hence, by the Weak Nullstellensatz, $J = k[x_1, \ldots, x_{n+1}]$.

# Proof of the Nullstellensatz

Note that $1 \in J = k[x_1, \ldots, x_{n+1}]$, so there is a linear combination of the generators of $J$ that is equal to 1. More explicitly, for some $a_1, \ldots, a_{n+1} \in k[x_1, \ldots, x_{n+1}]$,

$$1 = a_{n+1} \cdot (x_{n+1} f - 1) + \sum_{i=1}^{m} a_i f_i.$$

# Proof of the Nullstellensatz

Note that $1 \in J = k[x_1, \ldots, x_{n+1}]$, so there is a linear combination of the generators of $J$ that is equal to 1. More explicitly, for some $a_1, \ldots, a_{n+1} \in k[x_1, \ldots, x_{n+1}]$,

$$1 = a_{n+1} \cdot (x_{n+1} f - 1) + \sum_{i=1}^{m} a_i f_i.$$

Now, we use one more trick. Since these are free variables, we may substitute $x_{n+1} = 1/f$ (note that this cancels out the $x_{n+1} f - 1$ term).

# Proof of the Nullstellensatz

Note that $1 \in J = k[x_1, \ldots, x_{n+1}]$, so there is a linear combination of the generators of $J$ that is equal to 1. More explicitly, for some $a_1, \ldots, a_{n+1} \in k[x_1, \ldots, x_{n+1}]$,

$$1 = a_{n+1} \cdot (x_{n+1} f - 1) + \sum_{i=1}^{m} a_i f_i.$$

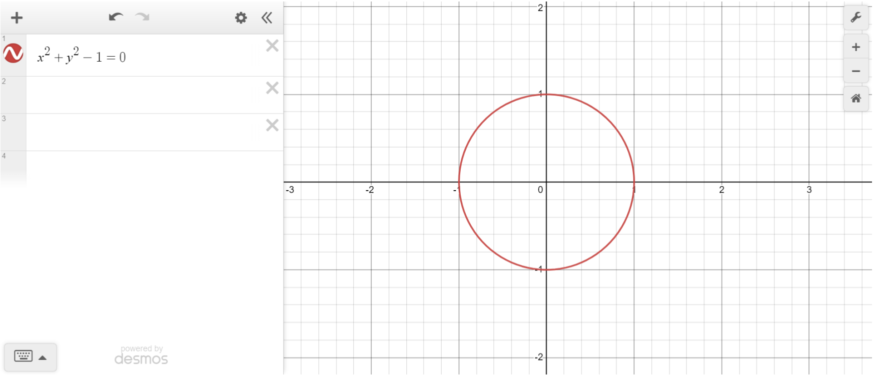
Now, we use one more trick. Since these are free variables, we may substitute $x_{n+1} = 1/f$ (note that this cancels out the $x_{n+1} f - 1$ term). Plugging this in for $x_{n+1}$ will give us rational functions on the right-hand side. So, we multiply by a high enough power of $f$, say $f^m$, to clear out all denominators. So, we obtain

$$f^m = \sum_{i=1}^{m} a_i' f_i.$$

So, we have shown that a power of $f$ lies in $F = (f_1, \ldots, f_m)$. So, $f \in \sqrt{I}$ and the Strong Nullstellensatz holds.

# Application

We return to $f(x, y) = \{x^2 + y^2 - 1\}$. We now ask again, which polynomials in $\mathbb{C}[x, y]$ vanish on $V((f))$?




We know $I(V((f)) = \sqrt{(f)}$. You can convince yourself that $\sqrt{(f)} = (f)$, so *only multiples of $f$ vanish on $V((f))$*!

# Consequences

There are many useful consequences of the Nullstellensatz.

- There is a one-to-one correspondence between radical ideals and varieties.
- There is a one-to-one correspondence between prime ideals and irreducible varieties.
- There is a one-to-one correspondence between maximal ideals in $k[x_1, \ldots, x_n]$ and points in $k^n$. Namely, for a point $a = (a_1, \ldots, a_n) \in k^n$, then $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal in $k[x_1, \ldots, x_n]$.

# Thank You!

Presentation made with help from *Algebraic Curves* by William Fulton along with various online sources like Wikipedia.

A huge thanks to my mentor Riley Guyett for all the help, explanations, and guidance this fall! And thanks to the DRP team for organizing the program this semester! :)