Basic notions in algebraic geometry

Valerio Talamanca (Università Roma Tre)

Topics in Commutative Algebra

University of Sulaimani, Sulaimani

October 14-15, 2021

Suggested book

Algebraic Curves
by
William Fulton

http://www.math.lsa.umich.edu/~wfulton/

What is algebraic geometry?

Algebraic geometry is the study of geometric structures defined by polynomials.

What is algebraic geometry?

Algebraic geometry is the study of geometric structures defined by polynomials.

(a) Descartes 1596-1650

(b) Fermat 1607-1665

Affine space and algebraic sets

Definition

Let $\mathbf{k}$ be a field. The *n*-dimensional affine space $\mathbb{A}^n(\mathbf{k})$ or simply $\mathbb{A}^n$, is

$$\mathbb{A}^n(\mathbf{k}) = \{(a_1, \dots a_n) \mid a_i \in \mathbf{k} \ i = 1, \dots, n\}$$

Affine space and algebraic sets

Algebraic geometry is the study of geometric structures defined by polynomials.
To link polynomials with set we need the following:

Definition

Let $F \in \mathbf{k}[x_1, \dots x_n]$ then the **zero locus** of F is

$$Z(F) = \{P = (a_1, \dots a_n) \in \mathbb{A}^n \mid F(P) = f(a_1, \dots a_n) = 0\}$$

Affine space and algebraic sets

Algebraic geometry is the study of geometric structures defined by polynomials.
To link polynomials with set we need the following:

Definition

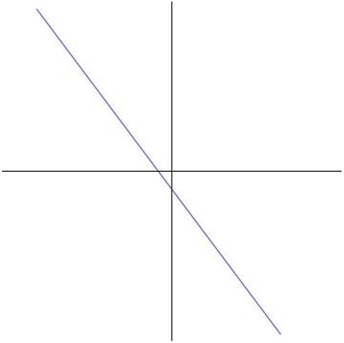
Let $f \in \mathbf{k}[x_1, \dots x_n]$ then the **zero locus** of f is

$$Z(F) = \{P = (a_1, \dots a_n) \in \mathbb{A}^n \mid F(P) = f(a_1, \dots a_n) = 0\}$$

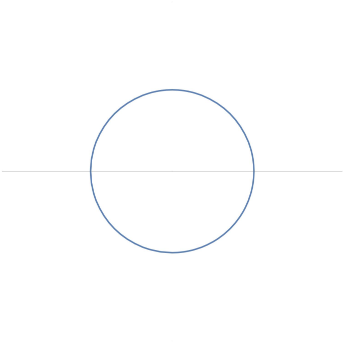
If $T \subset \mathbf{k}[x_1, \dots x_n]$ is a subset, the **zero locus** of T is

$$Z(T) = \{P \in \mathbb{A}^n \mid F(P) = 0 \ \forall F \in T\}$$

Curves in the real plane

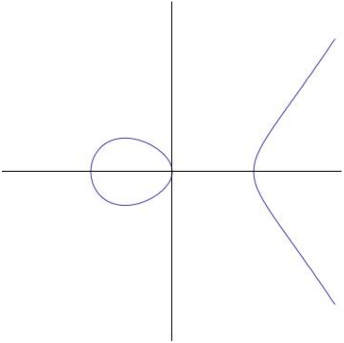


(a) $Z(3x + 4y + 2)$

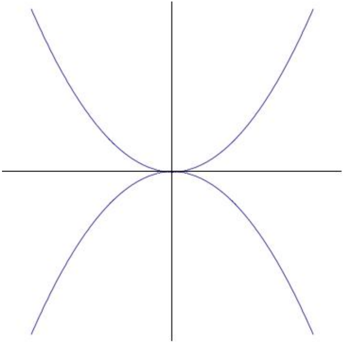


(b) $Z(x^2 + y^2 - 4)$

Curves in the real plane



(a) $Z(y^2 - x^3 + x) \subset \mathbb{A}^2(\mathbb{R})$



(b) $Z(y^2 - x^4) \subset \mathbb{A}^2(\mathbb{R})$

Curves in the real plane

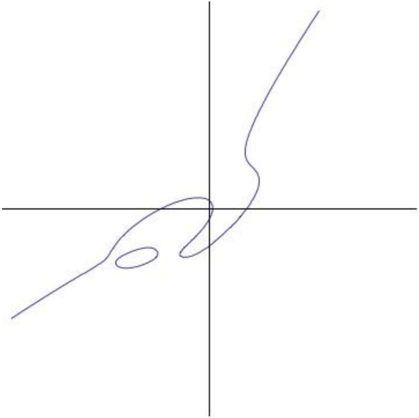


Figure: $Z(F) \subset \mathbb{A}^2(\mathbb{R})$

where $F(x, y) = ((y + x)^2 + 6(x - y)^3 - 3)(6(x + y^2 + (x - y)^2)) + 1$

Surfaces in $\mathbb{A}^3(\mathbb{R})$: Clebesch's cubic

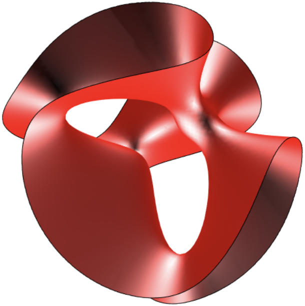


Figure: $Z(F) \subset \mathbb{A}^2(\mathbb{R})$

where $F(x, y, z) = 81(x^3 + y^3 + z^3) - 9(x^2 + y^2 + z^2) - 189(x^2y + x^2z + xy^2 + xz^2 + y^2z + yz^2) + 54xyz - 9(x + y + z) + 126(xy + xz + yz) - 1$

Surfaces in $\mathbb{A}^3(\mathbb{R})$: Barth's sestic

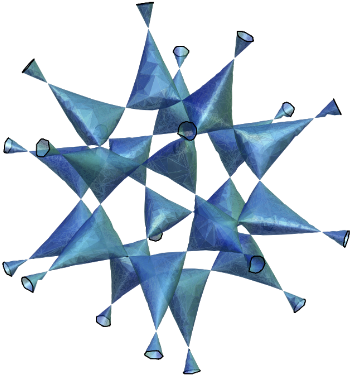


Figure: $Z(F) \subset \mathbb{A}^2(\mathbb{R})$

$F(x, y, z) = 4(\phi^2x^2 - y^2)(\phi^2y^2 - z^2)(\phi^2z^2 - x^2) - (1 + 2\phi)(x^2 + y^2 + z^2 - 1)^2$
where ϕ is the golden ratio.

Affine space and algebraic sets

We define the building blocks of our geometry as follows:

Definition

A subset Y of $\mathbb{A}^n$ is called an (affine) algebraic set if there exists a subset T of $\mathbf{k}[x_1, \dots x_n]$ such that Y is zero locus of T, i.e. $Y = Z(T)$.

A simple example: degree one polynomials

Suppose T consists of a finite number of linear polynomial, say $T = \{F_1, \dots, F_k\}$, and suppose

$$F_i(x_1, \dots, x_n) = a_{i1}x_1 + \dots + a_{kn}x_n + b_k$$

Then the algebraic set $Y = Z(T)$ is nothing else than the set of solutions of the system of linear equations:

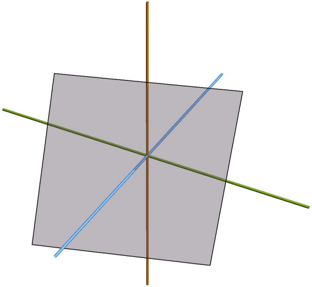
$$\begin{cases} a_{11}x_1 & + & \dots & +a_{1n}x_n & = b_1 \\ \vdots & & & \vdots & \\ a_{k1}x_1 & + & \dots & +a_{kn}x_n & = b_k \end{cases}$$

A simple example: degree one polynomials

The theorem of Rouché - Capelli, gives us the complete answer: let A be the matrix of the coefficient of the system and $\tilde{A}$ the complete matrix of the sistem. Then the system defines an non empty algebraic set X of $\mathbb{A}^n$ if and only if $\mathrm{rank}(A) = \mathrm{rank}(\tilde{A})$. Furthermore the dimension of X equals $n - \mathrm{rank}(A)$.

A simple example: degree one polynomials

The theorem of Rouché - Capelli, gives us the complete answer: let A be the matrix of the coefficient of the system and $\tilde{A}$ the complete matrix of the sistem. Then the system defines an affine subspace X of $\mathbb{A}^n$ if and only if $\operatorname{rank}(A) = \operatorname{rank}(\tilde{A})$. Furthermore the dimension of X equals $n - \operatorname{rank}(A)$. It also follows that there exists a bijection between X and $\mathbb{A}^d$ where $d = n - \operatorname{rank}(A)$.



The plane $x - 3y + z - 2 = 0$ in $\mathbb{A}^3(\mathbb{R})$

Conics in the affine plane

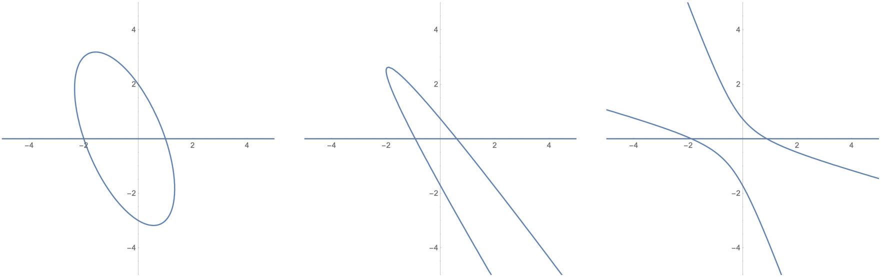
A conic $\mathcal{C} = Z(F) \subset \mathbb{A}^2$ is the zero locus of a quadratic polynomial in $\mathbf{k}[x, y]$:

$$F(x, y) = a_0 + a_1 x + a_2 y + a_3 x^2 + a_4 y^2 + a_5 xy$$

Conics in the affine plane

A conic $\mathcal{C} = Z(F)$ is the zero locus of a quadratic polynomial in $\mathbf{k}[x,\ y]$:

$$F(x,y) = a_0 + a_1x + a_2y + a_3x^2 + a_4y^2 + a_5xy$$

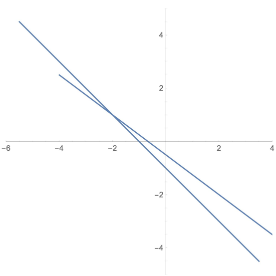


(a) $Z(3x^2+y^2+2xy + 3x + y - 6)$ (b) $Z(9x^2+4y^2+12xy+3x+4y-5)$ (c) $Z(3x^2+4y^2+12xy+3x+4y-5)$

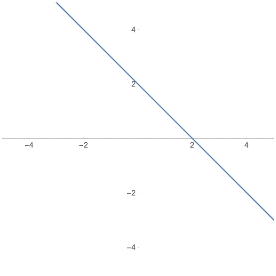
Figure: Irreducible conics in the real plane

Conics in the affine plane

But we also have the so-called degenerate conics



(a) $Z(3x^2+y^2+7xy+5x+6y+2)$



(b) $Z(x^2+y^2+2xy-4x-4y+4)$

Figure: Degenerate conics in the real plane

Classification of conics in the affine plane

How to distinguish non-degenerate conics from degenerate ones?

Degenerate vs non degenerate conics

How to distinguish non-degenerate conics from degenerate ones? Given $\mathcal{C} = Z(F)$ where $F(x, y) = a_0 + a_1x + a_2y + a_3x^2 + a_4y^2 + a_5xy$ set

$$A_F = \begin{pmatrix} a_0 & \frac{1}{2}a_1 & \frac{1}{2}a_2 \\ \frac{1}{2}a_1 & a_3 & \frac{1}{2}a_5 \\ \frac{1}{2}a_2 & \frac{1}{2}a_5 & a_4 \end{pmatrix} \qquad B_F = \begin{pmatrix} a_3 & \frac{1}{2}a_5 \\ \frac{1}{2}a_5 & a_4 \end{pmatrix}$$

- $\mathcal{C}$ is **degenerate** if and only $\operatorname{rank}(A_F) < 3$.
- $\mathcal{C}$ is **simply degenerate** if $\operatorname{rank}(A_F) = 2$.
- $\mathcal{C}$ is**doubly degenerate** if $\operatorname{rank}(A_F) = 1$.
- If $\det(B_F) \neq 0$, then $\mathcal{C}$ is called a **central conic**
- If $\det(B_F) = 0$, then $\mathcal{C}$ is called a **parabola**

Classification of conics over an algebraically closed field

First of all we need maps!

Classification of conics over an algebraically closed field

First of all we need maps!

Definition

An affine equivalence $T : \mathbb{A}^2 \to \mathbb{A}^2$ is the composition of an invertible linear transformation and a translation, so if $P = (x, y)$ and $T(P) = (x', y')$, we have

$$x' = a_{11}x + a_{12}y + b_0$$
$$y' = a_{21}x + a_{22}y + b_1$$

where $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ is an invertible matrix, and $b_0, b_1 \in k$.

Classification of conics over an algebraically closed field

First of all we need maps!

Definition

An affine equivalence $T : \mathbb{A}^2 \to \mathbb{A}^2$ is the composition of an invertible linear transformation and a translation, so if $P = (x, y)$ and $T(P) = (x', y')$, we have

$$\begin{aligned} x' &= a_{11}x + a_{12}y + b_0 \\ y' &= a_{21}x + a_{22}y + b_1 \end{aligned}$$

where $\left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)$ is an invertible matrix, and $b_0, b_1 \in k$.

Definition

Two conics $\mathcal{C}$ and $\mathcal{D}$ are **affinely equivalent** if there exists an affine transformation $T : \mathbb{A}^2 \to \mathbb{A}^2$ such that $T(\mathcal{C}) = \mathcal{D}$.

Classification of conics over an algebraically closed field

It can be shown that the properties of being non degenerate, simply degenerate and doubly degenerate are preserved under affine transformations (as it should be), as well as the property to be central.

Theorem

Let $\mathbf{k}$ *be an algebraically closed field. Any affine conic in* $\mathbb{A}^2(\mathbf{k})$ *is affinely equivalent to one (and only one) of the following:*

- $x^2 + y^2 - 1 = 0$ *center conic*
- $y^2 - x = 0$ *parabola*
- $x^2 + y^2 = 0$ *degenerate center conic*
- $y^2 - 1 = 0$ *degenerate parabola*
- $y^2 = 0$ *doubly degenerate conic*

Classification of conics over $\mathbb{R}$

Theorem

Any affine conic in $\mathbb{A}^2(\mathbb{R})$ is affinely equivalent to one (and only one) of the following:

- $x^2 + y^2 - 1 = 0$ *ellipse*
- $x^2 + y^2 + 1 = 0$ *ellipse with no real points*
- $y^2 - x = 0$ *parabola*
- $x^2 - y^2 - 1 = 0$ *iperbole*
- $x^2 - y^2 = 0$ *degenerate iperbole*
- $y^2 - 1 = 0$ *degenerate parabola*
- $y^2 + 1 = 0$ *degenerate parabola with no real points*
- $y^2 = 0$ *doubly degenerate conic*

The algebraic key fact behind the classification result

Theorem

a) *Let A be a $n \times n$ symmetric matrix with complex coefficients of rank r, then A is congruent to a matrix of the form*

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

b) *Let A be a $n \times n$ symmetric matrix with real coefficients of rank r, then A is congruent to a matrix of the form*

$$\begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Properties of affine algebraic sets

Recall that the zero locus of $T \subset \mathbf{k}[x_1, \dots x_n]$ is a subset, the zero locus of T is

$$Z(F) = \{P \in \mathbb{A}^n \mid F(P) = 0 \ \forall F \in T\}$$

and that a subset Y of $\mathbb{A}^n$ is called an (affine) algebraic set if there exists a subset T of $\mathbf{k}[x_1, \dots x_n]$ such that Y is zero locus of T, i.e. $Y = Z(T)$. If $T = \{F\}$ the ideal generated by f is denoted by (F) and the relative zero locus by $Z(F)$.
Immediate properties

- $Z(0) = \mathbb{A}^n(\mathbf{k})$
- $Z(1) = \emptyset$
- If $T \subseteq S$ the $Z(S) \subseteq Z(T)$

Properties of algebraic sets

Z1) If $\mathfrak{a}$ is the ideal generated by $T \subset \mathbf{k}[x_1, \ldots, x_n]$ then $Z(T) = Z(\mathfrak{a})$.

Proof Since $T \subseteq \mathfrak{a}$ one has $Z(\mathfrak{a}) \subseteq Z(T)$. Suppose $P \in Z(T)$, then $H(P) = 0$ for all $H \in T$. Let G be an element of $\mathfrak{a}$ then G is of the form $G = F_1 H_1 + \ldots F_n H_n$ with $H_i \in T$. Then

$$G(P) = (F_1 H_1 + \ldots F_n H_n)(P) = F_1(P) H_1(P) + \ldots F_n(P) H_n(P) = 0$$

and so $P \in Z(\mathfrak{a})$ so $Z(T) \subseteq Z(\mathfrak{a})$.

Properties of algebraic sets

Z2) Let $\{\mathfrak{a}_\alpha\}_{\alpha \in A}$ be any collection of ideals. Set $T = \bigcup_{\alpha \in A} \mathfrak{a}_\alpha$. Then $Z(T) = \bigcap_{\alpha \in A} Z(I)$.

Proof Let $P \in Z(T)$. Given any $F \in \mathfrak{a}_\alpha$ we have $F(P) = 0$, and so $P \in Z(\mathfrak{a}_\alpha)$, since α is arbitrary we have $P \in \bigcap_{\alpha \in A} Z(\mathfrak{a}_\alpha)$, hence we have $Z(T) \subseteq \bigcap_{\alpha \in A} Z(\mathfrak{a})$.
Next suppose $P \in \bigcap_{\alpha \in A} Z(\mathfrak{a}_\alpha)$. Let $F \in \bigcup_{\alpha \in A} \mathfrak{a}_\alpha$. Then $F \in \mathfrak{a}_\alpha$ for some α. Hence $F(P) = 0$, because $P \in \bigcap_{\alpha \in A} Z(\mathfrak{a}_\alpha)$, thus $P \in Z(\mathfrak{a})$. Hence we have $\bigcap_{\alpha \in A} Z(\mathfrak{a}_\alpha) \subseteq Z(T)$

Thus the intersection of any family of algebraic sets is an algebraic set

Properties of algebraic sets

Z3) Let $\mathfrak{a}, \mathfrak{b}$ be two ideals in $\mathbf{k}[x_1, \dots x_n]$. Then $Z(\mathfrak{a}) \cup Z(\mathfrak{b}) = Z(\mathfrak{a}\mathfrak{b})$.

Proof Since $\mathfrak{a}\mathfrak{b}$ is contained in both $\mathfrak{a}$ and $\mathfrak{b}$, we have that $Z(\mathfrak{a}\mathfrak{b})$ contains both $Z(\mathfrak{a})$ and $Z(\mathfrak{b})$, therefore $Z(\mathfrak{a}) \cup Z(\mathfrak{b}) \subseteq Z(\mathfrak{a}\mathfrak{b})$.
To prove that $Z(\mathfrak{a}\mathfrak{b}) \subseteq Z(\mathfrak{a}) \cup Z(\mathfrak{b})$ suppose $P \notin Z(\mathfrak{a}) \cup Z(\mathfrak{b})$, then P does not belong to either $Z(\mathfrak{a})$ or $Z(\mathfrak{b})$. Thus we can find $F \in Z(\mathfrak{a})$ and $G \in Z(\mathfrak{b})$, such that

$$F(P) \neq 0 \neq G(P).$$

Hence $(FG)(P) = F(P)G(P) \neq 0$ and so P does not belong to $Z(\mathfrak{a}\mathfrak{b})$, which yields that $Z(\mathfrak{a}\mathfrak{b}) \subseteq Z(\mathfrak{a}) \cup Z(\mathfrak{b})$.

The ideal associated to a subset of $\mathbb{A}^n(\mathbf{k})$

Given X a subset of $\mathbb{A}^n(\mathbf{k})$ we define $\mathrm{I}(X)$ the **ideal associated to X** by setting

$$I(X) = \{F \in \mathbf{k}[x_1, \dots x_n] \mid F(P) = 0 \ \forall P \in X\}$$

Exercises

Verify that $\mathrm{I}(X)$ is an ideal.

We have to show the following

- Given $F, G \in \mathrm{I}(X)$, then $F \pm G \in \mathrm{I}(X)$.
- Given $F \in \mathrm{I}(X)$ and $h \in \mathbf{k}[x_1, \dots x_n]$ then $FG \in \mathrm{I}(X)$.

The ideal associated to a subset of $\mathbb{A}^n(\mathbf{k})$

Given X a subset of $\mathbb{A}^n(\mathbf{k})$ we define $\mathrm{I}(X)$ the **ideal associated to X** by setting

$$\mathrm{I}(X) = \{F \in \mathbf{k}[x_1, \dots x_n] \mid F(P) = 0 \ \forall P \in X\}$$

Let us verify that $\mathrm{I}(X)$ is in effect an ideal of $\mathbf{k}[x_1, \dots x_n]$
We have to show the following

- Given $F, G \in \mathrm{I}(X)$, then $F \pm G \in \mathrm{I}(X)$.
- Given $F \in \mathrm{I}(X)$ and $H \in \mathbf{k}[x_1, \dots x_n]$ then $FH \in \mathrm{I}(X)$.

To prove the first assertion note that by definition $F(P) = G(P) = 0$ for all $P \in X$. So

$$(F \pm G)(P) = F(P) \pm G(P) = 0 \pm 0 = 0$$

for all $P \in X$.

The ideal associated to a subset of $\mathbb{A}^n(\mathbf{k})$

Given X a subset of $\mathbb{A}^n(\mathbf{k})$ we define $\mathrm{I}(X)$ the **ideal associated to X** by setting

$$\mathrm{I}(X) = \{F \in \mathbf{k}[x_1, \ldots x_n] \mid F(P) = 0 \ \forall P \in X\}$$

Let us verify that $\mathrm{I}(X)$ is in effect an ideal of $\mathbf{k}[x_1, \ldots x_n]$
We have to show the following

- Given $F, G \in \mathrm{I}(X)$, then $F \pm G \in \mathrm{I}(X)$.
- Given $F \in \mathrm{I}(X)$ and $H \in \mathbf{k}[x_1, \ldots x_n]$ then $FG \in \mathrm{I}(X)$.

To prove the first assertion note that by definition $F(P) = G(P) = 0$ for all $P \in X$. So

$$(F \pm G)(P) = F(P) \pm G(P) = 0 \pm 0 = 0$$

for all $P \in X$. To prove the second assertion note that $(FH)(P) = F(P)H(P)$ so if $F \in \mathrm{I}(X)$ and $P \in X$, we have

$$(FH)(P) = F(P)H(P) = 0H(P) = 0.$$

and so $FH \in \mathrm{I}(X)$.

The ideal associated to a subset of $\mathbb{A}^n(\mathbf{k})$

Given X a subset of $\mathbb{A}^n(\mathbf{k})$ we define $\mathsf{I}(X)$ the **ideal associated to X** by setting

$$\mathsf{I}(X) = \{F \in \mathbf{k}[x_1, \dots x_n] \mid F(P) = 0 \ \forall P \in X\}$$

Immediate properties

A1) $\mathsf{I}(\emptyset) = \mathbf{k}[x_1, \dots x_n]$

A2) $X \subseteq Y \implies \mathsf{I}(Y) \subseteq \mathsf{I}(X)$

Further elementary properties

A3) $\mathrm{I}(Z(\mathfrak{a})) \supseteq \mathfrak{a}$ for any ideal $\mathfrak{a}$ in $\mathbf{k}[x_1, \ldots x_n]$

If $F \in \mathfrak{a}$ then by definition $F(P) = 0$ for all $P \in Z(\mathfrak{a})$ and so $F \in \mathrm{I}(Z(\mathfrak{a}))$.

The equality does not hold in general. For example take

$$\mathfrak{a} = (x^2) \subset \mathbf{k}[x, y].$$

Then

$$Z(\mathfrak{a}) = \{(0, y) \in A^2(\mathbf{k})\}.$$

Therefore x belongs to $\mathrm{I}(Z(\mathfrak{a}))$, but x does not belong to (x^2).

Further elementary properties

A4) $Z(\mathrm{I}(X)) \supseteq X$ for any $X \subset \mathbb{A}^n(\mathbf{k})$.

If $P \in X$, then $F(P) = 0$ for all $F \in I(X)$ and hence $P \in Z(I(X))$

Also in this case the equality does not hold in general. For example take

$$X = \{(x, y) \in \mathbb{A}^2(\mathbf{k}) \ : \ x - y = 0 \text{ and } x \neq 0\}$$

Then each $F \in \mathrm{I}(X)$ is a multiple of $x - y$, for it has to vanish on all the point of X i.e. if we substitute $x = y$ in f it has an infinite number of zeros and hence it has to be identically zero, i.e. $x - y$ divides f. Thus $\mathrm{I}(X) = (x - y)$, and it follows that

$$Z(\mathrm{I}(X)) = \{(x, y) \in \mathbb{A}^2(\mathbf{k}) \ : \ x - y = 0\} \supset X$$

Further elementary properties

Exercises

- $\mathsf{I}(Z(\mathsf{I})T))) = \mathsf{I}(T)$
- $Z(\mathsf{I}(Z(X))) = Z(X)$

Question

Is it true that $\mathsf{I}(\mathbb{A}^n(\mathbf{k})) = (0)$*?*

Question

Is it true that $\mathsf{I}(\mathbb{A}^n(\mathbf{k})) = (0)$*?*

Equivalently is the zero polynomial the only polynomial that vanishes identically on all $\mathbb{A}^n(\mathbf{k})$?

Question

Is it true that $\mathsf{I}(\mathbb{A}^n(\mathbf{k})) = (0)$*?*

Equivalently is the zero polynomial the only polynomial that vanishes identically on all $\mathbb{A}^n(\mathbf{k})$?

It depends on the field $\mathbf{k}$. For simplicity we start with $\mathbb{A}^1(\mathbf{k})$. If k is a finite field of characteristic p, then by Fermat's little theorem $a^p = a$ for all $a \in \mathbf{k}$, hence the polynomial $x^p - x$ vanishes identically on $\mathbb{A}^1(\mathbf{k})$ and so $x^p - x \in \mathsf{I}(\mathbb{A}^1(\mathbf{k}))$.

Question

Is it true that $\mathrm{I}(\mathbb{A}^n(\mathbf{k})) = (0)$*?*

Equivalently is the zero polynomial the only polynomial that vanishes identically on all $\mathbb{A}^n(\mathbf{k})$?

It depends on the field $\mathbf{k}$. For simplicity we start with $\mathbb{A}^1(\mathbf{k})$. If k is a finite field of characteristic p, then by Fermat's little theorem $a^p = a$ for all $a \in \mathbf{k}$, hence the polynomial $x^p - x$ vanishes identically on $\mathbb{A}^1(\mathbf{k})$ and so $x^p - x \in \mathrm{I}(\mathbb{A}^1(\mathbf{k}))$.

If $n > 1$ then

$$F(x_1, \dots, x_n) = (x_1^p - x_1)(x_2^p - x_2) \cdots (x_n^p - x_n)$$

vanishes on all $\mathbb{A}^n(\mathbf{k})$, and so belongs to $\mathrm{I}(\mathbb{A}^n(\mathbf{k}))$.

Question

Is it true that $\mathrm{I}(\mathbb{A}^n(\mathbf{k})) = (0)$?

Equivalently is the zero polynomial the only polynomial that vanishes identically on all $\mathbb{A}^n(\mathbf{k})$?

It depends on the field $\mathbf{k}$. For simplicity we start with $\mathbb{A}^1(\mathbf{k})$. If k is a finite field of characteristic p, then by Fermat's little theorem $a^p = a$ for all $a \in \mathbf{k}$, hence the polynomial $x^p - x$ vanishes identically on $\mathbb{A}^1(\mathbf{k})$ and so $x^p - x \in \mathrm{I}(\mathbb{A}^1(\mathbf{k}))$.

If $n > 1$ then

$$F(x_1, \dots, x_n) = (x_1^p - x_1)(x_2^p - x_2) \cdots (x_n^p - x_n)$$

vanishes on all $\mathbb{A}^n(\mathbf{k})$, and so belongs to $\mathrm{I}(\mathbb{A}^n(\mathbf{k}))$.

On the other hand if $\mathbf{k}$ is infinite $\mathrm{I}(\mathbb{A}^n(\mathbf{k})) = (0)$.

Question

If $\mathfrak{a}$ *is a proper ideal of* $\mathbf{k}[x_1, \dots x_n]$ *is it true that* $Z(\mathfrak{a})$ *is non void?*

Question

If $\mathfrak{a}$ is a proper ideal of $\mathbf{k}[x_1, \dots x_n]$ is it true that $Z(\mathfrak{a})$ is non void?

Also in this case the answer depends on the field $\mathbf{k}$.

Question

If $\mathfrak{a}$ is a proper ideal of $\mathbf{k}[x_1, \dots x_n]$ is it true that $Z(\mathfrak{a})$ is non void?

Also in this case the answer depends on the field $\mathbf{k}$. For example if we take $\mathbf{k} = \mathbb{Q}$ and $\mathfrak{a}(x^2 + y^2 + 1)$ then $Z(\mathfrak{a})$ is empty.

Question

If $\mathfrak{a}$ is a proper ideal of $\mathbf{k}[x_1, \dots x_n]$ is it true that $Z(\mathfrak{a})$ is non void?

Also in this case the answer depends on the field $\mathbf{k}$. For example if we take $\mathbf{k} = \mathbb{Q}$ and $\mathfrak{a}(x^2 + y^2 + 1)$ then $Z(\mathfrak{a})$ is empty.

On the other hand if $\mathbf{k}$ is algebraically closed then we will see shortly that $Z(\mathfrak{a})$ is always non empty whenever $\mathfrak{a}$ is a proper ideal of $\mathbf{k}[x_1, \dots x_n]$.
From now on we assume that $\mathbf{k}$ is algebraically closed.

Hilbert's Basis Theorem

Theorem

Every ideal in $\mathbf{k}[x_1, \dots x_n]$ *is finitely generated.*

Hilbet's Basis Theorem

Theorem

Every ideal in $\mathbf{k}[x_1, \ldots x_n]$ is finitely generated.

This implies that given any ideal $\mathfrak{a} \subset \mathbf{k}[x_1, \ldots x_n]$ we have that there exist $F_1, \ldots, F_d$ such that $\mathfrak{a} = (F_1, \ldots F_d)$ and hence

$$Z(\mathfrak{a}) = Z(F_1, \ldots F_d)$$

so we have only to check the vanishing of a finite number of polynomials.

Hilbert's Nullenstellensazt (strong form)

Given an ideal in $\mathfrak{a}$ in $\mathbf{k}[x_1, \dots x_n]$ we define $\sqrt{\mathfrak{a}}$, the **radical of $\mathfrak{a}$** to be

$$\sqrt{\mathfrak{a}} = \left\{ F \in \mathbf{k}[x_1, \dots x_n] \ : \ F^d \in \mathfrak{a} \text{ for some } d \geq 1 \right\}$$

Furthermore an ideal $\mathfrak{a}$ is called a **radical** ideal if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

Hilbert's Nullenstellensazt (strong form)

Given an ideal in $\mathfrak{a}$ in $\mathbf{k}[x_1, \ldots x_n]$ we define $\sqrt{\mathfrak{a}}$, the **radical of $\sqrt{\mathfrak{a}}$** to be

$$\sqrt{\mathfrak{a}} = \left\{ F \in \mathbf{k}[x_1, \ldots x_n] \ : \ F^d \in \mathfrak{a} \text{ for some } d \geq 1 \right\}$$

Theorem

Let $\mathbf{k}$ be an algebraically closed field. If $\mathfrak{a}$ is an ideal of $\mathbf{k}[x_1, \ldots x_n]$ then $\mathrm{I}(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$

Hilbert's Nullenstellensazt (strong form)

Given an ideal in $\mathfrak{a}$ in $\mathbf{k}[x_1, \dots x_n]$ we define $\sqrt{\mathfrak{a}}$, the **radical of** $\sqrt{\mathfrak{a}}$ to be

$$\sqrt{\mathfrak{a}} = \left\{ F \in \mathbf{k}[x_1, \dots x_n] \;:\; F^d \in \mathfrak{a} \text{ for some } d \geq 1 \right\}$$

Theorem

Let $\mathbf{k}$ *be an algebraically closed field. If* $\mathfrak{a}$ *is an ideal of* $\mathbf{k}[x_1, \dots x_n]$ *then* $\mathrm{I}(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$

One inclusion is evident namely:

$$\mathrm{I}(Z(\mathfrak{a})) \supseteq \sqrt{\mathfrak{a}}$$

for if $F \in \sqrt{\mathfrak{a}}$, then $f^d \in \mathfrak{a}$, and hence $f^d(P) = 0$ for all $P \in Z(\mathfrak{a})$ but this clearly imples $F(P) = 0$ for all $P \in Z(\mathfrak{a})$.

Hilbert's Nullenstellensatz (strong form)

Let $\mathcal{A}_n$ denote the set of all algebraic subset of $\mathbb{A}^n(\mathbf{k})$ and by $\mathcal{R}_n$ the set of radical ideal in $\mathbf{k}[x_1, \ldots x_n]$. As a consequence of Hilbert's Nullenstellensatz we have that the map

$$\begin{aligned} \mathcal{R}_n &\longrightarrow \mathcal{A}_n \\ \mathfrak{a} &\longmapsto Z(\mathfrak{a}) \end{aligned}$$

is a bijection whose inverse is

$$\begin{aligned} \mathcal{A}_n &\longrightarrow \mathcal{R}_n \\ X &\longmapsto \mathrm{I}(X) \end{aligned}$$

Hilbert's Nullenstellensatz (strong form)

Let $\mathcal{A}_n$ denote the set of all algebraic subset of $\mathbb{A}^n(\mathbf{k})$ and by $\mathcal{R}_n$ the set of radical ideal in $\mathbf{k}[x_1, \ldots x_n]$. As a consequence of Hilbert's Nullenstellensatz we have that the map

$$\begin{aligned} \mathcal{R}_n &\longrightarrow \mathcal{A}_n \\ \mathfrak{a} &\longmapsto Z(\mathfrak{a}) \end{aligned}$$

is a bijection whose inverse is

$$\begin{aligned} \mathcal{A}_n &\longrightarrow \mathcal{R}_n \\ X &\longmapsto \mathrm{I}(X) \end{aligned}$$

In particular if $\mathfrak{a}$ is a proper ideal, then also $\sqrt{\mathfrak{a}}$ is a proper ideal and so $Z(\mathfrak{a})$ is a proper subset of $\mathbb{A}^n(\mathbf{k})$. In particular $Z(\mathfrak{a})$ is not void.

The topology defined by algebraic sets

Recall that we can define a topology on a set X by means of its closed subset: i.e. if we a family $\mathcal{C} = \{C_\alpha\}_{\alpha \in A}$, they define a topology on X (and the C_i's are the closed sets in this topology) if and only if the family enjoys the following properties:

- $X \in \mathcal{C}$ and $\emptyset \in \mathcal{C}$.
- The union of a finite number of elements of $\mathcal{C}$ is an element of $\mathcal{C}$.
- The interesection of an arbitrary collection of elements in $\mathcal{C}$ is an element of $\mathcal{C}$.

The topology defined by algebraic sets

Recall that we can define a topology on a set X by means of its closed subset: i.e. if we a family $\mathcal{C} = \{C_\alpha\}_{\alpha \in A}$, they define a topology on X (and the C_i's are the closed sets in this topology) if and only if the family enjoys the following properties:

- $X \in \mathcal{C}$ and $\emptyset \in \mathcal{C}$.
- The union of a finite number of elements of $\mathcal{C}$ is an element of $\mathcal{C}$.
- The interesection of an arbitrary collection of elements in $\mathcal{C}$ is an element of $\mathcal{C}$.

It follows that the family $\{Z(\mathfrak{a}) : \mathfrak{a} \text{ is a radical ideal in } \mathbf{k}[x_1, \ldots x_n]\}$ defines a topology on $\mathbb{A}^n(\mathbf{k})$. This topology is called the **Zariski topology** The open sets of this topology are, by definition, the complements of the algebraic sets.

Zariski Topology: an example

Let $X = \mathbb{A}^1(\mathbf{k})$ which subset are Zariski closed?

Since $\mathbf{k}[x]$ is a principal ideal domain any Zariski closed subset is of the form $Z(F)$ for some $F \in \mathbf{k}[x]$. But a polynomial of degree n has at most n distinct roots, hence all Zariski closed subset are finite subset of $\mathbb{A}^1(\mathbf{k})$.

Conversely if Z is a finite subset of $\mathbb{A}^1(\mathbf{k})$ say $Z = \{\alpha_1, \dots \alpha_n\}$ then the polynomial

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

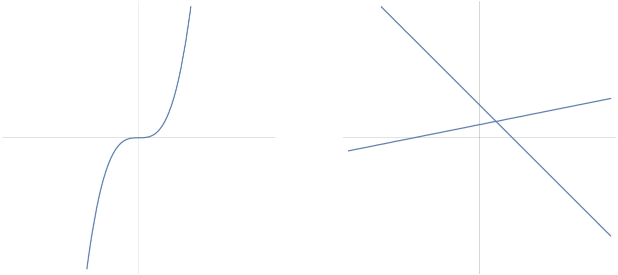
is such that $Z(F) = Z$. Thus the Zariski closed subsets coincide with the finite subsets of $\mathbb{A}^1(\mathbf{k})$, and hence the open sets are the cofinite sets, i.e. the sets whose complement is finite. In particular every open set is dense and the topology is not Hausdorff.

Irriedeucible sets

Let X be a topological space. We say that X is **irreducible** if it is not the union of two proper closed subset, and reducible otherwise.

Irriedeucible sets

Let X be a topological space. We say that X is **irreducible** if it is not the union of two proper closed subset, and reducible otherwise.



(a) $Z(y - x^3)$ (b) $Z(-2+x+x^2+7y-4xy-5y^2)$

The curve in fig. (a) is irreducible, while the curve of fig. (b) is reducible

Irrieducible sets

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements.

Proof To prove that the set of irreducible subspaces of X admits maximal elements for the inclusion relation we will use Zorn's Lemma:

Irriducible sets

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements.

The maximal elements of the set of irreducible subspace are called the **irreducible components** of X.

Proof To prove that the set of irreducible subspaces of X admits maximal elements for the inclusion relation we will use Zorn's Lemma:

Zorn's Lemma

If A is a partially ordered such that every chain in A has an upper bound in A then A contains at least one maximal element.

Irriducible sets

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements.

Proof To prove that the set of irreducible subspaces of X admits maximal elements for the inclusion relation we will use Zorn's Lemma:

Zorn's Lemma

If A is a partially ordered such that every chain in A has an upper bound in A then A contains at least one maximal element.

So let $X_1 \subset X_2 \subset \ldots \subset X_i \subset X_{i+1} \subset \ldots$ be a chain of irreducible subspace. We want to show that $\cup_i X_i$ is also irreducible, and so the chain has an upper bound.

Irriducible sets

So let $X_1 \subset X_2 \subset \ldots \subset X_i \subset X_{i+1} \subset \ldots$ be a chain of irreducible subspace. We want to show that $\cup_i X_i$ is also irreducible, and so the chain has an upper bound.

So suppose that $\cup_i X_i$ is reducible, i.e. there exists Y and Z proper closed subset of $\cup_i X_i$ such that $Y \cup Z = \cup_i X_i$. Since both Y and Z proper closed subset of $\cup_i X_i$ it exists k such that X_k is not contained in Y and h such that X_h is not contained in Z.

Irriducible sets

So let $X_1 \subset X_2 \subset \ldots \subset X_i \subset X_{i+1} \subset \ldots$ be a chain of irreducible subspace. We want to show that $\cup_i X_i$ is also irreducible, and so the chain has an upper bound.

So suppose that $\cup_i X_i$ is reducible, i.e. there exists Y and Z proper closed subset of $\cup_i X_i$ such that $Y \cup Z = \cup_i X_i$. Since both Y and Z proper closed subset of $\cup_i X_i$ it exists k such that X_k is not contained in Y and h such that X_h is not contained in Z.

But then for all $n \geq \max\{h, k\}$ we have that X_n is not contained in Y or Z. But then $X_n \cap Y$ and $X_n \cap Z$ are two closed proper subset of X_n such that their union is X_n, contradicting the irreducibility of X_n

So we can use Zorn's Lemma.

Irrieducible sets

So we were proving

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements.

and we have established the existence of maximal elements.

Irriducible sets

So we were proving

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation, and X is the union of this maximal elements.

and we have established the existence of maximal elements.

Next note that the maximal elements are actually closed, this follows from

Fact

If $Y \subset X$ is irreducible then also its closure is irreducible.

For if Z and W are proper closed subset of $\overline{Y}$ such that $Z \cup W = Y$, then $Z \cap Y$ and $W \cap Y$ are proper closed subset of Y such that $(Z \cap Y) \cup (W \cap Y) = Y$

Irriducible sets

So we were proving

Theorem

Let X be a topological space. The set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements.

and we have established the existence of maximal elements.
Next note that the maximal elements are actually closed, this follows from

Fact

If $Y \subset X$ is irreducible then also its closure is irreducible.

For if Z and W are proper closed subset of $\overline{Y}$ such that $Z \cup W = Y$, then $Z \cap Y$ and $W \cap Y$ are proper closed subset of Y such that $(Z \cap Y) \cup (W \cap Y) = Y$
Finally the union of the maximal elements is all of X because the set consisting of one point are clearly irreducible and hence contained in a maximal irreducible subspace.

Irrieducible sets

Lemma

If X is irreducible then every open subset is dense and irreducible

Irriducible sets

Lemma

If X is irreducible then every open subset is dense and irreducible

Proof Suppose U is a non empty open subset of X. If $U = X$ there is nothing to prove, so we suppose that U is properly contained in X. Let $Y = X \setminus U$, then $\overline{U}$ and Y are two closed subset such that

$$X = \overline{U} \cup Y.$$

Irrieducible sets

Lemma

If X is irreducible then every non empty open subset is dense and irreducible

Proof Suppose U is a non empty open subset of X. If $U = X$ there is nothing to prove, so we suppose that U is properly contained in X. Let $Y = X \setminus U$, then $\overline{U}$ and Y are two closed subset such that

$$X = \overline{U} \cup Y.$$

It follows that one of them must not be proper, as X is irreducible. Since U is non empty and is not all of X we have that Y is a proper closed subset of X, and hence $\overline{U} = X$, i.e. U is dense in X.

Irriducible sets

Corollary

If X is irreducible then X is not Hausdorff

Irriducible sets

Corollary

If X is irreducible then X is not Hausdorff

Proof If Y is Hausdorff space then for every pair of points $y_1, y_2 \in Y$ there exist two open sets Y_1 and Y_2, with $y_i \in Y_i$, such that $Y_1 \cap Y_2 = \emptyset$. This cannot happen if X is irreducible as every opens set is dense and hence the intersection of any pair of open set cannot be empty.

Irriedducible sets

Proposition

If X is the union of finitely many irreducible subspace $Z_1, \ldots, Z_m$ then every irreducible components of X coincide with one of the Z_j. If, in addition, the $Z_j \not\subset Z_i$ for all $i \neq j$, then $Z_1, \ldots, Z_m$ are the irreducible components of X.

Irrieducible sets

Proposition

If X is the union of finitely many irreducible subspace $Z_1, \ldots, Z_m$ then every irreducible components of X coincide with one of the Z_j. If, in addition, the $Z_j \not\subset Z_i$ for all $i \neq j$, then $Z_1, \ldots, Z_m$ are the irreducible components of X.

Proof Let Z be an irreducible component of X. Then

$$Z = (Z_1 \cap Z) \cup \ldots \cup (Z \cap Z_m)$$

and hence, being Z irreducible and maximal among irreducible, we have that Z is equal to Z_j. Thus every irreducible component is found among the Z_i, so if there is no inclusion relation among them each of them must be an irreducible component.

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

We want to characterize which algebraic set are irreducible in terms of the ideal that defines the set

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

We want to characterize which algebraic set are irreducible in terms of the ideal that defines the algebraic set

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ *is irreducible if and only* $\mathrm{I}(X)$ *is a prime ideal.*

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ is irreducible if and only $\mathrm{I}(X)$ is a prime ideal.

Proof Recall that an ideal $\mathfrak{a}$ is a prime ideal, if whenever a product ab belongs to $\mathfrak{a}$, then either $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ is irreducible if and only $\mathrm{I}(X)$ is a prime ideal.

Proof Recall that an ideal $\mathfrak{a}$ is a prime ideal, if whenever a product ab belongs to $\mathfrak{a}$, then either $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

Suppose that X is not irreducible i.e.

$$X = X_1 \cup X_2$$

with $X_i \subsetneq X$, X_i closed subset of X, $(i = 1, 2)$.

Irreducible sets in $\mathbb{A}^n(\mathbf{k})$

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ is irreducible if and only $\mathsf{I}(X)$ is a prime ideal.

Proof Recall that an ideal $\mathfrak{a}$ is a prime ideal, if whenever a product ab belongs to $\mathfrak{a}$, then either $a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

Suppose that X is not irreducible i.e.

$$X = X_1 \cup X_2$$

with $X_i \subsetneq X$, X_i closed subset of X, $(i = 1, 2)$. Then

$$\mathsf{I}(X_i) \supsetneq \mathsf{I}(X), i = 1, 2$$

So we can find $F_1 \in I(X_1) \setminus \mathsf{I}(X)$ and $F_2 \in I(X_2) \setminus \mathsf{I}(X)$.
Since $F_1 F_2$ vanishes on $X_1 \cup X_2 = X$ it follows that $F_1 F_2$ belongs to $\mathsf{I}(X)$.
yielding that $\mathsf{I}(X)$ is not a prime ideal .

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ is irreducible if and only $\mathrm{I}(X)$ is a prime ideal.

Proof So we have proven that if X is reducible then $\mathrm{I}(X)$ is not a prime ideal. To complete the proof we have to show that if $\mathrm{I}(X)$ is not a prime ideal then X is reducible.

Irriducible sets in $\mathbb{A}^n(\mathbf{k})$

Proposition

$X \subset \mathbb{A}^n(\mathbf{k})$ is irreducible if and only $\mathrm{I}(X)$ is a prime ideal.

Proof So we have proven that if X is reducible then $\mathrm{I}(X)$ is not a prime ideal. To complete the proof we have to show that if $\mathrm{I}(X)$ is not a prime ideal then X is reducible.
So suppose that $\mathrm{I}(X)$ is not a prime ideal. Then there exist F_1, F_2 with $F_i \notin \mathrm{I}(X), (i = 1, 2)$, such that $F_1 F_2 \in \mathrm{I}(X)$. Set

$$X_1 = X \cap Z(F_1) \quad \text{and} \quad X_2 = X \cap Z(F_2).$$

Then X_1 and X_2 are proper closed subsets of X such that $X_! \cup X_2 = X$.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Definition

An irreducible affine algebraic set in $\mathbb{A}^n(\mathbf{k})$ is called an **affine variety**

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Definition

An irreducible affine algebraic set in $\mathbb{A}^n(\mathbf{k})$ is called an **affine variety**

Note that if X is affine variety, then $\mathrm{I}(X)$ is prime and hence radical, and so $Z(\mathrm{I}(X)) = X$. Similarly if $\mathfrak{p}$ is a prime ideal of $\mathbf{k}[x_1, \dots x_n]$ then $\mathrm{I}(Z(\mathfrak{p})) = \mathfrak{p}$.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Definition

An irreducible affine algebraic set in $\mathbb{A}^n(\mathbf{k})$ is called an **affine variety**

Theorem

Any algebraic set in $\mathbb{A}^n(\mathbf{k})$ is the union of a finite number of affine varieties that are not contained in each other. Explicitly if $X \subset \mathbb{A}^n(\mathbf{k})$ is an algebraic set then are unique $X_1, \ldots, X_k$ affine varieties such that

$$X = X_1 \cup X_2 \cup \cdots \cup X_k.$$

and $X_i \not\subset X_j$, for all i, j with $i \neq j$.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

We need to start using the fact that $\mathbf{k}[x_1, \ldots x_n]$ is a Noetherian ring. One property of Noetherian rings is the following

Fact

Let R be a Noetherian ring. Then every non empty collection of ideals admits a maximal member.

As a consequence we have that every non empty collection of algebraic set admits a minimal element.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

We need to start using the fact that $\mathbf{k}[x_1, \ldots x_n]$ is a Noetherian ring. One property of Noetherian rings is the following

Fact

Let R be a Noetherian ring. Then every non empty collection of ideals admits a maximal member.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

We need to start using the fact that $\mathbf{k}[x_1, \dots x_n]$ is a Noetherian ring. One property of Noetherian rings is the following

Fact

Let R be a Noetherian ring. Then every non empty collection of ideals admits a maximal member.

As a consequence we have

Lemma

Every non empty collection of algebraic set admits a minimal element.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Lemma

Every non empty collection of algebraic set admits a minimal element.

To prove the lemma we can argue as follows: let $\mathcal{X}$ be a collection of algebraic set, and consider the following collection of ideals

$$\mathcal{I} = \left\{ \mathfrak{a} \subset \mathbf{k}[x_1, \dots x_n] \ : \ \mathfrak{a} = \mathrm{I}(X) \text{ for some } X \in \mathcal{X} \right\}$$

Then $\mathcal{I}$ admits a maximal member say $\mathfrak{m}$. This means that if $\mathfrak{a}$ belongs to $\mathcal{I}$ and $\mathfrak{m} \subseteq \mathfrak{a}$ then $\mathfrak{m} = \mathfrak{a}$. Set $M = Z(\mathfrak{m})$. Next recall that the map $\mathfrak{a} \mapsto Z(\mathfrak{a})$ is order reversing. Thus if $X \in \mathcal{S}$ is such that $X \subseteq M$, then

$$\mathfrak{m} = \mathrm{I}(M) \subseteq \mathrm{I}(X)$$

and so $\mathfrak{m} = \mathrm{I}(X)$, which yields $X = M$, and so X is minimal.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Theorem

Any algebraic set in $\mathbb{A}^n(\mathbf{k})$ is the union of a finite number of affine varieties that are not contained in each other. Explicitly if $X \subset \mathbb{A}^n(\mathbf{k})$ is an algebraic set then there exist $X_1, \dots X_k$ affine varieties such that

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

and $X_i \not\subset X_j$, for all i, j with $i \neq j$. Furthermore the X_i's are uniquely determined (up to the ordering).

Proof Consider the collection $\mathcal{S}$ of all algebraic subset of $\mathbb{A}^n(\mathbf{k})$ for which one cannot find a finite number of irreducible subset whose union is X. It has a minimal element X. Now clearly X is not irreducible and hence there exist X_1 and X_2 proper closed subset of X, such that $X_1 \cup X_2 = X$.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Proof Consider the collection $\mathcal{S}$ of all algebraic subset of $\mathbb{A}^n(\mathbf{k})$ for which one cannot find a finite number of irreducible subset whose union is X. It has a minimal element X. Now clearly X is not irreducible and hence there exist X_1 and X_2 proper closed subset of X, such that $X_1 \cup X_2 = X$. The minimality of X implies that X_1 and X_2 are not in $\mathcal{S}$. Therefore

$$X_1 = Y_1 \cup \ldots \cup Y_m \qquad \text{and} \qquad X_2 = Z_1 \cup \ldots \cup Z_d$$

where all the Y_i and Z_d are irreducible. But then

$$X = Y_1 \cup \ldots \cup Y_m \cup Z_1 \cup \ldots \cup Z_d$$

which is a contradiction. So every algebraic set X can be covered by a finite number of affine varieties say $X_1, \ldots, X_k$. To get the second condition, simply throw away any X_i such that $X_i \subset X_j$ for $i \neq j$.

Affine variety in $\mathbb{A}^n(\mathbf{k})$

Theorem

Any algebraic set in $\mathbb{A}^n(\mathbf{k})$ is the union of a finite number of affine varieties that are not contained in each other. Explicitly if $X \subset \mathbb{A}^n(\mathbf{k})$ is an algebraic set then there exist $X_1, \dots X_k$ affine varieties such that

$$X = X_1 \cup X_2 \cup \cdots \cup X_k$$

and $X_i \not\subset X_j$, for all i, j with $i \neq j$. Furthermore the X_i's are uniquely determined (up to the ordering).

To show uniqueness, let $X = Y_1 \cup \dots \cup Y_m$ be another such decomposition. Then $X_i = \cup_j (Y_j \cap X_i)$ so $X_i \subseteq Y_{j(i)}$ for some $j(i)$. In the same way one founds $Y_j \subseteq X_{i(j)}$, putting the two together we get

$$X_i \subseteq Y_{j(i)} \subset X_{i(j(i))}$$

but then $X_i = X_{i(j(i))}$, and so $X_i = Y_{j(i)}$. Likewise each Y_j is equal to some $X_{i(j)}$.

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Now we would like to completely determine the affine varieties in $\mathbb{A}^2(\mathbf{k})$.

Fact

Let F and G be polynomial in $\mathbf{k}[x, y]$ Suppose that F and G have no common factor. Then $Z(F) \cap Z(G)$ consist of finitely many points.

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Now we would like to completely determine the affine varieties in $\mathbb{A}^2(\mathbf{k})$.

Fact

Let F and G be polynomial in $\mathbf{k}[x, y]$ Suppose that F and G have no common factor. Then $Z(F) \cap Z(G)$ consist of finitely many points.

Proof Since F, G have no common factor in $\mathbf{k}[x, y] = \mathbf{k}[x][y]$ they also have no factor in the principal ideal domain $\mathbf{k}(x)[y]$, thus there exists $R_1, R_2 \in \mathbf{k}(x)[y]$ such that $R_1 F + R_2 G = 1$. Write

$$R_1 = \frac{N_1}{D_1} \qquad \text{and} \qquad R_2 = \frac{N_2}{D_2}$$

with $N_1 N_2 \in \mathbf{k}[x, y]$ and $D_1 D_2 \in k[x]$.
Set

$$D = D_1 D_2 \quad \text{and} \quad A_1 = D_2 N_1,\ A_2 = D_1 N_2$$

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Proof Since F, G have no common factor in $\mathbf{k}[x, y] = \mathbf{k}[x][y]$ they also have no factor in the principal ideal domain $\mathbf{k}(x)[y]$, thus there exists $R_1, R_2 \in \mathbf{k}(x)[y]$ such that $R_1 F + R_2 G = 1$. Write

$$R_1 = \frac{N_1}{D_1} \qquad \text{and} \qquad R_2 = \frac{N_2}{D_2}$$

with $N_1 N_2 \in \mathbf{k}[x, y]$ and $D_1 D_2 \in k[x]$.
Set

$$D = D_1 D_2 \quad \text{and} \quad A_1 = D_2 N_1, \; A_2 = D_1 N_2$$

Then $A_1 A_2 \in \mathbf{k}[x, y]$, and

$$D = DR_1 F + R_2 G = D\Big(\frac{N_1}{D_1} F + \frac{N_2}{D_2} G\Big) = A_1 F + A_2 G$$

Thus if $(a, b) \in Z(F, G)$, then $D(a) = 0$. But D has only finitely many zeros. Thus there are only finitely many choices for the x-coordinates of points in $Z(F, G)$, and similarly for the y-coordinates.

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Now we would like to completely determine the affine varieties in $\mathbb{A}^2(\mathbf{k})$.

Fact

Let F and G be polynomial in $\mathbf{k}[x, y]$ Suppose that F and G have no common factor. Then $Z(F) \cap Z(G)$ consist of finitely many points.

An **affine curve** in $\mathbb{A}^2(\mathbf{k})$ is an algebraic set of the form $Z(F)$ with $F \in \mathbf{k}[x, y]$ irreducible
As consequence we have that the only proper affine variety in $\mathbb{A}^2(\mathbf{k})$ are:

- Points
- Affine curves

Affine variety in $\mathbb{A}^2(\mathbf{k})$

One more consequence of

Fact

Let F and G be polynomial in $\mathbf{k}[x, y]$ Suppose that F and G have no common factor. Then $Z(F) \cap Z(G)$ consist of finitely many points.

is

Corollary

Let F belong to $k[x, y]$. Suppose that $F = \prod_{i=1}^{n} F_i^{n_i}$ is the decomposition of F into distinct irreducible factor in $k[x, y]$, then $Z(F_1)$, $\ldots$, $Z(F_n)$ are the irreducible components of $Z(F)$ and $\mathrm{I}(Z(F)) = (F_1 \cdots F_n)$.

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Fact

Let F and G be polynomial in $\mathbf{k}[x, y]$ Suppose that F and G have no common factor. Then $Z(F) \cap Z(G)$ consist of finitely many points.

Corollary

Let F belong to $k[x, y]$. Suppose that $F = \prod_{i=1}^{d} F_i^{n_i}$ is the decomposition of F into distinct irreducible factor in $k[x, y]$, then $Z(F_1), \ldots, Z(F_n)$ are the irreducible components of $Z(F)$ and $\mathrm{I}(Z(F)) = (F_1 \cdots F_n)$.

Proof: We have that every pair F_i, F_j has no component in common (as they are irreducible and distinct). So $Z(F_i) \cap Z(F_j)$ consist in a finite set points, so none of them is contained in another. Furthermore $Z(F_i)$ is irreducible for all $i's$, and

$$Z(F) = \cup_{i=1}^{d} Z(F_i).$$

It follows $Z(F_1), \ldots, Z(F_n)$ are the irreducible components of $Z(F)$.

Affine variety in $\mathbb{A}^2(\mathbf{k})$

Corollary

Let F belong to $k[x, y]$. Suppose that $F = \prod_{i=1}^{d} F_i^{n_i}$ is the decomposition of F into distinct irreducible factor in $k[x, y]$, then $Z(F_1)$, $\ldots$, $Z(F_n)$ are the irreducible components of $Z(F)$ and $\mathrm{I}(Z(F)) = (F_1 \cdots F_n)$.

Proof: We have that every pair F_i, F_j has no component in common (as they are irreducible and distinct). So $Z(F_i) \cap Z(F_j)$ consist in a finite set points, so none of them is contained in another. Furthermore $Z(F_i)$ is irreducible for all $i's$, and

$$Z(F) = \cup_{i=1}^{d} Z(F_i).$$

It follows $Z(F_1)$, $\ldots$, $Z(F_n)$ are the irreducible components of $Z(F)$. Then

$$\mathrm{I}(Z(F)) = \mathrm{I}(\cup_{i=1}^{d} Z(F_i)) = \cap_{i=1}^{d} \mathrm{I}(Z(F_i)) = \cap_{i=1}^{d} (F_i) = (F_1 \cdots F_n)$$

Polynomial functions and rational functions

Definition

Let $X \subset \mathbb{A}^n(\mathbf{k})$ be an affine variety. The quotient ring $\mathcal{O}_X = \mathbf{k}[x_1, \ldots x_n]/\operatorname{I}(X)$ is called the **coordinate ring** of X

To any element h of $\mathcal{O}_X$ we can associate a polynomial function on X, simply setting $h(P) := g(P)$, where $g \in \mathbf{k}[x_1, \ldots x_n]$ is any poynomial in $\mathbf{k}[x_1, \ldots x_n]$ that reduces to h modulo $\operatorname{I}(X)$.
Moreover $I(X)$ is a prime ideal and so $\mathcal{O}_X$ is an integral domain. Its quotient ring is denoted by $\mathbf{k}(X)$ and is called the **function field** of X.
To each $\phi \in \mathbf{k}(X)$, we can associate a **rational function** on X, i.e. a function that is not defined for every point of X but only on a dense subset. Given $P \in X$ we say that ϕ is **defined** at P if it is possible to find a "denominator" for ϕ that doesn't vanish at P, i.e. if we can write $\phi = h_1/h_2$ with $h_1, h_2 \in \mathcal{O}_X$ and $h_2(P) \neq 0$.

Polynomial functions and rational functions

So suppose that $\phi \in \mathbf{k}(X)$, is defined at $P \in X$, then we define its value $\phi(P)$, simply by setting:

$$\phi(P) = h_1(P)/h_2(P)$$

Where $\phi = h_1/h_2$ We have to check that $\phi(P)$ does not depend on the choice of h_1 and h_2. So suppose that g_1 and g_2 belonging to $\mathcal{O}_X$ are also such that $\phi = g_1/g_2$ and $h_2(P) \neq 0$. Then

$$h_1/h_2 = g_1/g_2 \Longrightarrow h_1 g_2 - g_1 h_2 \in \mathrm{I}(X)$$

Therefore

$$0=(h_1 g_2-g_1 h_2)(P)=h_1(P)g_2(P)-g_1(P)h_2(P)\Rightarrow h_1(P)/h_2(P)=g_1(P)/g_2(P)$$

Polynomial functions and rational functions

So suppose that $\phi \in \mathbf{k}(X)$, is defined at $P \in X$, then we define its value $\phi(P)$, simply by setting:

$$\phi(P) = h_1(P)/h_2(P)$$

Where $\phi = h_1/h_2$ We have to check that $\phi(P)$ does not depend on the choice of h_1 and h_2. So suppose that g_1 and g_2 belonging to $\mathcal{O}_X$ are also such that $\phi = g_1/g_2$ and $h_2(P) \neq 0$. Then

$$h_1/h_2 = g_1/g_2 \Longrightarrow h_1g_2 - g_1h_2 \in \mathrm{I}(X)$$

Therefore

$$0 = (h_1g_2 - g_1h_2)(P) = h_1(P)g_2(P) - g_1(P)h_2(P) \Rightarrow h_1(P)/h_2(P) = g_1(P)/g_2(P)$$

If $P \in X$ is a point in which ϕ is not defined then P is called a **pole** of ϕ. The set of poles of a rational function ϕ is called the pole set of ϕ and is denote by $\mathcal{P}(\phi)$.

Polynomial functions and rational functions

Example

Let $F(x, y) = y^2 - x^3 + x$ and let $\mathcal{C}$ be the associated affine curve. Consider the rational function $\phi = \frac{x}{y} \in \mathbf{k}(\mathcal{C})$ By the way in which has been presented f is regular at all point $P = (a_1, a_2)$ of $\mathbb{C}_F$ for which $a_2 \neq 0$, so it is already regular at all point but $P_0 = (0, 0)$, $P_1 = (1, 0)$, $P_2 = (-1, 0)$. On the other hand

$$f = \frac{x}{y} = \frac{x}{y}\frac{y}{y} = \frac{xy}{y^2} = \frac{xy}{x^3 - x} = \frac{y}{x^2 - 1} \mod (F)$$

showing the regularity of ϕ at P_0 (actually P_0 is a zero of f). The remaining two points are true poles of f

Note that working $\mod (F)$ means for example that

$$y^2 = x^3 - x \mod (F)$$

The local ring at a point

Recall that a ring is called **local** if it has a unique maximal ideal.

Let $X \subset \mathbb{A}^n(\mathbf{k})$ be an affine variety. Given $P \in X$ the**local ring** of X at P, is the set of all rational function on X that are defined at P and it will be denoted by $\mathcal{O}_{X,P} \subseteq \mathbf{k}(X)$.

The local ring at a point

Recall that a ring is called **local** if it has a unique maximal ideal.

Let $X \subset \mathbb{A}^n(\mathbf{k})$ be an affine variety. Given $P \in X$ the **local ring** of X at P, is the set of all rational function on X that are defined at P and it will be denoted by $\mathcal{O}_{X,P} \subseteq \mathbf{k}(X)$.

Lemma

$\mathcal{O}_{X,P} \subseteq \mathbf{k}(X)$ *is a local ring*

Proof Consider $\mathfrak{m} = \{\phi \in \mathcal{O}_{X,P} \ : \phi(P) = 0\}$. Clearly $\mathfrak{m}$ is an ideal of $\mathcal{O}_{X,P}$. Moreover every $\psi \in \mathcal{O}_{X,P} \setminus \mathfrak{m}$ is invertible. But then every ideal of $\mathcal{O}_{X,P}$ different of (1) consist of non units and so is contained in $\mathfrak{m}$.

The local ring at a point

Recall that a ring is called **local** if it has a unique maximal ideal.

Let $X \subset \mathbb{A}^n(\mathbf{k})$ be an affine variety. Given $P \in X$ the **local ring** of X at P, is the set of all rational function on X that are defined at P and it will be denoted by $\mathcal{O}_{X,P} \subseteq \mathbf{k}(X)$.

Lemma

$\mathcal{O}_{X,P} \subseteq \mathbf{k}(X)$ *is a local ring*

Proof Consider $\mathfrak{m} = \{\phi \in \mathcal{O}_{X,P} \; : \phi(P) = 0\}$. Clearly $\mathfrak{m}$ is an ideal of $\mathcal{O}_{X,P}$. Moreover every $\psi \in \mathcal{O}_{X,P} \setminus \mathfrak{m}$ is invertible. But then every ideal of $\mathcal{O}_{X,P}$ different of (1) consist of non units and so is contained in $\mathfrak{m}$.

So we have the following chain of inclusions $\mathcal{O}_X \subset \mathcal{O}_{X,P} \subset \mathbf{k}(X)$

The local ring at a point

Proposition

Let $X \subset \mathbb{A}^n(\mathbf{k})$ an irreducible affine set.

a) *Let $\phi \in \mathbf{k}(X)$. Then the pole set of ϕ is an affine subset of X.*

b) $\mathcal{O}_X = \bigcap_{P \in X} \mathcal{O}_{X,P}$

Proof a) Let $\phi \in \mathbf{k}(X)$ and set $J_\phi = \{G \in \mathbf{k}[x_1, \dots x_n] \ : \ \overline{G}\phi \in \mathcal{O}_X\}$, where $\overline{G}$ denotes the class of G modulo $\mathrm{I}(X)$. Then J_ϕ is an ideal of $\mathbf{k}[x_1, \dots x_n]$ which contains $\mathrm{I}(X)$. Thus $Z(J_\phi) \subset X$.
Now $P \in Z(J_\phi)$ if and only if f is not defined at P. To see this note that if ϕ is defined at P then $\phi = \overline{F}/\overline{G}$ with $F, G \in \mathbf{k}[x_1, \dots x_n]$ and G non vanishing at P and hence $\overline{G}\phi = \overline{F} \in \mathcal{O}_X$ and so $P \notin Z(J_\phi)$. Conversely if P does not belong to $Z(J_\phi)$, then there exist $G \in J_\phi$ that does not vanish at P. Then, by definition of J_ϕ, $\phi = \overline{F}/\overline{G}$ and so ϕ is defined at P.

The local ring at a point

It remains to show part b), namely

$$\mathcal{O}_X = \bigcap_{P \in X} \mathcal{O}_{X,P}$$

The local ring at a point

It remains to show part b), namely

$$\mathcal{O}_X = \bigcap_{P \in X} \mathcal{O}_{X,P}$$

Clearly $\mathcal{O}_X \subseteq \bigcap_{P \in X} \mathcal{O}_{X,P}$. To prove the reverse inclusion note that if f is defined at every point then $Z(J_f)$ is empty, where J_f is as in part a), i.e. $J_f = \{G \in \mathbf{k}[x_1, \ldots x_n] \ : \ \overline{G} f \in \mathcal{O}_X\}$. Hence (by the nullestellenstaz) 1 belongs to J_f. But then $f = 1 \cdot f \in \mathcal{O}_X$.

Polynomial maps

Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be two affine varieties. A map

$$T : X \to Y$$

is said to be a **polynomial map** if there exists $T_1, \ldots, T_m \in \mathbf{k}[x_1, \ldots x_n]$ such that for each $P = (a_1, \ldots a_n) \in X$ we have

$$T(P) = (T_1(a_1, \ldots a_n), \ldots, T_m(a_1, \ldots a_n)).$$

Polynomial maps

Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ be two affine varieties. A map $T : X \to Y$ is said to be a **polynomial map** if there exists $T_1, \ldots, T_m \in \mathbf{k}[x_1, \ldots x_n]$ such that for each $P = (a_1, \ldots a_n) \in X$ we have

$$T(P) = (T_1(a_1, \ldots a_n), \ldots, T_m(a_1, \ldots a_n)).$$

Note that such polynomial mapping induces a homomorphism

$$T^* : \mathcal{O}_Y \to \mathcal{O}_X$$

which is defined as follows: first we get a homomorphism $\overline{T} : \mathbf{k}[y_1, \ldots y_m] \to \mathbf{k}[x_1, \ldots x_n]$, by setting

$$\overline{T}(G) = G(T_1, \ldots, T_m).$$

Next note that $\overline{T}(\mathrm{I}(Y)) \subset \mathrm{I}(X)$. For if $P = (a_1, \ldots a_n) \in$X and $G \in I(Y)$, then

$$(\overline{T}(G)) = G(T_1(a_1, \ldots a_n), \ldots, T_m(a_1, \ldots a_n))$$

which vanishes because $(T_1(a_1, \ldots a_n), \ldots, T_m(a_1, \ldots a_n))$ belongs to Y.

Polynomial maps

Since $\overline{T}(\mathrm{I}(Y)) \subset \mathrm{I}(X)$, we get a homorphism between the quotients

$$T^* : \mathcal{O}_Y = \mathbf{k}[y_1, \dots, y_m]/\,\mathrm{I}(Y) \to \mathbf{k}[x_1, \dots x_n]/\,\mathrm{I}(X) = \mathcal{O}_X$$

Conversely given an homomorphism $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we can construct a polynomial map as follows:

Polynomial maps

Since $\overline{T}(\mathrm{I}(Y)) \subset \mathrm{I}(X)$, we get a homomorphism between the quotient rings

$$T^* : \mathcal{O}_Y = \mathbf{k}[y_1, \ldots, y_m]/\,\mathrm{I}(Y) \to \mathbf{k}[x_1, \ldots x_n]/\,\mathrm{I}(X) = \mathcal{O}_X$$

Conversely given an homomorphism $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we can construct a polynomial map as follows:
choose $T_i \in \mathbf{k}[x_1, \ldots, x_n]$ so that the class modulo $I(X)$ of T_i coincide with the class of $\gamma(\overline{x_i})$ (here $\overline{x_i}$ denotes the class of x_i modulo $I(Y)$).
Then $T = (T_1, \ldots, T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$. We have to show that it maps X to Y.

Polynomial maps

Conversely given an homomorphism $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we can construct a polynomial map as follows:
choose $T_i \in \mathbf{k}[x_1, \ldots, x_n]$ so that the class modulo $I(X)$ of T_i coincide with the class of $\gamma(\overline{y_i})$ (here $\overline{y_i}$ denotes the class of y_i modulo $\mathrm{I}(Y)$).
Then $T = (T_1, \ldots, T_m)$ is a polynomial map from $\mathbb{A}^n$ to $\mathbb{A}^m$. We have to show that it maps X to Y. Consider the homomorphism

$$\overline{T} : \mathbf{k}[y_1, \ldots, y_m] \to \mathbf{k}[x_1, \ldots, x_n]$$

defined as above. Our choice of T_i's implies that if $F \in I(Y)$ then

$$\begin{aligned}
\overline{T}(F) &= F(T_1, \ldots, T_m) \mod \mathrm{I}(X) \\
&= F(\gamma(\overline{y_1}), \ldots \gamma(\overline{y_m})) \mod \mathrm{I}(X) \\
&= \gamma(F) \mod \mathrm{I}(X) \\
&= 0 \mod \mathrm{I}(X).
\end{aligned}$$

Hence $\overline{T}(I(Y)) \subset \mathrm{I}(X)$.

Polynomial maps

Given $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we have constructed a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, such that $\overline{T} : \mathbf{k}[y_1, \ldots, y_m] \to \mathbf{k}[x_1, \ldots, x_n]$ has the property that $\overline{T}(I(Y)) \subset \mathrm{I}(X)$.

Polynomial maps

Given $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we have constructed a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, such that $\overline{T} : \mathbf{k}[y_1, \ldots, y_m] \to \mathbf{k}[x_1, \ldots, x_n]$ has the property that $\overline{T}(I(Y)) \subset \mathrm{I}(X)$.

We want to show that this implies that $T(X) \subset Y$.

Polynomial maps

Given $\gamma : \mathcal{O}_Y \to \mathcal{O}_X$, we have constructed a polynomial map $T : \mathbb{A}^n \to \mathbb{A}^m$, such that $\overline{T} : \mathbf{k}[y_1, \ldots, y_m] \to \mathbf{k}[x_1, \ldots, x_n]$ has the property that $\overline{T}(I(Y)) \subset \mathrm{I}(X)$.

We want to show that this implies that $T(X) \subset Y$.

So suppose $P = (a_1, \ldots a_n)$ belong to X. If $T(P)$ does not belong to Y it must exists $G \in \mathrm{I}(Y)$ such that $G(T(P)) \neq 0$. But then $\overline{T}(G)$ does not vanish at P, i.e. $\overline{T}(G)$ does not belong to $\mathrm{I}(X)$ which contradicts the fact that $\overline{T}(I(Y)) \subset \mathrm{I}(X)$.
Thus T restricts to a polynomial map from X to Y, and $T^* = \gamma$

Polynomial maps

Fact

Thus there is a one to one correspondence between polynomial maps from X to Y and ring homomorphisms from $\mathcal{O}_Y$ to $\mathcal{O}_X$.

Polynomial maps

Fact

Thus there is a one to one correspondence between polynomial maps from X to Y and ring homomorphisms from $\mathcal{O}_Y$ to $\mathcal{O}_X$.

A polynomial map $T : X \to Y$ is called an **isomorphism** if it has an inverse $S : Y \to X$, which is also a polynomial map.

Corollary

Two affine varieties X and Y are isomorphic if and only if the corresponding coordinate rings $\mathcal{O}_X$ and $\mathcal{O}_Y$ are isomorphic as rings.

Example of a polynomial map

Let $F = y^2 - x^6 - 2x^4 - 2x^2 - 1$ and $G = y^2 - x^3 - 2x^2 - 2x - 1$. Then the map

$$\phi : \mathbb{C}_F \longrightarrow \mathbb{C}_G$$
$$P = (a_1, a_2) \longmapsto \phi(P) = (a_1^2, a_2)$$

is a polynomial map (indeed $T_1(x, y) = x^2$ and $T_2(x, y) = y$). In the figure below the two red points are mapped by ϕ in the red point on the right. Same goes for the green points.