ALGEBRAIC CURVES

TSE-YU SU

21st November 2025

CONTENTS

1 AFFINE ALGEBRAIC SETS

1.1 *Affine Space and Algebraic Sets*

1.1 DEFINITION. Let k be a field, we define the **affine n-space** $\mathbb{A}^n(k)$,or $\mathbb{A}^n$ if k is clear, to be the set of n-tuples of elements of k.

If $F \in k[X_1, ..., X_n]$, a point $P = (a_1, ..., a_n)$ is said to be a **zero** of F if

$F(P) = F(a_1, ..., a_n) = 0$. For $F \neq const$, the set of zeros of F is called the **hypersurface** defined by F, and is denoted by V(F). If F is of degree 1, V(F) is called a **hyperplane** in $\mathbb{A}^n$.

For S: a set of polynomials in $k[X_1, ..., X_n]$, define V(S) to be the set of all common zeros of $F \in S$.

A subset $X \subseteq \mathbb{A}^n(k)$ is called an **affine algebraic set**, or simply **algebraic set**, if $X = V(S)$ for some S.

Can verify that the set of all algebraice sets in $\mathbb{A}^n$ forms a topology, called **Zariski topology**, where the closed sets are exactly the algebraic sets.

Here are some facts about algebraic sets:

- If I is the ideal in $k[X_1, ..., X_n]$ generated by S, then V(S) = V(I). Therefore we can restrict to the case V(I).
- If $\{I_\alpha\}$ is **any** collection of ideals, then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$. So the intersection of **any** collection of algebraic sets is also an algebraic set.
- If $I \subseteq J$, then $V(I) \supseteq V(J)$.
- For polynomials F, G, $V(F) \cup V(G) = V(FG)$, and for ideals I, J, $V(I) \cup V(J) = V(IJ)$. So any **finite union** of algebraic sets is also algebraic.
- $V(0) = \mathbb{A}^n, V(1) = V(k[X_1, ..., X_n]) = \varnothing$. And $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$. So any finite subset of $\mathbb{A}^n$ is algebraic.
- $V(IJ) = V(I \cap J)$. The $\supseteq$ is clear, now prove $\subseteq$. Let $P \in V(IJ)$, then for every $F \in I, G \in J$, $FG(P) = 0$. Hence for $H \in I \cap J$, $H^2(P) = 0$, so $H(P) = 0$.

1.2 *The Ideal of a Set of Points*

For any $X \subseteq \mathbb{A}^n$, consider those polynomials in $k[X_1, ..., X_n]$ which vanish on X, these polynomials form an ideal $\lhd k[X_1, ..., X_n]$, called the ideal of X, written $I(X) = \{F \in k[X_1, ..., X_n] | F(X) = \{0\}\}$.

The following properties show some relation between ideals and algebraic sets.

- If $X \subseteq Y$, then $I(X) \supseteq I(Y)$
- $I(\varnothing) = k[X_1, ..., X_n]$. $I(\mathbb{A}^n) = 0$. $I(\mathbb{A}^n) = 0$ if k is not finite. A counterexample is $0 \neq x(x-1) \in I(\mathbb{A}^1(\mathbb{Z}_2)) \lhd \mathbb{Z}_2[x]$
- $I(\{a_1, ..., a_n\}) = (X_1 - a_1, ..., X_n - a_n)$
- $S \subseteq I(V(S))$ and $X \subseteq V(I(X))$
- $V(I(V(S))) = V(S)$ and $I(V(I(X))) = I(X)$.

An ideal which is the ideal of an algebraic set, satisfies the following property:

$$\text{If } I = I(X), \text{ and } F^n \in I \text{ for some } n \in \mathbb{N}, \text{ then } F \in I.$$

Consequently, $I(X) = \mathrm{Rad}(I(X)) = \sqrt{I(X)}$ is radical.

1.3 *The Hilbert Basis Theorem*

We defined an algebraic set by any set of polynomials, but in fact finitely many will suffice.

1.2 THEOREM. *Every algebraic set is the intersection of a finite number of hypersurfaces.*

In order to prove this theorem, it suffices to show any ideal $I \lhd k[X_1, ..., X_n]$ is finitely generated by $(F_1, ..., F_s)$, then $V(I) = V(F_1) \cap V(F_2) \cap ... \cap V(F_n)$.

1.3 THEOREM (Hilbert Basis Theorem). *If* R *is a Noetherian ring, then* R[X] *is also Noetherian. Consequetly,* $R[X_1, ..., X_n]$ *is Noetherian.*

1.4 *Irreducible Components of an Algebraic Set*

An algebraic set may be the union of serveral smaller algebraic sets. An algebraic set $V \subseteq \mathbb{A}^n$ is said to be **reducible** if $V = V_1 \cup V_2$, where $V_1 \neq V \neq V_2$ are algebraic. Otherwise V is **irreducible**.

1.4 PROPOSITION. *An algebraic set* V *is irreducible if and only if* I(V) *is prime.*

We want to show that an algebraic set is the union of finitely many irreducible algebraic sets. If V is reducible, write $V = V_1 \cup V_2$, if V_2 is reducible, write $V_2 = V_3 \cup V_4$, need to show this process stops.

Since $k[X_1, ..., X_n]$ is Noetherian, each set of ideals has an maximal element, consequently, any collection of algebraic sets in $\mathbb{A}^n$ has an minimal element.

1.5 THEOREM. *Let* V *be an algebraic set in* $\mathbb{A}^n(k)$*, then there are unique irreducible algebraic sets* $V_1, ..., V_m$ *such that* $V = V_1 \cup V_2 \cup ... \cup V_m$ *and* $V_i \not\subseteq V_j$ *for* $i \neq j$*.*

Proof. Let $\mathcal{S}$ be the set of all algebraic sets $V \subseteq \mathbb{A}^n$ which is not the union of a finite number of irreducible. Choose an minimal element V in $\mathcal{S}$, clearly V is reducible, say $V = V_1 \sup V_2$, where $V_i \neq V$. But then $V_i \subsetneq V$, so V_i is a union of finitely many irreducible algebraic sets, hence so is $V = V_1 \cup V_2$, a contradiction. To show $V_i \not\subseteq V_j$ for $i \neq j$, simply delete every algebraic set which is contained in another bigger algebraic set.

To show uniqueness, let $V = W_1 \cup ... \cup W_s$. Since $V_i = V \cap V_i = \cup_j (W_j \cap V_i)$, and V_i is irreducible, $V_i \subseteq W_{j(i)}$ for some $j(i)$. Similarly, $W_{j(i)} \subseteq V_{k(j(i))}$ for some $k(j(i))$, but then $V_i \subseteq V_{k(j(i))}$, hence $i = k(j(i))$ and $V_i = W_{j(i)}$. Likewise $W_j = V_{i(j)}$ for some $i(j)$, so $s = n$ and $W_i = V_i$ after renumbering. □

These $V_1, ..., V_n$ are called the irreducible components of V, and $V = V_1 \cup ... \cup V_n$ is the decomposition of V into irreducible components.

1.5 *Algebraic Subsets of the Plane*

Will classify all irreducible algebraic sets of $\mathbb{A}^2(k)$ in this subsection. Once this classification has been done, by Theorem 1.2 we have found all algebraic sets.

1.6 PROPOSITION. *Let* $F, G \in k[X, Y]$ *with no common factors. Then* $V(F, G) = V(F) \cap V(G)$ *is a finite set of points.*

Proof. Consider $A = (F, G) \cap k[X]$, can see A is an ideal of $k[X]$. Since $k[X]$ is PID, $A = (f(X))$. So $FH + GK = f(X)$ for some $H, K \in k[X, Y]$. Thus the X−component of points in $V(F, G)$ are roots of $f(X)$, which is finitely many. Similarly, the Y−component of points in $V(F,G)$ are roots of some $g \in k[Y]$. Hence $V(F,G) \subseteq \{(a,b)|f(a) = g(b) = 0\}$, which is finite. $\square$

1.7 COROLLARY. *If* F *is irreducible in* $k[X,Y]$*, and if* $V(F)$ *is infinite, then* $I(V(F)) = (F)$ *and* $V(F)$ *is irreducible.*

Proof. Take $G \in I(V(F))$, clearly $G(V(F)) = \{0\}$, hence $V(F) \subseteq V(F,G)$, and $V(F,G)$ is infinite. By the previous proposition F, G must have common factor, since F is irreducible this common factor can only be F, so $G \in (F)$, and thus $I(V(F)) = (F)$, and by proposition 1.4 $V(F)$ is irreducible. $\square$

1.8 COROLLARY. *Suppose k is infinite, then the irreducible algebraic subsets of $\mathbb{A}^2(k)$ are:*

$\mathbb{A}^2(k)$,

$\varnothing$,

points,

irreducible plane curves $V(F)$

where F *is an irreducible polynomial and* $V(F)$ *is infinite.*

Note: Not all zero sets of irreducible polynomial in $k[X,Y]$ is infinte, for example $X^2 + Y^2 \in \mathbb{R}[X,Y]$ is irreducible, but the zero set $\{(0,0)\}$ is finite.

1.9 COROLLARY. *Assume k is algebraically closed, and* $F \in k[X,Y]$*. Let* $F = F_1^{n_1} \ldots F_r^{n_r}$ *be the decomposition of* F *into irreducible factors. Then* $V(F) = V(F_1) \cup \ldots \cup V(F_r)$ *is the decomposition of* F *into irreducible components, and* $I(V(F)) = (F_1F_2 \ldots F_r)$.

Proof. $V(F) = V(F_1) \cup \ldots \cup V(F_r)$ is clear. Since k is algebraically closed, $V(F_i)$ is infinite, and by the previous corollary $V(F_i)$ is irreducible.

(Note: The cases such as $X^2 + Y^2 \in \mathbb{R}[X,Y]$, which is irreducible but has finite zero set, won't happen.)

Also, since $F_i \nmid F_j$, there's no inclusion relation among $V(F_i)$.

The next part $I(V(F)) = (F_1F_2 \ldots F_r)$ is also clear.

$\square$

The following problem shows why we usually require k to be algebraically closes.

QUESTION. Show that every algebraic subset of $\mathbb{A}^2(\mathbb{R})$ is equal to some $V(F)$, where $F \in \mathbb{R}[X,Y]$.

Proof. It suufices to show any finite set of points $\{(a_1,b_1), \ldots, (a_r,b_r)\}$ in $\mathbb{A}^2(\mathbb{R})$ can be written as $V(F)$ for some $F \in \mathbb{R}[X,Y]$.

Since $(X-a)^2 + (Y-b)^2$ has only one zero (a,b) in $\mathbb{A}^2(\mathbb{R})$, $F = \prod_{i=i}^{r}((X-a_i)^2 + (Y-b_i)^2)$ is the desired polynomial. $\square$

1.6 *Hilbert's Nullstellensatz*

we assume k is algebraically closed in this subsection.

Want to find the exact relation between algebraic sets and ideals. Will first prove a weaker theorem:

1.10 THEOREM (Weak Nullstellensatz). *If* I *is a proper ideal in* $k[X_1, ..., X_n]$, *then* $V(I) \neq \emptyset$.

Proof. Since I is contained in some maximal ideal $\mathfrak{m}$, and $V(\mathfrak{m}) \subseteq V(I)$, it suffices to show for every maximal ideals $\mathfrak{m}$, $V(\mathfrak{m}) \neq \emptyset$.

Will use the following fact:

Fact: If k is algebraically closed, then maximal ideals of $k[X_1, ..., X_n]$ are of the form $(X_1 - a_1, ..., X_n - a_n)$.

By the above fact $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\} \neq \emptyset$. □

1.11 THEOREM (Hilbert's Nullstellensatz). *Let* I *be an ideal in* $k[X_1, ..., X_n]$, k *is algebraically closed. Then* $I(V(I)) = Rad(I)$.

Proof. $Rad(I) \subseteq I(V(I))$ is easy. For another direction, suppose $G \in I(V(F_1, ..., F_r))$, $F_i \in k[X_1, ..., X_n]$, let $J = (F_1, ..., F_r, X_{n+1}G - 1) \subseteq k[X_1, ..., X_n, X_{n+1}]$, can see $V(J) \subseteq \mathbb{A}^n = \emptyset$. Apply Weak Nullstellensatz to J, $J = k[X_1, ..., X_n, X_{n+1}]$. So $1 = \sum A_i(X_1, ..., X_{n+1})F_i + B(X_1, ..., X_{n+1}) \cdot (X_{n+1}G - 1)$.

Let $Y = \frac{1}{X_{n+1}}$, multiply the above equation sufficiently many times by Y, that the X_{n+1}-degree of each monomial terms is negative. (For example, $X_1X_{n+1}^3 + X_2^3X_{n+1}^5 \xrightarrow{\times Y^5} X_1Y^2 + X_2^3 = P(\{X_i | i = 1, ..., n\}, Y)$)

Then we get an equation $Y^N = \sum C_i(X_1, ..., Y)F_i + D(X_1, ..., X_n, Y) \cdot (G - Y) \in k[X_1, ..., X_n, Y]$, substitute $Y = G$, it follows that $G^N \in (F_1, ..., F_r)$. □

Here are some immediate corollary, for k : algebraically closed:

1.12 COROLLARY. *There is a one-to-one correspondence between* ***radical ideals*** *and* ***algebraic sets****.*

1.13 COROLLARY. *If* I *is prime, then* V(I) *is irreducible. There is a one-to-one correspondence between* ***prime ideals*** *and* ***irreducible algebraic sets****. The maximal ideals correspond to points.*

1.14 COROLLARY. *Let* $F = F_1^{n_1} ... F_r^{n_r}$ *be the decomposition of* F *into irreducible factors, then* $V(F) = V(F_1) \cup ... \cup V(F_r)$ *is the decomposition of* V(F) *into irreducible components, and* $I(V(F)) = (F_1F_2...F_r)$.

There is a one-to-one correspondence between ***irreducible polynomials****(up to multiplying by a unit) and* ***irreducible hypersurfaces*** *in* $\mathbb{A}^n(k)$*. Remenber that a hypersurface is the zero set of a polynomial.*

$$\begin{aligned} \text{Radical ideals} &\leftrightarrow \text{Algebraic sets} \\ \text{Prime ideals} &\leftrightarrow \text{Irreducible algebraic sets} \\ \text{Irreducible polynomials} &\leftrightarrow \text{Irreducible hypersurfaces} \end{aligned}$$

1.15 COROLLARY. *Let* I *be an ideal in* $k[X_1, \dots, X_n]$, *then* $V(I)$ *is a finite set if and only if* $k[X_1, \dots, X_n]/I$ *is a finite dimensional vector space over* k. *In this case the number of points in* $V(I)$ *is less or equal to* $\dim_k(k[X_1, \dots, X_n]/I)$.

Proof. □