Algebraic Curves

William Fulton

December 23, 2021

Contents

This notes seems a good companion

1 Affine Algebraic Sets

1.1 Affine Space and Algebraic Sets

Let k be any field. By $\mathbb{A}^n(k)$, or simply $\mathbb{A}^n$, we shall mean the Cartesian product of k with itself n times. We call $\mathbb{A}^n(k)$ **affine n-space** over k; its elements will be called **points**. In particular, $\mathbb{A}^1(k)$ is the **affine line**, $\mathbb{A}^2(k)$ is the **affine space**

If $F \in k[X_1, \dots, X_n]$, a point $P = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ is called a **zero** of F if $F(P) = 0$. If F is not a constant, the set of zeros of F is called the **hypersurface** defined by F, and is denoted by $V(F)$. A hypersurface in $\mathbb{A}^2(k)$ is called an **affine plane curve**. If F is a polynomial of degree one, $V(F)$ is called a **hyperplane** in $\mathbb{A}^n(k)$; if $n = 2$, it is a **line**

More generally, if S is any set of polynomials in $k[X_1, \dots, X_n]$, we let $V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$, $V(S) = \bigcap_{F \in S} V(F)$. If $S = \{F_1, \dots, F_r\}$, we usually write $V(F_1, \dots, F_r)$. A subset $X \subseteq \mathbb{A}^n(k)$ is an **affine algebraic set**, or simply an **algebraic set**, if $X = V(S)$ for some S

1. If I is the ideal in $k[X_1, \dots, X_n]$ generated by S, then $V(S) = V(I)$; so every algebraic set $V(I)$ is equal to some ideal I

2. If $\{I_\alpha\}$ is any collection of ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.

3. If $I \subset J$, then $V(I) \supset V(J)$

4. $V(FG) = V(F) \cup V(G)$

   $x \in V(FG) \Leftrightarrow FG(x) \Leftrightarrow F(x) = 0 \vee G(x) = 0$ since k is a field and $k[X_1, \dots, X_n]$ is a domain

   $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$

5. $V(0) = \mathbb{A}^n(k)$, $V(1) = \emptyset$, $V(X_1 - a_1, \dots, X_n - a_n) = \{(a_1, \dots, a_n)\}$ for $a_i \in k$. So any finite subset of $\mathbb{A}^n(k)$ is an algebraic set

Exercise 1.1.1. Show that each of the following sets is not algebraic

1. $A = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) \mid y = \sin x\}$

Proof. 1. Suppose $f \in I(A)$ and fix a $a \in \mathbb{R}$, then $f(x, a) \in \mathbb{R}[x]$ but has infinitely many solutions, a contradiction

$\square$

1.2 The Ideal of a Set of Points

For any subset $X \subseteq \mathbb{A}^n(k)$, we consider those polynomials that vanish on X; they form an ideal in $k[X_1, \dots, X_n]$, called the **ideal** of X, and written $I(X)$, $I(X) = \{F \in k[X_1, \dots, X_n] \mid F(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}$.

1. If $X \subset Y$, then $I(X) \supset I(Y)$

2. $I(\emptyset) = k[X_1, \dots, X_n]$ $I(\mathbb{A}^n(k)) = (0)$ if k is an infinite field; $I(\{(a_1, \dots, a_n)\}) = (X_1 - a_1, \dots, X_n - a_n)$ for $a_1, \dots, a_n \in k$

3. $I(V(S)) \supset S$ for any set S of polynomials; $V(I(X)) \supset X$ for any set X of points

4. $V(I(V(S))) = V(S)$ for any set S of polynomials; $I(V(I(X))) = I(X)$ for any set X of points. So if X is an algebraic set, $X = V(I(X))$; and if J is an ideal of an algebraic set, $I(V(J)) = J$

An ideal that is the ideal of an algebraic set has a property not shared with all ideals: if $J = I(X)$ and $F^n \in I$ for some integer $n > 0$, then $F \in I$. If I is any ideal in a ring R, we define the **radical** of I, written $\mathrm{Rad}(I)$, to be $\{a \in R \mid a^n \in I$ for some integer $n > 0\}$. Then $\mathrm{Rad}(I)$ is an ideal containing I. An ideal I is called a **radical ideal** if $I = \mathrm{Rad}(I)$. So we have

5. $I(X)$ is a radical ring for any $X \subset \mathbb{A}^n(k)$

Exercise 1.2.1. Let F be a nonconstant polynomial in $k[X_1, \dots, X_n]$, k algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 1$ and $V(F)$ is infinite if $n \geq 2$

Proof. $\mathbb{A}^1(k) \setminus V(F)$ is infinite. Now if $\mathbb{A}^n(k) \setminus V(F)$ is infinite, then for each $(a_1, \dots, a_n, a_{n+1}) \in V(F)$, $(\mathbb{A}^n(k) \setminus V(F)) \times \{a_{n+1}\}$ is infinite.

$V(F) = \bigcup_{a_1 \in k} \cdots \bigcup_{a_{n-1} \in k} V(F(a_1, \dots, a_{n-1}, X_n))$ □

1.3 The Hilbert Basis Theorem

Theorem 1.1. *Every algebraic set is the intersection of a finite number of hypersurface*

Proof. Let the algebraic set be $V(I)$ for some ideal $I \subset k[X_1, \dots, X_n]$. It is enough to show that I is finitely generated, for if $I = (F_1, \dots, F_r)$, then $V(I) = V(F_1) \cap \cdots \cap V(F_r)$. To prove this we need some algebra: □

A ring is **Noetherian** if every ideal in the ring is finitely generated. Fields and PID's are Noetherian rings. Theorem, therefore, is a consequence of

Theorem 1.2 (Hilbert Basis Theorem)**.** *If R is a Noetherian ring, then $R[X_1, \dots, X_n]$ is a Noetherian ring*

Proof. Since $R[X_1, \dots, X_n] \cong R[X_1, \dots, X_{n-1}][X_n]$, the theorem will follow by induction if we can prove that $R[X]$ is Noetherian whenever R is Noetherian. Let I be an ideal in $R[X]$. We must find a finite set of generators for I

If $F = \sum_{i=0}^{d} a_i X^i \in R[X]$, $a_d \neq 0$, we call a_d the leading coefficient of F. Let J be the set of leading coefficients of all polynomials in I. It is easy to check that J is an ideal in R, so there are polynomials $F_1, \dots, F_r \in I$ whose leading coefficients generate J. Take an integer N larger than the degree of each F_i. For each $m \leq N$, let J_m be the ideal in R consisting of all leading coefficients of all polynomials $F \in I$ s.t. $\deg(F) \leq m$. Let $\{F_{m,j}\}$ be a finite set of polynomials in I of degree $\leq m$ whose leading coefficients generate

J_m. Let I' be the ideal generated by the F_i's and all the $F_{m,j}$'s. It suffices to show that $I = I'$

Suppose I' were smaller than I; let G be an element of I of lowest degree that is not in I'. If $\deg(G) > N$, we can find polynomials Q_i s.t. $\sum Q_i F_i$ and G have the same leading term. But then $\deg(G - \sum Q_i F_i) < \deg G$ so $G - \sum Q_i F_i \in I'$ and so $G \in I'$. Similarly if $\deg(G) = m \leq N$, we can lower the degree by subtracting off $\sum Q_j F_{m,j}$ for some Q_j. This proves the theorem $\square$

Corollary 1.3. *$k[X_1, \dots, X_n]$ is Noetherian for any field k.*

Exercise 1.3.1. Let I be an ideal in a ring R, $\pi : R \to R/I$ the natural homomorphism

1. Show that for every ideal J' of R/I, $\pi^{-1}(J') = J$ is an ideal of R containing I. And for every ideal J of R containing I, $\pi(J) = J'$ is an ideal of R/I.

   This sets up a natural one-to-one correspondence between ideals of R/I and ideals of R that contains I

2. Show that J' is a radical ideal iff J is radical. Similarly for prime and maximal ideals

3. Show that J' is finitely generated if J is. Conclude that R/I is Noetherian if R is Noetherian. Any ring of the form $k[X_1, \dots, X_n]/I$ is Noetherian

1.4 Irreducible Components of an Algebraic Set

An algebraic set $V \subset \mathbb{A}^n$ is **reducible** if $V = V_1 \cup V_2$ where V_1 and V_2 are algebraic sets in $\mathbb{A}^n$ and $V_i \neq V$ for $i = 1, 2$. Otherwise V is reducible

Proposition 1.4. *An algebraic set V is irreducible iff $I(V)$ is prime*

Proof. If $I(V)$ is not prime and suppose $F_1 F_2 \in I(V)$, $F_1, F_2 \notin I(V)$. Then $V = (V \cap V(F_1)) \cup (V \cap V(F_2))$ and $V \cap V(F_i) \subsetneq V$, so V is reducible

If $V = V_1 \cup V_2$ and $V_i \subsetneq V$, then $I(V_i) \supsetneq I(V)$; let $F_i \in I(V_i) \setminus I(V)$. Then $F_1 F_2 \in I(V)$, so $I(V)$ is not prime $\square$

We want to show that an algebraic set is the union of a finite number of irreducible algebraic set.s

Lemma 1.5. *Let $\mathcal{I}$ be any nonempty collection of ideals in a Noetherian ring R. Then $\mathcal{I}$ has a maximal member*

Proof. Choose (using the axiom of choice) an ideal from each subset of $\mathcal{I}$. Let I_0 be the chosen ideal for $\mathcal{I}$ itself. Let $\mathcal{I}_1 = \{I \in \mathcal{I} \mid I \supsetneq I_0\}$, and let I_1 be the chosen ideal of $\mathcal{I}$, etc. It suffices to show that some $\mathcal{I}_n$ is empty. If not let $I = \bigcup_{i=0}^{\infty} I_i$, an ideal of R. Let $F_1, \dots, F_r$ generate I; each $F_i \in I_n$ if n is chosen sufficiently large. But then $I_n = I$, so $I_{n+1} = I_n$, a contradiction □

It follows that any collection of algebraic sets in $\mathbb{A}^n(k)$ has a minimal member. For if $\{V_\alpha\}$ is such a collection, take a maximal member $I(V_{\alpha_0})$ from $\{I(V_\alpha)\}$, then V_{α_0} is the minimal

Theorem 1.6. *Let V be an algebraic set in $\mathbb{A}^n(k)$. Then there are unique irreducible algebraic sets $V_1, \dots, V_m$ s.t. $V = V_1 \cup \dots \cup V_m$ and $V_i \not\subset V_j$ for all $i \neq j$*

Proof. Let $\mathcal{I} = \{$algebraic sets $V \subset \mathbb{A}^n(k) \mid V$ is not the union of a finite number of irreducible algebrai We want to show that $\mathcal{I}$ is empty. If not, let V be a minimal member of $\mathcal{I}$. Since $V \in \mathcal{I}$, V is not irreducible, so $V = V_1 \cup V_2$, $V_i \subsetneq V$. Then $V_i \notin \mathcal{I}$, so $V_i = V_{i1} \cup \dots \cup V_{im_i}$, V_{ij} irreducible. But then $V = \bigcup_{i,j} V_{ij}$, a contradiction.

So any algebraic set V may be written as $V = V_1 \cup \dots \cup V_m$, V_i irreducible. We can throw away any V_i s.t. $V_i \subset V_j$ for some $i \neq j$. To show uniqueness, let $V = W_1 \cup \dots \cup W_m$. Then $V_i = \bigcup_j (W_j \cap V_i)$, so $V_i \subset W_{j(i)}$ for some $j(i)$ since V_i is irreducible. Similarly $V_{j(i)} \subset V_k$ for some k. □

The V_i are called the **irreducible components** of V; $V = V_1 \cup \dots \cup V_m$ is the **decomposition** of V into irreducible components

Exercise 1.4.1.

1. Show that $V(Y - X^2) \subset \mathbb{A}^2(\mathbb{C})$ is irreducible; in fact, $I(V(Y - X^2)) = (Y - X^2)$
2. Decompose $V(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ into irreducible components

Proof.

1. Consider $h : \mathbb{C}[X, Y] \to \mathbb{C}[X]$ by $h(f(x, y)) = f(x, x^2)$. This is a homomorphism and thus $\mathbb{C}[X, Y]/(Y - X^2) \cong \mathbb{C}[X]$. Thus $(Y - X^2)$ is prime
2. Solution is finite

□

Exercise 1.4.2. If $V = V_1 \cup \dots \cup V_r$ is the decomposition of an algebraic set into irreducible components, show that $V_i \not\subset \bigcup_{j \neq i} V_j$

Proof. suppose $V_i \subset \bigcup_{j \neq i} V_j$, then $V_i = \bigcup_{j \neq i}(V_j \cap V_i)$ □

Exercise 1.4.3. Show that $\mathbb{A}^n(k)$ is irreducible if k is infinite

Proof. $\mathbb{A}^1(k)$ is irreducible

For each $a \in k$, $\mathbb{A}^n(k) \times \{a\}$ is irreducible □

1.5 Algebraic Subsets of the Plane

Proposition 1.7. *Let F and G be polynomials in $k[X, Y]$ with no common factors. Then $V(F, G) = V(F) \cap V(G)$ is a finite set of points*

Proof. F and G have no common factors in $k[X][Y]$, so they also have no common factors in $k(X)[Y]$. Since $k(X)[Y]$ is a PID, $(F, G) = (1)$ in $k(X)[Y]$, so $RF + SG = 1$ for some $R, S \in k(X)[Y]$. There is a nonzero $D \in kX$ s.t. $DR = A, DS = B \in k[X, Y]$. Therefore $AF + BG = D$. If $(a, b) \in V(F, G)$ then $D(a) = 0$. But D has only a finite number of zeros, this shows that a finite number of X-coordinates appear among the points of $V(F, G)$. Since the same reasoning applies to the Y-coordinates, there can be only a finite number of points □

Corollary 1.8. *If F is an irreducible polynomials in $k[X, Y]$ s.t. $V(F)$ is infinite, then $I(V(F)) = (F)$ and $V(F)$ is irreducible*

Proof. If $G \in I(V(F))$, then $V(F, G)$ is infinite, so F divides G by the proposition, i.e., $G \in (F)$. $V(F)$ is irreducible follows from Proposition 1.4. □

Corollary 1.9. *Suppose k is infinite. Then the irreducible algebraic subsets of $\mathbb{A}^2(k)$ are: $\mathbb{A}^2(k)$, $\emptyset$, points, and irreducible plane curves $V(F)$ where F is an irreducible polynomial and $V(F)$ is infinite*

Proof. Let V be an irreducible algebraic set in $\mathbb{A}^2(k)$. If V is finite or $I(V) = (0)$, V is of the required type. Otherwise $I(V)$ contains a nonconstant polynomial F; since $I(V)$ is prime, some irreducible polynomial factor of F belongs to $I(V)$, so we may assume F is irreducible. Then $I(V) = (F)$; for if $G \in I(V)$, $G \notin (F)$, then $V \subset V(F, G)$ is finite. □

Corollary 1.10. *Assume k is algebraically closed, F a nonconstant polynomial in $k[X, Y]$. Let $F = F_1^{n_1} \dots F_r^{n_r}$ be the decomposition of F into irreducible factors. Then $V(F) = V(F_1) \cup \dots \cup V(F_r)$ is the decomposition of $V(F)$ into irreducible components, and $I(V(F)) = (F_1, \dots, F_r)$*

Proof. No F_i divides any F_j, $j \neq i$, so there are no inclusion relations among the $V(F_i)$. And $I(\bigcup_i V(F_i)) = \bigcap_i I(V(F_i)) = \bigcap_i (F_i)$. Since any polynomial divisible by each F_i is also divisible by $F_1 \cdots F_r$, $\bigcap_i (F_i) = (F_1 \cdots F_r)$. Note that the $V(F_i)$ are infinite since k is algebraically closed $\square$

1.6 Hilbert's Nullstellensatz

Assume k is algebraically closed

Theorem 1.11 (Weak Nullstellensatz)**.** *If I is a proper ideal in $k[X_1, \dots, X_n]$, then $V(I) \neq \emptyset$*

Proof. We may assume that I is a maximal ideal, for there is a maximal ideal J containing I and $V(J) \subset V(I)$. So $L = k[X_1, \dots, X_n]/I$ is a field, and k may be regared as a subfield of L

Suppose we knew that $k = L$, then for each i there is an $a_i \in k$ s.t. the I-residue of X_i is a_i, or $X_i - a_i \in I$. But $(X_1 - a_1, \dots, X_n - a_n)$ is a maximal ideal, so $I = (X_1 - a_1, \dots, X_n - a_n)$ and $V(I) = \{(a_1, \dots, a_n)\} \neq \emptyset$

Thus we have reduced problem to showing:

Claim (\(\))*: If an algebraically closed field k is a subfield of a field L, and there is a ring homomorphism from $k[X_1, \dots, X_n]$ onto L (identity on k), then $k = L$

This will be proved later $\square$

Theorem 1.12 (Hilbert's Nullstellensatz)**.** *Let I be an ideal in $k[X_1, \dots, X_n]$, then $I(V(I)) = Rad(I)$*

This says the following: if $F_1, \dots, F_r$ and G are in $k[X_1, \dots, X_n]$ and G vanishes whenever $F_1, \dots, F_r$ vanish, then there is an equation $G^N = A_1F_1 + A_2F_2 + \cdots + A_rF^r$ for some $N > 0$ and some $A_i \in k[X_1, \dots, X_n]$

Proof. $\mathrm{Rad}(I) \subset I(V(I))$ is easy. Suppose $G \in I(V(F_1, \dots, F_r))$, $F_i \in k[X_1, \dots, X_n]$. Let $J = (F_1, \dots, F_r, X_{n+1}G - 1) \subset k[X_1, \dots, X_n, X_{n+1}]$. Then $V(J) \subset \mathbb{A}^{n+1}(k)$ is empty, since G vanishes whenever all that F_i's are zero. Applying the Weak Nullstellensatz to J, we see that $1 \in J$, so there is an equation $1 = \sum A_i(X_1, \dots, X_{n+1})F_i + B(X_1, \dots, X_{n+1})(X_{n+1}G - 1)$. Let $Y = 1/X_{n+1}$, and multiply the equation by a higher power of Y, so that an equation $Y^N = \sum C_i(X_1, \dots, X_n, Y)F_i + D(X_1, \dots, X_n, Y)(G - Y)$ in $k[X_1, \dots, X_n, Y]$ results. Substituting G for Y gives the required equation $\square$

Corollary 1.13. *If I is a radical ideal in $k[X_1, \dots, X_n]$, then $I(V(I)) = I$. So there is a one-to-one correspondence between radical ideals and algebraic sets*

Corollary 1.14. *If I is a prime ideal, 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*