

Introduction

Oh hey, it's another one of these independent studies. Me and a friend are going to be going through William Fulton's *Algebraic Curves*. It will be hard, it will be long, and it might not work out for me, but who cares.

Contents

Introduction	1
Affine Algebraic Sets	1
Algebraic Preliminaries	1
Affine Space and Algebraic Sets	4
The Ideal of a Set of Points	5

Affine Algebraic Sets

Algebraic Preliminaries

We will assume all rings are commutative with unity, where \mathbb{Z} is the integers, \mathbb{Q} is the rationals, \mathbb{R} is the reals, and \mathbb{C} is the complex numbers.

Any integral domain R has a quotient field K , which contains R as a subring, and any element in K may be written as a not necessarily unique ratio of two elements of R . Any one-to-one ring homomorphism from R to a field L extends uniquely to a ring homomorphism from K to L .

If R is a ring, then $R[x]$ is the ring of polynomials with coefficients in R . The degree of a nonzero polynomial $\sum a_i x^i$ is the largest integer d such that $a_d \neq 0$. The polynomial is monic if $a_d = 1$.

The ring of polynomials in n variables over R is $R[x_1, \dots, x_n]$. We write $R[x, y]$ and $R[x, y, z]$ if $n = 2$ and 3 respectively. Monomials in $R[x_1, \dots, x_n]$ are of the form $x^{(i)} := x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$, where i_j are nonnegative integers, and the degree of the monomial is $i_1 + \cdots + i_n$. Every $F \in R[x_1, \dots, x_n]$ has a unique expression $F = \sum a_{(i)} x^{(i)}$, where $x^{(i)}$ are monomials, and $a_{(i)} \in R$. We say F is homogeneous of degree d if all $a_{(i)}$ are zero except for monomials of degree d . The polynomial F is written as $F = F_0 + F_1 + \cdots + F_d$, where F_i is a form of degree i , and $d = \deg(F)$ for $F_d \neq 0$.

The ring R is a subring of $R[x_1, \dots, x_n]$, and the ring $R[x_1, \dots, x_n]$ is characterized by the following: if $\varphi: R \rightarrow S$ is a ring homomorphism, and s_1, \dots, s_n are elements in S , then there is a unique extension of φ to a ring homomorphism $\bar{\varphi}: R[x_1, \dots, x_n] \rightarrow S$ such that $\bar{\varphi}(x_i) = s_i$. The image of F under $\bar{\varphi}$ is written $F(s_1, \dots, s_n)$. The ring $R[x_1, \dots, x_n]$ is canonically isomorphic to $R[x_1, \dots, x_{n-1}][x_n]$.

An element $a \in R$ is called irreducible if it is not a unit or zero, and any factorization $a = bc$ with $b, c \in R$ is such that either b or c is a unit. A domain R is a unique factorization domain (UFD) if every nonzero element in R can be factored uniquely up to units and ordering.

If R is a UFD with quotient field K , then any irreducible element $F \in R[x]$ remains irreducible when considered in $K[x]$.

Theorem (Gauss's Lemma for \mathbb{Z}): If $F \in \mathbb{Z}[x]$ is a monic polynomial that is irreducible, then F is irreducible in $\mathbb{Q}[x]$.

If F and G are polynomials in $R[x]$ with no common factors in $R[x]$, then they have no common factors in $K[x]$.

If R is a UFD, then $R[x]$ is also a UFD, and consequently $k[x_1, \dots, x_n]$ is a UFD for any field k . The quotient field of $k[x_1, \dots, x_n]$ is written $k(x_1, \dots, x_n)$ and is called the field of rational functions in n variables over k .

If $\varphi: R \rightarrow S$ is a ring homomorphism, $\ker(\varphi) := \varphi^{-1}(0)$. The kernel is an ideal in R . An ideal in R is proper if $I \neq R$, and a proper ideal is known as maximal if it is not contained in any larger proper ideal.^I An ideal \mathfrak{p} is prime if, whenever $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.^{II}

Let k be a field and I a proper ideal in $k[x_1, \dots, x_n]$. The canonical homomorphism π from $k[x_1, \dots, x_n]$ to $k[x_1, \dots, x_n]/I$ restricts to a ring homomorphism from k to $k[x_1, \dots, x_n]/I$. We regard k as a subring of $k[x_1, \dots, x_n]/I$, which is a vector space over k .

If R is an integral domain, then $\text{char}(R)$, the characteristic of R , is the smallest integer p such that

$$\underbrace{1 + 1 + \dots + 1}_{p \text{ times}} = 0.$$

If p exists, we say $\text{char}(R) = p$, else 0.

Note that if $\varphi: \mathbb{Z} \rightarrow R$ is the unique ring homomorphism from \mathbb{Z} to R ,^{III} then $\ker(\varphi) = \langle p \rangle$, so $\text{char}(R)$ is prime or 0.

If R is a ring, and $F \in R[x]$, and a is a root of F , then $F = (x - a)G$ for some unique polynomial $G \in R[x]$. A field k is algebraically closed if any nonconstant $F \in k[x]$ has a root.

Exercise (Exercise 1.1): Let R be an integral domain.

- (a) If F and G are forms of degree r and s respectively in $R[x_1, \dots, x_n]$, show that FG is a form of degree $r + s$.
- (b) Show that any factor of a form in $R[x_1, \dots, x_n]$ is also a form.

Exercise (Exercise 1.2): Let R be a UFD and K the quotient field of R . Show that every element $z \in K$ may be written as $z = a/b$, where $a, b \in R$ have no common factors. This representative is unique up to units of R .

Solution: Since $K = \text{Frac}(R)$, we know that every $z \in K$ is of the form $z = \frac{a}{b}$. Since R a unique factorization domain, $\gcd(a, b)$ is unique and well-defined. Set $c \cdot \gcd(a, b) = a$ and $d \cdot \gcd(a, b) = b$. Then,

$$\begin{aligned} z &= \frac{a}{b} \\ &= \frac{c \cdot \gcd(a, b)}{d \cdot \gcd(a, b)} \\ &= \frac{c}{d}. \end{aligned}$$

We show that this is unique up to units. Suppose

$$\begin{aligned} z &= \frac{c}{d} \\ &= \frac{c'}{d'}. \end{aligned}$$

Then, by the properties of the field of fractions, we know that

$$c'd = cd',$$

and since R is a UFD, we know that $\gcd(c, d) = \gcd(c', d') = 1$, so $c = u_1 c'$ and $d = u_2 d'$.

Exercise (Exercise 1.3): Let R be a principal ideal domain, and let P be a nonzero proper prime ideal in R .

- (a) Show that P is generated by an irreducible element.

^IAlternatively, an ideal I is maximal if the quotient ring R/I is a field.

^{II}Alternatively, an ideal \mathfrak{p} is prime if R/\mathfrak{p} is an integral domain.

^{III}This is because \mathbb{Z} is initial in the category of rings. See Aluffi.

- (b) Show that P is maximal.

Solution:

- (a) Since P is principal, we know that $P = \langle a \rangle$ for some $a \in R$. We know that a cannot be a unit, as otherwise $P = R$, contradicting the assumption that P is proper, and that $a \neq 0$ as P is not zero.

Suppose toward contradiction that $\langle a \rangle \subsetneq \langle b \rangle$ for some $b \in R$. Then, $a = bc$ for some $c \in R$. If $c \notin \langle a \rangle$, then since $\langle a \rangle$ is prime, we must have $b \in \langle a \rangle$, contradicting strict inclusion. Thus, $c \in \langle a \rangle$, so $c = at$ for some $t \in R$. Therefore, we have $a = abt$, so $bt = 1_R$, and $\langle b \rangle = R$.

- (b) Since R is a PID, and P is prime, we know that $P = \langle a \rangle$ is generated by an irreducible element. Thus, if $\langle a \rangle \subsetneq \langle b \rangle$, then $a = bc$ for some $c \in R$. Since we have unique factorization (as all PIDs are UFDs), and a is irreducible, this means either b or c is a unit. If b is a unit, then $\langle b \rangle = R$, and if c is a unit, then $\langle b \rangle = \langle a \rangle$. Thus, $\langle a \rangle$ is maximal.

Exercise (Exercise 1.4): Let k be an infinite field, $f \in k[x_1, \dots, x_n]$. Suppose $F(a_1, \dots, a_n) = 0$ for all $a_1, \dots, a_n \in k$. Show that $f = 0$.

Exercise (Exercise 1.5): Let k be any field. Show that there are an infinite number of irreducible monic polynomials in $k[x]$.

Solution: Suppose F_1, \dots, F_n were all the irreducible monic polynomials in $k[x]$. Consider the polynomial $P = F_1 F_2 \cdots F_n + 1$. We note that P is monic. We will show that P is irreducible.

Suppose toward contradiction that P were reducible. We know that $k[x]$ is a principal ideal domain, so $P \in \langle F_i \rangle$ for some irreducible monic F_i . However, we know that, for any F_i , $1 \leq i \leq n$, $P \nmid F_i$, as, applying the division algorithm to P , we get

$$P = (F_i) \prod_{j \neq i} F_j + 1,$$

where $r \neq 0$. Thus, P is not reducible and monic, so there are infinitely many irreducible monic polynomials in $k[x]$.

Exercise (Exercise 1.6): Show that any algebraically closed field is infinite.

Solution: Note that if k is any field, then there are infinitely many irreducible monic polynomials in $k[x]$. If k is algebraically closed, then $(x - a)$, for $a \in k$, is the only irreducible monic polynomial. Since there are infinitely many irreducible monic polynomials in $k[x]$, there are infinitely many $a \in k$ such that $(x - a)$ is irreducible in $k[x]$. Thus, k is infinite.

Exercise (Exercise 1.7): Let k be any field, and $F \in k[x_1, \dots, x_n]$, with $a_1, \dots, a_n \in k$.

- (a) Show that

$$F = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n},$$

where $\lambda_{(i)} \in k$.

- (b) If $F(a_1, \dots, a_n) = 0$, show that $F = \sum_{i=1}^n (x_i - a_i) G_i$ for some not necessarily unique $G_i \in k[x_1, \dots, x_n]$.

Solution:

- (a) We let

$$G = F(x_1 + a_1, x_2 + a_2, \dots, x_n + a_n).$$

Then, since $G \in k[x_1, \dots, x_n]$, we have

$$G = \sum \lambda_{(i)} x_1^{i_1} \cdots x_n^{i_n}.$$

Then, we have

$$F = \sum \lambda_{(i)} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}.$$

(b) Note that if $F(a_1, \dots, a_n) = 0$, then $(x_i - a_i) \mid F(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$. Thus, we have

$$F(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n) = (x_i - a_i) \underbrace{g(a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)}_{G_i}.$$

This yields

$$F(x_1, \dots, x_n) = \sum_{i=1}^n (x_i - a_i) G_i.$$

Affine Space and Algebraic Sets

Definition. If k is a field, then when we write $\mathbb{A}^n(k)$, or \mathbb{A}^n , to be the cartesian product of k with itself n times.

We call $\mathbb{A}^n(k)$ the affine n -space over k . Its elements are called points. We call $\mathbb{A}^1(k)$ the affine line and $\mathbb{A}^2(k)$ the affine plane.

Definition. If $F \in k[x_1, \dots, x_n]$, then $P = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ is called a zero of F if $F(P) = F(a_1, \dots, a_n) = 0$.

If F is not constant, then the zeros of F are called the hypersurface defined by F , defined by $V(F)$. A hypersurface in $\mathbb{A}^2(k)$ is called an affine plane curve.

If F is a polynomial of degree 1, then $V(F)$ is called a hyperplane in $\mathbb{A}^n(k)$; if $n = 2$, then an affine hyperplane is a line.

Definition. If S is any set of polynomials in $k[x_1, \dots, x_n]$, then $V(S) = \{P \in \mathbb{A}^n \mid F(P) = 0 \text{ for all } F \in S\}$. In other words, $V(S) = \bigcap_{F \in S} V(F)$. If $S = \{F_1, \dots, F_r\}$, we write $V(F_1, \dots, F_r)$.

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

Proposition:

- (1) If I is the ideal in $k[x_1, \dots, x_n]$ generated by S , then $V(S) = V(I)$; thus, every algebraic set is equal to $V(I)$ for some ideal I .
- (2) If $\{I_\alpha\}$ is a collection of ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.
- (3) If $I \subseteq J$, then $V(I) \supseteq V(J)$.
- (4) For any polynomials F, G , $V(FG) = V(F) \cup V(G)$. Furthermore, $V(I) \cup V(J) = V(\{FG \mid F \in I, G \in J\})$.
- (5) We have that $V(0) = \mathbb{A}^n(k)$, $V(1) = \emptyset$, $V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ for $a_i \in k$. Thus, any finite subset of $\mathbb{A}^n(k)$ is an algebraic set.

Exercise (Exercise 1.8): Show that the algebraic subsets of $\mathbb{A}^1(k)$ are just the finite subsets together with $\mathbb{A}^1(k)$ itself.

Solution: Since $k[x]$ is a principal ideal domain, we know that the zero set $V(S)$ for any $S \subseteq k[x]$ is of the form $V(\langle f \rangle) = V(f)$, where $f \in k[x]$. Since f is a polynomial, f has finitely many roots, so there are finitely many elements in the algebraic subset.

Additionally, since $0 \in k[x]$, we know that k is also an algebraic subset.

Exercise (Exercise 1.14): Let F be a nonconstant polynomial in $k[x_1, \dots, x_n]$, where k is algebraically closed. Show that $\mathbb{A}^n(k) \setminus V(F)$ is infinite if $n \geq 1$ and that $V(F)$ is infinite if $n \geq 2$. Conclude that the complement of any proper algebraic set is infinite.

Solution: We know that k is infinite as k is algebraically closed.

Let $F \in k[x_1, \dots, x_n] \cong k[x_1, \dots, x_{n-1}][x_n]$. In the base case with $n = 1$, we know that there are finitely many roots in $A^1(k)$, so we have the base case. If $n \geq 2$, then we write $F = \sum G_i x_n^i$. We know that since F is nonzero, then there is at least one nonzero G_i . We showed in Exercise 1.4 that there is some $a_1, \dots, a_{n-1} \in k$ such that $G_i(a_1, \dots, a_{n-1}) \neq 0$. Thus, $F(a_1, \dots, a_{n-1}, x_n)$ is not the zero polynomial, meaning there are finitely many roots, and thus infinitely many non-roots. Thus, there are infinitely many $a_1, \dots, a_n \in k$ with $a_1, \dots, a_n \neq 0$.

We write $F = \sum G_i x_n^i$. We know that if all the G_i are constant, then we have a single-variable polynomial in x_n , and any choice of $a_1, \dots, a_{n-1} \in k$ provide other elements of $V(F)$. We assume that there is some G_i that is a non-constant polynomial in x_1, \dots, x_{n-1} . Since G_i is nonzero, we may use the previous paragraph to state that G_i has infinitely many non-roots, and for each choice of those a_1, \dots, a_{n-1} , we have a polynomial in x_n . This polynomial has a root, meaning there are infinitely many roots.

Exercise (Exercise 1.15): Let $V \subseteq A^n(k)$ and $W \subseteq A^m(k)$ be algebraic sets. Show that

$$V \times W = \{(a_1, \dots, a_n, b_1, \dots, b_m) \mid (a_1, \dots, a_n) \in V, (b_1, \dots, b_m) \in W\}$$

is an algebraic set in $A^{n+m}(k)$. It is called the product of V and W .

Solution: Consider the set of polynomials in $k[x_1, \dots, x_n, x_{n+1}, \dots, x_{n+m}]$ given by $P = F(x_1, \dots, x_n) + G(x_{n+1}, \dots, x_{n+m})$, where F is a polynomial in the ideal whose algebraic set is V and G is an ideal in the algebraic set whose ideal is W . Then, the collection of zeros are those of the form $(a_1, \dots, a_n, b_1, \dots, b_m)$, where $(a_1, \dots, a_n) \in V$ and $(b_1, \dots, b_m) \in W$.

The Ideal of a Set of Points

Definition. If $X \subseteq A^n(k)$, then the polynomials that vanish on X form an ideal in $k[x_1, \dots, x_n]$, called the ideal of X , or $I(X)$.

$$I(X) := \{F \in k[x_1, \dots, x_n] \mid F(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in X\}.$$

The following hold.

- If $X \subseteq Y$, then $I(X) \supseteq I(Y)$.
- We have $I(\emptyset) = k[x_1, \dots, x_n]$, $I(A^n(k)) = \langle 0 \rangle$ if k is infinite, and $I(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for $a_1, \dots, a_n \in k$.
- We have $I(V(S)) \supseteq S$ for any set S of polynomials, and $V(I(X)) \supseteq X$ for any set X of points.
- We have $V(I(V(S))) = V(S)$ for any set of polynomials S , and $I(V(I(X))) = I(X)$ for any set X of points. If V is an algebraic set, $V = V(I(V))$ and if I is the ideal of an algebraic set, then $I = I(V(I))$.

Definition. If I is any ideal in a ring R , we define the radical of I , written $\text{rad}(I) = \{a^n \mid a \in I \text{ for some } n > 0\}$. We have that $\text{rad}(I)$ is an ideal containing I . An ideal I is called a radical ideal if $I = \text{rad}(I)$.

- We have $I(X)$ is a radical ideal for any $X \subseteq A^n(k)$.

Exercise (Exercise 1.16): Let V and W be algebraic sets in $A^n(k)$. Show that $V = W$ if and only if $I(V) = I(W)$.

Solution: Let $V = W$. Then, if $F \in I(V)$, then $F = 0$ on W , so $F \in I(W)$, and vice versa.

Suppose $I(V) = I(W)$. We know that $V(I(V)) = V$ and $V(I(W)) = W$. Thus, if $(a_1, \dots, a_n) \in V$, we know that for all $F \in I(W)$, that $F(a_1, \dots, a_n) = 0$ as $F \in I(V)$, meaning $(a_1, \dots, a_n) \in V(I(W)) = W$. By symmetry, we have $V = W$.

Exercise (Exercise 1.17):

- Let V be an algebraic set in $A^n(k)$ and $P \in A^n(k)$ not a point in V . Show that there is a polynomial $F \in k[x_1, \dots, x_n]$ such that $F(Q) = 0$ for all $Q \in V$ but $F(P) \neq 0$.
- Let P_1, \dots, P_r be distinct points in $A^n(k)$ not in an algebraic set V . Show that there are polynomials $F_1, \dots, F_r \in I(V)$ such that $F_i(P_j) = \delta_{ij}$.
- With P_1, \dots, P_r and V as in (b), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ such that $G_i(P_j) = a_{ij}$ for all i and j .

Solution:

- (a) We know that there is some $F \in I(V)$ such that $F(P) \neq 0$. Letting $a = F(P)$, we have that $\frac{1}{a}F(P) = 1$.
- (b) We find $F_i \in I(V \cup \{P_{-i}\})$, where $\{P_{-i}\} = \{P_1, \dots, P_r\} \setminus \{P_i\}$. Applying (a) to F_i , we get that $F_i(P_i) = 1$ and $F_i(P_j) = 0$ for $j \neq i$. By symmetry, this holds for F_1, \dots, F_r .
- (c) With P_1, \dots, P_r and V as in (b), find F_1, \dots, F_r as in b. Then, $G_i = \sum_j a_{ij} F_j$ yields our desired outcome.

Exercise (Exercise 1.18): Let I be an ideal in a ring R . If $a^n \in I$ and $b^m \in I$, show that $(a + b)^{n+m} \in I$. Show that $\text{rad}(I)$ is a (radical) ideal. Show that any prime ideal is radical.

Solution:

- Applying binomial theorem, we have

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^{n+m-k} b^k$$

$\in I,$

where $a^0 = b^0 := 1$.

- We have $I \subseteq \text{rad}(I)$, since we can take $n = 1$. If $a, b \in \text{rad}(I)$, we know that there is some n such that $a^n, b^m \in I$, so by the same logic as above, $(a - b)^{n+m} \in I$, meaning $a - b \in \text{rad}(I)$. Now, if $a \in \text{rad}(I)$ and $x \in R$, then we have that $a^n \in I$ for some n , meaning $x^n a^n \in I$ as I is an ideal, so $(xa)^n \in I$, so $xa \in \text{rad}(I)$, so $\text{rad}(I)$ is an ideal.
- Let I be prime, and let $a \in \text{rad}(I)$. Then, $a^n \in I$ for some $n > 0$, meaning $(a)(a^{n-1}) \in I$. Then, either $a \in I$, or $a^{n-1} \in I$, so by the implicit inductive hypothesis, we have $a \in I$, so $\text{rad}(I) \subseteq I$, so $\text{rad}(I) = I$.

Exercise (Exercise 1.20): Show that for any ideal I in $k[x_1, \dots, x_n]$, $V(I) = V(\text{rad}(I))$, and $\text{rad}(I) \subseteq I(V(I))$.

Solution:

- Clearly, $V(\text{rad}(I)) \subseteq V(I)$ because $I \subseteq \text{rad}(I)$. We know that if $P \in V(I)$, then there is some polynomial $F \in I$ such that $F(P) = 0$.

Exercise (Exercise 1.21): Show that any $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle \subseteq k[x_1, \dots, x_n]$ is a maximal ideal, and that the natural homomorphism from k to $k[x_1, \dots, x_n]/I$ is an isomorphism.