Algebraic Geometry.

Alec Zabel-Mena

September 22, 2023

Contents

Chapter 1

Affine Algebraic Sets

1.1 Affine n-Space and Algebraic Sets

Definition. Let k be a field. We define **affine n-space** over k to be the cartesian product $\mathbb{A}^n(k) = \underbrace{k \times \cdots \times k}_{n\text{-times}}$. If the field k is understood, we write $\mathbb{A}^n$. We call the elements of $\mathbb{A}^(k)$ **affine points**. We call $\mathbb{A}^1(k)$ and $\mathbb{A}^2(k)$ the **affine line** and **affine plane** over k, respectively.

Definition. Let k be a field, and let $f \in k[x_1, \ldots, x_n]$. We call an affine point $P \in \mathbb{A}^n(k)$ a **zero**, or **root** of f if $f(P) = 0$, where $f(P)$ is understood to be $f(a_1, \ldots, a_n)$, where $P = (a_1, \ldots, a_n)$. We call the set of zeros of f, $V(f)$ the **hypersurface** defined by f. We call hypersurfaces in $\mathbb{A}^2(k)$ **affine plane curves**. If $\deg f = 1$, we call $V(f)$ a **hyperplane**. We call hypersurfaces in $\mathbb{A}^1(k)$ **lines**.

Example 1.1. The following curves in figure 1.1 define algebraic sets.

Definition. Let k be a field, and S any set of polynomials in $k[x_1, \ldots, x_n]$. We define the **set of zeros** of S to be the set $V(S) = \{P \in \mathbb{A}^n(k) : f(P) = 0 \text{ for all } f \in S\}$. We call a subset X of $\mathbb{A}^n(k)$ an **affine algebraic set** if $X = V(S)$ for some set S of polynomials.

Lemma 1.1.1. *The following are true for any field k.*

(1) If $\mathfrak{a}$ is an ideal in $k = [x_1, \ldots, x_n]$ generated by a set $S \subseteq k[x_1, \ldots, x_n]$, then $V(\mathfrak{a}) = V(S)$.

(2) If $\{\mathfrak{a}_\alpha\}$ is a collection of ideals of $k[x_1, \ldots, x_n]$, then

$$V\Big(\bigcup \mathfrak{a}_\alpha\Big) = \bigcap V(\mathfrak{a}_\alpha)$$

(3) If $\mathfrak{a} \subseteq \mathfrak{b}$ are ideals, then $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$.

(4) If $f, g \in k[x_1, \ldots, x_n]$, then $V(fg) = V(f) \cup V(g)$.

(5) $V(0) = \mathbb{A}^n(k)$ and $V(1) = \emptyset$.

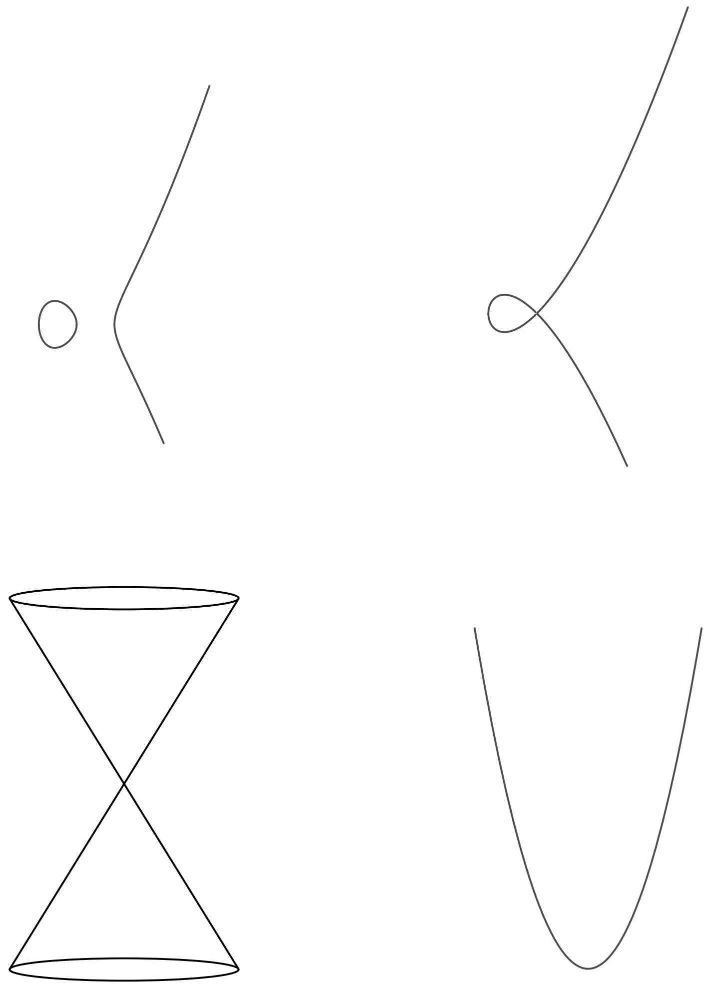

Figure 1.1: Affine Algebraic Sets in $\mathbb{A}^2(\mathbb{R})$ and $\mathbb{A}^3(\mathbb{R})$.

Proof. First, let S be a set of polynomials in $k[x_1, \ldots, x_n]$. Let $\mathfrak{a} = (S)$ the ideal generated by S. Then if $f \in S$ is a polynomia, $f \in I$. Then if $P \in \mathbb{A}^n$ is a zero of f in S, it is a zero of f in $\mathfrak{a}$, hence $V(S) \subseteq V(\mathfrak{a})$. Conversely, we have that if $f \in \mathfrak{a}$, then by suppostion, $f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) + \cdots + f_n(x_1, \ldots, x_n) + \ldots$. Now, if $f(P) = 0$ in I, then we have $f_i(P) = 0$ for every i. This makes $f(P) = 0$ in S, so that $V(\mathfrak{a}) \subseteq V(S)$.

Now, consider the collection $\{\mathfrak{a}_\alpha\}$ of ideals in $k[x_1, \ldots, x_n]$. Let $P \in V(\bigcup \mathfrak{a}_\alpha)$. Then for every $f \in \bigcup \mathfrak{a}_\alpha$, $f(P) = 0$ for each α. So that $P \in \bigcap V(\mathfrak{a}_\alpha)$. Again, on the otherhand, if $P \in \bigcap V(\mathfrak{a}_\alpha)$, $P \in V(\mathfrak{a}_\alpha)$ for all α so that $P \in V(\bigcup \mathfrak{a}_\alpha)$.

Let $\mathfrak{a}$ and $\mathfrak{b}$ ideals in $k[x_1, \ldots, x_n]$, where $\mathfrak{a} \subseteq \mathfrak{b}$. Let $P \in V(\mathfrak{b})$. Then for every polynomial $f \in \mathfrak{b}$, $f(P) = 0$, so that $f(P) = 0$ when $f \in \mathfrak{a}$, hence $P \in V(\mathfrak{a})$. This makes $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$.

Consider now the polynomials $f, g \in k[x_1, \ldots, x_n]$. Certainly if $P \in V(fg)$ it is a root of fg; ie.e. $fg(P) = 0$. This makes $f(P) = 0$ or $g(P) = 0$ so that $V(fg) \subseteq V(f) \cup V(g)$. On the otherhand if P is a root of f, or a root of g, it is a root of fg making $V(f) \cup V(f) \subseteq V(fg)$, and equality is established.

Finally, observe that the zero polynomial $0(x_1, \ldots, x_n)$ has all its coefficients 0, so that any point $P \in \mathbb{A}^n$ is a zero. This makes $V(0) = \mathbb{A}^n$. Likewise, the constant polynomial

$1(x_1, \ldots, x_n)$ has its 0-th coefficient 1 so that it has not points $P \in \mathbb{A}^n$ as roots. That is $V(1) = \emptyset$. ■

Corollary. *Finite unions of algebraic sets are algebraic.*

Example 1.2. (1) Let k be a field, and consider $\mathbb{A}^1(k)$. Let $f \in k[x]$ be a polynomial of degree n. Then f has at most n roots in k. Now, if $\mathfrak{a}$ is an ideal in k, since k is a PID, we also get $\mathfrak{a} = (f)$ for some $f \in k[x]$. That is $|V(\mathfrak{a})| \leq n$, and so any algebraic set in $\mathbb{A}^1(k)$ is necessarily finite, except, possibly $\mathbb{A}^1(k)$.

(2) Let k be a finite field with p^m elements, where $p, m \in \mathbb{Z}^+$ and p is prime. Then k is the splitting field of the polynomial $f(x_n) = x_n^{p^m} - x_n$ over the finite field $\mathbb{F}_p$. Suppose then that there is no set S of polynomials in $k[x_1, \ldots, x_n]$ for which $X = V(S)$, for some $X \in \mathbb{A}^n(k)$. Choose then a point $P \in X$ and a polynomial $g \in S$. Then we have $g(x_1, \ldots, x_n) = g_1(\tilde{X})x_n + \cdots + g_n(\tilde{X})x_n$. Notice that if P is a root of f; i.e. $P \in V(f)$; i.e. $P^{p^m} - P = 0$, then since $P^{p^m} - P$ is a generator for k as a multiplicative group, it generates S. That is, S must contain the point P as a root for g, notice $P^{p^m} = P$ so that $g(P) = g_1(P)P + \cdots + g_n(P)P = 0$ in k. This contradicts that $X \neq V(S)$. This makes every set of $\mathbb{A}^n(k)$ algebraic for any finite field.

(3) By the corollory to lemma 1.1.1, we have that finite unions of algebraic sets are algebraic. Now, consider the field $\mathbb{Q}$, and let $f_q(x) = x + \frac{q}{2}$ in $\mathbb{Q}[x]$. We have that there are $X \subseteq \mathbb{A}^1(\mathbb{Q})$ algebraic, ini where $X = V(f_q)$. Notice however, that the polynomial

$$f(x) = \prod_{q \in \mathbb{Q}} f_q(x)$$

has no roots in $\mathbb{Q}$, as that would imply that for some $n \in \mathbb{Z}^+$, $\sqrt[n]{2} \in \mathbb{Q}$. That is, there is no $X \subseteq \mathbb{A}^1(\mathbb{Q})$ for which $X = V(\prod f_q) = \bigcup V(f_q)$. In general, the countable union of algebraic sets need not be algebraic.

Example 1.3. (1) Let k be a field, and $X = \{(t, t^2, t^3) \in \mathbb{A}^3(k) : t \in k\}$. If k is finite, this is algebraic. Suppose that k is infinite, and consider the polynomial $f(x_1, x_2, x_3) = x_1 + x_2^2 + x_3^3$. Notice that the point $0 \in X$ is a root of f, and that if P is a root of f, then $P \in X$. That is, $X = V(f)$ making X algebraic.

(2) Let $X = \{(\cos t, \sin t) \in \mathbb{A}^2(\mathbb{R}) : t \in \mathbb{R}\}$. Consider the polynomial $f(x, y) = x^2 + y^2 - 1$. Since we have that $\cos^2 t + \sin^2 t = 1$, $X = V(f)$ and X is algebraic.

(3) Let $X = \{(r, \sin t) \in \mathbb{A}^2(\mathbb{R}) : r = \sin t, t \in \mathbb{R}\}$. Consider the polynomial $f(x, y) = x - y$. Then $X = V(f)$.

Lemma 1.1.2. *Let k be a field and $C \subseteq \mathbb{A}^2(k)$ an affine plane curve. Let $L\mathbb{A}^2(k)$ a line not contained in C. Then C and L intersect at no more than n points; that is, $C \cap L$ is finite with at most n points.*

Proof. Let $C = V(f)$ where $f \in k[x, y]$ is a polynomial of degree n, and let $L = V(l)$ where $l(x, y) = y - ax + b$, for some $a, b \in k$. We have that $f(x, y) = f_1(x)y + f_2(x)y^2$. Now, notice that if X, Y is a root of l, then $l(X, Y) = Y - aX + b = 0$, so that $Y = aX + b$. Now, consider a point $P = (X, Y) \in C \cap L = V(f) \cap V(l)$. Then $f(X, Y) = f(X, aX + b) = f_1(X)(aX + b) + f_2(X)(aX + b)^2$. Since f has finitely many roots, there are finitely many $P = (X, Y)$ satisfying $f(X, Y) = 0$ Moreover, f has at most n roots. We finally observe that $C \cap L = V(f(x, ax + b))$. Which shows that $C \cap L$ is finite, and has at most n points. ■

Example 1.4. The following sets are not algebraic.

(1) $X = \{(x, y) \in \mathbb{A}^2(\mathbb{R}) : y = \sin x\}$. Let L be a line in $\mathbb{A}^2(\mathbb{R})$. Notice then that L intersects X at inifinitely many points, so that X cannot be algebraic.

(2) $X = \{(z, w) \in \mathbb{A}^2(\mathbb{C}) : |z|^2 + |w|^2 = 1\}$, where $|x + iy|^2 = x^2 + y^2$ for all $x, y \in \mathbb{R}$. Let $f(z, w) = |z|^2 + |w|^2 - 1$, and suppose that $X = V(f)$. Let L be a line in $\mathbb{A}^2(\mathbb{C})$ Then $|L \cap X| = 4$; however $\deg f = 2$, so that X cannot be algebraic.

(3) $X = \{(\cos t, \sin t, t) \in \mathbb{A}^3(\mathbb{R}) : t \in \mathbb{R}\}$. As in (1), there is a line L intersecting X at infinitely many points.

Theorem 1.1.3. *Let k be an algebraically closed field, Then for $n \geq 1$, the complement of an algebraic set is infinite.*

Proof. Observe that since k is algebraically closed, k is infinite, so that $\mathbb{A}^n(k)$ is infinite. Now, suppose $n = 1$, and let $f \in k[x]$ a nonconstant polynomail, and let $X = V(f)$ an algebraic set. Since f has at most finitely many roots, we get $|X|$ is finite, so that $\mathbb{A}^1(k) \backslash X$ is infinite. Moreover since $k[x]$ is a PID, every algebraic set is of the form $X = V(f)$.

Now, suppose that $n > 1$, Let $S \subseteq k[x_1, \ldots, x_n]$. Let X be an algebraic set with $X = V(S)$. Then $S = (f_1, \ldots, f_m, \ldots)$. Now, if $P \in \mathbb{A}^{n-1}(k)$, then each $f_i(P, x_n) \in k[x_n]$ has finitely many roots. So that the polynomial $f_1(P, x_n) + \cdots + f_m(P, x_n) + \ldots$ has finitely many roots. This makes X finite, and hence $\mathbb{A}^n(k) \backslash X$ is infinite. ■

Corollary. *If $f \in k[x_1, \ldots, x_n]$ is nonconstant, then $V(f)$ is infinite.*

Proof. consider $f \in k[x_1, \ldots, x_n]$ nonconstant. Observe that

$$f(x_1, \ldots, x_n) = \sum f_i(x_1, \ldots, x_{n-1}) x_n^i$$

Where $f_i \in k[x_1, \ldots, x_{n-1}]$. Now, suppose that $P = (a_1, \ldots, a_{n-1})$, then

$$f(P, x_n) = \sum f_i(a_1, \ldots, a_{n-1}) x_n^i$$

has at most n roots in $k[x_n]$. However, notice that since $\mathbb{A}^n(k)$ is infinite, there are infinitely many choices for P, so that if $Q = (P, a_n)$ is a root of f, then f has infinitely many roots. That is, $V(f)$ is finite. ■

Lemma 1.1.4. *Let k be a field, and let $X \subseteq \mathbb{A}^n(k)$ and $Y \subseteq \mathbb{A}^m(k)$ algebraic sets. Then $X \times Y$ is an algebraic set in $\mathbb{A}^{n+m}(k)$.*

Proof. Since $\mathbb{A}^m(k)$ and $\mathbb{A}^n(k)$ are cartesian products, we have that $\mathbb{A}^m(k) \times \mathbb{A}^n(k) = \mathbb{A}^{m+n}(k)$. Then $X \times Y = (X, Y)$. Now, let $S \subseteq k[x_1, \dots, x_m]$ and $T \subseteq k[x_1, \dots, x_n]$ such that $X = V(S)$ and $Y = V(T)$. Let $P \in X \times Y$, then $P = (A, B)$ where $A = (a_1, \dots, a_m)$ and $B = (b_1, \dots, b_n)$. Let $f = f_1 + \cdots + f_d + \cdots \in S$ and $g = g_1 + \cdots + g_l \in T$. Consider then $f \times g((x_1, \dots, x_m), (y_1, \dots, y_n)) = f(x_1, \dots, x_m)g(y_1, \dots, y_n)$. Since $f(A) = 0$ and $g(B) = 0$, then $f \times g(P) = f(A)g(B) = 0$ so that $P \in V(f) \times V(g)$. Conversely, let $P \in V(f) \times V(g)$. Then $P = (A, B)$ where $A \in \mathbb{A}^m(k)$ and $B \in \mathbb{A}^n(k)$, and $f \times g(P) = f(A)g(B) = 0$. Since $A \in V(f)$ and $B \in V(g)$, we get $f(A) = 0$ and $f(B) = 0$, so that $P \in X \times Y$. This makes $X \times Y = V(f) \times V(g)$. ■

1.2 Ideals

Lemma 1.2.1. *Let k be a field, and $X \times \mathbb{A}^n(k)$. Consider the set $I(X) = \{f \in k[x_1, \dots, x_n] : f(P) = 0$ for all $P \in X\}$. Then $I(X)$ forms an ideal of $k[x_1, \dots, x_n]$.*

Proof. Let $f, g \in I(X)$. Then for all $P \in X$, $f(P) = 0$, and $g(P) = 0$, so that $f + g(P) = f(P) + g(P) = 0$. Moreover, $-f(P) = 0$ as well. So I is a subgroup of $k[x_1, \dots, x_n]$ under addition. Now, take $f \in I(X)$ and $g \in k[x_1, \dots, x_n]$. Then $fg(P) = 0$ for all $P \in X$ which makes $I(X)$ into an ideal. ■

Definition. Let k be a field and $X \subseteq \mathbb{A}^n(k)$. We define the **ideal** of X to be the ideal $I(X) = \{f \in k[x_1, \dots, x_n] : f(P) = 0 \text{ for all } P \in X\}$ of $k[x_1, \dots, x_n]$.

Lemma 1.2.2. *Let k be a field. The following are true for all $X, Y \subseteq \mathbb{A}^n(k)$ and for all $S \subseteq k[x_1, \dots, x_n]$.*

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

(2) $I(\emptyset) = k[x_1, \dots, x_n]$ and $I(\mathbb{A}^n(k)) = (0)$.

(3) $S \subseteq I(V(S))$ and $X \subseteq V(I(X))$.

(4) $V(I(V(S))) = V(S)$ and $I(V(I(X))) = I(X)$.

Proof. Let $X, Y \subseteq \mathbb{A}^n(k)$, wiht $X \subseteq Y$. Let $f \in I(Y)$, then for all $P \in Y$, $f(P) = 0$. Now, since $P \in X$, we get for all $P \in X$ $f(P) = 0$ so that $f \in I(X)$.

Observe now that the polynomial $1(x_1, \dots, x_n) = 1$ has no points in $\mathbb{A}^n(k)$ as roots, so that $I(\emptyset) = k[x_1, \dots, x_n]$. Likewise, for the polynomial $0(x_1, \dots, x_n) = 0$, every point in $\mathbb{A}^n(k)$ is a root, so that $I(\mathbb{A}^n(k)) = (0)$.

For the third assertion, let $S \subseteq k[x_1, \dots, x_n]$. If $f \in V(S)$, then for every $P \in V(S)$, $f(P) = 0$, by definition. This makes $S \subseteq I(V(S))$. Likewise, if $X \subseteq \mathbb{A}^n(k)$ and $P \in X$, then for all $f \in I(X)$, $f(P) = 0$, so that $P \in V(I(X))$.

Lastly, let $P \in V(S)$, and $f \in I(V(S))$. By definition, $f(P) = 0$ so that $V(S) \subseteq V(I(V(S)))$. Conversely, let $P \in V(I(V(S)))$ then for every $f \in I(V(S))$, $f(P) = 0$, which puts $P \in V(S)$ so that $V(I(V(S))) \subseteq V(S)$. Likewise, by similar reasoning we conclude that $I(V(I(X))) = I(X)$. ■

Corollary. *If k is an infinite field, then for any $a_1, \dots, a_n \in k$, $I(a_1, \dots, a_n) = (x_1 - a_1, \dots, x_n - a_n)$.*

Proof. Let $f \in I(a_1, \dots, a_n)$. Since k is infinite, and $f(a_1, \dots, a_n) = 0$,

$$f(x_1, \dots, x_n) = \sum g_i(x_1, \dots, x_n)(x_i - a_i)$$

so $f \in (x_1 - a_1, \dots, x_n - a_n)$. Conversely, if $f \in (x_1 - a_1, \dots, x_n - a_n)$, we observe that $f \in I(a_1, \dots, a_n)$. ∎

Definition. Let I be an ideal of a ring R. We define the **radical** of I to be the set

$$\operatorname{Rad} I = \{a \in R : a^n \in I, \text{ for some } n \in \mathbb{Z}^+\}$$

We call I a **radical ideal** if $I = \operatorname{Rad} I$.

Lemma 1.2.3. *Let k be a field, then for any $X \subseteq \mathbb{A}^n(k)$, $I(X)$ is a radical ideal.*

Proof. For any $f \in I(X)$, notice that $f^n(P) = f(f^{n-1}(P)) = \cdots = \underbrace{f(f((P)))}_{n \text{ times}}$ ∎

Bibliography

[1] D. Dummit, *Abstract algebra*. Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra*. New York: Wiley, 1975.

[3] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra*. Addison-Wesly Series in Mathematics, CRC Press.

[4] D. Eisenbud, *Commutative Algebra: Wit a View Toward Algebraic Geometry*. Graduate Texts in Mathematics, Springer Verlag.

[5] R. Hartshorne, *Algebraic Geometry*. Graduate Texts in Mathematics, Springer Verlag.

[6] W. Fulton, *Algebraic Curves: An Introduction to ALgebraic Geometry*. Advanced Book Classics, Addison-Wesley.