Project Sigma

Algebraic Geometry

Yunhai Xiang

May 12, 2021

Contents

Chapter 1

Affine Algebraic Sets

Let k be a field and $n \in \mathbf{N}$, then the *affine space* $\mathbf{A}^n(k)$ of dimension n, or simply $\mathbf{A}^n$ if it does not cause confusion, is the same structure as the n-dimensional vector space k^n over k, except with affine maps as morphisms, where an affine map is a linear map shifted by a constant.

Definition 1.0.1. Suppose that $S \subseteq k[X_1, \ldots, X_n]$ for some $n \in \mathbf{N}$, we define

$$\mathcal{V}(S) = \{x \in \mathbf{A}^n(k) : \forall f \in S,\, f(x) = 0\}$$

as the *zero-locus* of S. A subset of $\mathbf{A}^n(k)$ that is the zero-locus of some S is called *(affine) algebraic*.

For example, in $\mathbf{A}^2(\mathbf{R})$, the sets $\mathcal{V}(\{Y\})$ and $\mathcal{V}(\{X\})$ are the x-axis and the y-axis, the set $\mathcal{V}(\{X, Y\})$ is the origin. The set $\mathcal{V}(\{f\})$, where $f \in k[X, Y]$ is polynomial of degree 2, is known as a *conic section*, for example, the circle $\mathcal{V}(\{X^2 + Y^2 - 1\})$, the parabola $\mathcal{V}(\{Y - X^2\})$, and the hyperbola $\mathcal{V}(\{XY - 1\})$. These are all examples of algebraic sets. The set $\mathbf{Z}$ considered as a subset of $\mathbf{A}^1(\mathbf{R})$ is obviously not algebraic, since a non-constant polynomial can not have infinitely many zeros. By the same reason, the set $\{(\cos t, \sin t, t) \in \mathbf{A}^3(\mathbf{R}) : t \in \mathbf{R}\}$ is also not algebraic, as the trig functions are 2π periodic. Next, we claim that to find all algebraic sets, we need not consider all subsets of $k[X_1, \ldots, X_n]$. Let R be a commutative ring, we recall the following theorems.

Theorem 1.0.2. *R is noetherian iff all ideals $I \subseteq R$ are finitely generated.*

Theorem 1.0.3 (Hilbert's Basis theorem)**.** *If R is noetherian, then so is $R[X_1, \ldots, X_n]$.*

Therefore $k[X_1, \ldots, X_n]$ is noetherian, and hence every for each $S \subseteq k[X_1, \ldots, X_n]$, the ideal $\langle S \rangle$ is generated by some $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. We claim that $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle) = \mathcal{V}(\{f_1, \ldots, f_m\})$. First, we know that $\mathcal{V}(\langle S \rangle) \subseteq \mathcal{V}(S)$ since $S \subseteq \langle S \rangle$. Conversely, suppose that $f \in \langle S \rangle$, then there exists $g_1, \ldots, g_\ell \in S$ and $\lambda_1, \ldots, \lambda_\ell \in k[X_1, \ldots, X_n]$ with $f = \lambda_1 g_1 + \cdots + \lambda_\ell g_\ell$. Suppose that $p \in \mathcal{V}(S)$, then $f(p) = \lambda_1 g_1(p) + \cdots + \lambda_\ell g_\ell(p) = 0$. Since all $p \in \mathcal{V}(S)$ is a zero of all $f \in \langle S \rangle$, we must have $\mathcal{V}(S) \subseteq \mathcal{V}(\langle S \rangle)$, and hence $\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$. The equality $\mathcal{V}(\langle S \rangle) = \mathcal{V}(\{f_1, \ldots, f_m\})$ is derived similarly. Hence all algebraic sets are the zero loci of ideals, and also all algebraic sets are the zero loci of finite sets. Conversely, we can define an ideal $\mathcal{I}(X)$ for each $X \subseteq \mathbf{A}^n(k)$.

Definition 1.0.4. Let $X \subseteq \mathbf{A}^n(k)$, then define the ideal $\mathcal{I}(X)$ of $k[X_1, \ldots, X_n]$ as

$$\mathcal{I}(X) = \{f \in k[X_1, \ldots, X_n] : \forall p \in X,\, f(p) = 0\}$$

which is a well-defined ideal as we can verify easily.

In fact, not only is $\mathcal{I}(X)$ an ideal, it is also a radical ideal. We recall that an radical ideal of a commutative ring R is an ideal $I \subseteq R$ with $I = \sqrt{I}$ where $\sqrt{I} = \{r \in R : \exists m > 0, r^m \in I\}$. In other words, a radical ideal is an ideal $I \subseteq R$ where for all $r \in R$, if $r^m \in I$ for some $m > 0$, then $r \in I$. To see that $\mathcal{I}(X)$ is a radical ideal, note that if $f^m \in \mathcal{I}(X)$ for some $m > 0$, then $f^m(p) = 0$ for all $p \in X$, then $f(p) = 0$ for all $p \in X$ as k is a field, hence $f \in \mathcal{I}(X)$.

Similar to how $\mathcal{V}(S) \subseteq \mathcal{V}(T)$ when $T \subseteq S \subseteq k[X_1, \ldots, X_n]$, we easily have $\mathcal{I}(X) \subseteq \mathcal{I}(Y)$ when $Y \subseteq X \subseteq \mathbf{A}^n(k)$. Let $f \in S \subseteq k[X_1, \ldots, X_n]$, then by definition f vanishes on all of $\mathcal{V}(S)$, therefore $f \in \mathcal{I}(\mathcal{V}(S))$. Let $p \in X \subseteq \mathbf{A}^n(k)$, then by definition p is a zero of all polynomials of $\mathcal{I}(X)$, therefore $p \in \mathcal{V}(\mathcal{I}(X))$. Hence we have $S \subseteq \mathcal{I}(\mathcal{V}(S))$ and $X \subseteq \mathcal{V}(\mathcal{I}(X))$. From these facts, we derive that $\mathcal{I}(X) = \mathcal{I}(\mathcal{V}(\mathcal{I}(X)))$ and $\mathcal{V}(S) = \mathcal{V}(\mathcal{I}(\mathcal{V}(S)))$. In fact, we have the following.

Theorem 1.0.5. There is a bijective correspondance

$$\{\text{radical ideals of } k[X_1, \ldots, X_n]\} \longleftrightarrow \{\text{algebraic sets of } \mathbf{A}^n(k)\}$$

given by $I \mapsto \mathcal{V}(I)$ and $X \mapsto \mathcal{I}(X)$.

whose proof we will delay until later in this note. This observation is central to algebraic geometry.

We observe that for a nonempty family of ideals $I_\alpha \subseteq k[X_1, \ldots, X_n]$ indexed by α, we have $\mathcal{V}(\sum_\alpha I_\alpha) = \mathcal{V}(\bigcup_\alpha I_\alpha) = \bigcap_\alpha \mathcal{V}(I_\alpha)$. This should be easy to verify, and it tells us that the arbitrary intersection of algebraic sets is algebraic. Next, we observe that for ideals $I, J \subseteq k[X_1, \ldots, X_n]$, we have $\mathcal{V}(I \cap J) = \mathcal{V}(I \cdot J) = \mathcal{V}(I) \cup \mathcal{V}(J)$, where the set $I \cdot J = \{fg : f \in I, g \in J\}$. Suppose that $p \in \mathcal{V}(I) \cup \mathcal{V}(J)$, assume without loss of generality that $p \in \mathcal{V}(I)$. For all $f \in I \cap J$, we have $f \in I$, so $f(p) = 0$, hence $p \in \mathcal{V}(I \cap J)$, thus $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cap J)$. On the other hand, for each $fg \in I \cdot J$, we have $(fg)(p) = f(p)g(p) = 0$, thus we have $\mathcal{V}(I) \cup \mathcal{V}(J) \subseteq \mathcal{V}(I \cdot J)$. Conversely, if $p \notin \mathcal{V}(I) \cup \mathcal{V}(J)$, then there exists $f \in \mathcal{V}(I)$ and $g \in \mathcal{V}(J)$ such that $f(p) \neq 0$ and $g(p) \neq 0$, and hence $(fg)(p) = f(p)g(p) \neq 0$ as k is a field. Since we know that $fg \in I \cdot J$ and $fg \in I \cap J$, we have $p \notin \mathcal{V}(I \cdot J)$ and $p \notin \mathcal{V}(I \cap J)$. Thus $\mathcal{V}(I \cap J), \mathcal{V}(I \cdot J) \subseteq \mathcal{V}(I) \cup \mathcal{V}(J)$, and hence we completed the proof. Moreover, since $IJ \subseteq I \cap J$, we have $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J) \subseteq \mathcal{V}(IJ)$, and since $I \cdot J \subseteq IJ$, we have $\mathcal{V}(IJ) \subseteq \mathcal{V}(I \cdot J) = \mathcal{V}(I) \cup \mathcal{V}(J)$. Hence $\mathcal{V}(IJ) = \mathcal{V}(I) \cup \mathcal{V}(J)$ as well.

Definition 1.0.6. An algebraic set V is *irreducible* if it cannot be written as $V = V_1 \cup V_2$ where the algebraic sets $V_1, V_2 \subset V$ properly, and such a set is called an *(algebraic) variety*.

Exercise 1.0.7. If $\mathcal{I}(X) = \mathcal{I}(Y)$ for algebraic sets X, Y, then $X = Y$.

Lemma 1.0.8. An algebraic set V is a variety iff $\mathcal{I}(V)$ is prime.

Proof. Suppose that $\mathcal{I}(V)$ is not prime, that $fg \in \mathcal{I}(V)$ and $f, g \notin \mathcal{I}(V)$. We claim that

$$V = (V \cap \mathcal{V}(\{f\})) \cup (V \cap \mathcal{V}(\{g\}))$$

Let $p \in V$, then $(fg)(p) = f(p)g(p) = 0$, thus $f(p) = 0$ or $g(p) = 0$ since k is a field. Hence we have $p \in \mathcal{V}(\{f\})$ or $p \in \mathcal{V}(\{g\})$. Therefore $V \subseteq (V \cap \mathcal{V}(\{f\})) \cup (V \cap \mathcal{V}(\{g\}))$, the other direction $(V \cap \mathcal{V}(\{f\})) \cup (V \cap \mathcal{V}(\{g\})) \subseteq V$ is obvious. Since $f \notin \mathcal{I}(V)$, exists $p \in V$ with $f(p) \neq 0$. Thus $p \notin \mathcal{V}(\{f\})$. Thus $V \neq V \cap \mathcal{V}(\{f\})$. Similarly, $V \neq V \cap \mathcal{V}(\{g\})$, so V is reducible. Conversely, assume $V = V_1 \cup V_2$ where $V_1, V_2 \subset V$ properly. We have $\mathcal{I}(V) \subset \mathcal{I}(V_1), \mathcal{I}(V_2)$ properly. Choose

$f \in \mathcal{I}(V_1) \setminus \mathcal{I}(V)$ and $g \in \mathcal{I}(V_2) \setminus \mathcal{I}(V)$. For $p \in V$, we have $p \in V_1$ or $p \in V_2$, thus $f(p) = 0$ or $g(p) = 0$, so $(fg)(p) = f(p)g(p) = 0$. Hence $fg \in \mathcal{I}(V)$, so $\mathcal{I}(V)$ is not prime. $\square$

Take, for example, the algebraic set $V = \mathcal{V}(\{f, g\}) \subseteq \mathbf{A}^3(\mathbf{R})$ where $f(x, y, z) = x^2 + y^2 + z^2 - 4$ and $g(x, y, z) = y^2 + z^2 - 1$. Then V is the intersection of the sphere of radius 2, and the cylinder of radius 1. We will see later that we have a decomposition of V

$$V = \mathcal{V}(\{x - \sqrt{3}, y^2 + z^2 - 1\}) \cup \mathcal{V}(\{x + \sqrt{3}, y^2 + z^2 - 1\})$$

into algebraic varieties. This is easy to visualize and check that it is true. In fact, we can do even better. We will show that each algebaic set has a unique decomposition into algebraic varieties. Suppose that R is a commutative ring, we recall the following theorem.

Theorem 1.0.9. *R is noetherian iff every nonempty set of ideals has a maximal element.*

Theorem 1.0.10. *If V is an algebraic set, then V has a unique decomposition $V = V_1 \cup \cdots \cup V_m$, where $V_1, \ldots, V_m$ are varieties such that no one of them is contained in another.*

Proof. Suppose that $\mathcal{L}$ is the set of algebraic sets that do not admit a finite variety decomposition, we will show that $\mathcal{L} = \emptyset$. Suppose the contrary, then $\mathcal{L}$ has a minimal element V w.r.t inclusion by Theorem 1.0.9 on $\mathcal{I}[\mathcal{L}]$. Since $V \in A$, we have V is reducible, hence $V = V_1 \cup V_2$ with algebraics sets $V_1, V_2 \subset V$ properly. Since V is minimal, we must have $V_1, V_2 \notin \mathcal{L}$. Thus V_1, V_2 admit finite variety decompositions, contradiction. Next, we show the uniqueness. Let $V = V_1 \cup \cdots \cup V_m = W_1 \cup \cdots \cup W_h$ be decompositions, then $V_i = (V_i \cap W_1) \cup \cdots \cup (V_i \cap W_h)$, which by the irreducibility of V_i, tells us that $V_i \subseteq W_{\sigma(i)}$ for some $\sigma(i)$. Similarly $W_j \subseteq V_{\delta(j)}$ for some $\delta(j)$. Thus $V_i \subseteq W_{\sigma(i)} \subseteq V_{\delta(\sigma(i))}$. However, $V_i \subseteq V_{\delta(\sigma(i))}$ implies that $V_i = V_{\delta(\sigma(i))}$, so $i = \delta(\sigma(i))$ and $V_i = W_{\sigma(i)}$. $\square$

By developing this general theory further, we will take a look at the affine plane $\mathbf{A}^2(k)$ and find all its algebraic subsets. From what we showed above, it suffice to find all algebraic varieties. From there, we will conclude that the irreducible algebraic subsets of $\mathbf{A}^2(k)$ are the empty set $\emptyset$, the whole space $\mathbf{A}^2(k)$, single points, and irreducible plane curves $\mathcal{V}((F))$, where F is an irreducible polynomial and $\mathcal{V}((F))$ is infinite.

Proposition 1.0.11. *Let $F, G \in k[X, Y]$ be coprime, then $\mathcal{V}((F, G))$ is a finite set of points.*

Proof. Since F, G are coprime in $k[X, Y]$, they are coprime in $k(X)[Y]$ as well. Since $k(X)[Y]$ is PID, $(F, G) = (1)$, hence $RF + SG = 1$ for some $R, S \in k(X)[Y]$. Choose nonzero $D \in k[X]$ with $DR = A$ and $DS = A$ such that $A, B \in k[X, Y]$, then $AF + BG = D$. If $(a, b) \in \mathcal{V}((F, G))$ then $D(a) = 0$, but D has only finite number of zeros. $\square$

We claim that if $F \in k[X, Y]$ is irreducible and $\mathcal{V}((F))$ is infinite, then $\mathcal{I}(\mathcal{V}((F))) = (F)$ and $\mathcal{V}(F)$ is irreducible. If $G \in \mathcal{I}(\mathcal{V}((F)))$ then $\mathcal{V}((F, G))$ is infinite, so $G \in (F)$. Hence $(F) \subseteq \mathcal{I}(\mathcal{V}((F)))$.

Proposition 1.0.12. *Suppose that k is algebraically closed and F is a nonconstant polynomial in $k[X, Y]$ with decomposition $F = F_1^{n_1} \cdots F_r^{n_r}$, then $\mathcal{V}((F)) = \mathcal{V}((F_1)) \cup \cdots \cup \mathcal{V}((F_r))$ is the decomposition of $\mathcal{V}((F))$, and $\mathcal{I}(\mathcal{V}((F))) = (F_1 \cdots F_r)$.*