AFFINE VARIETIES

Algebraic sets

Let k be a field. We define the *affine n-space* to be k^n and denote it by $\mathbf{A}^n$. One reason for using this notation is to treat $\mathbf{A}^n$ as a space of points rather than a k-vector space. Given a subset S of the polynomial ring $k[x_1, \ldots, x_n]$ we define the *zero locus* or *vanishing set* of S to be

$$V(S) = \{a \in \mathbf{A}^n : f(a) = 0 \text{ for every } f \in S\}.$$

A subset X of $\mathbf{A}^n$ is said to be an (affine) *algebraic set* if $X = V(S)$ for some $S \subset k[x_1, \ldots, x_n]$; i.e., algebraic sets are solution sets of polynomial equations. If $S = \{f_1, \ldots, f_k\}$, then we write $V(S)$ simply as $V(f_1, \ldots, f_k)$. We now present some simple examples of algebraic sets.

Example 1. (a) Both $\emptyset$ and X are algebraic sets since

$$\emptyset = V(1) = V(k[x_1, \ldots, x_n]) \quad \text{and} \quad \mathbf{A}^n = V(\emptyset) = V(0).$$

(b) A point $a = (a_1, \ldots, a_n) \in \mathbf{A}^n$ is an algebraic set since

$$\{a\} = V(x_1 - a_1, \ldots, x_n - a_n).$$

(c) Every vector subspace of $\mathbf{A}^n$ is an algebraic set. Let X be a subspace of $\mathbf{A}^n$ and let $\{v_1, \ldots, v_m\}$ be its basis. Then we can extend it to a basis $\{v_1, \ldots, v_n\}$ of $\mathbf{A}^n$. Now if we define a linear map $L : \mathbf{A}^n \to \mathbf{A}^n$ defined as $L(v_k) = \delta_{k>m} v_k$. It can then be easily seen that $\ker L = X$. If $(a_{ij})_{1 \leqslant i,j \leqslant n}$ is the matrix corresponding to L and $f_i(x) = a_{i1}x_1 + \cdots + a_{in}x_n$, then $X = V(f_1, \ldots, f_n)$.

More simply one can also observe that X can be expressed as the vanishing set of the homogeneous polynomials corresponding to the rows of the matrix of the canonical projection map $\pi : \mathbf{A}^n \to \mathbf{A}^n/X$.

(d) $\mathbf{Z}$ (as a subset of $\mathbf{R}$ or $\mathbf{C}$) is not an algebraic set. Can you see why?

Observe that $V(\cdot)$ is an inclusion reversing operator; i.e., if $S_1 \subset S_2 \subset k[x_1, \ldots, x_n]$, then $V(S_1) \supset V(S_2)$. We now record some elementary properties of algebraic sets.

Lemma 2.

(a) *If $S \subset k[x_1, \ldots, x_n]$ and $\mathfrak{a}$ is the ideal generated by S, then*

$$V(S) = V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}).$$

(b) *If $\{S_i\}_i \subset k[x_1, \ldots, x_n]$, then*

$$V\left(\bigcup_i S_i\right) = \bigcap_i V(S_i).$$

(c) *If $S_1, S_2 \subset k[x_1, \ldots, x_n]$, then*

$$V(S_1) \cup V(S_2) = V(S_1 S_2).$$

The proof of the above lemma follows immediately from the definition of $V(\cdot)$. Note that the part (a) above tells us that as we transition from algebraic objects (ideals) to geometric objects (algebraic sets) some information is lost; i.e., we cannot recover an ideal $\mathfrak{a}$ back from the resulting algebraic set $V(\mathfrak{a})$.

The above lemma along with Example 1(a) implies that algebraic sets form closed sets of a topology on $\mathbf{A}^n$. This topology is called the *Zariski topology* named after the influential algebraic geometer Oscar Zariski (1899 - 1986). The induced topology on an algebraic set X is called the *Zariski topology on X*. Note that the closed sets under this topology are precisely the algebraic sets contained in X.

We will see shortly that the Zariski topology is not so well-behaved or interesting in its own regard. For instance, it is not Hausdorff. Moreover, the open sets in Zariski topology are very large or equivalently the closed sets are very small. However, Zariski topology provides us a convenient large to work with. For instance, we can talk about continuous maps.

It might seem not so feasible to work with infinitely many polynomial defining an algebraic set. Fortunately, Hilbert basis theorem comes to our rescue. Recall that the Hilbert basis theorem says that if A is a Noetherian ring, then so is the polynomial ring $A[x_1, \ldots, x_n]$. Due to this it immediately follows that every algebraic set X is a zero locus of only finitely many polynomials for if $X = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $k[x_1, \ldots, x_n]$, then $\mathfrak{a} = (f_1, \ldots, f_k)$ for some $f_i \in k[x_1, \ldots, x_n]$ and so we have $X = V(f_1, \ldots, f_k)$.

Above we consider the map V which takes us from ideals to algebraic sets. Now we introduce a map which does the opposite. Let X be any subset of $\mathbf{A}^n$. Then we define the *ideal* of X as

$$I(X) = \{f \in k[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in X\},$$

i.e., $I(X)$ is the collection of all polynomials that vanish on X. It is easily verified that $I(X)$ is an ideal. In fact, $I(X)$ is a radical ideal. Moreover, it is also pretty obvious that $I(\cdot)$ is an inclusion reversing operator. We record some more properties of $I(X)$ below.

Claim 3.

(a) *If $S \subset k[x_1, \ldots, x_n]$, then $S \subset I(V(S))$.*
(b) *If $X \subset \mathbf{A}^n$, then $V(I(X)) = \overline{X}$.*

Proof. (a): Follows immediately from the definition.

(b): First note that $X \subset V(I(X))$. To show that $V(I(X))$ is the smallest closed set containing X, let $Y = V(\mathfrak{a})$ be a closed set containing X. Then we have $I(Y) = I(V(\mathfrak{a})) \subset I(X)$. Applying V we get

$$V(I(X)) \subset V(I(V(\mathfrak{a}))) \subset V(\mathfrak{a}) = Y$$

as $\mathfrak{a} \subset I(V(\mathfrak{a}))$. This shows that $V(I(X)) = \overline{X}$. □

Due to above result we have $V(I(X)) = X$ for an algebraic set X. Thus the map $V \circ I$ is identity on collection of algebraic sets. In particular, the map I is injective on the collection of algebraic sets. This can also be proven directly from the definition. However, the map $I \circ V$ is not identity on the collection of ideals of $k[x_1, \ldots, x_n]$. For instance, if $\mathfrak{a}$ is not a radical ideal, then $I(V(\mathfrak{a})) \neq \mathfrak{a}$. For instance, $I(V(x^2)) = (x) \neq (x^2)$ for $\mathbf{A}^1$.

We remarked earlier that I is inclusion reversing. It is thus plausible to think that $I(\mathbf{A}^n) = 0$ and $I(a)$ is maximal for a point $a \in \mathbf{A}^n$. Note that $I(a)$ must be proper as $I(X) \neq (1)$ for $X \neq \emptyset$. The canonical ideal we can associate to the point $a = (a_1, \ldots, a_n)$ is $\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$. It is indeed true that $\mathfrak{m}_a$ is maximal and $I(a) = \mathfrak{m}_a$.

Claim 4. *We have* $I(\mathbf{A}^n) = 0$.

Proof. Follows by induction on n. □

Exercise 1. Show that the ideal $\mathfrak{m}_a$ is maximal for a point $a \in \mathbf{A}^n$.

Claim 5. *If* $a \in \mathbf{A}^n$, *then* $I(a) = \mathfrak{m}_a$.

Proof. It is clear that $\mathfrak{m}_a \subset I(a)$ by definition of $\mathfrak{m}_a$. Because $\mathfrak{m}_a$ is maximal and $I(a)$ is proper, the conclusion follows. □

We now have the following maps

$$\left\{\begin{matrix}\text{algebraic sets}\\ \text{in } \mathbf{A}^n\end{matrix}\right\} \begin{matrix}\xrightarrow{I}\\ \xleftarrow{V}\end{matrix} \left\{\begin{matrix}\text{radical ideals in}\\ k[x_1, \ldots, x_n]\end{matrix}\right\}.$$

We want to see if this defines a bijective correspondence, i.e., we want to know if $I(V(\mathfrak{a})) = \mathfrak{a}$ for every radical ideal $\mathfrak{a}$ of $k[x_1, \ldots, x_n]$. This is precisely the statement of Hilbert's Nullstellensatz whose equivalent versions we state below.

Theorem 6 (Hilbert's Nullstellensatz)**.** *The following statements are equivalent:*

(a) *If* $\mathfrak{a}$ *is a proper ideal of* $k[x_1, \ldots, x_n]$, *then* $V(\mathfrak{a}) \neq 0$.
(b) *If* $\mathfrak{a}$ *is a radical ideal of* $k[x_1, \ldots, x_n]$, *then* $I(V(\mathfrak{a})) = \mathfrak{a}$.
(c) *Every maximal ideal of* $k[x_1, \ldots, x_n]$ *is of the form* $\mathfrak{m}_a$ *for some* $a \in \mathbf{A}^n$.

Proof. The proof of the implication $(a) \Rightarrow (b)$ is nontrivial and uses Robinowitsch trick.

$(b) \Rightarrow (c)$: Let $\mathfrak{m}$ be a maximal ideal of $k[x_1 \ldots, x_n]$. Then $I(V(\mathfrak{m})) = \mathfrak{m} \neq (1)$ and so we have $V(\mathfrak{m}) \neq \emptyset$. Let $a \in V(\mathfrak{m})$. Then we have

$$\mathfrak{m} = I(V(\mathfrak{m})) \subset I(a) = \mathfrak{m}_a.$$

Because $\mathfrak{m}$ is maximal we conclude that $\mathfrak{m} = \mathfrak{m}_a$.

$(c) \Rightarrow (a)$: Let $\mathfrak{a}$ be a proper ideal of $k[x_1, \ldots, x_n]$. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}_a$ of $k[x_1, \ldots, x_n]$. It now follows that

$$\{a\} = V(\mathfrak{m}_a) \subset V(\mathfrak{a})$$

and so $V(\mathfrak{a}) \neq \emptyset$. □

Note that we did not assume the underlying field k to be algebraically closed to prove equivalences but k is assumed to be algebraically closed for any of the equivalent statement in the theorem above to hold.