1. Affine Algebraic Sets

We introduce affine spaces and define an affine algebraic set as the common zeroes of a set of polynomials. We study some basic properties of algebraic sets, and use the Hilbert basis theorem to show that every algebraic set is the intersection of finitely many hypersurfaces.

1.1. **Affine spaces and affine algebraic sets.** In the entire course, a ring always means a commutative ring with a multiplicative identity 1, and a field always means an algebraically closed field of characteristic 0, unless otherwise specified. Here a field $\Bbbk$ is *algebraically closed* if every non-constant polynomial $f(x) \in \Bbbk[x]$ has a root in $\Bbbk$. For example, $\mathbb{C}$ is an algebraically closed field of characteristic 0, but $\mathbb{R}$ is not algebraically closed. Although many theorems can be generalised to other fields, their statements are often simpler with these extra assumptions on the underlying field.

Definition 1.1. Let $\Bbbk$ be a field, $n \in \mathbb{Z}_+$. An n-dimensional *affine space* over $\Bbbk$ is the set

$$\{(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in \Bbbk\}.$$

denoted by $\mathbb{A}^n_\Bbbk$ (or simply $\mathbb{A}^n$ if the field is understood in the context).

This notion is actually quite familiar. It is simply the set $\Bbbk^n$ of n-tuples of elements in $\Bbbk$. However, we do not use the notation $\Bbbk^n$ in algebraic geometry because we are not just interested in its structure as a vector space. Indeed, the geometric objects that we will study are some subsets of affine spaces. More precisely,

Definition 1.2. A subset $X \subseteq \mathbb{A}^n_\Bbbk$ is called an *affine algebraic set* (or simply *algebraic set*) if there is a set S of polynomials in $\Bbbk[x_1, \cdots, x_n]$, such that

$$X = \{(a_1, \cdots, a_n) \in \mathbb{A}^n_\Bbbk \mid f(a_1, \cdots, a_n) = 0 \text{ for all } f \in S\}.$$

In such a case we say X is the algebraic set defined by S and write $X = \mathbb{V}(S)$.

In this definition S could have finitely many or infinitely many elements. If S contains only finitely many polynomials, say, $S = \{f_1, f_2, \cdots, f_r\}$, we usually write $X = \mathbb{V}(f_1, f_2, \cdots, f_r)$ instead of $X = \mathbb{V}(\{f_1, f_2, \cdots, f_r\})$ for simplicity. In particular we have

Definition 1.3. An algebraic set $X \subseteq \mathbb{A}^n_\Bbbk$ is called a *hypersurface* if $X = \mathbb{V}(f)$ for some non-constant polynomial $f \in \Bbbk[x_1, \cdots, x_n]$.

Example 1.4. Consider subsets of $\mathbb{A}^1$. The set $X_1 = \{5\}$ is an algebraic set because $X_1 = \mathbb{V}(x-5)$. One can also say $X_1 = \mathbb{V}((x-5)^2)$, or even $X_1 = \mathbb{V}(x(x-5), (x-1)(x-5))$. We see that different choices of S in Definition 1.2 could possibly define the same algebraic set X. The set $X_2 = \{5, 7\}$ is an algebraic set because $X_2 = \mathbb{V}((x-5)(x-7))$. Many other subsets of $\mathbb{A}^1$ are also algebraic sets. You will find all of them in an exercise.

Example 1.5. Consider subsets of $\mathbb{A}^2$. Examples of algebraic sets are $\mathbb{V}(y-x^2)$ which is a parabola, and $\mathbb{V}(xy)$ which is the union of two coordinate axes. They are both hypersurfaces in $\mathbb{A}^2$. The algebraic set $\mathbb{V}(x-5, y-7)$ contains only one point. It is not a hypersurface because we cannot define it by one non-constant polynomial (but we do not prove this fact).

Example 1.6. Let $\mathbb{k} = \mathbb{Q}$ (it is not algebraically closed but I just want to mention this piece of history) and $n = 2$. For every $m \geqslant 3$, the set $X = \mathbb{V}(x^m + y^m - 1) \in \mathbb{A}^2_{\mathbb{Q}}$ is a historically important algebraic set. Obviously X contains points $(1, 0)$ and $(0, 1)$ for all m, and $(-1, 0)$ and $(0, -1)$ for even m. The fact that these are the only points in X is one of the deepest results in mathematics. An equivalent formulation of this result is the so-called Fermat's Last Theorem, which was conjectured in 1637, and proved in 1995.

Here are some simple and useful properties of algebraic sets.

Proposition 1.7. *We consider subsets in $\mathbb{A}^n$.*

(1) *Let S_1 and S_2 be two sets of polynomials in $\mathbb{k}[x_1, \cdots, x_n]$. If $S_1 \supseteq S_2$, then $\mathbb{V}(S_1) \subseteq \mathbb{V}(S_2)$. In other words, the correspondence $\mathbb{V}$ is inclusion-reversing.*

(2) *$\varnothing$ and $\mathbb{A}^n$ are both algebraic sets.*

(3) *The intersection of any collection of algebraic sets in $\mathbb{A}^n$ is an algebraic set.*

(4) *The union of finitely many algebraic sets in $\mathbb{A}^n$ is an algebraic set.*

Proof. We leave the proof as an exercise. □

We introduce some algebraic language that we need to use later.

Definition 1.8. Let R be a ring (a commutative ring with 1).

(1) For any subset $S \subseteq R$, the ideal

$$I = \{r_1 f_1 + \cdots + r_k f_k \mid k \in \mathbb{Z}_+; r_1, \cdots, r_k \in R; f_1, \cdots, f_k \in S\}$$

is called the *ideal generated by S*. We say S is a *set of generators of I*.

(2) An ideal I is said to be *finitely generated* if it is generated by a finite set $S = \{f_1, \cdots, f_m\} \subseteq R$. We write $I = (f_1, \cdots, f_m)$.

(3) An ideal I is *principal* if it is generated by one element $f \in R$. We write $I = (f)$.

Notice that the notation in Definition 1.8 is slightly different from, indeed, simpler than what we used in Algebra 2B (which was $I = Rf_1 + \cdots + Rf_m$ if I is finitely generated, or $I = Rf$ if I is principal). The notation here is more often used in algebraic geometry.

Example 1.9. Let $I \subseteq \mathbb{Z}$ be the ideal of all even integers. Then one can say $I = (2)$, or $I = (-2)$, or $I = (2, 4)$ (4 is obviously redundant), or $I = (4, 6)$ (do you see why?). We can even take S to be evething in I, then the ideal generated by S is still I. Upshot: there are usually many choices for the generators of a given ideal.

Lemma 1.10. *For any subset $S \subseteq \Bbbk[x_1, \cdots, x_n]$, let $I \subseteq \Bbbk[x_1, \cdots, x_n]$ be the ideal generated by S. Then $\mathbb{V}(S) = \mathbb{V}(I)$.*

Proof. We need to show mutual inclusions between $\mathbb{V}(S)$ and $\mathbb{V}(I)$. The inclusion in one direction $\mathbb{V}(S) \supseteq \mathbb{V}(I)$ follows from the fact that $S \subseteq I$ and Proposition 1.7 (1).

We prove $\mathbb{V}(S) \subseteq \mathbb{V}(I)$. For every point $p = (a_1, \cdots, a_n) \in \mathbb{V}(S)$, we need to show that $p \in \mathbb{V}(I)$. Since I is generated by S, every element $g \in I$ can be written in the form $g = r_1 f_1 + \cdots + r_k f_k$ for some $k \in \mathbb{Z}_+$, $r_1, \cdots, r_k \in \Bbbk[x_1, \cdots, x_n]$ and $f_1, \cdots, f_k \in S$. By assumption $f_1(p) = \cdots = f_k(p) = 0$, which implies $g(p) = r_1(p)f_1(p) + \cdots + r_k(p)f_k(p) = 0$. Therefore $p \in \mathbb{V}(I)$. It follows that $\mathbb{V}(S) \subseteq \mathbb{V}(I)$. $\square$

This lemma shows that every algebraic set $X \subseteq \mathbb{A}^n$ can be defined by an ideal $I \subseteq \Bbbk[x_1, \cdots, x_n]$. Notice that different ideals could still define the same algebraic set.

Example 1.11. Consider $X = \{0\} \subseteq \mathbb{A}^1$. Consider two principal ideals $I_1 = (x)$ and $I_2 = (x^2)$ in $\Bbbk[x]$. Then $X = \mathbb{V}(I_1) = \mathbb{V}(I_2)$.

Among the many ideals that define the same algebraic set, we will see next week which one is "the best". Stay tuned!