2. Nullstellensatz

We will introduct radical ideals, and use Nullstellensatz to establish the $\mathbb{V}-\mathbb{I}$ correspondence between radical ideals and algebraic sets. We will also see the geometric meaning of prime ideals and maximal ideals.

2.1. **Nullstellensatz and $\mathbb{V}-\mathbb{I}$ correspondence.** Recall the $\mathbb{V}$ map in Definition 1.2. By Lemma 1.10, it defines a surjective map

$$\mathbb{V}:\{\text{ideals in } \Bbbk[x_1,\cdots,x_n]\}\longrightarrow\{\text{algebraic sets in } \mathbb{A}^n\}. \tag{2.1}$$

However the map is not injective as different ideals could possibly define the same algebraic set. Among all ideals that define the same algebraic set, we want to choose a "good" one, so that we can establish a one-to-one correspondence between "good" ideals in $\Bbbk[x_1,\cdots,x_n]$ and algebraic sets in $\mathbb{A}^n$. We start with some algebra.

Definition 2.1. Let I be an ideal in a ring R. The *radical of I* is

$$\sqrt{I}=\{f\in R\mid f^n\in I \text{ for some } n\in\mathbb{Z}_+\}.$$

An ideal I is said to be a *radical ideal* if $I=\sqrt{I}$.

Lemma 2.2. *Let I be an ideal in a ring R. Then $\sqrt{I}$ is an ideal in R containing I.*

Proof. We leave it as an exercise. □

This definition does not look very intuitive at a first glance. But it will be clear why we define it this way after we relate it to some geometry. We give a quick example.

Example 2.3. Consider the ideals $I_1=(x)$ and $I_2=(x^2)$ in $\Bbbk[x]$. It is not difficult to find out that $\sqrt{I_1}=\sqrt{I_2}=(x)$. Therefore I_1 is a radical ideal in $\Bbbk[x]$ while I_2 is not. We leave the details in an exercise.

Definition 2.4. For any subset $X\subseteq\mathbb{A}^n$,

$$\mathbb{I}(X):=\{f\in\Bbbk[x_1,\cdots,x_n]\mid f(p)=0 \text{ for all } p\in X\}$$

is called the *ideal of X*.

In other words, $\mathbb{I}(X)$ consists of all polynomials that vanish on X. Notice that this definition makes sense for any subset $X\subseteq\mathbb{A}^n$ which is not necessarily algebraic.

Example 2.5. For the subset $X=\{0\}\subseteq\mathbb{A}^1$, $\mathbb{I}(X)$ is the set of all $f(x)\in\Bbbk[x]$ such that $f(0)=0$. Therefore $\mathbb{I}(X)=(x)\subseteq\Bbbk[x]$.

Lemma 2.6. *The map $\mathbb{I}$ has the following properties:*

(1) *Let X_1 and X_2 be two subsets of $\mathbb{A}^n$. If $X_1\supseteq X_2$, then $\mathbb{I}(X_1)\subseteq\mathbb{I}(X_2)$.*

(2) *For any subset* $X \subseteq \mathbb{A}^n$, $\mathbb{I}(X)$ *is a radical ideal in* $\Bbbk[x_1, \cdots, x_n]$.

Proof. (1) For any $f \in \mathbb{I}(X_1)$, we have that $f(p) = 0$ for every $p \in X_1$. In particular, since $X_1 \supseteq X_2$, $f(p) = 0$ for every $p \in X_2$. Hence $f \in \mathbb{I}(X_2)$. It follows that $\mathbb{I}(X_1) \subseteq \mathbb{I}(X_2)$.

(2) We first show $\mathbb{I}(X)$ is an ideal. For any $f, g \in \mathbb{I}(X)$ and $r \in \Bbbk[x_1, \cdots, x_n]$, we have $(f+g)(p) = f(p) + g(p) = 0$ and $(rf)(p) = r(p)f(p) = 0$ for all $p \in X$. Therefore $f + g, rf \in \mathbb{I}(X)$, hence $\mathbb{I}(X)$ is an ideal. Then we need to show that $\sqrt{\mathbb{I}(X)} = \mathbb{I}(X)$. We have that

$$\begin{aligned} f \in \sqrt{\mathbb{I}(X)} &\iff \exists\ m \in \mathbb{Z}_+ \text{ such that } f^m \in \mathbb{I}(X) \\ &\iff \exists\ m \in \mathbb{Z}_+ \text{ such that } f(p)^m = 0 \text{ for any } p \in X \\ &\iff f(p) = 0 \text{ for any } p \in X \\ &\iff f \in \mathbb{I}(X). \end{aligned}$$

It follows that $\sqrt{\mathbb{I}(X)} = \mathbb{I}(X)$, hence the ideal $\mathbb{I}(X)$ is radical. □

We return to the question at the beginning of the section. The $\mathbb{V}$-map (2.1) hits all algebraic sets in $\mathbb{A}^n$, but each algebraic set can be hit by many different ideals. However, the $\mathbb{I}$-map in Definition 2.4 assigns to each algebraic set in $\mathbb{A}^n$ a radical ideal in $\Bbbk[x_1, \cdots, x_n]$. Therefore if we only consider the radical ideals, there is hope that the two maps

$$\{\text{radical ideals } I \subseteq \Bbbk[x_1, \cdots, x_n]\} \underset{\mathbb{I}}{\overset{\mathbb{V}}{\rightleftarrows}} \{\text{algebraic sets } X \subseteq \mathbb{A}^n\} \tag{2.2}$$

are inverse to each other, hence establish a one-to-one correspondence between radical ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. This holds as long as $\Bbbk$ is algebraically closed. The proof relies on the so-called Nullstellensatz, which is a difficult theorem.

Definition 2.7. An ideal I in a ring R is *proper* if $I \neq R$.

Theorem 2.8 (Hilbert's Nullstellensatz)**.** *For any algebraically closed field* $\Bbbk$,

(1) *Let* I *be any proper ideal in* $\Bbbk[x_1, \cdots, x_n]$. *Then* $\mathbb{V}(I) \neq \varnothing$.

(2) *Let* I *be any ideal in* $\Bbbk[x_1, \cdots, x_n]$. *Then* $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

Proof. Non-examinable. Interested reader can find the proof in [Section 3.10, Reid, Undergraduate Algebraic Geometry] or [Section 1.7, Fulton, Algebraic Curves]. □

Proposition 2.9. *For any algebraically closed field* $\Bbbk$,

(1) *Assume* I *is a radical ideal in* $\Bbbk[x_1, \cdots, x_n]$ *and* X *is an algebraic set in* $\mathbb{A}^n$. *Then* $X = \mathbb{V}(I)$ *if and only if* $I = \mathbb{I}(X)$.

(2) *Assume* I_1 *are* I_2 *radical ideals in* $\Bbbk[x_1, \cdots, x_n]$, $X_1 = \mathbb{V}(I_1)$ *and* $X_2 = \mathbb{V}(I_2)$. *Then* $I_1 \subseteq I_2$ *(resp.* $I_1 \subsetneq I_2$*) if and only if* $X_1 \supseteq X_2$ *(resp.* $X_1 \supsetneq X_2$*).*

Proof. (1) We prove "$\Longrightarrow$". By Nullstellensatz 2.8 we have $\mathbb{I}(X) = \mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$ since I is a radical ideal.

We prove "$\Longleftarrow$". The algebraic set X can be written as $X = \mathbb{V}(J)$ for some ideal $J \subseteq \Bbbk[x_1, \cdots, x_n]$. By Nullstellensatz 2.8, $\mathbb{V}(I) = \mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(J))) = \mathbb{V}(\sqrt{J})$. Since $\sqrt{J} \supseteq J$ by Lemma 2.2, we have $\mathbb{V}(I) = \mathbb{V}(\sqrt{J}) \subseteq \mathbb{V}(J) = X$ by Proposition 1.7 (1). It remains to show that $X \subseteq \mathbb{V}(I)$. For every point $p \in X$, by the definition of $\mathbb{V}$, we need to show that $f(p) = 0$ for every $f \in I$. This is clear since $I = \mathbb{I}(X)$.

(2) The equivalence "$I_1 \subseteq I_2 \Longleftrightarrow X_1 \supseteq X_2$" follows from Proposition 1.7 (1) and Lemma 2.6 (1). By (1), we see that if one of the inclusions is an equality, then so is the other. Therefore if one of them is a strict inclusion, then so is the other. □

In other words, Proposition 2.9 shows that $\mathbb{V}$ and $\mathbb{I}$ induce mutually inverse bijections between radical ideals in $\Bbbk[x_1, \cdots, x_n]$ and algebraic sets in $\mathbb{A}^n$. Moreover, the bijection is inclusion-reversing. Next time we will see how this correspondence relates algebra and geometry.