

# Chapter 1

## Hilbert's Nullstellensatz

Hilbert's Nullstellensatz may be seen as the starting point of algebraic geometry. It provides a bijective correspondence between affine varieties, which are geometric objects, and radical ideals in a polynomial ring, which are algebraic objects. In this chapter, we give proofs of two versions of the Nullstellensatz. We exhibit some further correspondences between geometric and algebraic objects. Most notably, the coordinate ring is an affine algebra assigned to an affine variety, and points of the variety correspond to maximal ideals in the coordinate ring.

Before we get started, let us fix some conventions and notation that will be used throughout the book. By a **ring** we will always mean a commutative ring with an identity element 1. In particular, there is a ring  $R = \{0\}$ , the **zero ring**, in which  $1 = 0$ . A ring  $R$  is called an **integral domain** if  $R$  has no zero divisors (other than 0 itself) and  $R \neq \{0\}$ . A **subring** of a ring  $R$  must contain the identity element of  $R$ , and a homomorphism  $R \rightarrow S$  of rings must send the identity element of  $R$  to the identity element of  $S$ .

If  $R$  is a ring, an  **$R$ -algebra** is defined to be a ring  $A$  together with a homomorphism  $\alpha: R \rightarrow A$ . In other words, by an algebra we will mean a commutative, associative algebra with an identity element. A **subalgebra** of an algebra  $A$  is a subring that contains the image  $\alpha(R)$ . If  $A$  and  $B$  are  $R$ -algebras with homomorphisms  $\alpha$  and  $\beta$ , then a map  $\varphi: A \rightarrow B$  is called a **homomorphism of ( $R$ -)algebras** if  $\varphi$  is a ring homomorphism, and  $\varphi \circ \alpha = \beta$ . If  $A$  is a nonzero algebra over a field  $K$ , then the map  $\alpha$  is injective, so we may view  $K$  as a subring of  $A$ . With this identification, a homomorphism of nonzero  $K$ -algebras is just a ring homomorphism fixing  $K$  elementwise.

One of the most important examples of an  $R$ -algebra is the ring of polynomials in  $n$  indeterminates with coefficients in  $R$ , which is written as  $R[x_1, \dots, x_n]$ . If  $A$  is any  $R$ -algebra and  $a_1, \dots, a_n \in A$  are elements, then there is a unique algebra homomorphism  $\varphi: R[x_1, \dots, x_n] \rightarrow A$  with  $\varphi(x_i) = a_i$ , given by applying  $\alpha$  to the coefficients of a polynomial and substituting  $x_i$  by  $a_i$ . Clearly the image of  $\varphi$  is the smallest subalgebra of  $A$

containing all  $a_i$ , i.e., the subalgebra of  $A$  generated by the  $a_i$ . We write this image as  $R[a_1, \dots, a_n]$ , which is consistent with the notation  $R[x_1, \dots, x_n]$  for a polynomial ring. We say that  $A$  is **finitely generated** if there exist  $a_1, \dots, a_n$  with  $A = R[a_1, \dots, a_n]$ . Thus an algebra is finitely generated if and only if it is isomorphic to the quotient ring  $R[x_1, \dots, x_n]/I$  of a polynomial ring by an ideal  $I \subseteq R[x_1, \dots, x_n]$ . By an **affine ( $K$ -)algebra** we mean a finitely generated algebra over a field  $K$ . An **affine ( $K$ -)domain** is an affine  $K$ -algebra that is an integral domain.

Recall that the definition of a module over a ring is identical to the definition of a vector space over a field. In particular, an ideal in a ring  $R$  is the same as a submodule of  $R$  viewed as a module over itself. Recall that a module does not always have a basis (= a linearly independent generating set). If it does have a basis, it is called **free**. If  $M$  is an  $R$ -module and  $S \subseteq M$  is a subset, we write  $(S)_R = \langle S \rangle$  for the submodule of  $M$  generated by  $S$ , i.e., the set of all  $R$ -linear combinations of  $S$ . (The index  $R$  may be omitted if it is clear which ring we have in mind.) If  $S = \{m_1, \dots, m_k\}$  is finite, we write  $(S)_R = (m_1, \dots, m_k)_R = \langle m_1, \dots, m_k \rangle$ . In particular, if  $a_1, \dots, a_k \in R$  are ring elements, then  $(a_1, \dots, a_k)_R = \langle a_1, \dots, a_k \rangle$  denotes the ideal generated by them.

## 1.1 Maximal Ideals

Let  $a \in A$  be an element of a nonzero algebra  $A$  over a field  $K$ . As in field theory,  $a$  is said to be **algebraic** (over  $K$ ) if there exists a nonzero polynomial  $f \in K[x]$  with  $f(a) = 0$ . We say that  $A$  is **algebraic** (over  $K$ ) if every element from  $A$  is algebraic. Almost everything that will be said about affine algebras in this book has its starting point in the following lemma.

**Lemma 1.1** (Fields and algebraic algebras). *Let  $A$  be an algebra over a field  $K$ .*

- (a) *If  $A$  is an integral domain and algebraic over  $K$ , then  $A$  is a field.*
- (b) *If  $A$  is a field and is contained in an affine  $K$ -domain, then  $A$  is algebraic.*

*Proof.* (a) We need to show that every  $a \in A \setminus \{0\}$  is invertible in  $A$ . For this, it suffices to show that  $K[a]$  is a field. We may therefore assume that  $A = K[a]$ . With  $x$  an indeterminate, let  $I \subseteq K[x]$  be the kernel of the map  $K[x] \rightarrow A$ ,  $f \mapsto f(a)$ . Then  $A \cong K[x]/I$ . Since  $A$  is an integral domain,  $I$  is a prime ideal, and since  $a$  is algebraic over  $K$ ,  $I$  is nonzero. Since  $K[x]$  is a principal ideal domain, it follows that  $I = (f)$  with  $f \in K[x]$  irreducible, so  $I$  is a maximal ideal. It follows that  $A \cong K[x]/I$  is a field.

(b) By way of contradiction, assume that  $A$  has an element  $a_1$  that is not algebraic. By hypothesis,  $A$  is contained in an affine  $K$ -domain  $B = K[a_1, \dots, a_n]$  (we may include  $a_1$  in the set of generators). We

can reorder  $a_2, \dots, a_n$  in such a way that  $\{a_1, \dots, a_r\}$  forms a maximal  $K$ -algebraically independent subset of  $\{a_1, \dots, a_n\}$ . Then the field of fractions  $\text{Quot}(B)$  of  $B$  is a finite field extension of the subfield  $L := K(a_1, \dots, a_r)$ . For  $b \in \text{Quot}(B)$ , multiplication by  $b$  gives an  $L$ -linear endomorphism of  $\text{Quot}(B)$ . Choosing an  $L$ -basis of  $\text{Quot}(B)$ , we obtain a map  $\varphi: \text{Quot}(B) \rightarrow L^{m \times m}$  assigning to each  $b \in \text{Quot}(B)$  the representation matrix of this endomorphism. Let  $g \in K[a_1, \dots, a_r] \setminus \{0\}$  be a common denominator of all the matrix entries of all  $\varphi(a_i)$ ,  $i = 1, \dots, n$ . So  $\varphi(a_i) \in K[a_1, \dots, a_r, g^{-1}]^{m \times m}$  for all  $i$ . Since  $\varphi$  preserves addition and multiplication, we obtain

$$\varphi(B) \subseteq K[a_1, \dots, a_r, g^{-1}]^{m \times m}.$$

$K[a_1, \dots, a_r]$  is isomorphic to a polynomial ring and therefore factorial (see, for example, Lang [33, Chapter V, Corollary 6.3]). Take a factorization of  $g$ , and let  $p_1, \dots, p_k$  be those irreducible factors of  $g$  that happen to lie in  $K[a_1]$ . Let  $p \in K[a_1]$  be an arbitrary irreducible element. Then  $p^{-1} \in A \subseteq B$  since  $K[a_1] \subseteq A$  and  $A$  is a field. Applying  $\varphi$  to  $p^{-1}$  yields a diagonal matrix with all entries equal to  $p^{-1}$ , so there exists a nonnegative integer  $s$  and an  $f \in K[a_1, \dots, a_r]$  with  $p^{-1} = g^{-s} \cdot f$ , so  $g^s = p \cdot f$ . By the irreducibility of  $p$ , it follows that  $p$  is a  $K$ -multiple of one of the  $p_i$ . Since this holds for all irreducible elements  $p \in K[a_1]$ , every element from  $K[a_1] \setminus K$  is divisible by at least one of the  $p_i$ . But none of the  $p_i$  divides  $\prod_{i=1}^k p_i + 1$ . This is a contradiction, so all elements of  $A$  are algebraic.  $\square$

The following proposition is an important application of Lemma 1.1. A particularly interesting special case of the proposition is that  $A \subseteq B$  is a subalgebra and  $\varphi$  is the inclusion.

**Proposition 1.2** (Preimages of maximal ideals). *Let  $\varphi: A \rightarrow B$  be a homomorphism of algebras over a field  $K$ , and let  $\mathfrak{m} \subset B$  be a maximal ideal. If  $B$  is finitely generated, then the preimage  $\varphi^{-1}(\mathfrak{m}) \subseteq A$  is also a maximal ideal.*

*Proof.* The map  $A \rightarrow B/\mathfrak{m}$ ,  $a \mapsto \varphi(a) + \mathfrak{m}$ , has kernel  $\varphi^{-1}(\mathfrak{m}) =: \mathfrak{n}$ . So  $A/\mathfrak{n}$  is isomorphic to a subalgebra of  $B/\mathfrak{m}$ . By Lemma 1.1(b),  $B/\mathfrak{m}$  is algebraic over  $K$ . Hence the same is true for the subalgebra  $A/\mathfrak{n}$ , and  $A/\mathfrak{n}$  is also an integral domain. By Lemma 1.1(a),  $A/\mathfrak{n}$  is a field and therefore  $\mathfrak{n}$  is maximal.  $\square$

*Example 1.3.* We give a simple example that shows that intersecting a maximal ideal with a subring does not always produce a maximal ideal. Let  $A = K[x]$  be a polynomial ring over a field and let  $B = K(x)$  be the rational function field. Then  $\mathfrak{m} := \{0\} \subset B$  is a maximal ideal, but  $A \cap \mathfrak{m} = \{0\}$  is not maximal in  $A$ .  $\triangleleft$

Before drawing a “serious” conclusion from Proposition 1.2 in Proposition 1.5, we need a lemma.

**Lemma 1.4.** *Let  $K$  be a field and  $P = (\xi_1, \dots, \xi_n) \in K^n$  a point in  $K^n$ . Then the ideal*

$$\mathfrak{m}_P := (x_1 - \xi_1, \dots, x_n - \xi_n) \subseteq K[x_1, \dots, x_n]$$

*in the polynomial ring  $K[x_1, \dots, x_n]$  is maximal.*

*Proof.* It is clear from the definition of  $\mathfrak{m}_P$  that every polynomial  $f \in K[x_1, \dots, x_n]$  is congruent to  $f(\xi_1, \dots, \xi_n)$  modulo  $\mathfrak{m}_P$ . It follows that  $\mathfrak{m}_P$  is the kernel of the homomorphism  $\varphi: K[x_1, \dots, x_n] \rightarrow K$ ,  $f \mapsto f(\xi_1, \dots, \xi_n)$ , so  $K[x_1, \dots, x_n]/\mathfrak{m}_P \cong K$ . This implies the result.  $\square$

Together with Lemma 1.4, the following proposition describes all maximal ideals in a polynomial ring over an algebraically closed field. Recall that a field  $K$  is called *algebraically closed* if every nonconstant polynomial in  $K[x]$  has a root in  $K$ .

**Proposition 1.5** (Maximal ideals in a polynomial ring). *Let  $K$  be an algebraically closed field, and let  $\mathfrak{m} \subset K[x_1, \dots, x_n]$  be a maximal ideal in a polynomial ring over  $K$ . Then there exists a point  $P = (\xi_1, \dots, \xi_n) \in K^n$  such that*

$$\mathfrak{m} = (x_1 - \xi_1, \dots, x_n - \xi_n).$$

*Proof.* By Proposition 1.2, the intersection  $K[x_i] \cap \mathfrak{m}$  is a maximal ideal in  $K[x_i]$  for each  $i = 1, \dots, n$ . Since  $K[x_i]$  is a principal ideal domain,  $K[x_i] \cap \mathfrak{m}$  has the form  $(p_i)_{K[x_i]}$  with  $p_i$  an irreducible polynomial. Since  $K$  is algebraically closed, we obtain  $(p_i)_{K[x_i]} = (x_i - \xi_i)_{K[x_i]}$  with  $\xi_i \in K$ . So there exist  $\xi_1, \dots, \xi_n \in K$  with  $x_i - \xi_i \in \mathfrak{m}$ . With the notation of Lemma 1.4, it follows that  $\mathfrak{m}_P \subseteq \mathfrak{m}$ , so  $\mathfrak{m} = \mathfrak{m}_P$  by Lemma 1.4.  $\square$

We make a definition before giving a refined version of Proposition 1.5.

**Definition 1.6.** *Let  $K[x_1, \dots, x_n]$  be a polynomial ring over a field.*

(a) *For a set  $S \subseteq K[x_1, \dots, x_n]$  of polynomials, the **affine variety** given by  $S$  is defined as*

$$\mathcal{V}(S) = \mathcal{V}_{K^n}(S) := \{(\xi_1, \dots, \xi_n) \in K^n \mid f(\xi_1, \dots, \xi_n) = 0 \text{ for all } f \in S\}.$$

*The index  $K^n$  is omitted if no misunderstanding can occur.*

(b) *A subset  $X \subseteq K^n$  is called an **affine ( $K$ -)variety** if  $X$  is the affine variety given by a set  $S \subseteq K[x_1, \dots, x_n]$  of polynomials.*

**Remark.** In the literature, affine varieties are sometimes assumed to be irreducible. Moreover, the definition of an affine variety is sometimes made only in the case that  $K$  is algebraically closed.  $\triangleleft$

**Theorem 1.7** (Correspondence points–maximal ideals). *Let  $K$  be an algebraically closed field and  $S \subseteq K[x_1, \dots, x_n]$  a set of polynomials. Let  $\mathcal{M}_S$  be the set of all maximal ideals  $\mathfrak{m} \subset K[x_1, \dots, x_n]$  with  $S \subseteq \mathfrak{m}$ . Then the map*

$$\Phi: \mathcal{V}(S) \rightarrow \mathcal{M}_S, (\xi_1, \dots, \xi_n) \mapsto (x_1 - \xi_1, \dots, x_n - \xi_n)$$

is a bijection.

*Proof.* Let  $P := (\xi_1, \dots, \xi_n) \in \mathcal{V}(S)$ . Then  $\Phi(P)$  is a maximal ideal by Lemma 1.4. All  $f \in S$  satisfy  $f(P) = 0$ , so  $f \in \Phi(P)$ . It follows that  $\Phi(P) \in \mathcal{M}_S$ . On the other hand, let  $\mathfrak{m} \in \mathcal{M}_S$ . By Proposition 1.5,  $\mathfrak{m} = (x_1 - \xi_1, \dots, x_n - \xi_n)$  with  $(\xi_1, \dots, \xi_n) \in K^n$ , and  $S \subseteq \mathfrak{m}$  implies  $(\xi_1, \dots, \xi_n) \in \mathcal{V}(S)$ . This shows that  $\Phi$  is surjective.

To show injectivity, let  $P = (\xi_1, \dots, \xi_n)$  and  $Q = (\eta_1, \dots, \eta_n)$  be points in  $\mathcal{V}(S)$  with  $\Phi(P) = \Phi(Q) =: \mathfrak{m}$ . For each  $i$ , we have  $x_i - \xi_i \in \mathfrak{m}$  and also  $x_i - \eta_i \in \mathfrak{m}$ , so  $\xi_i - \eta_i \in \mathfrak{m}$ . This implies  $\xi_i = \eta_i$ , since otherwise  $\mathfrak{m} = K[x_1, \dots, x_n]$ .  $\square$

**Corollary 1.8** (Hilbert's Nullstellensatz, first version). *Let  $K$  be an algebraically closed field and let  $I \subsetneq K[x_1, \dots, x_n]$  be a proper ideal in a polynomial ring. Then*

$$\mathcal{V}(I) \neq \emptyset.$$

*Proof.* Consider the set of all proper ideals  $J \subsetneq K[x_1, \dots, x_n]$  containing  $I$ . Using Zorn's lemma, we conclude that this set contains a maximal element  $\mathfrak{m}$ . (Instead of Zorn's lemma, we could also use the fact that  $K[x_1, \dots, x_n]$  is Noetherian (see Corollary 2.13). But even then, the axiom of choice, which is equivalent to Zorn's lemma, would have to be used to do the proof without cheating. See Halmos [24] to learn more about Zorn's lemma and the axiom of choice.) So  $\mathfrak{m}$  is a maximal ideal with  $I \subseteq \mathfrak{m}$ . Now  $\mathcal{V}(I) \neq \emptyset$  follows by Theorem 1.7.  $\square$

- Remark.** (a) To see that the hypothesis that  $K$  is algebraically closed cannot be omitted from Corollary 1.8, consider the example  $K = \mathbb{R}$  and  $I = (x^2 + 1) \subsetneq \mathbb{R}[x]$ .
- (b) Hilbert's Nullstellensatz is really a theorem about systems of polynomial equations. Indeed, let  $f_1, \dots, f_m \in K[x_1, \dots, x_n]$  be polynomials. If there exist polynomials  $g_1, \dots, g_m \in K[x_1, \dots, x_n]$  such that

$$\sum_{i=1}^m g_i f_i = 1, \tag{1.1}$$

then obviously the system of equations

$$f_i(\xi_1, \dots, \xi_n) = 0 \quad \text{for } i = 1, \dots, m \tag{1.2}$$

has no solutions. But the existence of  $g_1, \dots, g_m$  satisfying (1.1) is equivalent to the condition  $(f_1, \dots, f_m) = K[x_1, \dots, x_n]$ . So Hilbert's Nullstellensatz says that if the obvious obstacle (1.1) to solvability does not exist, and if  $K$  is algebraically closed, then indeed the system (1.2) is solvable. In other words, for algebraically closed fields, the obvious

obstacle to the solvability of systems of polynomial equations is the only one! In Chapter 9 we will see how it can be checked algorithmically whether the obstacle (1.1) exists (see (9.4) on page 123).  $\triangleleft$

## 1.2 Jacobson Rings

The main goal of this section is to prove the second version of Hilbert's Nullstellensatz (Theorem 1.17). We start by defining the spectrum and the maximal spectrum of a ring.

**Definition 1.9.** *Let  $R$  be a ring.*

(a) The **spectrum** of  $R$  is the set of all prime ideals in  $R$ :

$$\operatorname{Spec}(R) := \{P \subset R \mid P \text{ is a prime ideal}\}.$$

(b) The **maximal spectrum** of  $R$  is the set of all maximal ideals in  $R$ :

$$\operatorname{Spec}_{\max}(R) := \{P \subset R \mid P \text{ is a maximal ideal}\}.$$

(c) We also define the **Rabinowitsch spectrum** of  $R$  as the set

$$\operatorname{Spec}_{\text{rab}}(R) := \{R \cap \mathfrak{m} \mid \mathfrak{m} \in \operatorname{Spec}_{\max}(R[x])\},$$

where  $R[x]$  is the polynomial ring over  $R$ . This is an ad hoc definition, which is not found in the standard literature and will be used only within this section.

**Remark.** The idea of using an additional indeterminate for proving the second version of Hilbert's Nullstellensatz goes back to J. L. Rabinowitsch [45], and is often referred to as Rabinowitsch's trick. This made my student Martin Kohls suggest that the set from Definition 1.9(c) be called the Rabinowitsch spectrum.  $\triangleleft$

We have the inclusions

$$\operatorname{Spec}_{\max}(R) \subseteq \operatorname{Spec}_{\text{rab}}(R) \subseteq \operatorname{Spec}(R).$$

Indeed, the second inclusion follows since for any prime ideal  $P \subset S$  in a ring extension  $S$  of  $R$ , the intersection  $R \cap P$  is a prime ideal in  $R$ . The first inclusion is proved in Exercise 1.3. Only the second inclusion will be used in this book. Exercise 1.4 gives an example in which both inclusions are strict. The importance of the Rabinowitsch spectrum is highlighted by Proposition 1.11.

Recall that for an ideal  $I \subseteq R$  in a ring  $R$ , the **radical ideal** of  $I$  is defined as

$$\sqrt{I} := \{f \in R \mid \text{there exists a positive integer } k \text{ with } f^k \in I\}.$$

$I$  is called a **radical ideal** if  $\sqrt{I} = I$ . For example, a nonzero ideal  $(a) \subseteq \mathbb{Z}$  is radical if and only if  $a$  is square-free. Recall that every prime ideal is a radical ideal.

**Lemma 1.10.** *Let  $R$  be a ring,  $I \subseteq R$  an ideal, and  $\mathcal{M} \subseteq \text{Spec}(R)$  a subset. Then*

$$\sqrt{I} \subseteq \bigcap_{\substack{P \in \mathcal{M}, \\ I \subseteq P}} P.$$

*If there exist no  $P \in \mathcal{M}$  with  $I \subseteq P$ , the intersection is to be interpreted as  $R$ .*

*Proof.* Let  $a \in \sqrt{I}$ , so  $a^k \in I$  for some  $k$ . Let  $P \in \mathcal{M}$  with  $I \subseteq P$ . Then  $a^k \in P$ . Since  $P$  is a prime ideal, it follows that  $a \in P$ .  $\square$

**Proposition 1.11** (The raison d'être of the Rabinowitsch spectrum). *Let  $I \subseteq R$  be an ideal in a ring. Then*

$$\sqrt{I} = \bigcap_{\substack{P \in \text{Spec}_{\text{rab}}(R), \\ I \subseteq P}} P.$$

*If there exist no  $P \in \text{Spec}_{\text{rab}}(R)$  with  $I \subseteq P$ , the intersection is to be interpreted as  $R$ .*

*Proof.* The inclusion “ $\subseteq$ ” follows from Lemma 1.10 and the fact that  $\text{Spec}_{\text{rab}}(R) \subseteq \text{Spec}(R)$ .

To prove the reverse inclusion, let  $a$  be in the intersection of all  $P \in \text{Spec}_{\text{rab}}(R)$  with  $I \subseteq P$ . Consider the ideal

$$J := (I \cup \{ax - 1\})_{R[x]} \subseteq R[x]$$

generated by  $I$  and by  $ax - 1$ . Assume that  $J \subsetneq R[x]$ . By Zorn's lemma, there exists  $\mathfrak{m} \in \text{Spec}_{\text{max}}(R[x])$  with  $J \subseteq \mathfrak{m}$ . We have  $I \subseteq R \cap J \subseteq R \cap \mathfrak{m} \in \text{Spec}_{\text{rab}}(R)$ , so by hypothesis,  $a \in \mathfrak{m}$ . But also  $ax - 1 \in \mathfrak{m}$ , so  $\mathfrak{m} = R[x]$ . This is a contradiction, showing that  $J = R[x]$ . In particular, we have

$$1 = \sum_{j=1}^n g_j b_j + g(ax - 1) \tag{1.3}$$

with  $g, g_1, \dots, g_n \in R[x]$  and  $b_1, \dots, b_n \in I$ . Let  $R[x, x^{-1}]$  be the ring of Laurent polynomials and consider the map  $\varphi: R[x] \rightarrow R[x, x^{-1}]$ ,  $f \mapsto f(x^{-1})$ . Applying  $\varphi$  to both sides of (1.3) and multiplying by some  $x^k$  yields

$$x^k = \sum_{j=1}^n h_j b_j + h(a - x) \quad \text{with} \quad h_j = x^k \varphi(g_j) \quad \text{and} \quad h = x^{k-1} \varphi(g).$$

For  $k \geq \max\{\deg(g_1), \dots, \deg(g_n), \deg(g) + 1\}$ , all  $h_j$  and  $h$  lie in  $R[x]$ , so we may substitute  $x = a$  in the above equation and obtain

$$a^k = \sum_{j=1}^n h_j(a)b_j \in I,$$

so  $a \in \sqrt{I}$ . This completes the proof.  $\square$

We get the following important consequence.

**Corollary 1.12** (Intersecting prime ideals). *Let  $R$  be a ring and  $I \subseteq R$  an ideal. Then*

$$\sqrt{I} = \bigcap_{\substack{P \in \text{Spec}(R), \\ I \subseteq P}} P.$$

*If there exist no  $P \in \text{Spec}(R)$  with  $I \subseteq P$ , the intersection is to be interpreted as  $R$ .*

*Proof.* This follows from Lemma 1.10 and Proposition 1.11.  $\square$

**Theorem 1.13** (Intersecting maximal ideals). *Let  $A$  be an affine algebra and  $I \subseteq A$  an ideal. Then*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \in \text{Spec}_{\max}(A), \\ I \subseteq \mathfrak{m}}} \mathfrak{m}.$$

*If there exist no  $\mathfrak{m} \in \text{Spec}_{\max}(A)$  with  $I \subseteq \mathfrak{m}$ , the intersection is to be interpreted as  $A$ .*

*Proof.* The inclusion “ $\subseteq$ ” again follows from Lemma 1.10.

Let  $P \in \text{Spec}_{\text{rab}}(A)$ . Then  $P = A \cap \mathfrak{m}$  with  $\mathfrak{m} \in \text{Spec}_{\max}(A[x])$ . But  $A[x]$  is finitely generated as an algebra over a field, so by Proposition 1.2 it follows that  $P \in \text{Spec}_{\max}(A)$ . We conclude that

$$\text{Spec}_{\text{rab}}(A) \subseteq \text{Spec}_{\max}(A).$$

(In fact, equality holds, but we do not need this.) Now the inclusion “ $\supseteq$ ” follows from Proposition 1.11.  $\square$

We pause here to make a definition, which is inspired by Theorem 1.13.

**Definition 1.14.** *A ring  $R$  is called a **Jacobson ring** if for every proper ideal  $I \subsetneq R$  the equality*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \in \text{Spec}_{\max}(R), \\ I \subseteq \mathfrak{m}}} \mathfrak{m}$$

*holds.*



So Theorem 1.13 says that every affine algebra is a Jacobson ring. A further example is the ring  $\mathbb{Z}$  of integers (see Exercise 1.6). So one wonders whether the polynomial ring  $\mathbb{Z}[x]$  is Jacobson, too. This is indeed the case. It is an instance of the general fact that every finitely generated algebra  $A$  over a Jacobson ring  $R$  is again a Jacobson ring. A proof is given in Eisenbud [17, Theorem 4.19]. There we also find the following: If  $\alpha$  is the homomorphism making  $A$  into an  $R$ -algebra, then for every  $\mathfrak{m} \in \text{Spec}_{\max}(A)$  the preimage  $\alpha^{-1}(\mathfrak{m})$  is also maximal. This is in analogy to Proposition 1.2.

A typical example of a non-Jacobson ring is the formal power series ring  $K[[x]]$  over a field  $K$  (see Exercise 1.2). A similar example is the ring of all rational numbers with odd denominator.

We can now prove the second version of Hilbert's Nullstellensatz. To formulate it, a bit of notation is useful.

**Definition 1.15.** Let  $K$  be a field and  $X \subseteq K^n$  a set of points. The (**vanishing**) **ideal** of  $X$  is defined as

$$\begin{aligned} \mathcal{I}(X) &= \mathcal{I}_{K[x_1, \dots, x_n]}(X) \\ &:= \{f \in K[x_1, \dots, x_n] \mid f(\xi_1, \dots, \xi_n) = 0 \text{ for all } (\xi_1, \dots, \xi_n) \in X\}. \end{aligned}$$

The index  $K[x_1, \dots, x_n]$  is omitted if no misunderstanding can occur.

**Remark 1.16.** It is clear from the definition that the ideal of a set of points is always a radical ideal.  $\triangleleft$

**Theorem 1.17** (Hilbert's Nullstellensatz, second version). Let  $K$  be an algebraically closed field and let  $I \subseteq K[x_1, \dots, x_n]$  be an ideal in a polynomial ring. Then

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

*Proof.* We start by showing the inclusion “ $\supseteq$ ”, which does not require  $K$  to be algebraically closed. Let  $f \in \sqrt{I}$ , so  $f^k \in I$  for some  $k$ . Take  $(\xi_1, \dots, \xi_n) \in \mathcal{V}(I)$ . Then  $f(\xi_1, \dots, \xi_n)^k = 0$ , so  $f(\xi_1, \dots, \xi_n) = 0$ . This shows that  $f \in \mathcal{I}(\mathcal{V}(I))$ .

For the reverse inclusion, assume  $f \in \mathcal{I}(\mathcal{V}(I))$ . In view of Theorem 1.13, we need to show that  $f$  lies in every  $\mathfrak{m} \in \mathcal{M}_I$ , where

$$\mathcal{M}_I = \{\mathfrak{m} \in \text{Spec}_{\max}(K[x_1, \dots, x_n]) \mid I \subseteq \mathfrak{m}\}.$$

So let  $\mathfrak{m} \in \mathcal{M}_I$ . By Theorem 1.7,  $\mathfrak{m} = (x_1 - \xi_1, \dots, x_n - \xi_n)_{K[x_1, \dots, x_n]}$  with  $(\xi_1, \dots, \xi_n) \in \mathcal{V}(I)$ . This implies  $f(\xi_1, \dots, \xi_n) = 0$ , so  $f \in \mathfrak{m}$ . This completes the proof.  $\square$

The following corollary is the heart of what we call the algebra–geometry lexicon. We need an (easy) lemma.

**Lemma 1.18.** Let  $K$  be a field and  $X \subseteq K^n$  an affine variety. Then

$$\mathcal{V}(\mathcal{I}(X)) = X.$$

*Proof.* By assumption,  $X = \mathcal{V}(S)$  with  $S \subseteq K[x_1, \dots, x_n]$ . So  $S \subseteq \mathcal{I}(X)$ , and applying  $\mathcal{V}$  yields

$$\mathcal{V}(\mathcal{I}(X)) \subseteq \mathcal{V}(S) = X \subseteq \mathcal{V}(\mathcal{I}(X)).$$

The lemma follows.  $\square$

**Corollary 1.19** (Ideal–variety correspondence). *Let  $K$  be an algebraically closed field and  $n$  a positive integer. Then there is a bijection between the sets*

$$\mathcal{A} := \{I \subseteq K[x_1, \dots, x_n] \mid I \text{ is a radical ideal}\}$$

and

$$\mathcal{B} := \{X \subseteq K^n \mid X \text{ is an affine variety}\},$$

given by

$$\mathcal{A} \rightarrow \mathcal{B}, \quad I \mapsto \mathcal{V}(I)$$

and the inverse map

$$\mathcal{B} \rightarrow \mathcal{A}, \quad X \mapsto \mathcal{I}(X).$$

Both maps reverse inclusions, i.e., if  $I, J \in \mathcal{A}$ , then

$$I \subseteq J \iff \mathcal{V}(J) \subseteq \mathcal{V}(I),$$

and the corresponding statement holds for the inverse map.

*Proof.* If  $I \in \mathcal{A}$  is a radical ideal, it follows from the Nullstellensatz (Theorem 1.17) that  $\mathcal{I}(\mathcal{V}(I)) = I$ . On the other hand, take  $X \in \mathcal{B}$ . Then  $\mathcal{I}(X) \in \mathcal{A}$  by Remark 1.16, and  $\mathcal{V}(\mathcal{I}(X)) = X$  by Lemma 1.18. This shows that the given maps are inverses to each other. The last statement follows since  $I \subseteq J$  implies  $\mathcal{V}(J) \subseteq \mathcal{V}(I)$  for  $I, J \in \mathcal{A}$ , and  $X \subseteq Y$  implies  $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$  for  $X, Y \in \mathcal{B}$ . Now apply  $\mathcal{I}$  and  $\mathcal{V}$  to get the converse implications.  $\square$

### 1.3 Coordinate Rings

The next part of the algebra–geometry lexicon is provided by assigning to an affine variety  $X$  an affine algebra, the coordinate ring  $K[X]$ , which encodes the properties of  $X$ .

**Definition 1.20.** *Let  $K$  be a field and  $X \subseteq K^n$  an affine variety. Let  $I := \mathcal{I}(X) \subseteq K[x_1, \dots, x_n]$  be the ideal of  $X$ . Then the **coordinate ring** of  $X$  is the quotient ring*

$$K[X] := K[x_1, \dots, x_n]/I.$$

*The coordinate ring is sometimes also called the **ring of regular functions** on  $X$ .*

**Remark 1.21.** (a) Every element of the coordinate ring  $K[X]$  of an affine variety is a class  $f + I$  with  $f \in K[x_1, \dots, x_n]$ . Such a class yields a well-defined function  $X \rightarrow K$ , given by  $(\xi_1, \dots, \xi_n) \mapsto f(\xi_1, \dots, \xi_n)$ , and different classes yield different functions. So  $K[X]$  can be identified with an algebra of functions  $X \rightarrow K$ . The functions from  $K[X]$  are called **regular functions**. They are precisely those functions  $X \rightarrow K$  that are given by polynomials.

- (b) If  $X = \mathcal{V}(J)$  with  $J \subseteq K[x_1, \dots, x_n]$  an ideal, then it is not necessarily true that  $K[X] = K[x_1, \dots, x_n]/J$ . However, if  $K$  is algebraically closed, then  $K[X] = K[x_1, \dots, x_n]/\sqrt{J}$  by the Nullstellensatz (Theorem 1.17).  $\triangleleft$

The following lemma compares ideals in a quotient ring  $R/I$  to ideals in  $R$ . It is rather boring and elementary, but very important.

**Lemma 1.22** (Ideals in quotient rings). *Let  $R$  be a ring and let  $I \subseteq R$  be an ideal. Consider the sets*

$$\mathcal{A} := \{J \subseteq R \mid J \text{ is an ideal and } I \subseteq J\}$$

and

$$\mathcal{B} := \{\mathcal{J} \subseteq R/I \mid \mathcal{J} \text{ is an ideal}\}.$$

The map

$$\Phi: \mathcal{A} \rightarrow \mathcal{B}, \quad J \mapsto \{a + I \mid a \in J\} = J/I$$

is an inclusion-preserving bijection with inverse map

$$\Psi: \mathcal{B} \rightarrow \mathcal{A}, \quad \mathcal{J} \mapsto \{a \in R \mid a + I \in \mathcal{J}\}.$$

If  $J \in \mathcal{A}$ , then

$$R/J \cong (R/I) / \Phi(J), \tag{1.4}$$

and there are equivalences

$$J \text{ is a prime ideal} \iff \Phi(J) \text{ is a prime ideal}$$

and

$$J \text{ is a maximal ideal} \iff \Phi(J) \text{ is a maximal ideal}.$$

Moreover, if  $J = (a_1, \dots, a_n)_R$  with  $a_i \in R$ , then  $\Phi(J) = (a_1 + I, \dots, a_n + I)_{R/I}$ .

*Proof.* It is easy to check that  $\Phi$  and  $\Psi$  are inclusion-preserving maps and that  $\Psi \circ \Phi = \text{id}_{\mathcal{A}}$  and  $\Phi \circ \Psi = \text{id}_{\mathcal{B}}$ . The isomorphism (1.4) follows since  $\Phi(J)$  is the kernel of the epimorphism  $R/I \rightarrow R/J$ ,  $a + I \mapsto a + J$ . Both equivalences follow from (1.4). The last statement is also clear.  $\square$

If  $X \subseteq K^n$  is an affine variety, then a **subvariety** is a subset  $Y \subseteq X$  that is itself an affine variety in  $K^n$ . We can now prove a correspondence between subvarieties of a variety and radical ideals in the coordinate ring.

**Theorem 1.23** (Correspondence subvarieties–radical ideals). *Let  $X$  be an affine variety over an algebraically closed field  $K$ . Then there is an inclusion-reversing bijection between the set of subvarieties  $Y \subseteq X$  and the set of radical ideals  $J \subseteq K[X]$ . The bijection is given by mapping a subvariety  $Y \subseteq X$  to  $\mathcal{I}(Y)/\mathcal{I}(X) \subseteq K[X]$ , and mapping an ideal  $J \subseteq K[X]$  to*

$$\mathcal{V}_X(J) := \{x \in X \mid f(x) = 0 \text{ for all } f \in J\}.$$

*If  $J \subseteq K[X]$  is the ideal corresponding to a subvariety  $Y$ , then*

$$K[Y] \cong K[X]/J,$$

*with an isomorphism given by  $K[X]/J \rightarrow K[Y]$ ,  $f + J \mapsto f|_Y$ .*

*Restricting our bijection to subvarieties consisting of one point yields a bijection*

$$X \rightarrow \operatorname{Spec}_{\max}(K[X]), \quad x \mapsto \mathcal{I}(\{x\})/\mathcal{I}(X).$$

*Proof.* All claims are shown by putting Corollary 1.19 and Lemma 1.22 together.  $\square$

Another correspondence between points and algebraic objects that relates to the coordinate ring is given in Exercise 1.11. The next theorem tells us which types of rings occur as coordinate rings of affine algebras. To state it, we need a definition.

**Definition 1.24.** *Let  $R$  be a ring.*

- (a) *An element  $a \in R$  is called **nilpotent** if there exists a positive integer  $k$  with  $a^k = 0$ .*
- (b) *The set of all nilpotent elements is called the **nilradical** of  $R$ , written as  $\operatorname{nil}(R)$ . (So the nilradical is equal to the radical ideal  $\sqrt{\{0\}}$  of the zero ideal, which by Corollary 1.12 is the intersection of all prime ideals.)*
- (c)  *$R$  is called **reduced** if  $\operatorname{nil}(R) = \{0\}$ . (In particular, every integral domain is reduced.)*

**Theorem 1.25** (Coordinate rings and reduced algebras). *Let  $K$  be a field.*

- (a) *For every affine  $K$ -variety  $X$ , the coordinate ring  $K[X]$  is a reduced affine  $K$ -algebra.*
- (b) *Suppose that  $K$  is algebraically closed, and let  $A$  be a reduced affine  $K$ -algebra. Then there exists an affine  $K$ -variety  $X$  with  $K[X] \cong A$ .*

*Proof.* (a) With  $I = \mathcal{I}(X)$ , we have  $K[X] = K[x_1, \dots, x_n]/I$ , so  $K[X]$  is an affine algebra, and it is reduced since  $I$  is a radical ideal.

(b) Choose generators  $a_1, \dots, a_n$  of  $A$ . Then the epimorphism

$$\varphi: K[x_1, \dots, x_n] \rightarrow A, \quad f \mapsto f(a_1, \dots, a_n)$$

yields  $A \cong K[x_1, \dots, x_n]/I$  with  $I = \ker(\varphi)$ . Since  $A$  is reduced,  $I$  is a radical ideal. Set  $X := \mathcal{V}(I)$ . By the Nullstellensatz (Theorem 1.17),  $I = \mathcal{I}(X)$ , so  $A \cong K[X]$ .  $\square$

**Remark.** The affine variety  $X$  in Theorem 1.25(b) is not uniquely determined. In fact, in the proof we have given,  $X$  depends on the choice of the generators of  $A$ . However, given the correct concept of an isomorphism of varieties (see Definition 3.4), it can be shown that all affine varieties with coordinate ring  $A$  are isomorphic. In fact, we get a bijective correspondence between isomorphism classes of affine  $K$ -varieties and isomorphism classes of reduced affine  $K$ -algebras.  $\triangleleft$

## Exercises for Chapter 1

**1.1 (Some counterexamples).** Give examples which show that none of the hypotheses in Lemma 1.1(a) and (b) and in Proposition 1.2 can be omitted.

**1.2 (Formal power series ring).** Consider the formal power series ring

$$K[[x]] := \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in K \right\}$$

over a field  $K$ .

- (a) Show that  $K[[x]]$  is an integral domain.
- (b) Show that all power series  $f = \sum_{i=0}^{\infty} a_i x^i$  with  $a_0 \neq 0$  are invertible in  $K[[x]]$ . Assuming for a moment that  $K$  is only a ring, show that  $f$  is invertible if and only if  $a_0$  is invertible in  $K$ .
- (c) Show that  $K[[x]]$  has exactly one maximal ideal  $\mathfrak{m}$ , i.e.,  $K[[x]]$  is a local ring (see Definition 6.7).
- (d) Show that  $K[[x]]$  is not a Jacobson ring.
- (e) Show that the ring

$$L := \left\{ \sum_{i=k}^{\infty} a_i x^i \mid k \in \mathbb{Z}, a_i \in K \right\}$$

of formal Laurent series is a field. The field  $L$  of formal Laurent series is often written as  $K((x))$ .

- (f) Is  $K[[x]]$  finitely generated as a  $K$ -algebra?

**1.3 (Maximal spectrum and Rabinowitsch spectrum).** Let  $R$  be a ring. Show that

$$\mathrm{Spec}_{\max}(R) \subseteq \mathrm{Spec}_{\mathrm{rab}}(R).$$

(Solution on page 217)

**\*1.4 (Three types of spectra).** Let  $R = K[[y]]$  be the formal power series ring over a field  $K$ , and let  $S = R[z]$  be a polynomial ring over  $R$ . Show that

$$\operatorname{Spec}_{\max}(S) \subsetneq \operatorname{Spec}_{\text{rab}}(S) \subsetneq \operatorname{Spec}(S).$$

*Hint:* Consider the ideals  $(y)_S$  and  $(z)_S$ .

**1.5 (Jacobson rings).** Show that for verifying that a ring  $R$  is a Jacobson ring it is enough to check that every prime ideal  $P \in \operatorname{Spec}(R)$  is an intersection of maximal ideals.

**1.6 ( $\mathbb{Z}$  is a Jacobson Ring).** Show that the ring  $\mathbb{Z}$  of integers is a Jacobson ring.

**1.7 (Explicit computations with a variety).** Consider the ideal

$$I = (x_1^4 + x_2^4 + 2x_1^2x_2^2 - x_1^2 - x_2^2) \subseteq \mathbb{R}[x_1, x_2].$$

- (a) Determine  $X := \mathcal{V}(I) \subseteq \mathbb{R}^2$  and draw a picture.
- (b) Is  $I$  a prime ideal? Is  $I$  a radical ideal?
- (c) Does Hilbert's Nullstellensatz (Theorem 1.17) hold for  $I$ ?

**1.8 (Colon ideals).** If  $I$  and  $J \subseteq R$  are ideals in a ring, the **colon ideal** is defined as

$$I : J := \{a \in R \mid a \cdot b \in I \text{ for all } b \in J\}.$$

In this exercise we give a geometric interpretation of the colon ideal.

- (a) Set  $\mathcal{M} := \{P \in \operatorname{Spec}(R) \mid I \subseteq P \text{ and } J \not\subseteq P\}$  and show that

$$\sqrt{I} : J = \bigcap_{P \in \mathcal{M}} P.$$

- (b) Let  $K$  be a field and  $X, Y \subseteq K^n$  such that  $Y$  is an affine variety. Show that

$$\mathcal{I}(X) : \mathcal{I}(Y) = \mathcal{I}(X \setminus Y).$$

**1.9 (A generalization of Hilbert's Nullstellensatz).** Let  $K$  be a field and  $\bar{K}$  its algebraic closure. Let  $I \subseteq K[x_1, \dots, x_n]$  be an ideal in a polynomial ring. Show that

$$\mathcal{I}_{K[x_1, \dots, x_n]}(\mathcal{V}_{\bar{K}^n}(I)) = \sqrt{I}.$$

**1.10 (Order-reversing maps).** This exercise puts Corollary 1.19 and its proof in a more general framework. Let  $\mathcal{A}'$  and  $\mathcal{B}'$  be two partially ordered sets. Let  $\varphi: \mathcal{A}' \rightarrow \mathcal{B}'$  and  $\psi: \mathcal{B}' \rightarrow \mathcal{A}'$  be maps satisfying the following properties:

- (1) If  $a_1, a_2 \in \mathcal{A}'$  with  $a_1 \leq a_2$ , then  $\varphi(a_1) \geq \varphi(a_2)$ ;
- (2) if  $b_1, b_2 \in \mathcal{B}'$  with  $b_1 \leq b_2$ , then  $\psi(b_1) \geq \psi(b_2)$ ;
- (3) if  $a \in \mathcal{A}'$ , then  $\psi(\varphi(a)) \geq a$ ;
- (4) if  $b \in \mathcal{B}'$ , then  $\varphi(\psi(b)) \geq b$ .

Set  $\mathcal{A} := \psi(\mathcal{B}')$  and  $\mathcal{B} := \varphi(\mathcal{A}')$ , and show that the restriction

$$\varphi|_{\mathcal{A}}: \mathcal{A} \rightarrow \mathcal{B}$$

is a bijection with inverse map  $\psi|_{\mathcal{B}}$ .

*Remark:* In the light of this exercise, all that is needed for the proof of Corollary 1.9 is that all radical ideals in  $K[x_1, \dots, x_n]$  occur as vanishing ideals of sets of points in  $K^n$  (which is a consequence of Theorem 1.17). Another typical situation in which this exercise applies is the correspondence between subgroups and intermediate fields in Galois theory.

**1.11 (Points of a variety and homomorphisms).** Let  $K$  be a (not necessarily algebraically closed) field and  $X$  a  $K$ -variety. Construct a bijection between  $X$  and the set

$$\mathrm{Hom}_K(K[X], K) := \{\varphi: K[X] \rightarrow K \mid \varphi \text{ is an algebra homomorphism}\}.$$

*Remark:* In the language of affine schemes, an algebra homomorphism  $K[X] \rightarrow K$  induces a morphism  $\mathrm{Spec}(K) \rightarrow \mathrm{Spec}(K[X])$ . Such a morphism is called a  $K$ -rational point of the affine scheme associated to  $X$ .



<http://www.springer.com/978-3-642-03544-9>

A Course in Commutative Algebra

Kemper, G.

2011, XII, 248 p., Hardcover

ISBN: 978-3-642-03544-9