# ALGEBRAIC GEOMETRY (NMAG401)

JAN ŠŤOVÍČEK

## Contents



## 1. Affine varieties

The basic objects which we will be concerned with in this chapter are the solution sets of systems of polynomial equations over a field.

In what follows, $K$ will be a field and $\overline{K}$ will denote its algebraic closure. Algebraically closed fields are important because they are often best behaved from the viewpoint of solving polynomial equations. Typical examples of fields which we may consider are $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\overline{\mathbb{Q}}$, finite fields $\mathbb{F}_q$ and their algebraic closures $\overline{\mathbb{F}_q}$.

The set of all polynomials over $K$ in variables $x_1, \dots, x_n$ will be denoted by $K[x_1, x_2, \dots, x_n]$. The polynomials with the natural operations form a commutative $K$-algebra. Recall that a *commutative $K$-algebra* is, by definition, a set $R$ together with structures of

(1) a commutative ring $(R, +, -, 0, *, 1)$ and
(2) a vector space $(R, +, -, 0, k \cdot - \ (k \in K))$,

such that the operations $+, -, 0$ are common to both the structures and, moreover, for each $k \in K$ and $f, g \in R$ we have the equality $(k \cdot f) * g = k \cdot (f * g)$.

We will encounter several others $K$-algebras further in the text. In practice one usually denotes the multiplication in $R$ and the scalar multiplication by elements of $K$ by the same symbol. This does not cause any confusion since if $R$ has at least two elements, the field $K$ can be identified with a subfield of $R$ via the embedding

$$K \rightarrowtail R, \qquad k \mapsto k \cdot 1.$$

We will also need the notion of homomorphism of $K$-algebras, which is by definition simply a map $\varphi\colon R \to S$ between $K$-algebras which is simultaneously a homomorphism of rings and vector spaces.

Version from November 26, 2018.

Another basic notion is one of *affine space* of dimension $n \geq 1$ over the field $K$. It is defined simply as the Cartesian product

$$\mathbb{A}^n_K = \underbrace{K \times K \times \cdots \times K}_{n \text{ times}}$$

Given a point $P = (a_1, \dots, a_n)$ of the affine space $\mathbb{A}^n_K$ and a polynomial $f \in K[x_1, x_2, \dots, x_n]$, the value of $f$ at $P$ is

$$f(P) = f(a_1, \dots, a_n) \in K.$$

It is useful to note that if $P$ is fixed, the map

$$K[x_1, x_2, \dots, x_n] \to K, \qquad f \mapsto f(P)$$

is a homomorphisms of $K$-algebras which is called *evaluation homomorphism.*

We say that $P$ is a *zero* of $f$ if $f(P) = 0$. Given a set $S \subseteq K[x_1, x_2, \dots, x_n]$, the set of all common zeros of all the polynomials in $S$ will be denoted by $\mathrm{V}(S)$. That is,

$$\mathrm{V}(S) = \{P \in \mathbb{A}^n_K \mid f(P) = 0 \ (\forall f \in S)\}$$

If $S = \{f_1, \dots, f_r\}$ is finite, we will often write $\mathrm{V}(f_1, \dots, f_r)$ in place of $\mathrm{V}(S)$.

This brings us to a key definition.

**Definition.** An *affine algebraic set* over a field $K$ is a subset of an affine space $\mathbb{A}^n_K$ of the form $\mathrm{V}(S)$, where $n \geq 1$ and $S \subseteq K[x_1, x_2, \dots, x_n]$ is a set of polynomials.

Thus, an affine algebraic set is none other than the solution set of a (possibly infinite) system of polynomial equations over $K$. We will often leave out the adjective 'affine' where there is no danger of confusion, e.g. before we start to discuss projective geometry and projective algebraic sets.

Some elementary properties of algebraic sets are summarized in the following lemma.

**Lemma 1.** *Let $K$ be a field and $n \geq 1$. Then:*

1. *$\varnothing$ and $\mathbb{A}^n_K$ are algebraic sets.*
2. *Arbitrary intersections of algebraic subsets of $\mathbb{A}^n_K$ are again algebraic sets.*
3. *Finite unions of algebraic subsets of $\mathbb{A}^n_K$ are again algebraic sets.*

*Proof.* (1) We have $\varnothing = \mathrm{V}(1)$ a $\mathbb{A}^n_K = \mathrm{V}(0)$.

(2) Use that $\bigcap_{i \in I} \mathrm{V}(S_i) = \mathrm{V}(\bigcup_{i \in I} S_i)$.

(3) One checks that given sets $S_1, \dots, S_n$ of polynomials, we have

$$\mathrm{V}(S_1) \cup \mathrm{V}(S_2) \cup \cdots \cup \mathrm{V}(S_r) = \mathrm{V}(S_1 S_2 \cdots S_r),$$

where

$$S_1 S_2 \cdots S_r = \{f_1 f_2 \cdots f_r \mid f_i \in S_i \ (\forall i = 1, 2, \dots, r)\}. \qquad \square$$

Lemma 1 is on one hand completely constructive, but on the other hand especially part (3) may lead to inconveniently large systems of equations in direct computations.

The main point of the latter lemma is that algebraic sets fit well with the definition of the collection of closed sets in a topological space. To that end, let us recall the definition of a topological space, which is meant to be an abstraction of the properties of open and closed subsets of Euclidean spaces, so that one can abstractly argue about notions like continuous maps, dense subsets or closures of sets.

**Definition.** A *topological space* is a pair $(X, \tau)$, where $X$ is a set and $\tau$ is a set of subsets of $X$ such that:

(1) $\varnothing$ and $X$ belong to $\tau$.
(2) Arbitrary unions $\bigcup_{i \in I} U_i$ of elements $U_i \in \tau$ are again in $\tau$.
(3) Finite intersections $U_1 \cap U_2 \cap \cdots \cap U_r$ of elements $U_1, U_2, \ldots, U_r \in \tau$ are elements of $\tau$.

The subsets of $X$ which belong to $\tau$ are called *open subsets* of $X$ and their complements are called *closed subsets* of $X$.

As was already mentioned, algebraic subsets of $\mathbb{A}^n_K$ then form closed subsets of a topology by Lemma 1.

**Definition.** The topology on $\mathbb{A}^n_K$ whose closed subsets are the algebraic sets is called the *Zariski topology.*

In order to exhibit one of the crucial properties of the Zariski topology, we need the following

*Observation.* Consider a set $S \subseteq K[x_1, x_2, \ldots, x_n]$ of polynomials and let $I$ be the ideal generated by $S$. In details,

$$I = \{\sum_{i=1}^{r} a_i f_i \mid r \geq 0, f_1, \ldots, f_r \in S \text{ and } a_1, \ldots, a_r \in K[x_1, x_2, \ldots, x_n]\},$$

i.e. $I$ consists of all linear combinations of elements of $S$ with coefficients from the ring $K[x_1, x_2, \ldots, x_n]$.

Then we have $\mathrm{V}(S) = \mathrm{V}(I)$. Indeed, on one hand $\mathrm{V}(S) \supseteq \mathrm{V}(I)$ since $S \subseteq I$. On the other hand, any point $P \in \mathrm{V}(S)$ is a zero of each polynomial from $I$ by the above description of $I$.

Therefore, one can expect that properties of algebraic sets will depend on those of ideals of polynomial rings. One fundamental feature of these rings is that they are noetherian.

**Definition.** A commutative ring $R$ is called *noetherian* if it satisfies either of the equivalent conditions (the equivalence is not proved here, we refer to standard courses or textbooks in commutative algebra, e.g. to [AM69, Chapter 6]):

(1) Each ideal $I \subseteq R$ is finitely generated, i.e. there is $r \geq 0$ and polynomials $f_1, f_2, \ldots, f_r \in I$ such that
$$I = \{\sum_{i=1}^{r} a_i f_i \mid a_1, \ldots, a_r \in K[x_1, x_2, \ldots, x_n]\}.$$
(2) Each non-decreasing chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ of $R$ stabilizes. That is, there exists $N \geq 1$ such that $I_N = I_{N+1} = I_{N+2} = \cdots$.

**Proposition 2** (Hilbert Basis Theorem)**.** *If $R$ is a noetherian ring, so is the ring $R[x]$. In particular, $K[x_1, x_2, \dots, x_n]$ is noetherian for each field $K$ and natural number $n \geq 1$.*

*Proof.* See for instance [AM69, Theorem 7.5]. $\square$

We obtain as immediate consequences chain conditions of algebraic sets and their complements, as well as the fact that each algebraic set is determined by a finite collection of equations.

**Corollary 3.** *For each algebraic set $X \subseteq \mathbb{A}^n_K$ there exist $r \geq 0$ and polynomials $f_1, f_2, \dots, f_r \in K[x_1, x_2, \dots, x_n]$ so that $X = \mathrm{V}(f_1, f_2, \dots, f_r)$.*

*Proof.* Let $I \subseteq K[x_1, x_2, \dots, x_n]$ be an ideal such that $X = \mathrm{V}(I)$ (we are using the previous observation) and choose a set of generators $f_1, f_2, \dots, f_r$ of $I$. Then $X = \mathrm{V}(f_1, f_2, \dots, f_r)$. $\square$

**Corollary 4.** *Let $K$ be a field and $n \geq 1$.*

(1) *Each non-increasing chain $X_0 \supseteq X_1 \supseteq X_2 \supseteq \cdots$ of algebraic (equivalently: Zariski closed) subsets of $\mathbb{A}^n_K$ stabilizes.*
(2) *Each non-decreasing chain $U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$ of Zariski open subsets of $\mathbb{A}^n_K$ stabilizes.*

*Proof.* In view of De Morgan laws, it suffices to prove the first statement. To that end, consider a chain $X_0 \supseteq X_1 \supseteq X_2 \supseteq \cdots$ of algebraic subsets of $\mathbb{A}^n_K$ and for each $X_j$ an ideal $I_j \subseteq K[x_1, x_2, \dots, x_n]$ such that $X_j = \mathrm{V}(I_j)$.

We may without loss of generality assume that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Indeed, note that $\mathrm{V}(I_2) = \mathrm{V}(I_1 + I_2)$, $\mathrm{V}(I_3) = \mathrm{V}(I_1 + I_2 + I_3)$, and in general $\mathrm{V}(I_j) = \mathrm{V}(\sum_{k=1}^{j} I_k)$. We can therefore replace each $I_j$ by the sum $\sum_{k=1}^{j} I_k$ and the sums are ordered by the inclusion as required.

However, the chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ must stabilize by Proposition 2. That is, there is $N \geq 1$ such that $I_N = I_{N+1} = I_{N+2} = \cdots$, and hence $X_N = X_{N+1} = X_{N+2} = \cdots$. $\square$

The latter corollary inspires the coming definition.

**Definition.** A topological space $(X, \tau)$ is *noetherian* if each non-decreasing chain $U_0 \subseteq U_1 \subseteq U_2 \subseteq \cdots$ of open subsets stabilizes.

*Example.* Consider the natural Euclidean topology on the set of complex numbers. It is *not* noetherian since we for instance have the strictly increasing chain of open discs $U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots$ as in Figure 1:

$$U_j = \{z \in \mathbb{C} \mid ||z|| < j\}.$$

*Example.* Since a non-zero polynomial in $\mathbb{C}[x]$ has only finitely many zeros, algebraic subsets of $\mathbb{A}^1_{\mathbb{C}}$ are precisely the finite subsets of $\mathbb{A}^1_{\mathbb{C}}$ and all of $\mathbb{A}^1_{\mathbb{C}}$. It is now easy to verify condition (1) from Corollary 4 for $\mathbb{A}^1_{\mathbb{C}}$ directly.

By now we know that $\mathbb{A}^n_K$ is a noetherian topological space. More generally, given any algebraic subset $X \subseteq \mathbb{A}^n_K$, the algebraic subsets of $X$ form a topology on $X$, which is again called the *Zariski topology* and which is obviously again noetherian.

Although the following definition in principle makes sense for arbitrary topological spaces, it is mainly useful for the noetherian ones.

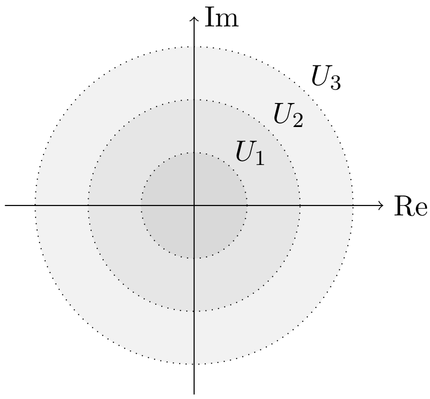


FIGURE 1. The reason why the Euclidean topology on $\mathbb{C}$ is not noetherian.

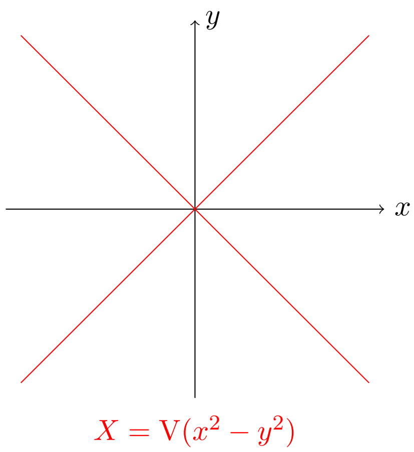


FIGURE 2. An example of a reducible algebraic set – $X$ is the union of $X_1 = \mathrm{V}(x - y)$ and $X_2 = \mathrm{V}(x + y)$.

**Definition.** A non-empty topological space $(X, \tau)$ is called *reducible* if it can be expressed as $X = X_1 \cup X_2$ where $X_1, X_2 \subsetneqq X$ are proper closed subsets. Otherwise it is called *irreducible*.

A simple example of a reducible algebraic set can be seen in Figure 2. Note also that if we work over an infinite field, both the lines in Figure 2 are already irreducible. This is because an algebraic proper subset of a line is finite.

There is a special terminology for algebraic sets which are irreducible.

**Definition.** An irreducible affine algebraic set is called an *affine variety*.

*Remark.* The terminology is unfortunately not completely unified in the literature. Some authors use the term ‘variety’ for all algebraic sets and then they speak of ‘irreducible varieties’ when necessary.

The main result about irreducibility is the following theorem, which in particular implies that each algebraic set $X$ can be expressed in a unique

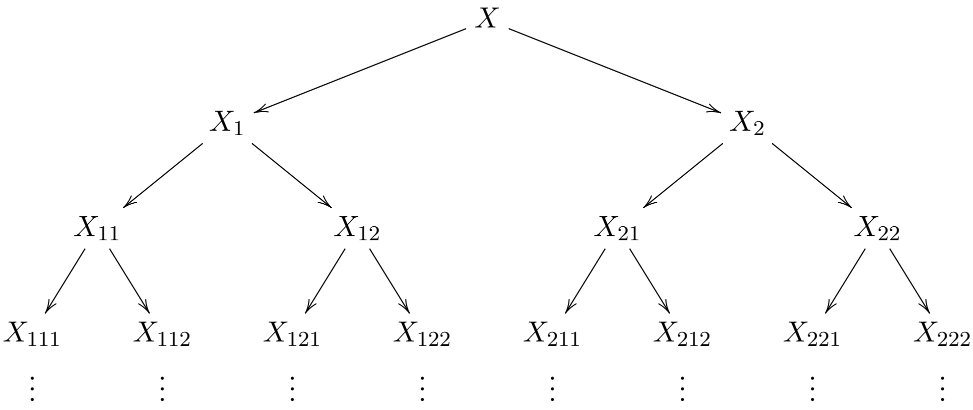

FIGURE 3. A tree of closed subsets of $X$ in the proof of Theorem 5.

way as an irredundant union of varieties. The varieties in such an expression are called the *irreducible components* of $X$.

**Theorem 5.** *Let $(X, \tau)$ be a non-empty noetherian topological space. Then there exists an expression $X = Z_1 \cup Z_2 \cup \cdots \cup Z_r$ where $r \geq 1$ and $Z_1, Z_2, \dots, Z_r$ are irreducible closed subsets of $X$ such that $Z_i \not\subseteq Z_j$ whenever $i \neq j$. Such an expression of $X$ is unique up to reordering the terms in the union.*

*Proof.* We first claim that $X$ can be expressed as a finite union of irreducible closed subsets (see also the remark below for another and perhaps more standard argument). If $X$ itself is irreducible, we are done. Otherwise we can express $X$ as a union $X = X_1 \cup X_2$ of closed subsets properly contained in $X$. If both $X_1$ and $X_2$ are irreducible, we are done. If not, say if $X_1$ is reducible, we write $X_1 = X_{11} \cup X_{12}$, and similarly for $X_2$. If we continue like that by induction, we can construct a tree as in Figure 3. It is at most countable, it has $X$ as the root and each vertex has at most two children, all the arrows stand for proper inclusions of closed subsets of $X$, and its leaves are labeled by irreducible subsets.

If the tree is finite, we are done as $X$ is the union of the irreducible closed subsets at the leaves by the construction. Thus, let us assume for the moment that the tree is infinite. Since all the vertices have finitely many children, we can use a combinatorial result, so-called Kőnig's Lemma, which says that the tree must have an infinite branch

$$X \xrightarrow{\supsetneq} X_{i_1} \xrightarrow{\supsetneq} X_{i_1 i_2} \xrightarrow{\supsetneq} X_{i_1 i_2 i_3} \xrightarrow{\supsetneq} \cdots .$$

However, the existence of such a branch contradicts the assumption on $(X, \tau)$, so the tree must have been finite and the claim is proved.

Let now consider an expression $X = Z_1 \cup Z_2 \cup \cdots \cup Z_r$ with all the $Z_i$ irreducible and $r \geq 1$ smallest possible. Then clearly $Z_i \not\subseteq Z_{i'}$ whenever $i \neq i'$, or else we would have $X = Z_1 \cup \cdots \cup Z_{i-1} \cup Z_{i+1} \cup \cdots \cup Z_r$

To prove the uniqueness, suppose that $X = Y_1 \cup \cdots \cup Y_s$ is another expression with the $Y_j$ irreducible and $Y_j \not\subseteq Y_{j'}$ whenever $j \neq j'$. Note that for each $1 \leq i \leq r$ we have

$$Z_i = Z_i \cap X = Z_i \cap \bigcup_{j=1}^{s} Y_j = \bigcup_{j=1}^{s} (Z_i \cap Y_j).$$

Since $Z_i$ is irreducible, we must have $Z_i = Z_i \cap Y_j$, or in other words $Z_i \subseteq Y_j$ for some $1 \leq j \leq s$. Similarly, for any $Y_j$ there exists $Z_{i'}$ such that $Y_j \subseteq Z_{i'}$. By combining the two observations, for each $i$ there are indices $j$ and $i'$ such that

$$Z_i \subseteq Y_j \subseteq Z_{i'}.$$

However, in such a situation the assumptions enforce $i = i'$ and $Z_i = Y_j$. Moreover, given any $i$, the index $j$ such that $Z_i = Y_j$ must be unique. Similarly, for each $j$ there exists a unique $i$ with $Y_j = Z_i$. It follows that $r = s$ and there is a permutation $\sigma$ such that $Z_i = Y_{\sigma(i)}$ for each $1 \leq i \leq r$. $\square$

*Remark.* The existence part of the latter theorem is often proved without Kőnig's Lemma using the following observation about noetherian topological spaces:

Given any *non-empty* collection $\mathcal{S}$ of closed subsets of a noetherian topological space $(X, \tau)$, there exists an element of $\mathcal{S}$ which is minimal with respect to inclusion. To see that, suppose that the converse is true. Since $\mathcal{S}$ is non-empty, we can pick a closed set $Z_1 \in \mathcal{S}$. Since $Z_1$ is not minimal, there exists $Z_2 \in \mathcal{S}$ with $Z_1 \supsetneqq Z_2$. Since $Z_2$ is not minimal in $\mathcal{S}$ either, we find $Z_3 \in \mathcal{S}$ such that $Z_2 \supsetneqq Z_3$, and so on. By induction, we can thus construct a chain

$$Z_1 \supsetneqq Z_2 \supsetneqq Z_3 \supsetneqq Z_4 \supsetneqq \cdots$$

in $\mathcal{S}$, which again contradicts the assumption that $(X, \tau)$ is noetherian.

In fact, the latter observation characterizes noetherian topological spaces.

Suppose now that $(X, \tau)$ is a noetherian topological space. At this point we can easily prove that each closed subset $Z \subseteq X$ is a finite union of irreducible ones, which implies the existence part of Theorem 5. Indeed, if this is not the case, there must be a closed subset $Z \subseteq X$ which is not a finite union of irreducible ones and is minimal such with respect to inclusion. In particular $Z$ is not irreducible itself, so that $Z = Z_1 \cup Z_2$ for some $Z_1, Z_2 \subsetneqq Z$. By the minimality, both $Z_1$ and $Z_2$ are finite unions of irreducible closed subsets, and so must be $Z$ – a contradiction.

We conclude the section by an algebraic characterization of irreducibility. Given a set of polynomials $S$, we defined the set $\mathrm{V}(S) = \{P \in \mathbb{A}^n_K \mid f(P) = 0\ (\forall f \in S)\}$ of their common zeros. We can also reverse the process, start with a subset $X$ of an affine space $\mathbb{A}^n_K$ and consider the set of all polynomials which vanish everywhere on $X$.

**Definition.** The *ideal of a set* $X \subseteq \mathbb{A}^n_K$ is defined as

$$\mathrm{I}(X) = \{f \in K[x_1, x_2, \ldots, x_n] \mid f(P) = 0\ (\forall P \in X)\}.$$

One readily checks that $\mathrm{I}(X) \subseteq K[x_1, x_2, \ldots, x_n]$ is indeed an ideal of the polynomial ring, so the terminology is consistent. Basic properties of the two assignments $S \mapsto \mathrm{V}(S)$ and $X \mapsto \mathrm{I}(X)$ and their relation are summarized in the following lemma.

**Lemma 6.** *Let $K$ be a field, $n \geq 1$, $X, X_1, X_2 \subseteq \mathbb{A}^n_K$ and $S, S_1, S_2 \subseteq K[x_1, x_2, \ldots, x_n]$.*

(1) *If $X_1 \subseteq X_2$, then $\mathrm{I}(X_1) \supseteq \mathrm{I}(X_2)$.*
(2) *If $S_1 \subseteq S_2$, then $\mathrm{V}(S_1) \supseteq \mathrm{V}(S_2)$.*
(3) *$\mathrm{I}(\varnothing) = K[x_1, x_2, \ldots, x_n]$ and, if the field $K$ is infinite, we also have $\mathrm{I}(\mathbb{A}^n_K) = \{0\}$.*
(4) *$\mathrm{I}(\mathrm{V}(S)) \supseteq S$ and $\mathrm{V}(\mathrm{I}(X)) \supseteq X$. Moreover, $\overline{X} := \mathrm{V}(\mathrm{I}(X))$ is the smallest algebraic subset of $\mathbb{A}^n_K$ containing $X$. In other words, $\overline{X}$ is the closure of $X$ with respect to the Zariski topology.*
(5) *$\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) = \mathrm{I}(X)$ and $\mathrm{V}(\mathrm{I}(\mathrm{V}(S))) = \mathrm{V}(S)$.*

*Proof.* Parts (1), (2), (3) and (4) are completely straightforward once one unravels the definitions. The single exception is the equality $\mathrm{I}(\mathbb{A}^n_K) = \{0\}$ for $K$ infinite, where we refer to Exercise 5.

To prove (5), note that $\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) \supseteq \mathrm{I}(X)$ and $\mathrm{V}(\mathrm{I}(X)) \supseteq X$ by (4), and hence also $\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) \subseteq \mathrm{I}(X)$ by (1). It follows that $\mathrm{I}(\mathrm{V}(\mathrm{I}(X))) = \mathrm{I}(X)$ and the proof of the other equality is analogous. $\square$

Now one easily obtains the following important result.

**Theorem 7.** *Let $K$ be a field and $X \subseteq \mathbb{A}^n_K$ a non-empty algebraic set. Then $X$ is irreducible if and only if $\mathrm{I}(X)$ is a prime ideal of $K[x_1, x_2, \ldots, x_n]$.*

*Proof.* We prove an equivalence between the negations. Note that non-emptiness of $X$ implies that $\mathrm{I}(X) \subsetneqq K[x_1, x_2, \ldots, x_n]$.

Suppose first that $I(X)$ is not a prime ideal, so that there exist polynomials $f_1, f_2 \notin \mathrm{I}(X)$ such that $f_1 \cdot f_2 \in \mathrm{I}(X)$. Consider for $i = 1, 2$ the algebraic sets

$$X_i = \mathrm{V}(\mathrm{I}(X) \cup \{f_i\}).$$

Since $f_i$ does not vanish everywhere on $X$, we have $X_1, X_2 \subsetneqq X$. On the other hand, each $P \in X$ is a zero of $f_1$ or $f_2$ because $f_1 \cdot f_2 \in \mathrm{I}(X)$, so we have $X = X_1 \cup X_2$. It follows that $X$ is reducible.

The other implication is similar. Suppose that $X = X_1 \cup X_2$ and $X_1, X_2 \subsetneqq X$. Then $\mathrm{I}(X_1), \mathrm{I}(X_2) \supsetneqq \mathrm{I}(X)$ (indeed, if we had $\mathrm{I}(X_i) = \mathrm{I}(X)$, then $X_i = \mathrm{V}(\mathrm{I}(X_i)) = \mathrm{V}(\mathrm{I}(X)) = X$ by Lemma 6(4), which is a contradiction). It follows that we can choose $f_1 \in \mathrm{I}(X_1) \setminus \mathrm{I}(X)$ and $f_2 \in \mathrm{I}(X_2) \setminus \mathrm{I}(X)$, and that $f_1 \cdot f_2$ vanishes everywhere on $X$. Hence $f_1 \cdot f_2 \in \mathrm{I}(X)$ and $\mathrm{I}(X)$ is not a prime ideal. $\square$

**Exercises.**

(1) Describe the algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}_q}$ where $q$ is a power of a prime number.
(2) Let $K$ be an algebraically closed field and $f, g \in K[x, y]$. Show that
   (a) the algebraic set $\mathrm{V}(f)$ is infinite and
   (b) if $f, g$ are coprime in $K[x, y]$, then the algebraic set $\mathrm{V}(f, g)$ is finite.
(3) Show that if $K$ is algebraically closed, the subvarieties of the affine plane $\mathbb{A}^2_K$ are precisely
   (a) singletons $\{P\}$, $P \in \mathbb{A}^2_K$,
   (b) subsets of the form $\mathrm{V}(f)$ with $f \in K[x, y]$ irreducible (these are called *irreducible plane curves*), and

(c) $\mathbb{A}^2_K$ itself.

(4) Show that if $K$ is algebraically closed and $f \in K[x,y]$ is irreducible (or more generally square-free, i.e. not divisible by a square of an irreducible polynomial), then $\mathrm{I}(\mathrm{V}(f)) = (f)$. Hint: Use Exercise 2.

(5) Show that $\mathrm{I}(\mathbb{A}^n_K) = \{0\}$ if $K$ is an infinite field.

Hint: Use induction on $n$. Write $f \in K[x_1, x_2, \ldots, x_n]$ as $f = \sum_{i=1}^d f_i x_n^i$ with $f_0, \ldots, f_d \in K[x_1, x_2, \ldots, x_{n-1}]$. Then note that if $P = (a_1, \ldots, a_{n-1}) \in \mathbb{A}^{n-1}_K$ and $f_i(P) \neq 0$ for some $i$, then $f(a_1, \ldots, a_{n-1}, x) \in K[x]$ has only finitely many zeros.

(6) Show that a non-empty topological space $(X, \tau)$ is irreducible if and only if each non-empty subset of $X$ is dense.

(7) Proving irreducibility of an algebraic set is in general a difficult task. The following criterion is sometimes useful (see e.g. Exercise 3 in Section 2).

Let $f\colon X \to Y$ by a continuous map between non-empty topological spaces.

(a) Prove that if $X$ is irreducible and $f$ is surjective, than $Y$ is irreducible.

(b) Prove more generally that if $X$ is irreducible and $f$ has dense image in $Y$, then $Y$ is irreducible.

(8) Let $(X, \tau)$ be a topological space and $U \subseteq X$ a dense open subset. Show that $X$ is irreducible if and only if $U$ is irreducible.

## 2. Polynomial and rational maps

So far we have studied algebraic sets alone, as isolated objects. Now we are going to discuss possible choices of classes of maps connecting them. Since algebraic sets are defined in terms of vanishing of polynomials, the most natural choice is to consider maps which are on coordinates given by evaluating polynomials.

**Definition.** Let $K$ be a field and $X \subseteq \mathbb{A}^n_K$ and $Y \subseteq \mathbb{A}^\ell_K$ be algebraic sets. A map $f\colon X \to Y$ is a *polynomial map* if there exist polynomials $f_1, f_2, \ldots, f_\ell \in K[x_1, x_2, \ldots, x_n]$ such that for each $P = (a_1, a_2, \ldots, a_n) \in X$ we have

$$f(P) = \big(f_1(P), f_2(P), \ldots, f_\ell(P)\big).$$

**Lemma 8.** *Let $X, Y, Z$ be an algebraic sets over $K$. Then:*

(1) *If $f\colon X \to Y$ and $g\colon Y \to Z$ are polynomial maps, so is the composition $g \circ f\colon X \to Z$. Moreover, the identity map $\mathrm{id}_X\colon X \to X$ is a polynomial map.*

(2) *Polynomial maps $f\colon X \to Y$ are continuous with respect to the Zariski topologies on $X$ and $Y$.*

*Proof.* (1) Suppose that $X \subseteq \mathbb{A}^n_K$, $Y \subseteq \mathbb{A}^\ell_K$ and $Z \subseteq \mathbb{A}^m_K$. If $f\colon X \to Y$ is a polynomial map given by $f_1, f_2, \ldots, f_\ell \in K[x_1, x_2, \ldots, x_n]$ and $g\colon Y \to Z$ is given by $g_1, g_2, \ldots, g_m \in K[y_1, y_2, \ldots, y_\ell]$, then the composition $g \circ f\colon X \to Z$ is given by $h_1, h_2, \ldots, h_m \in K[x_1, x_2, \ldots, x_n]$, where

$$h_i(x_1, \ldots, x_n) := g_i\big(f_1(x_1, \ldots, x_n), \ldots, f_\ell(x_1, \ldots, x_n)\big). \tag{1}$$

The identity map $\mathrm{id}_X$ is given by the monomials $x_1, x_2, \ldots, x_n$.

(2) Suppose that $f\colon X \to Y$ is a polynomial map given by polynomials $f_1, f_2, \dots, f_\ell \in K[x_1, x_2, \dots, x_n]$ (i.e. $X \subseteq \mathbb{A}^n_K$ and $Y \subseteq \mathbb{A}^\ell_K$. We must show that $f^{-1}(Z)$ is Zariski closed in $X$ for each Zariski closed subset $Z \subseteq Y$. Fix such a subset $Z \subseteq Y$ and some polynomials $g_1, g_2, \dots, g_m \in K[y_1, y_2, \dots, y_\ell]$ such that $Z = \mathrm{V}(g_1, g_2, \dots, g_m)$. Then the $g_i$ define a polynomial map

$$\begin{aligned} g\colon Y &\to \mathbb{A}^m_K, \\ P &\mapsto \big(g_1(P), g_2(P), \dots g_m(P)\big). \end{aligned}$$

Clearly, $f^{-1}(Z)$ is the preimage of the origin $(0, 0, \dots, 0) \in \mathbb{A}^m_K$ under the composition $g \circ f\colon X \to \mathbb{A}^m_K$. In particular,

$$f^{-1}(Z) = \mathrm{V}(h_1, \dots, h_m),$$

where the polynomials $h_i$ are as in (1). □

*Remark.* The proof of Lemma 8(2) in fact shows that Zariski topology is defined precisely in such a way that

(1) polynomial maps are continuous, and
(2) singletons are Zariski closed.

An important special case of polynomial maps are those where the target algebraic set is the affine line.

**Definition.** The set $\{f\colon X \to \mathbb{A}^1_K \mid f \text{ is a polynomial map}\}$ is called the *coordinate ring* of $X$ and denoted by $K[X]$.

The terminology may need some comments. Since $\mathbb{A}^1_K = K$ and $K$ is naturally a $K$-algebra, the set of maps polynomial $f\colon X \to \mathbb{A}^1_K$ has a natural $K$-algebra structure too, with the operations defined pointwise. To be more specific, if $f_1, f_2\colon X \to \mathbb{A}^1_K$ are polynomial maps and $k \in K$, we can define $f_1 + f_2$, $f_1 \cdot f_2$ and $kf_1$ in such a way that for each $P \in X$ we put

$$\begin{aligned} (f_1 + f_2)(P) &= f_1(P) + f_2(P), \\ (f_1 \cdot f_2)(P) &= f_1(P) \cdot f_2(P), \quad \text{and} \\ (kf_1)(P) &= k(f_1(P)). \end{aligned}$$

We leave it for the reader to check that these new maps are again polynomial maps. The zero and the unit in the algebra of polynomial maps $X \to \mathbb{A}^1_K$ are just the constant maps with the corresponding value in $K$. We will always consider $K[X]$ with this $K$-algebra structure.

We defined the coordinate ring of $X$ as a ring of certain functions on $X$, but there is also a different, more algebraic point of view.

**Lemma 9.** *Let $X \subseteq \mathbb{A}^n_K$ be an algebraic set. Then there is an isomorphism of $K$-algebras*

$$\begin{aligned} K[x_1, x_2, \dots, x_n]/\,\mathrm{I}(X) &\to K[X] \\ f + \mathrm{I}(X) &\mapsto (P \mapsto f(P)). \end{aligned}$$

*Proof.* Any polynomial $f \in K[x_1, x_2, \dots, x_n]$ tautologically defines a polynomial map $X \to \mathbb{A}^1_K$ which sends each $P \in X$ to $f(P)$. One readily checks that this assignment defines a homomorphism of $K$-algebras

$$\varphi\colon K[x_1, x_2, \dots, x_n] \to K[X].$$

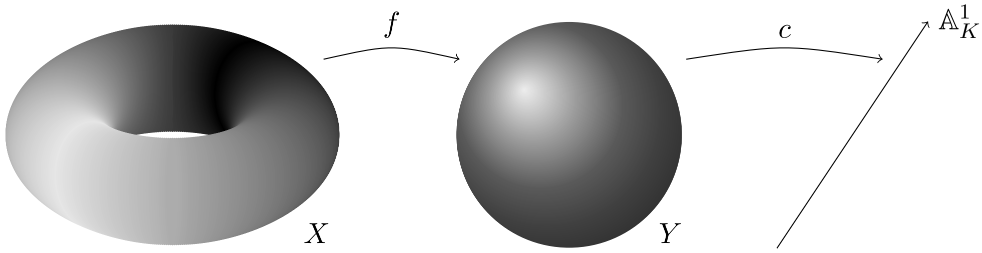


FIGURE 4. An illustration how the map $f^*\colon K[Y] \to K[X]$ acts. It is defined via $f^*\colon c \mapsto c \circ f$.

Since any polynomial map $X \to \mathbb{A}^1_K$ has to be given by some polynomial $f$ by the very definition, this homomorphism of algebras is surjective. However $\varphi$ may not be injective. In fact, the polynomials in the kernel are precisely those which vanish on all of $X$, or in other words, the kernel of $\varphi$ is precisely $\mathrm{I}(X)$. The conclusion follows from the isomorphism theorem. $\square$

This observation is rather important for it allows us to deduce algebraic properties of $K[X]$. For instance, $K[X]$ is always a noetherian ring since $K[x_1, x_2, \ldots, x_n]$ is such. Another consequence of the lemma, which follows together with Theorem 7 and which we will use later in the section, is the following.

**Corollary 10.** *An algebraic set $X$ over $K$ is irreducible if and only if its coordinate ring $K[X]$ is a domain.*

Let us now explain the word 'coodrinate' in the term coordinate ring. This is related to so-called coordinate functions. If $X \subseteq \mathbb{A}^n_K$ and $1 \le i \le n$, the *i-th coordinate function* is the function given by

$$\begin{aligned} c_i\colon X &\to \mathbb{A}^1_K, \\ P = (a_1, a_2, \ldots, a_n) &\mapsto a_i. \end{aligned}$$

This is a polynomial function which, under the isomorphism of Lemma 9, corresponds to the coset $x_i + \mathrm{I}(X)$. Since the ring $K[x_1, x_2, \ldots, x_n]/\,\mathrm{I}(X)$ is generated as a $K$-algebra by the cosets $x_1 + \mathrm{I}(X), x_2 + \mathrm{I}(X), \ldots, x_n + \mathrm{I}(X)$, so is $K[X]$ generated as a $K$-algebra by $c_1, c_2, \ldots, c_n$.

Next we will focus on how coordinate rings interact with polynomial maps between algebraic sets. To this end, let $f\colon X \to Y$ be a polynomial map and $c\colon Y \to \mathbb{A}^1_K$ an element of $K[Y]$. Then the composition $c \circ f\colon X \to \mathbb{A}^1_K$ is again a polynomial map, hence an element of $K[X]$. If we fix $f$ and vary $c$, we obtain a map

$$\begin{aligned} f^*\colon K[Y] &\to K[X], \\ c &\mapsto c \circ f. \end{aligned}$$

The situation is illustrated in Figure 4.

It is straightforward to check directly from the definitions that the just defined map $f^*$ is a homomorphism of $K$-algebras. To summarize, we have a procedure which produces from every polynomial map $f\colon X \to Y$ a homomorphism of $K$-algebras $f^*\colon K[Y] \to K[X]$. We again collect some elementary properties of this procedure.

**Lemma 11.** *If $f\colon X \to Y$ and $g\colon Y \to Z$ are polynomial maps, then $(g \circ f)^* = f^* \circ g^*$. Moreover, $\mathrm{id}_X^* = \mathrm{id}_{K[X]}$.*

*Proof.* The first part essentially just a reformulation of the associativity of the composition $c \circ (g \circ f) = (c \circ g) \circ f$ for each polynomial map $c\colon Z \to \mathbb{A}^1_K$. The second part is trivial. □

*Remark.* The latter lemma together with Lemma 8(1) has a natural interpretation from the point of view of the theory of categories. On one hand, we have a category of algebraic sets over $K$ and polynomial maps among them. On the other hand we have the category of commutative $K$-algebras and homomorphisms among them. The latter lemma says that there is a contravariant functor between the two which sends an algebraic set $X$ to its coordinate ring $K[X]$ and a polynomial map $f$ to the homomorphism $f^*$.

One of the main results presented in this section is that the assignment $f \mapsto f^*$ in fact provides us with a bijection between the sets of polynomial maps and homomorphisms. In the terminology used in the last remark, this can be rephrased to that the functor from the category of algebraic sets to that of commutative algebras is fully faithful.

**Theorem 12.** *Let $K$ be a field and $X, Y$ be algebraic sets over $K$. Then the assignments $f \mapsto f^*$ yields a bijection between the sets of*

(1) *polynomial maps $X \to Y$, and*
(2) *homomorphisms of $K$-algebras $K[Y] \to K[X]$.*

*Proof.* We start with showing that the assignment $f \mapsto f^*$ is injective. That is, given two polynomial maps $f, g\colon X \to Y$ such that $f^* = g^*$, we must prove that $f = g$. Suppose that $Y \subseteq \mathbb{A}^\ell_K$ and $c_1, c_2, \dots, c_\ell\colon Y \to \mathbb{A}^1_K$ are the coordinate functions for $Y$. Then the equality between $f^*$ and $g^*$ implies that for each $1 \le i \le \ell$ we have

$$c_i \circ f = f^*(c_i) = g^*(c_i) = c_i \circ g.$$

In particular, for any point $P \in X$ we have

$$c_i(f(P)) = c_i(g(P)),$$

or in other words, $f(P)$ and $g(P)$ have the same coordinates in $Y \subseteq \mathbb{A}^\ell_K$. This clearly means that $f(P) = g(P)$ for each $P \in X$, which is further equivalent to the fact that $f = g$.

Next we prove that $f \mapsto f^*$ is surjective. To this end, fix a homomorphism $\alpha\colon K[Y] \to K[X]$. Our task is to find $f\colon X \to Y$ such that $\alpha = f^*$. However, if such $f^*$ exists, it is unique by the previous part and it must satisfy

$$\alpha(c_i) = f^*(c_i) = c_i \circ f.$$

Thus, the only possible way to define $f$ is using the formula

$$f(P) = (\alpha(c_1)(P), \alpha(c_2)(P), \dots, \alpha(c_\ell)(P)) \tag{2}$$

for each $P \in X$. Note here that $\alpha(c_i) \in K[X]$, so in particular $\alpha(c_i)$ are polynomial maps $X \to \mathbb{A}^1_K$. Therefore, the formula (2) yields a polynomial map

$$f\colon X \to \mathbb{A}^\ell_K.$$

Our next task is to prove that the image of $f$ is contained in $Y$, so that $f$ actually is a polynomial map $f\colon X \to Y$. To see that, fix some polynomials $g_1, g_2, \dots, g_r \in K[y_1, y_2, \dots, y_\ell]$ such that $Y = \mathrm{V}(g_1, g_2, \dots, g_r)$. We must show that $g_j(f(P)) = 0$ for each $1 \le j \le r$ and $P \in X$. Using (2), this translates to the requirement that

$$g_j\big(\alpha(c_1)(P), \alpha(c_2)(P), \dots, \alpha(c_\ell)(P)\big) = 0.$$

To obtain the latter identity, it suffices to prove that

$$g_j\big(\alpha(c_1), \alpha(c_2), \dots, \alpha(c_\ell)\big) = 0$$

in the coordinate ring $K[X]$. Since $\alpha\colon K[Y] \to K[X]$ is a homomorphism of $K$-algebras, we have

$$g_j\big(\alpha(c_1), \alpha(c_2), \dots, \alpha(c_\ell)\big) = \alpha\big(g_j(c_1, c_2, \dots, c_\ell)\big),$$

so it suffices to prove the identity

$$g_j(c_1, c_2, \dots, c_\ell) = 0$$

in the coordinate ring $K[Y]$. Since the $K$-algebra operations on $K[Y]$ are defined pointwise, it suffices to check the identity

$$g_j\big(c_1(Q), c_2(Q), \dots, c_\ell(Q)\big) = 0$$

for each point $Q = (b_1, b_2, \dots, b_\ell) \in Y$. However, we have $c_i(Q) = b_i$ by the definition of the coordinate functions, and hence

$$g_j\big(c_1(Q), c_2(Q), \dots, c_\ell(Q)\big) = g_j(b_1, b_2, \dots, b_\ell) = g_j(Q).$$

Now $g_j(Q)$ vanishes for each $1 \le j \le r$ and $Q \in Y$ because we started with $Y = \mathrm{V}(g_1, g_2, \dots, g_\ell)$. The conclusion is that, indeed, $f(P) \in Y$ for each $P \in X$ and the recipe (2) defines a polynomial map $f\colon X \to Y$.

Finally, we verify that $\alpha = f^*$ as homomorphisms $K[Y] \to K[X]$. We see immediately from (2) that $\alpha(c_i) = f^*(c_i)$ holds for the coordinate functions $c_1, c_2, \dots, c_\ell \in K[Y]$. As the coordinate functions generate $K[Y]$ as a $K$-algebra, this implies that the homomorphisms $\alpha$ and $f^*$ are equal, as required. □

We call two algebraic sets $X$ and $Y$ over $K$ *isomorphic* if there exist polynomial maps $f\colon X \to Y$ and $g\colon Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. An isomorphism of algebraic sets is a bijection and, moreover, the coordinates of $Y$ polynomial depend on those of $X$ and vice versa.

A typical class of isomorphism are so-called *affine coordinate changes*. These are isomorphism

$$\begin{aligned} f\colon \mathbb{A}^n_K &\to \mathbb{A}^n_K, \\ (a_1, a_2, \dots, a_n) &\mapsto M \cdot (a_1, a_2, \dots, a_n)^t + \vec{c}, \end{aligned}$$

where $M$ is an invertible $n \times n$ matrix over $K$, $\vec{c} \in K^n$ is a column vector, and we use the natural vector space structure on $\mathbb{A}^n_K$. The inverse $f^{-1}$ sends $(b_1, b_2, \dots, b_n)$ to $M^{-1} \cdot (b_1, b_2, \dots, b_n)^t - M^{-1} \cdot \vec{c}$. More generally, if $Y \subseteq \mathbb{A}^n_K$ is an algebraic set, so is the image $f(Y) \subseteq \mathbb{A}^n_K$ and $f$ induces an isomorphism between $Y$ and $f(Y)$. This is often used to simplify the form of a collection of polynomial equations defining $Y$.

An immediate consequence of Theorem 12 is an algebraic characterization of when algebraic sets are isomorphic.

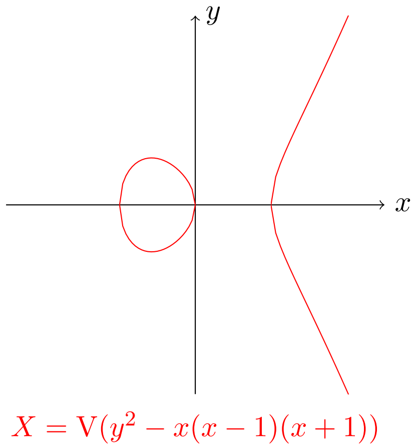


FIGURE 5. The zero set of the polynomial $y^2 - x(x-1)(x+1)$ over the field of real numbers.

**Corollary 13.** *Two algebraic sets $X$ and $Y$ are isomorphic if and only if their coordinate rings $K[X]$ and $K[Y]$ are isomorphic $K$-algebras.*

There is another class of maps between algebraic sets (or more precisely certain subsets of them) which is very useful in practice – rational maps. For simplicity we will restrict our attention only to varieties over infinite fields. The coordinate ring $K[X]$ of a variety $X$ is a domain, so we can form the quotient field which we denote by $K(X)$ and call the *function field* of $X$.

*Example.* If $X = \mathbb{A}^n_K$, then $K[X] = K[x_1, x_2, \dots, x_n]$ and

$$K(X) = K(x_1, x_2, \dots, x_n) = \left\{ \frac{f}{g} \mid f, g \in K[x_1, x_2, \dots, x_n], g \neq 0 \right\}.$$

*Example.* Let $K = \mathbb{C}$ (in fact, the example would work for any algebraically closed field $K$ of characteristic different from 2) and let $X$ be the variety $X = \mathrm{V}(y^2 - x(x-1)(x+1)) \subseteq \mathbb{A}^2_K$. The real part $X \cap \mathbb{A}^2_{\mathbb{R}}$ is depicted in Figure 5.

The coordinate ring of $X$ is isomorphic to $K[x,y]/(y^2 - x(x-1)(x+1))$ and the coset of $x$ in $K[X]$ is transcendental over $K$ since no non-zero polynomial $g \in K[x]$ is contained in $(y^2 - x(x-1)(x+1))$ (use Exercise 4 in Section 1). Thus, $K(X)$ has a subfield isomorphic to $K(x)$ and the coset of $y$ is algebraic over $K(x)$ since it satisfies the equation $y^2 - x(x-1)(x+1) = 0$. It follows that $K(X)$ is a quadratic extension of $K(x)$,

$$K(X) \cong K(x)[\sqrt{x(x-1)(x+1)}].$$

If $X$ is a variety, the elements $\frac{f}{g} \in K(X)$ are called *rational functions* on $X$. In fact, the fraction $\frac{f}{g}$ only defines a function

$$\begin{aligned} U &\to \mathbb{A}^1_K, \\ P &\mapsto \frac{f(P)}{g(P)} \end{aligned} \tag{3}$$

on the Zariski open subset $U = X \setminus \mathrm{V}(g)$, which is non-empty, so dense since $X$ is irreducible. Later on in

A word of warning is due here. Although the polynomial rings over a field $K[x_1, x_2, \ldots, x_n]$ are well known to be unique factorization domains (UFDs for short), coordinate rings $K[X]$ of varieties other than affine spaces very often do *not* possess the unique factorization property. In particular, there is often nothing like a unique reduced fraction expressing an element of $K(X)$.

We simply have to consider different fractions $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ expressing the same element of $K(X)$, which may a priori define different functions as in (3). However, if both $\frac{f_1(P)}{g_1(P)}$ and $\frac{f_2(P)}{g_2(P)}$ are defined for $P \in X$, then the values in $K$ are equal since the equality of fractions in $K(X)$ means that $f_1 g_2 = f_2 g_1$ in $K[X]$ and hence also $f_1(P) \cdot g_2(P) = f_2(P) \cdot g_1(P)$ in $K$.

*Example.* Let $K$ be a field and $X = \mathrm{V}(x_1x_4 - x_2x_3) \subseteq \mathbb{A}^4_K$. We can identify $X$ with the set of all singular $2 \times 2$ matrices $\left(\begin{smallmatrix} x_1 & x_2 \\ x_3 & x_4 \end{smallmatrix}\right)$ over $K$. Then we have $\frac{x_1}{x_2} = \frac{x_3}{x_4} \in K(X)$. The functions defined by the fractions using the rule (3) return for a given $2 \times 2$ matrix in the domain of definition a scalar $k \in K$ which is the ratio of the first and the second column. However, the first fraction defines a function on $U_1 = X \setminus \mathrm{V}(x_2)$ while the second one on $U_2 = X \setminus \mathrm{V}(x_4)$.

Since the two functions give the same values on $U_1 \cap U_2$, we can 'glue' them together to a function $r\colon U \to \mathbb{A}^1_K$, where $U = U_1 \cup U_2 = X \setminus \mathrm{V}(x_2, x_4)$. It can be shown that there is *no* single expression $\frac{f}{g} = \frac{x_1}{x_2}$ in $K(X)$ which would define $r$ via (3) on all of $U$. We cannot do better in the sense that we need at least two different ways to express the fraction to define $r$.

The above considerations motivate the following definition.

**Definition.** Let $X$ be a variety, $P \in X$ and $r \in K(X)$. We say that $r$ is *regular* at $P$ if there exist $f, g \in K[X]$, $g \neq 0$ such that $r = \frac{f}{g} \in K(X)$ and $\frac{f(P)}{g(P)}$ is defined. Otherwise, $P$ is called a *pole* of $r$.

**Lemma 14.** *Let $X$ be a variety and $r \in K(X)$. The set of poles of $r$ is an algebraic subset of $X$ and the set of points at which $r$ is regular is non-empty and Zariski open in $X$.*

*Proof.* The set of poles of $r$ can be obtained as

$$\bigcap_{\frac{f}{g} = r} \mathrm{V}(g),$$

which is obviously an algebraic set by Lemma 1(2), so Zariski closed in $X$. The set of points at which $r$ is regular is then Zariski open in $X$. □

Similarly to the definition of polynomial maps between algebraic sets, we can define rational maps between varieties as those which are coordinatewise computed by rational functions.

**Definition.** Let $X \subseteq \mathbb{A}^n_K$ and $Y \subseteq \mathbb{A}^\ell_K$ be varieties over $K$. A *rational map* from $X$ to $Y$ is a map $r\colon U \to Y$ given by the assignment

$$r(P) = \big(r_1(P), r_2(P), \ldots, r_\ell(P)\big)$$

for each $P \in U$, where $r_1, r_2, \ldots, r_\ell \in K(X)$ are rational functions on $X$ and $U$ is the (non-empty Zariski open) subset of all the points of $X$ at which all the $r_i$ are regular. The points in $U$ are called the *regular* points of $r$ and the points in $X \setminus U$ the *poles* of $r$.

In other words, rational maps are defined in a very similar fashion to polynomial maps, as those whose coordinates are computed by rational functions. The only technical issue is that they are often not defined for all points of $X$. We will indicate this fact by the notation $r\colon X \dashrightarrow Y$.

The next question which we address is under which precisely conditions we can compose a pair of rational maps $r\colon X \dashrightarrow Y$ and $s\colon Y \dashrightarrow Z$. The composition of a pair of polynomial maps or the composition of a rational map followed by a polynomial map are always well defined rational maps. However, the situation is more delicate even if $r$ is a polynomial map and $s$ is a rational map, as the following example shows.

*Example.* Let $X = Y = Z = \mathbb{A}^1_K$ for any fixed infinite field $K$, let $r\colon \mathbb{A}^1_K \to \mathbb{A}^1_K$ be the constant map which sends each $t \in K$ to 0 and let $s\colon \mathbb{A}^1_K \dashrightarrow \mathbb{A}^1_K$ be the rational map which sends $t \in K \setminus \{0\}$ to $\frac{1}{t}$. Then there is no reasonable way to define a composition $s \circ r\colon \mathbb{A}^1_K \dashrightarrow \mathbb{A}^1_K$.

The obvious problem is that the image of $r$ is contained in the set of poles of $s$. We will show that this is in fact the only reason which may prevent us from defining the composition. We start with the following observation.

**Lemma 15.** *Let $X, Y$ be varieties over $K$ and let $r\colon X \dashrightarrow Y$ be a rational map. Let us denote the set of regular points of $r$ by $U$. Then the honest set-theoretic map $r\colon U \to Y$ is continuous (where $U$ carries the subset topology of the Zariski topology on $X$).*

*Proof.* We first treat the special case where $Y = \mathbb{A}^1_K$, i.e. where $r$ is computed by a single element $r_1 = \frac{f}{g} \in K(X)$. Given any point $P \in U$, we can choose $f, g$ so that $g(P) \neq 0$. It follows that $r(P') = \frac{f(P')}{g(P')}$ on a Zariski open neighborhood $U_P$ of $P$ in $U$. Indeed, we can simply take

$$U_P = \{P' \in U \mid g(P') \neq 0\}.$$

Now note that if $V \subseteq \mathbb{A}^1_K$ is Zariski open, then $r^{-1}(V) \cap U_P$ is Zariski open in $X$. This is clear if $V = \varnothing$. If, on the other hand, $V$ is non-empty, $V$ must be of the form $V = \mathbb{A}^1_K \setminus \{b_1, \ldots, b_r\}$, where $b_1, \ldots, b_r \in K = \mathbb{A}^1_K$ are finitely many elements of $K$. Then, however,

$$r^{-1}(V) \cap U_P = \big\{P' \in U_P \mid f(P') - b_i \cdot g(P') \neq 0 \ (\forall i \in \{1, \ldots, r\})\big\}.$$

If we let $P$ vary, the open subsets $U_P$, $P \in U$, cover $U$. Since $r^{-1}(V) \cap U_P$ is open for each $P$, so is

$$r^{-1}(V) = \bigcup_{P \in U} r^{-1}(V) \cap U_P.$$

Hence $r\colon U \to Y$ is continuous if $Y = \mathbb{A}^1_K$.

In the general case, we can use a similar trick as for Lemma 8(2). If $Y \subseteq \mathbb{A}^\ell_K$ and $Z = \mathrm{V}(g_1, g_2, \ldots, g_m) \subseteq Y$ is Zariski closed (here $g_1, g_2, \ldots, g_m \in$

$K[y_1, y_2, \ldots, y_\ell]$), then the compositions

$$g_i \circ r \colon U \to \mathbb{A}^1_K$$

are easily seen to be rational maps. Moreover, $Z = \bigcap_{i=1}^m g_i^{-1}(0)$ and, thus, $r^{-1}(Z) = \bigcap_{i=1}^m (g_i \circ r)^{-1}(0)$. Since all $(g_i \circ r)^{-1}(0) \subseteq U$ are closed by the first part, so is $r^{-1}(Z)$. □

Now suppose that $r \colon X \dashrightarrow Y$ and $s \colon Y \dashrightarrow Z$ are rational maps between varieties over $K$ and that the image of $r$ contains at least one point $P \in Y$ at which $s$ is regular. Under this condition, the composition $s \circ r \colon X \dashrightarrow Z$ can be naturally defined.

Indeed, suppose that we have rational maps $r \colon U \to Y$ and $s \colon V \to Z$, where $U \subseteq X$ and $V \subseteq Y$ are the sets of regular points of $r$ and $s$, respectively. Then $r(U) \cap V$ is nonempty, so is the preimage $r^{-1}(V) \cap U$. Hence we have a well defined composition

$$\begin{aligned} s \circ r \colon U \cap r^{-1}(V) &\to Z, \\ P &\mapsto s(r(P)), \end{aligned}$$

which is defined on the non-empty open subset $W := U \cap r^{-1}(V) \subseteq X$. If $\ell \geq 1$ is such that $Z \subseteq \mathbb{A}^\ell_K$, there are rational functions $u_1, u_2, \ldots, u_\ell \in K(X)$ which are regular at all $P \in W$ and such that

$$s(r(P)) = \big(u_1(P), u_2(P), \ldots, u_n(P)\big) \in Z$$

for each $P \in W$. This is proved completely analogously to Lemma 8(1). Since $W$ is dense in $X$ (Exercise 6 in Section 1), the rational functions $u_1, u_2, \ldots, u_\ell$ are uniquely determined by Exercise 6.

An important situation in which the composition $s \circ r$ is always defined is when the image $r(U)$ is Zariski dense in $Y$ (equivalently, when the preimage $r^{-1}(V)$ of any non-empty open subset $V \subseteq Y$ is again non-empty). For such rational maps $r \colon X \dashrightarrow Y$ we have an analogue of Theorem 12. Given any $s \in K(Y)$, the composition $s \circ r \colon X \dashrightarrow \mathbb{A}^1_K$ is represented by a unique element of $K(Y)$, and we have a $K$-algebra homomorphism

$$\begin{aligned} r^* \colon K(Y) &\to K(X), \\ s &\mapsto s \circ r, \end{aligned}$$

which operates as in Figure 4. Note that since the field $K(Y)$ has no non-trivial ideals, $r^*$ has to be injective.

**Theorem 16.** *Let $K$ be a field and $X, Y$ be varieties over $K$. Then the assignments $r \mapsto r^*$ yields a bijection between the sets of*

(1) *rational maps $X \dashrightarrow Y$ whose image is dense in $Y$, and*
(2) *homomorphisms of $K$-algebras $K(Y) \to K(X)$.*

*Proof.* The proof is completely analogous to that of Theorem 12, with minor modifications only.

To prove the injectivity, suppose that $Y \subseteq \mathbb{A}^\ell_K$ and that we have rational maps $r, s \colon X \dashrightarrow Y$ such that $r^* = s^*$. Since all the coordinate functions $c_1, c_2, \ldots, c_\ell \colon Y \to \mathbb{A}^1_K$ are actually elements of $K(Y)$, we deduce that $c_i \circ r = r^*(c_i)$ and $c_i \circ s = s^*(c_i)$ are the same rational functions $X \dashrightarrow \mathbb{A}^1_K$. In particular $c_i(r(P)) = c_i(s(P))$ for each $i = 1, 2, \ldots, \ell$ whenever both $r$ and

$s$ are regular at $P$. This just says that $r(P) = s(P)$ whenever both $r$ and $s$ are regular at $P$ or, in other words, that $r = s$ thanks to Exercise 6.

To prove surjectivity, suppose that we have a homomorphism $\alpha\colon K(Y) \to K(X)$. If we evaluate $\alpha$ at the coordinate functions $c_i =: Y \to \mathbb{A}^1_K$, $i = 1, 2, \dots, \ell$, we obtain rational function $r_i = \alpha(c_i) \in K(X)$. As in the proof of Theorem 12, we define our candidate preimage of $\alpha$ as

$$\begin{aligned} r\colon U &\to \mathbb{A}^\ell_K \\ P &\mapsto \big(r_1(P), r_2(P), \dots, r_\ell(P)\big) \end{aligned}$$

where $U$ is the set of all points $P \in X$ at which all the $r_i \in K(X)$ are regular. Using exactly the same argument as in the proof of Theorem 12, we observe that in fact $r(U) \subseteq Y$, so $r$ defines a map

$$r\colon U \to Y.$$

Clearly $r$ is a rational map and, since $r^*(c_i) = c_i \circ r = \alpha(c_i)$ for each $i = 1, 2, \dots, \ell$ and $c_1, c_2, \dots, c_\ell$ generate $K(Y)$ as a field extension of $K$, we have $r^* = \alpha$.

The last thing to observe is that the image of $r$ is dense in $Y$. To this end, recall that $r^*\colon K(Y) \to K(X)$ is injective. Given any polynomial function $g\colon Y \to \mathbb{A}^1_K$ which vanishes on $r(U) \subseteq Y$, we have $r^*(g) = g \circ r = 0$ in $K(X)$ and, hence, $g = 0$. Now the Zariski closure of $r(U)$ in $Y$ is precisely the set of common zeros in $Y$ of all such polynomial maps $g$ (recall Lemma 6(4)), which is clearly of $Y$. (Compare the argument to Exercise 8b.) □

Analogous to the notion of a polynomial isomorphism, one can study the situation where there are two mutually inverse rational maps between varieties. This is of course a much coarser way to compare two varieties, but nevertheless it is a very useful notion.

**Definition.** Let $K$ be a field and $X, Y$ be varieties over $K$. A rational map $r\colon X \dashrightarrow Y$ is called a *birational equivalence* if there exist a rational map $s\colon Y \dashrightarrow X$ such that both compositions $s \circ r$ and $r \circ s$ are defined and equal to the identity maps on $X$ and $Y$, respectively.

The varieties $X$ and $Y$ are *birationally equivalent* if there exists a birational equivalence $r\colon X \dashrightarrow Y$.

The birational equivalence is indeed an equivalence relation on varieties over $K$. Whereas the reflexivity and symmetry is trivial, the transitivity follows from the fact that a birational equivalence always has a dense image, which in turn follows from the coming lemma.

**Lemma 17.** *Suppose that $r\colon X \dashrightarrow Y$ is a birational equivalence with a rational inverse $s\colon Y \dashrightarrow X$, as above. Then there exist non-empty (hence dense) open sets $U \subseteq X$ and $V \subseteq Y$ such that $r$ and $s$ are defined on $U$ and $V$, respectively, and $r|_U\colon U \to V$ and $s|_V\colon V \to U$ are inverse bijections.*

$$\begin{tikzcd} X \arrow[r, dashed, shift left, "r"] & Y \arrow[l, dashed, shift left, "s"] \\ U \arrow[u, "\cup"] \arrow[r, shift left, "r|_U"] & V. \arrow[u, "\cup"'] \arrow[l, shift left, "s|_V"] \end{tikzcd}$$

*Proof.* Denote by $U' \subseteq X$ the set of regular points of $r$ and by $V' \subseteq Y$ the set of regular points of $s$. That is, we have actual maps $r\colon U' \to Y$ and $s\colon V' \to X$.

We define $U = U' \cap r^{-1}(V')$ and $V = V' \cap s^{-1}(U')$. Then clearly $r(U) \subseteq V'$ and, since $s(r(P)) = P$ for each point $P \in X$ where the composition is defined, it follows that $r(U) \subseteq s^{-1}(U')$. In particular, we have proved that $r(U) \subseteq V$ and, by symmetry, $s(V) \subseteq U$. It follows that $r$ and $s$ restrict to mutually inverse bijections between $U$ and $V$ since we assumed that $s(r(P)) = P$ and $r(s(Q)) = Q$ whenever defined. □

*Remark.* Suppose that $K = \overline{K}$ is algebraically closed and that $X, Y \subseteq \mathbb{A}^2_K$ are irreducible plane curves. That is, $X = \mathrm{V}(f)$ and $Y = \mathrm{V}(g)$ for some irreducible polynomials $f, g \in K[x, y]$.

In view of Exercise 3 in Section 1, non-empty open sets in $X$ are precisely complements of finite subsets of $X$ and the same is true for $Y$. In particular, if $r\colon X \dashrightarrow Y$ and $s\colon Y \dashrightarrow X$ are mutually inverse birational equivalences, they restrict to bijections

$$X \setminus \{P_1, P_2, \dots, P_k\} \rightleftarrows Y \setminus \{Q_1, Q_2, \dots, Q_m\}$$

for finite collections of points $P_1, P_2, \dots, P_k \in X$ and $Q_1, Q_2, \dots, Q_m \in Y$. We refer to Exercises 10 and 11 for explicit examples.

As a straightforward corollary of Theorem 16, we also get an algebraic characterization of birational equivalence.

**Corollary 18.** *Two varieties $X, Y$ over $K$ are birationally equivalent if and only if the function fields $K(X)$ and $K(Y)$ are isomorphic as $K$-algebras (i.e. as field extensions of $K$).*

An especially nice situation arises when a variety is birationally equivalent to an affine space.

**Definition.** A variety $X$ over an infinite field $K$ is *rational* if it is birationally equivalent to $\mathbb{A}^n_K$ for some $n \geq 1$.

The assumption that $K$ is infinite is imposed because then $\mathbb{A}^n_K$ indeed is a variety (Lemma 6(3)). It is also clear that $X$ can be birationally equivalent to $\mathbb{A}^n_K$ only for one natural number $n$. Indeed, the birational equivalence implies that $K(X) \cong K(x_1, x_2, \dots, x_n)$ and $n$ can be recovered as the transcendence degree of $K(X)$. That is, $n$ is the maximum number of elements $r_1, r_2, \dots, r_n \in K(X)$ which satisfy no polynomial equation $g(r_1, r_2, \dots, r_n) = 0$ with $0 \neq g \in K[x_1, x_2, \dots, x_n]$.

*Example.* Suppose that $K = \overline{K}$ is algebraically closed and that $X = \mathrm{V}(f) \subseteq \mathbb{A}^2_K$ is an irreducible plane curve.

It is well-known that the transcendence degree of $K(X)$ over $K$ is equal to one. To see that, assume without loss of generality that $f \in K[x,y]$ contains a non-zero term with a positive power of $y$ and suppose that $p \in K[x]$ is a non-zero polynomial. Since $f$ cannot divide $p$ in $K[x,y]$, the coset of $p$ is non-zero in $K[X]$ as well as in $K(X)$. It follows that $x \in K(X)$ is transcendental over $K$. Now $x$ and $y$ generate $K(X)$ as a field extension of $K$ and $y \in K(X)$ is algebraic over $K(x)$ because of the equality $f(x,y) = 0$.

It follows that if $X$ is rational, it must be birationally equivalent to $\mathbb{A}^1_K$.

We conclude the section by illustrating how the results in this section can be combined with a fact from abstract algebra to obtain a criterion for rationality of irreducible plane curves. It in particular says that the mere existence of maps like in Exercise 1 ensures that the curves are birational.

**Proposition 19.** *Let $K$ be an algebraically closed field and $X = \mathrm{V}(f) \subseteq \mathbb{A}^2_K$ be an irreducible plane curve. Then the following are equivalent:*

(1) *$X$ is rational.*
(2) *There is a non-constant rational map $r\colon \mathbb{A}^1_K \dashrightarrow X$.*

*Proof.* (1)$\Rightarrow$(2) We already know that if $X$ is rational, it must be birationally equivalent to $\mathbb{A}^1_K$ and any birational equivalence $r\colon \mathbb{A}^1_K \dashrightarrow X$ is certainly non-constant by Lemma 17.

(2)$\Rightarrow$(1) Suppose that $r\colon \mathbb{A}^1_K \dashrightarrow X$ is a non-constant rational map. We will first show that the image $r(U)$ is dense in $X$, where $U \subseteq \mathbb{A}^1_K$ is the domain of definition of $r$. Suppose for the moment that it is not, i.e. that the Zariski closure $\overline{r(U)}$ is a proper subset of $X$. However, then $\overline{r(U)}$ must be finite (Exercise 3 in Section 1), and therefore so is $r(U)$ itself. As $X$ is irreducible, so is $r(U)$ by Exercise 7 in Section 1. Being finite and irreducible, $r(U)$ must consist of a single point of $X$, or in other words, $r\colon U \to X$ is a constant map, which contradicts our assumption.

Since $r$ has a dense image, it induces a field embedding $r^*\colon K(X) \to K(\mathbb{A}^1_K) \cong K(t)$ by Theorem 16. Now we invoke a result in algebra which is known as Lüroth's theorem (see for instance [vdW49, Ch. VIII, §63]): If $L$ is a subfield of $K(t)$ such that $K \subsetneqq L \subseteq K(t)$, then $L = K(g)$ for some $g \in K(t)$. In particular, we have a $K$-algebra isomorphism $\alpha\colon K(t') \cong L$ given by $\alpha(t') = g$ in this case:

If we apply the result to $L = r^*(K(X)) \subseteq K(t)$, we can express $r^*$ as a composition of two $K$-algebra homomorphisms

$$K(X) \xrightarrow{\cong} K(t') \longrightarrow K(t), \tag{4}$$

where the first one is an isomorphism and the second one sends $t'$ to $g \in K(t)$. Now $X$ and $\mathbb{A}^1_K$ are birationally equivalent thanks to the first isomorphism and Corollary 18. □

*Remark.* A rational map $r\colon \mathbb{A}^1_K \dashrightarrow X$ as in Proposition 19(2) need not be a birational equivalence itself. For instance the polynomial map $r\colon t \mapsto (t^4, t^6)$ is a non-constant map $\mathbb{A}^1_{\mathbb{C}} \to \mathrm{V}(y^2 - x^3)$, but contrary to what Lemma 17 says about birational equivalences, there is no Zariski open subset $U \subseteq \mathbb{A}^1_{\mathbb{C}}$ for which the restriction $r|_U$ is injective.

The proof of Proposition 19 says instead that given non-constant $r\colon \mathbb{A}^1_K \dashrightarrow X$, we can express $r$ as a composition of two rational maps

$$\begin{tikzcd} X & & \mathbb{A}^1_K \arrow[ll, dashed, "r"'] \arrow[dl, dashed, "g"] \\ & \mathbb{A}^1_K \arrow[ul, dashed, "s"] & \end{tikzcd}$$

such that $s\colon \mathbb{A}^1_K \dashrightarrow X$ is a birational equivalence. To see this, apply Theorem 16 to the composition in (4).

**Exercises.**

(1) In each of the following cases, find a surjective polynomial map $f\colon \mathbb{A}^1_{\mathbb{C}} \to X$, describe the homomorphism of $\mathbb{C}$-algebras $f^*\colon \mathbb{C}[X] \to \mathbb{C}[\mathbb{A}^1_{\mathbb{C}}] \cong \mathbb{C}[t]$ and explain why $f^*$ is injective:
  (a) $X = \mathrm{V}(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2_{\mathbb{C}}$,
  (b) $X = \mathrm{V}(y^2 - x^3) \subseteq \mathbb{A}^2_{\mathbb{C}}$,
  (c) $X = \mathrm{V}(x^3 - yz, y^2 - xz, z^2 - x^2y) \subseteq \mathbb{A}^3_{\mathbb{C}}$.

(2) Show that in the polynomial maps $f\colon \mathbb{A}^1_{\mathbb{C}} \to X$ in Exercises 1b and 1c can be chosen to be bijective (even homeomorphisms with respect to Zariski topologies). Show that these maps are nevertheless *not* polynomial isomorphisms (in fact, $\mathbb{C}[X] \not\cong \mathbb{C}[t]$ as $\mathbb{C}$-algebras since the latter one is integrally closed while the former one is not).

(3) Use either Exercise 7 in Section 1 or Corollary 10 to show that the algebraic set $X$ from Exercise 1c is irreducible.

(4) Let $X$ be a variety over a field $K$ and $0 \neq r \in K(X)$ be rational function regular at a point $P \in X$. If $r(P) = 0$, then $r^{-1}$ has a pole at $P$.

(5) Find the pole set of $h \in \mathbb{C}(X)$ in the following cases:
  (a) $X = \mathrm{V}(x_1x_4 - x_2x_3) \subseteq \mathbb{A}^4_{\mathbb{C}}$ and $h = \frac{x_1}{x_2} = \frac{x_3}{x_4}$.
  (b) $X = \mathrm{V}(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2_{\mathbb{C}}$ and $h = \frac{y}{x}$.
  (c) $X = \mathrm{V}(y^2 - x^2(x+1)) \subseteq \mathbb{A}^2_{\mathbb{C}}$ and $h = \frac{y^2}{x^2}$.

(6) (a) Show that if $X$ is an algebraic set, $D \subseteq X$ is a dense subset (in the Zariski topology) and $f, g \in K[X]$ such that the restrictions $f|_D = g|_D$ are equal, then $f = g$ in $K[X]$.
  (b) Show that is $X$ is a variety, $D \subseteq X$ is a dense subset and $r, s \in K(X)$ are such that $r(P) = s(P)$ for each $P \in D$ at which both $r$ and $s$ are regular, then $r = s$ in $K(X)$.

Hint: Two elements $f, g \in K[X]$ (or in $K(X)$) are equal if and only their difference $f - g$ vanishes.

Beware that 6a and 6b above are not purely topological statements! There is indeed a standard result from topology which says that if $f, g\colon X \to Y$ is a continuous map between topological spaces, if $f$ and $g$ agree on a dense subset of $X$, and if $Y$ *is* a Hausdorff space, then $f = g$. However, Zariski topology is rarely Hausdorff (consider even just $\mathbb{A}^1_K$ for an infinite field $K$).

Here is an illustration what may go wrong in general. Let $Y = \{0,1\} \times \mathbb{R}/\sim$, a disjoint union of two real lines with the usual Euclidean topology where we identify $(0,t) \sim (1,t)$ for each $t \in \mathbb{R} \setminus \{0\}$.

Then $Y$ looks like a real line, but with the origin doubled, and any open neighborhoods of $[(0,0)]_\sim$ and $[(1,0)]_\sim \in Y$ intersect non-trivially. The two maps

$$\begin{aligned} f_i\colon \mathbb{R} &\to Y \\ t &\mapsto [(i,t)]_\sim, \end{aligned}$$

where $i = 0, 1$, are continuous and agree on the dense subset $D = \mathbb{R} \setminus \{0\} \subseteq \mathbb{R}$, but $f \neq g$.

(7) We have seen that a coordinate ring $K[X]$ of an algebraic set $X$ is generated as a $K$-algebra by the coordinate functions. The point of this exercise to show a converse statement, namely that any finite set of $K$-algebra generators of $K[X]$ can become the set of coordinate functions up to isomorphism.

Let $K$ be an infinite field, $X$ be an algebraic set over $K$ and suppose that $f_1, f_2, \dots, f_n \in K[X]$ generate the coordinate ring as a $K$-algebra.

(a) Show that there is a surjective $K$-algebra homomorphism

$$\alpha\colon K[y_1, y_2, \dots, y_n] \to K[X]$$

given by $\alpha(y_i) = f_i$, and that there is also a polynomial map

$$f\colon X \to \mathbb{A}^n_K$$

given by $f(P) = \big(f_1(P), f_2(P), \dots, f_n(P)\big)$.

(b) Show that $\alpha = f^*$. Hint: use Exercise 5 from Section 1 to identify $K[\mathbb{A}^n_K]$ with $K[y_1, y_2, \dots, y_n]$.

(c) Let $J = \{g \in K[y_1, y_2, \dots, y_n] \mid g(f_1, f_2, \dots, f_n) = 0 \text{ in } K[X]\}$. Show that $J$ is the kernel of $\alpha$ and also that $J = \mathrm{I}(f(X))$, the ideal of the image of $f$ in $\mathbb{A}^n_K$.

(d) Let $Y = \overline{f(X)}$ be the Zariski closure of the image of $f$ in $\mathbb{A}^n_K$. Show that $Y = \mathrm{V}(J)$ and $J = \mathrm{I}(Y)$.

(e) Show that the polynomial maps

$$X \xrightarrow{\ f\ } Y \xrightarrow{\ \subseteq\ } \mathbb{A}^n_K$$

correspond up to isomorphism of $K$-algebras to the $K$-algebra homomorphisms

$$K[X] \xleftarrow{\ \overline{\alpha}\ } K[y_1, y_2, \dots, y_n]/I \twoheadleftarrow K[y_1, y_2, \dots, y_n],$$

where $\overline{\alpha}$ maps $y_i + I$ to $f_i$.

(f) Show that $\overline{\alpha}$ is an isomorphism of $K$-algebras and, hence, the map $f\colon X \to Y$ is an isomorphism of algebraic sets. Finally, show that the compositions

$$f_1 \circ f^{-1}, f_2 \circ f^{-1}, \dots, f_n \circ f^{-1}\colon Y \to \mathbb{A}^1_K$$

coincide with the coordinate functions $c_1, c_2, \dots, c_n\colon Y \to \mathbb{A}^1_K$.

(8) Let $f\colon X \to Y$ be a polynomial map between algebraic sets over a field $K$ and denote by $f^*\colon K[Y] \to K[X]$ the induced homomorphism of the coordinate rings.

(a) Show that the Zariski closure $\overline{f(X)} \subseteq Y$ of the image of $f$ has a coordinate ring isomorphic to the image of the $K$-algebra homomorphism $f^*$. Hint: Use ideas from Exercise 7.
(b) Show in particular that $f^*$ is injective if and only if the image of $f$ is Zariski dense in $Y$ (this also follows directly from Exercise 6).
(c) Show also that $f^*$ is surjective if and only if $f$ is a closed immersion of algebraic sets, i.e. the image $f(X)$ is Zariski closed in $Y$ and $f$ induces a polynomial isomorphism to its image.

(9) Let $K$ be an infinite field and $X = \mathrm{V}(x_1x_4 - x_2x_3)$. Find explicit birational equivalences between $X$ and $\mathbb{A}^3_K$.

(10) Let $K$ be an algebraically closed field of characteristic different from 2 and let $f \in K[x, y]$ be an irreducible polynomial of total degree 2.
(a) Show that $X = \mathrm{V}(f)$ is a rational variety.
(b) Find explicit birational equivalences $\mathbb{A}^1_K \dashrightarrow X$ and $X \dashrightarrow \mathbb{A}^1_K$ for $f = x^2 + y^2 - 1$ and $f = x^2 - y^2 - 1$. Hint: the stereographic projection with the projection point on the curve.
(c) Describe the solutions over $\mathbb{Q}$ of each of the equations $x^2+y^2 = 1$ and $x^2 - y^2 = 1$. Hint: Specialize the above to $K = \mathbb{C}$.

(11) Find explicit birational equivalences between the affine line $\mathbb{A}^1_{\mathbb{C}}$ and the varieties $X = \mathrm{V}(y^2 - x^3)$ and $X = \mathrm{V}(y^2 - x^2(x + 1)) \subseteq \mathbb{A}^2_{\mathbb{C}}$. Describe the solutions over $\mathbb{Q}$ of the equation $y^2 - x^2(x + 1) = 0$.

## 3. Hilbert's Nullstellensatz and consequences

Hilbert's Nullstellensatz is a cornerstone result which establishes a very tight connection between the geometry of an algebraic set and the algebraic properties of its coordinate ring. It allows to completely answer natural questions like which ideals of $K[x_1, x_2, \dots, x_n]$ are of the form $\mathrm{I}(X)$ or what precise conditions a $K$-algebra $R$ must satisfy to be a coordinate ring of some algebraic set.

The price to pay for this is that we will assume almost everywhere from now on that our base field is algebraically closed. In the previous sections, we needed such an assumption only when we appealed to Lemma 6(3) (i.e. we needed $\mathbb{A}^n_K$ to be irreducible) or to Exercise 3 in Section 1 (i.e. we wanted to use the classification of subvarieties of the affine plane $\mathbb{A}^2_K$).

To start with, we briefly discuss basic facts about localization of commutative rings. Algebraically this means making certain elements of a ring formally invertible, in a way analogous to the construction of the field of rational numbers from the ring of integers (or to constructing quotient fields of commutative integral domains in general). The terminology comes from the relation to algebraic geometry, where localization allows to inspect algebraic sets more locally in the Zariski topology. Some details on that aspect will be included in the coming discussion too in this and especially in the next section.

It has certain formal advantages to use the following abstract definition of a localization via a universal property.

**Definition.** Let $R$ be a commutative ring an $S \subseteq R$ a set of elements. A *localization* of $R$ with respect to $S$ is a ring homomorphism $\alpha\colon R \to S^{-1}R$ from $R$ with the following properties:

(1) the element $\alpha(s)$ is invertible in $S^{-1}R$ for each $s \in S$,
(2) whenever $\beta\colon R \to T$ is another ring homomorphism with $\beta(s)$ invertible for each $s \in S$, then there exists a unique ring homomorphism $\overline{\beta}\colon S^{-1}R \to T$ such that $\beta = \overline{\beta} \circ \alpha$:

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & S^{-1}R \arrow[d, dotted, "\exists!\overline{\beta}"] \\ & T. \end{tikzcd}$$

The advantage of using this as a definition is that it determines $S^{-1}R$ *uniquely* up to isomorphism. To see that, observe first that if $\beta = \alpha$ in the definition, then necessarily $\overline{\beta} = \mathrm{id}_{S^{-1}R}$. Now if $\alpha\colon R \to S^{-1}R$ and $\beta\colon R \to S^{-1}R'$ are two localizations in the sense of the definition, then there exists ring homomorphism $\overline{\beta}\colon S^{-1}R \to S^{-1}R'$ and $\overline{\alpha}\colon S^{-1}R' \to S^{-1}R$ such that $\beta = \overline{\beta} \circ \alpha$ and $\alpha = \overline{\alpha} \circ \beta$:

$$\begin{tikzcd} & R \arrow[dl, "\alpha"'] \arrow[d, "\beta"] \arrow[dr, "\alpha"] & \\ S^{-1}R \arrow[r, dotted, "\overline{\beta}"'] & S^{-1}R' \arrow[r, dotted, "\overline{\alpha}"'] & S^{-1}R \end{tikzcd}$$

Then, however, $\alpha = \overline{\alpha} \circ \overline{\beta} \circ \alpha$, so $\overline{\alpha} \circ \overline{\beta} = \mathrm{id}_{S^{-1}R}$. For the same reason also $\overline{\beta} \circ \overline{\alpha} = \mathrm{id}_{S^{-1}R'}$. Thus, $\overline{\alpha}$ and $\overline{\beta}$ are mutually inverse ring isomorphisms.

To summarize, the only issue is to prove the *existence* of a localization. We may use various constructions in various situations to do so (two of them are shown below) or we may even guess what $S^{-1}R$ is in a particular case. As long as the result satisfies the two conditions in the definition, it is as good as any other ring homomorphism with the same properties.

A well known construction of the ring $S^{-1}R$ and the homomorphism $\alpha\colon R \to S^{-1}R$ is via fractions. To that end, note that we can assume without loss of generality that $S$ is closed under multiplication, i.e. $s_1, s_2 \in S$ implies that $s_1s_2 \in S$. This is because a product of two invertible elements is invertible in any ring. For a similar reason, we can without loss of generality assume that $1 \in S$.

If $S$ is closed under multiplication and contains $1 \in R$, we can construct $S^{-1}R$ as the set of fractions $\frac{r}{s}$, where $r \in R$ and $s \in S$. Formally, $\frac{r}{s}$ is a block $[(r,s)]_\sim$ of the equivalence relation on $R \times S$ given by

$$(r_1, s_1) \sim (r_2, s_2) \quad \text{if} \quad (\exists s \in S)(r_1s_2s = r_2s_1s \text{ in } R). \tag{5}$$

If $R$ is an integral domain and $0 \notin S$, or more generally when $S$ contains no zero divisors (i.e. no elements $s \in S$ such that $st = 0$ for non-zero $t \in R$), the equivalence simplifies to a more familiar condition

$$(r_1, s_1) \sim (r_2, s_2) \quad \text{if} \quad r_1s_2 = r_2s_1 \text{ in } R.$$

However, in the presence of zero divisors we need the more complicated condition even to make sure that $\sim$ is an equivalence. One reason is the general fact that whenever $st = 0$ and $s$ invertible in a ring, then $t$ must vanish in that ring. In the more complicated condition, we do none other than apply this principle to $t = r_1s_2 - r_2s_1$ in what is going to be the ring of fractions $S^{-1}R$.

The following facts can be found in any textbook for commutative algebra, e.g. in [AM69, Chapter 3]. The relation $\sim$ on $R \times S$ is indeed an equivalence relation and we can define ring operations the set $S^{-1}R := R \times S/\sim$ in the intuitive way:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1s_2 + r_2s_1}{s_1s_2}, \qquad 0_{S^{-1}R} = \frac{0}{1},$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}, \qquad 1_{S^{-1}R} = \frac{1}{1},$$
$$-\frac{r}{s} = \frac{-r}{s}.$$

This yields a well defined commutative ring structure on $S^{-1}R$ and the assignment

$$\alpha\colon R \to S^{-1}R,$$
$$r \mapsto \frac{r}{1}$$

is a well-defined ring homomorphism. If $R$ was a $K$-algebra, so is $S^{-1}R$, with the scalar multiplication $k \cdot \frac{r}{s}$ for $k \in K$ defined as $\frac{kr}{s}$. If $r, s \in S$, then the multiplicative inverse of $\frac{r}{s}$ exists in $S^{-1}R$ and is equal to $\frac{s}{r}$.

**Proposition 20.** [AM69, Proposition 3.1] *The homomorphism $\alpha\colon R \to S^{-1}R$ constructed above is a localization of $R$ with respect to $S$. If $\beta\colon R \to T$ is a ring homomorphism which makes all the elements of $S$ invertible, then the uniquely defined homomorphism $\overline{\beta}$ acts as*

$$\overline{\beta}\colon S^{-1}R \to T,$$
$$\frac{r}{s} \mapsto \frac{\beta(r)}{\beta(s)}.$$

One can also quickly see from the above construction when exactly $S^{-1}R$ degenerates to a one-element ring, i.e. when $\frac{0}{1} = \frac{1}{1}$ in $S^{-1}R$. According to (5), this happens if and only if $0 \in S$. As one often wants to exclude this degenerate option, this leads to a standard definition describing the sets of elements of $R$ with respect to which one wants to localize (i.e. the reasonable sets of denominators):

**Definition.** A set of elements $S$ of a commutative ring $R$ is called a *multiplicative set* provided that

(1) $1 \in S$ and $S$ is closed under multiplication ($s_1, s_2 \in S$ implies $s_1s_2 \in S$), and
(2) $0 \notin S$.

If we localize with respect to a single element $f \in R$, there is a more direct way to construct $\{f\}^{-1}R$ which reveals another aspect of the localization. In this case we will also use the customary shorter notation $R_f$ for the localized ring and call it the localization of $R$ at $f$.

**Lemma 21.** *Let $R$ be a commutative ring and $f \in R$. Then the homomorphism*

$$\begin{aligned}\alpha\colon R &\to R[x]/(xf-1),\\ r &\mapsto r+(xf-1)\end{aligned}$$

*is a localization of $R$ at $f$. In particular, if $R$ is a finitely generated commutative algebra over a field $K$, so is $R_f$.*

*Proof.* Given $g \in R[x]$, we will denote by $\overline{g} = g + (xf-1)$ the coset of $g$. We will prove that $\alpha$ is a localization directly from the definition. First of all, we have $\overline{x} \cdot \overline{f} - 1 = 0$ in $R[x]/(xf-1)$, so $\alpha(f) = \overline{f}$ is invertible in $R/(xf-1)$ with inverse $\overline{x}$. Secondly, any ring homomorphism $\beta\colon R \to T$ such that $\beta(f)$ is invertible in $T$ can be extended to a ring homomorphism

$$\begin{aligned}\beta_1\colon R[x] &\to T,\\ g(x) &\mapsto g\big(\beta(f)^{-1}\big).\end{aligned}$$

Since we have $\beta_1(xf-1) = \beta(x)\beta(f) - 1 = \beta(f)^{-1}\beta(f) - 1 = 0$, the map $\beta_1$ induces a unique ring homomorphism

$$\begin{aligned}\overline{\beta}\colon R[x]/(xf-1) &\to T,\\ \overline{g} &\mapsto g\big(\beta(f)^{-1}\big).\end{aligned}$$

One readily checks that $\overline{\beta} \circ \alpha = \beta$ and that $\overline{\beta}$ is uniquely determined by this property.

If $R$ is a finitely generated algebra over a field $K$, then we have

$$R \cong K[y_1, y_2, \dots, y_n]/(g_1, g_2, \dots, g_\ell)$$

for some $n, \ell \geq 0$ and $g_1, g_2, \dots, g_\ell \in K[y_1, y_2, \dots, y_n]$. Suppose that $f \in R$ corresponds to the coset of a polynomial $f_1 \in K[y_1, y_2, \dots, y_n]$. Then

$$R_f := R[x]/(xf-1) \cong K[y_1, y_2, \dots, y_n, x]/(g_1, g_2, \dots, g_\ell, xf_1 - 1),$$

which again is a finitely generated commutative algebra over a field. $\square$

If $R = K[X]$ is a coordinate ring and $f \in K[X]$, then the localization homomorphism $K[X] \to K[X]_f$ has a clear geometric interpretation, which we are going to explain now. This result still works for an arbitrary (not necessarily algebraically closed or even infinite) field and an easy instance for $K = \mathbb{R}$, $X = \mathbb{A}^1_R$ and $f = x \in \mathbb{R}[\mathbb{A}^1_\mathbb{R}] \cong \mathbb{R}[x]$ is depicted in Figure 6.

**Proposition 22.** *Let $K$ be a field, $X = \mathrm{V}(g_1, g_2, \dots, g_\ell) \subseteq \mathbb{A}^n_K$ and algebraic set and $f \in K[x_1, x_2, \dots, x_n]$. If we define an algebraic subset $Y \subseteq \mathbb{A}^{n+1}_K$ by $Y = \mathrm{V}(g_1, g_2, \dots, g_\ell, x_{n+1}f - 1)$ and we consider the map*

$$\begin{aligned}u\colon Y &\to X,\\ (a_1, a_2, \dots, a_n, a_{n+1}) &\mapsto (a_1, a_2, \dots, a_n),\end{aligned}$$

*then:*

1. *$u$ is an injective polynomial map and its image is the Zariski open subset $X_f := \{P \in X \mid f(P) \neq 0\}$ of $X$.*
2. *$u$ induces a homeomorphism $Y \to X_f$ (with respect to Zariski topologies).*

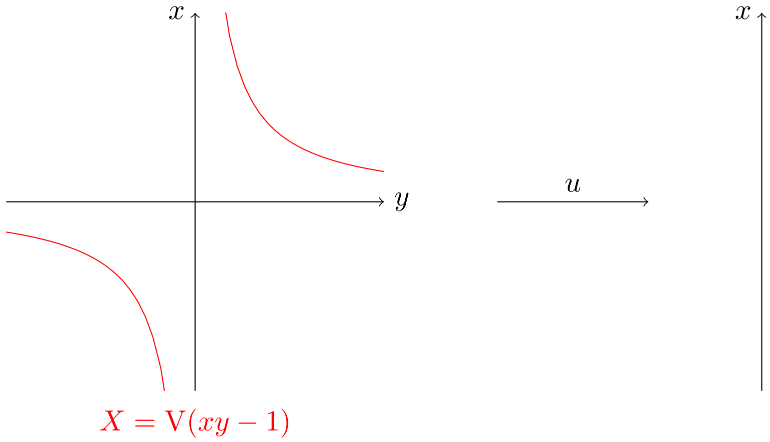


FIGURE 6. The easiest instance of Proposition 22. The polynomial map $u\colon (x,y) \mapsto x$ induces a homeomorphism between the red hyperbola and the Zariski open subset $\mathbb{A}^1_{\mathbb{R}} \setminus \{0\}$ of the line on the right. The algebra homomorphism $u^*\colon \mathbb{R}[x] \to \mathbb{R}[x,y]/(xy-1)$ is a localization of $\mathbb{R}[\mathbb{A}^1_{\mathbb{R}}] \cong \mathbb{R}[x]$ at the element $x$.

(3) *$u^*\colon K[X] \to K[Y]$ is a localization of $K[X]$ at $f$ (so that $K[Y] \cong K[X]_f$).*

*Proof.* (1) Given $Q = (a_1, a_2, \ldots, a_n, a_{n+1}) \in Y$, the last polynomial defining $Y$ says that $a_{n+1} \cdot f(a_1, a_2, \ldots, a_n) = 1$. This can be equivalently expressed as the condition that $f(a_1, a_2, \ldots, a_n) \neq 0$ and

$$a_{n+1} = \frac{1}{f(a_1, a_2, \ldots, a_n)}. \tag{6}$$

This shows that $u$ is injective and its image is precisely $X_f \subseteq X$.

(2) The map $u$ is clearly polynomial and hence continuous by Lemma 8(2). To show that $u\colon Y \to X_f$ is a homeomorphism, it remains to convince oneself that given any Zariski open subset $U \subseteq Y$, the image $u(U)$ is Zariski open in $X$. By Corollary 3, $U$ is of the form

$$U = Y \setminus \mathrm{V}(h_1, h_2, \ldots, h_m)$$

for some polynomials $h_1, h_2, \ldots, h_m \in K[x_1, x_2, \ldots, x_{n+1}]$. Note that for a point $(a_1, a_2, \ldots, a_n, a_{n+1}) \in Y$ we have $h_i(a_1, a_2, \ldots, a_n, a_{n+1}) = 0$ if and only if $\tilde{h}(a_1, a_2, \ldots, a_n) = 0$, where

$$\tilde{h}_i = f^{e_i} \cdot h_i\Big(x_1, x_2, \ldots, x_n, \frac{1}{f(x_1, x_2, \ldots, x_n)}\Big) \in K[x_1, x_2, \ldots, x_{n+1}]$$

and $e_i \geq 0$ is the highest exponent with which $x_{n+1}$ occurs in $h_i$. Therefore,

$$U = \{(a_1, a_2, \ldots, a_n, a_{n+1}) \mid \tilde{h}_i(a_1, a_2, \ldots, a_n) \neq 0 \text{ for some } i = 1, \ldots, m)\}$$

and

$$\begin{aligned} u(U) &= X_f \cap \{(a_1, a_2, \ldots, a_n) \mid \tilde{h}_i(a_1, a_2, \ldots, a_n) \neq 0 \text{ for some } i = 1, \ldots, m)\} \\ &= X \setminus \mathrm{V}(f\tilde{h}_1, f\tilde{h}_2, \ldots, f\tilde{h}_m). \end{aligned}$$

which is clearly Zariski open in $X$.

(3) Let $\alpha\colon K[X] \to K[X]_f$ be a localization of $K[X]$ at $f$. Since the polynomial function $f \in K[X]$ has an invertible image under $u^*\colon K[X] \to K[Y]$ (the multiplicative inverse of $f\colon Y \to \mathbb{A}^1_K$ is the $(n+1)$-st coordinate function $c_{n+1}\colon Y \to \mathbb{A}^1_K$, which is given by the polynomial $x_{n+1} \in K[x_1, x_2, \dots, x_{n+1}]$), the universal property of $\alpha$ yields the $K$-algebra homomorphism

$$\gamma\colon K[X]_f \to K[Y],$$
$$\frac{k}{f^e} \mapsto k \cdot x_{n+1}^e.$$

We must prove that $\gamma$ is a bijection. The surjectivity follows by a similar trick as in the proof of part (2). If $h \in K[x_1, x_2, \dots, x_{n+1}]$, $e \geq 0$ is the highest power of $x_{n+1}$ occuring in $h$ and

$$\tilde{h} = x_{n+1}^e \cdot h\Big(x_1, x_2, \dots, x_n, \frac{1}{f(x_1, x_2, \dots, x_n)}\Big) \in K[x_1, x_2, \dots, x_n],$$

then $h$ and $\gamma\big(\frac{\tilde{h}}{f^e}\big)$ define the same polynomial function on $Y$. Regarding the injectivity, suppose that $\gamma\big(\frac{k}{f^e}\big) = k \cdot x_{n+1}^e$ vanishes everywhere on $Y$. Since each point $Q = (a_1, a_2, \dots, a_n, a_{n+1})$ has non-zero last coordinate (thanks to (6)), the polynomial $k \in K[x_1, x_2, \dots, x_n]$ must vanish everywhere on $Y$ and, thus, $k$ vanishes everywhere on $X_f \subseteq \mathbb{A}^n_K$ as well. The product $kf$ vanishes even everywhere on $X$. Hence, $kf = 0$ in $K[X]$ by definition and $\frac{k}{f^e} = 0$ in $K[X]_f$ by (5). □

*Remark.* Proposition 22 entails a very important principle which will be used several times in the sequel. Namely, if $K$ is a field, $n \geq 0$ and $g_1, g_2, \dots, g_\ell, f_1, f_2, \dots, f_r \in K[x_1, x_2, \dots, x_n]$ for some $\ell, r \geq 0$, then we can view the set

$$Y' = \{P \in \mathbb{A}^n_K \mid g_i(P) = 0\ (\forall i \leq \ell) \text{ and } f_j(P) \neq 0\ (\forall j \leq r)\}$$

(which is a Zariski open subset of $V(g_1, g_2, \dots, g_\ell)$) as an algebraic set. We simply identify it via Proposition 22 with the honest algebraic subset

$$Y = V(g_1, g_2, \dots, g_\ell, x_{n+1} f_1 f_2 \cdots f_r - 1) \subseteq \mathbb{A}^{n+1}_K.$$

See Exercise 4 for a particular instance of such an identification.

After the preparation, we can focus on the weak version of Nullstellensatz. The algebraic core is contained in the following proposition whose proof we omit (it is taught in the introduction to commutative algebra and it can be found for instance in [AM69, Corollary 5.24] or [F08, §1.10, Proposition 4]).

**Proposition 23.** *Let $K$ be a field and $L$ be a finitely generated commutative $K$-algebra. If $L$ is a field too, then $L$ is a finite field extension of $K$.*

Now we can state and proof a weak version of Nullstellensatz. It guarantees the existence of a solution for a system of polynomial equations $f_i = 0$, $i \in I$ in variables $x_1, x_2, \dots, x_n$ over an algebraically closed field unless an obvious obstruction appears—there can be no solutions if there are polynomials $c_1, c_2, \dots, c_n$ and indices $i_1, i_2, \dots, i_n$ such that $c_1 f_{i_1} + c_2 f_{i_2} + \cdots + c_n f_{i_n} = 1$.

The algebraic closedness is essential here—the equation $x^2+1=0$ has no solution over the reals, but neither there exists $c \in \mathbb{R}[x]$ such that $c(x^2+1)=1$.

**Theorem 24** (Weak Nullstellensatz)**.** *Let $K$ be an algebraically closed field, $n \geq 1$ and $I \subsetneq K[x_1, x_2, \ldots, x_n]$ be a proper ideal. Then $\mathrm{V}(I)$ is non-empty (i.e. there exists a common zero $P \in \mathbb{A}^n_K$ to all the polynomials in $I$).*

*Proof.* The ideal $I$ embeds into a maximal ideal $M \subseteq K[x_1, x_2, \ldots, x_n]$ and it suffices to prove that $\mathrm{V}(M) \neq \varnothing$. However, $L = K[x_1, x_2, \ldots, x_n]/M$ is a field, so it is a finite field extension of $K$ by Proposition 23. Since all finite extensions are algebraic and, $K$ being algebraically closed, it has no algebraic extension except for $L = K$, we obtain an isomorphism of $K$-algebras

$$\alpha\colon K[x_1, x_2, \ldots, x_n]/M \xrightarrow{\cong} K.$$

Put $a_i = \alpha(x_i + M)$ and $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n_K$. Then we have for each $f \in M$:

$$f(P) = f\big(\alpha(x_1+M), \alpha(x_2+M), \ldots, \alpha(x_n+M)\big) = \alpha(f+M) = 0. \quad \square$$

Before we state the usual version of Hilbert's Nullstellensatz, we briefly recall the concept of a radical ideal.

**Definition.** If $R$ is a commutative ring and $I \subseteq R$ is an ideal, then the *radical* of $I$ is defined as

$$\sqrt{I} = \{f \in R \mid (\exists s \geq 1)(f^s \in I)\}.$$

An ideal is a *radical ideal* if $I = \sqrt{I}$. The ring $R$ is *reduced* if the zero ideal is a radical ideal, i.e. that for each $f \in R$ and $s \geq 1$ we have $f^s = 0 \implies f = 0$.

The following easy lemma summarizes what we need to know about radical ideals.

**Lemma 25.** *Let $I$ be an ideal in a commutative ring $R$.*

(1) *The radical $\sqrt{I}$ is a radical ideal and $I \subseteq \sqrt{I}$.*
(2) *The ideal $I$ is radical if and only if the quotient $R/I$ is reduced.*
(3) *The following implications hold:*

$$I \text{ maximal ideal} \implies I \text{ prime ideal} \implies I \text{ radical ideal.}$$

*Proof.* If $f^d \in I$ and $g^e \in I$, then $(f+g)^{d+e}, (fg)^{\max(d,e)}$ and $(-f)^d \in I$. Hence $\sqrt{I}$ is an ideal and clearly it contains $I$ and its radical is $\sqrt{I}$ again. Furthermore, $f^d \in I$ in $R$ if and only if $(f+I)^d = 0$ in $R/I$, which proves the second statement. Finally, it is well-known that $I$ is a maximal ideal if and only if $R/I$ is a field and $I$ is prime if and only if $R/I$ is a domain. Hence the last part follows from the obvious implications

$$R/I \text{ field} \implies R/I \text{ domain} \implies R/I \text{ reduced.} \quad \square$$

Note that if $X \subseteq \mathbb{A}^n_K$ is any subset, the ideal $\mathrm{I}(X) \subseteq K[x_1, x_2, \ldots, x_n]$ is a radical ideal (since $P \in \mathbb{A}^n_K$ is a zero of $f^d$, $d \geq 1$, if and only if $P$ is a zero of $f$). Hilbert's Nullstellensats says that the converse is true as well for algebraically closed fields—any radical ideal is the ideal of a subset of $X \subseteq \mathbb{A}^n_K$.

**Theorem 26** (Hilbert's Nullstellensatz)**.** *Let $K$ be an algebraically closed field, $n \geq 1$ and $J \subseteq K[x_1, x_2, \dots, x_n]$ be an ideal. Then* $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J}$.

*Proof.* We only need to prove the inclusion $\mathrm{I}(\mathrm{V}(J)) \subseteq \sqrt{J}$. Let us first choose some generators $g_1, g_2, \dots, g_\ell \in K[x_1, x_2, \dots, x_n]$ of the ideal $J$ and denote $X = \mathrm{V}(J) = \mathrm{V}(g_1, g_2, \dots, g_\ell) \subseteq \mathbb{A}^n_K$. Suppose that $f \in \mathrm{I}(X)$, then we clearly have

$$X \cap (\mathbb{A}^n_K \setminus \mathrm{V}(f)) = \varnothing.$$

Now we apply Proposition 22 to obtain a homeomorphism

$$u \colon Y = \mathrm{V}(x_{n+1}f - 1) \to \mathbb{A}^n_K,$$

whose image is precisely $\mathbb{A}^n_K \setminus \mathrm{V}(f)$. By our assumption, we have

$$\mathrm{V}(g_1, g_2, \dots, g_\ell, x_{n+1}f - 1) = u^{-1}(X) = \varnothing$$

Hence, by Theorem 24, the polynomials $g_1, g_2, \dots, g_\ell$ and $x_{n+1}f - 1$ generate the unit ideal in $K[x_1, x_2, \dots, x_{n+1}]$. If we identify $K[X]$ with the localization $K[x_1, x_2, \dots, x_n]_f$ via Proposition 22(3), this translates to the fact that the fractions $\frac{g_1}{1}, \frac{g_2}{1}, \dots, \frac{g_\ell}{1}$ generate the unit ideal in $K[x_1, x_2, \dots, x_n]_f$, i.e. there exist $\frac{c_1}{f^d}, \frac{c_2}{f^d}, \dots, \frac{c_\ell}{f^s} \in K[x_1, x_2, \dots, x_n]_f$ such that

$$\frac{c_1}{f^d} \cdot \frac{g_1}{1} + \frac{c_2}{f^d} \cdot \frac{g_2}{1} + \cdots + \frac{c_\ell}{f^d} \cdot \frac{g_\ell}{1} = 1.$$

If we multiply this expression by $f^d$, we obtain an equality

$$c_1 g_1 + c_2 g_2 + \cdots + c_\ell g_\ell = f^d$$

in $K[x_1, x_2, \dots, x_n]$, which says none other than $f \in \sqrt{J}$. $\square$

As an easy application, we can compute ideals of hypersurfaces (i.e. algebraic sets of the form $\mathrm{V}(f) \subseteq \mathbb{A}^n_K$ for a non-constant polynomial $f \in K[x_1, x_2, \dots, x_n]$) using the fact that $K[x_1, x_2, \dots, x_n]$ is a unique factorization domain. We refer to Exercise 5 for details. More interestingly, we can also prove that rational maps without poles are precisely the polynomial maps. Note that for this we indeed need that $K$ be algebraically closed; see Exercise 10 for a counterexample over $\mathbb{R}$. Before proving this fact, we introduce the following convention.

*Remark.* If $X \subseteq \mathbb{A}^n_K$ is an algebraic set and $K[X]$ its coordinate ring, we can define operators V and I relative to $X$. That is, if $S \subseteq K[X]$, we put

$$\mathrm{V}(S) = \{P \in X \mid f(P) = 0 \ (\forall f \in S)\} \subseteq X.$$

Similarly, if $Y \subseteq X$, we put

$$\mathrm{I}(Y) = \{f \in K[X] \mid f(P) = 0 \ (\forall P \in Y)\} \subseteq K[X].$$

These assignments satisfy completely analogous properties to those originally introduced in Section 1.

More importantly, if $K$ is algebraically closed, the corresponding analogues of Theorems 24 and 26 hold. That is, $\mathrm{V}(J) \neq \varnothing$ if $J \subsetneq K[X]$ is a proper ideal and $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J}$ for any ideal $J \subseteq K[X]$. This is in fact an easy consequence of the two theorems and we leave the proof of these facts to the reader (Exercise 8).

**Proposition 27.** *Let $K$ be an algebraically closed field, $X, Y$ be varieties over $K$ and $r\colon X \to Y$ be a rational map which is regular at every point of $X$. Then $r$ is a polynomial map.*

*Proof.* Since a rational map $r\colon X \to Y$ is defined by the assignment $r(P) = \big(r_1(P), r_2(P), \dots, r_\ell(P)\big)$, where $r_1, r_2, \dots, r_\ell \in K(X)$ are rational functions, it suffices to prove the proposition for rational functions (i.e. for $Y = \mathbb{A}^1_K$).

Let $r \in K(X)$ and recall from Lemma 14 that the set of poles of $r$ equals $Z = \mathrm{V}(\{g \mid r = \frac{f}{g} \text{ in } K(X)\})$. If $Z = \varnothing$, then the ideal generated by the possible denominators $g$ must be all of $K[X]$ by Theorem 24 and Exercise 8a. In other words, we have expressions

$$r = \frac{f_1}{g_1} = \frac{f_2}{g_2} = \cdots = \frac{f_r}{g_r} \in K(X)$$

and elements $c_1, c_2, \dots, c_r \in K[X]$ such that $c_1 \cdot g_1 + c_2 \cdot g_2 + \cdots + c_r \cdot g_r = 1$. It immediately follows that

$$r = \frac{c_1 \cdot f_1 + c_2 \cdot f_2 + \cdots + c_r \cdot f_r}{c_1 \cdot g_1 + c_2 \cdot g_2 + \cdots + c_r \cdot g_r} = c_1 \cdot f_1 + c_2 \cdot f_2 + \cdots + c_r \cdot f_r$$

in $K(X)$, so $r \in K[X]$ as was claimed. □

Another quick consequence of the Nullstellensatz is the following characterization of coordinate rings (up to isomorphism) among all commutative $K$-algebras.

**Proposition 28.** *Let $K$ be an algebraically closed field and $R$ be a commutative $K$-algebra. Then the following statements are equivalent:*

1. *$R$ is isomorphic to $K[X]$ for some algebraic set $X$ over $K$.*
2. *$R$ is a finitely generated reduced $K$-algebra.*

*Proof.* We already know that (1) $\implies$ (2). Conversely, suppose that $R$ is a finitely generated reduced $K$-algebra. That is, we have

$$R \cong K[x_1, x_2, \dots, x_n]/(f_1, f_2, \dots, f_\ell)$$

for some $n, \ell \geq 1$ and polynomials $f_1, f_2, \dots, f_\ell \in K[x_1, x_2, \dots, x_n]$. Moreover, the ideal $J = (f_1, f_2, \dots, f_\ell)$ is radical by Lemma 25. Thus, $J = \mathrm{I}(X)$ for $X = \mathrm{V}(J) \subseteq \mathbb{A}^n_K$ by Theorem 26 and, consequently, $R \cong K[X]$. □

Finally, we obtain the following dictionary between geometric objects related to $X$ and the corresponding algebraic objects related to $K[X]$.

**Proposition 29.** *Let $K$ be an algebraically closed field and $X$ be an algebraic set over $K$. Then there is an inclusion-reversing bijection*

$$\begin{aligned} \{\textit{subvarieties of } X\} &\longrightarrow \{\textit{prime ideals of } K[X]\}, \\ Y &\longmapsto \mathrm{I}(Y), \\ V(J) &\longleftarrow\!\shortmid J. \end{aligned}$$

*If we identify a point $P \in X$ with the subvariety $\{P\} \subseteq X$, the above assignment restricts to a bijection*

$$\begin{aligned} X &\longrightarrow \{\textit{maximal ideals of } K[X]\}, \\ P &\longmapsto \mathrm{I}(P). \end{aligned}$$

*Proof.* If $Y \subseteq X$ is an algebraic subset of $X$, then $\mathrm{V}(\mathrm{I}(Y)) = Y$. This follows quickly from Lemma 6(4). Moreover, $Y$ is irreducible if and only if $\mathrm{I}(Y)$ is a prime ideal of $K[X]$ by the same argument as for Theorem 7. Finally, if $J \subseteq K[X]$ is a prime ideal, it is radical by Lemma 25 and, thus, $\mathrm{V}(\mathrm{I}(J)) = J$ by Theorem 26 and Exercise 8b. This establishes the first bijection.

To obtain the second bijection, note that since the first one is an order antiisomorphism with respect to the inclusion, maximal ideals of $K[X]$ must correspond precisely to the minimal non-empty subvarieties of $X$. However, these minimal non-empty subvarieties of $X$ are clearly none other than the points of $X$. $\square$

*Remark.* The maximal ideals from the previous proposition have a very nice expression in terms of generators. Indeed, let $P = (a_1, a_2, \ldots, a_n) \in X$ be a point. If $K[X] = K[x_1, x_2, \ldots, x_n]/\mathrm{I}(X)$ is the coordinate ring and $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$ are the cosets of the variables (in other words, the coordinate functions), we have

$$\mathrm{I}(P) = (\overline{x_1 - a_1}, \overline{x_2 - a_2}, \ldots, \overline{x_n - a_n}).$$

This is very easy to see if $P = (0, 0, \ldots, 0)$ is the origin of $\mathbb{A}^n_K$. The general case is obtained by the corresponding affine coordinate change.

*Remark.* A important step in linear algebra is to introduce an abstract notion of vector space about which we can argue *without* a particular choice of a basis. Of course, we can choose a particular basis whenever necessary and typically we choose one best suited for the intended purpose.

Analogously, Proposition 29 allows us to manipulate with algebraic sets over $K$ *without* a priori choosing any particular coordinates. The point is that we can reconstruct the relevant structure on an algebraic set just from knowing its coordinate ring $R$ up to isomorphism.

More precisely, let $R$ be a finitely generated reduced $K$-algebra, where $K = \overline{K}$. In view of Proposition 29, we can put $X$ equal to the set of maximal ideals of $R$. The Zariski topology on $X$ is defined by declaring the closed sets to be precisely those of the form

$$\mathrm{V}(I) = \{M \subseteq R \text{ maximal ideal} \mid I \subseteq M\},$$

where $I \subseteq R$ runs over all ideals of $R$. It is straightforward to check such a topological space $X$ is homeomorphic to the algebraic set reconstructed from $R$ using particular coordinates as in Proposition 28.

However, we can learn even more about $X$ using the coordinate-free approach. Since $R$ should be the coordinate ring of $X$, any element $r \in R$ should define the corresponding 'polynomial function' $X \to K$ on the set $X$ of maximal ideals of $R$. If $M \in X$ is a maximal ideal, we can define the value of $r$ at $M$ as follows. Since $R/M$ is a finite field extension of $K$ by Proposition 23 and $K = \overline{K}$, we have a unique isomorphism of $K$-algebras $\varphi_M \colon R/M \to K$. The value $r$ at $M$ is then simply $\varphi_M(r+M) \in K$. One can check that also this abstract definition agrees with the ordinary polynomial functions which we obtain in Proposition 28. For all practical purposes, the knowledge of $X$ as a topological space and the ring of polynomial functions tells us everything about $X$. Recall in particular Theorem 12 in this context.

The significance of these observations is that they constitute a first step towards the concept of scheme, which is a basic notion of the modern language of algebraic geometry.

**Exercises.**

(1) Let $K$ be a field. Describe explicitly the localization of $R$ at an element $f$ in the following situations:
  (a) $R = K \times K$ and $f = (1, 0)$.
  (b) $R = K[x, y]/(xy)$ and $f = x$.
  (c) $R = K[x, y, z]/(xz, yz)$ and $f = y - z$.

(2) An element $e$ of a commutative ring $R$ is called *idempotent* if $e^2 = e$.
  (a) Show that if $e \in R$ is an idempotent, then the ideal $eR$ has a natural structure of a commutative ring. The operations are simply the restrictions of the operations on $R$, with the exception of the unity, which is $e$ for $eR$.
  (b) Show that if $e \in R$ is an idempotent, then so is $f = 1 - e$ and that $e \cdot f = 0$. Show that there is a ring isomorphism $\alpha\colon R \to eR \times fR$ given by $\alpha(r) = (er, fr)$. Find the images of $e$ and $f$ under $\alpha$ and describe how the inverse isomorphism $\alpha^{-1}\colon eR \times fR \to R$ acts.
  (c) With the same notation as before, show that the localization of $R$ at $e$ is isomorphic to the factor ring $R/(f)$ (this generalizes Exercise 1a).

(3) Show that if $R$ is a commutative ring, $I \subseteq R$ is an ideal and $S \subseteq R$ is a multiplicative set, then the operations of factoring out $I$ and of localizing at $S$ commute with one another.

  More precisely, show that there is a canonical isomorphism of rings $(S + I)^{-1}(R/I) \cong S^{-1}R/S^{-1}I$, where $S + I = \{s + I \mid s \in S\}$ and $S^{-1}I = \{\frac{i}{s} \mid i \in I \text{ and } s \in S\}$ is the ideal of $S^{-1}R$ generated by the image of $I$ under the localization homomorphism $R \to S^{-1}R$.

(4) Let $K$ be a field and $\mathrm{GL}_n(K)$ be the set of invertible $n \times n$ matrices over $K$. Using Proposition 22 and the remark after it, interpret $\mathrm{GL}_n(K)$ as an algebraic variety and compute its coordinate ring.

(5) Let $K$ be an algebraically closed field and $f \in K[x_1, x_2, \dots, x_n]$ be a non-constant polynomial. Show that $\mathrm{I}(\mathrm{V}(f)) \subseteq K[x_1, x_2, \dots, x_n]$ is again a principal ideal and it is generated by the largest square-free factor of $f$. That is, if $f = k \cdot p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$ with $p_1, p_2, \dots, p_r \in K[x_1, x_2, \dots, x_n]$ irreducible polynomials, $e_1, e_2, \dots, e_r \geq 0$ and $k$ a non-zero constant, then $\mathrm{I}(\mathrm{V}(f)) = (p_1 p_2 \cdots p_r)$. (Compare to Exercise 4 in Section 1.)

(6) Let $R$ be a commutative ring and $I, J \subseteq R$ be ideals.
  (a) Show that if $I, J$ are radical ideals, then so is $I \cap J$, but not necessarily $I + J$. Hint: consider $I = (y)$ and $J = (y - x^2)$ in $\mathbb{C}[x, y]$. The geometric reason for the issue with $I + J$ is that the line $\mathrm{V}(I)$ is tangent to the parabola $\mathrm{V}(J)$.
  (b) Show that $I \cap J = \sqrt{I \cdot J}$, but in general $I \cdot J \subsetneqq I \cap J$.

(7) Let $K$ be an algebraically closed field and $X, Y \subseteq \mathbb{A}^n_K$ algebraic sets. Show that $\mathrm{I}(X \cup Y) = \mathrm{I}(X) \cap \mathrm{I}(Y) = \sqrt{\mathrm{I}(X) \cdot \mathrm{I}(Y)}$ and $\mathrm{I}(X \cap Y) = \sqrt{\mathrm{I}(X) + \mathrm{I}(Y)}$.

(8) Let $X \subseteq \mathbb{A}^n_K$ be an algebraic set over an algebraically closed field $K$.
  (a) Prove that $\mathrm{V}(J) \neq \varnothing$ if $J \subsetneqq K[X]$ is a proper ideal of the coordinate ring of $X$.
  (b) Prove that $\mathrm{I}(\mathrm{V}(J)) = \sqrt{J}$ for any ideal $J \subseteq K[X]$.

  Here we use the convention from the Remark above Proposition 27. Hint: simply use Theorems 24 and 26.

(9) This exercise is devoted to explaining and justifying why taking a disjoint union of algebraic sets corresponds to taking a Cartesian product of their coordinate rings (over any field $K$).
  (a) Let $R$ be a commutative ring and $I, J \subseteq R$ ideals. Show that if $I + J = R$, then $I \cdot J = I \cap J$ and the map $R/I \cap J \to R/I \times R/J$ given by $r + (I \cap J) \mapsto (r + I, r + J)$ is an isomorphism of rings. This statement is known as the Chinese Remainder Theorem, because it generalizes the classical situation where $R = \mathbb{Z}$, $I = (m)$ and $J = (n)$, where $m$ and $n$ are coprime integers.
  (b) Show that if $X, Y \in \mathbb{A}^n_K$ are disjoint algebraic sets in $\mathbb{A}^n_K$, then $K[X \cup Y] \cong K[X] \times K[Y]$.
  (c) Now let $X \subseteq \mathbb{A}^n_K$ and $Y \subseteq \mathbb{A}^\ell_K$ be arbitrary algebraic sets. Show that we can always embed them as disjoint algebraic subsets into some $\mathbb{A}^m_K$. Hint: Without loss of generality $n = \ell$ and consider $X \times \{0\} \cup Y \times \{1\} \subseteq \mathbb{A}^m_K$ for $m = n + 1$.

(10) Let $K$ be a field and $X \subseteq \mathbb{A}^n_K$ and algebraic set. Show that $X$ is a finite set if and only if $K[X]$ has finite dimension as a vector space over $K$.

(11) Let $r\colon \mathbb{A}^1_\mathbb{R} \to \mathbb{A}^1_\mathbb{R}$ be the map given by the assignment $t \mapsto \frac{1}{t^2+1}$. Show that $r$ is a rational map which is regular at every point of $\mathbb{A}^1_\mathbb{R}$, but it is nevertheless *not* a polynomial map (compare with Proposition 27).

## 4. Local properties of algebraic sets

This section is devoted to setting up a framework for studying algebraic sets locally in the Zariski topology. Such an approach is usual in other geometric theories based on mathematical analysis, where one often restricts the attention to a suitably small open neighborhood of a point and argues there. Some properties of smooth manifolds or functions on them can be studied even on an arbitrary small open neigborhood of a point—for example derivatives of functions at that point. In order to be able to use similar arguments in algebraic geometry, we first turn the attention to open sets in the Zariski topology. Recall the following definition.

**Definition.** Let $(X, \tau)$ be a topological space. A set $\mathcal{B}$ of open subsets of $X$ is called a *basis* of the topology $\tau$ if it satisfies the following conditions:

(1) Every open subset $U \subseteq X$ is a union of sets in $\mathcal{B}$ (equivalently, $U = \bigcup_{V \in \mathcal{B}, V \subseteq U} V$).
(2) If $U, V \in \mathcal{B}$, then $U \cap V \in \mathcal{B}$.

*Remark.* Usually, one does not require condition (2) in the definition of a basis. Since $U \cap V$ is open for any pair $U, V \in \mathcal{B}$, it follows already from (1) that $U \cap V$ is a union of sets from $\mathcal{B}$. Condition (2) is a stronger version of this and we will impose it since the standard basis of Zariski topology (which is defined just below) has this property.

Suppose now that $K$ is any field and $X$ is an algebraic set over $K$. Then $U \subseteq X$ is Zariski open if and only if it is of the form $U = X \setminus \mathrm{V}(S)$ for a set $S \subseteq K[X]$. In other words,

$$U = X \setminus \bigcap_{f \in S} \mathrm{V}(f) = \bigcup_{f \in S} X_f,$$

where we use the notation

$$X_f = X \setminus \mathrm{V}(f) = \{P \in X \mid f(P) \neq 0\}.$$

**Lemma 30.** *Let $K$ be a field and $X$ be an algebraic set over $K$. Then the collection $\mathcal{B} = \{X_f \mid f \in K[X]\}$ is a basis of open sets for the Zariski topology.*

*Proof.* Every open set is a union of those from $\mathcal{B}$ by the above. If $f, g \in K[X]$, then

$$X_f \cap X_g = X \setminus (\mathrm{V}(f) \cup \mathrm{V}(g)) = X \setminus \mathrm{V}(fg) = X_{fg}. \qquad \square$$

*Remark.* The basic open sets of $X \subseteq \mathbb{A}^n_K$ as in Lemma 30 can themselves be viewed as affine algebraic subsets of $\mathbb{A}^{n+1}_K$ using Proposition 22. Not every Zariski open set is basic, however, see Exercise 1.

Now we are going to inspect functions on an arbitrarily small Zariski open neighborhood of a point of an algebraic set. Such functions (or more precisely, their germs, see below) will form local rings. To this end, recall an abstract definition.

**Definition.** A commutative ring $R$ is called *local* is it has precisely one maximal ideal.

We will use the following characterization as a convenient tool to recognize local rings. The point is that a sum of two non-invertible elements can very well be invertible in a general commutative ring (e.g. $1 = x + (1 - x)$ in $K[x]$), but not in a local ring.

**Lemma 31.** *Let $R$ be a commutative ring with at least two elements and let $M$ be the set of all non-invertible elements of $R$. Then the following are equivalent:*

(1) *$R$ is a local ring.*
(2) *$M$ is an ideal of $R$.*

*If the equivalent conditions hold, $M$ is the unique maximal ideal of $R$.*

*Proof.* Observe that an element $r \in R$ of an arbitrary commutative ring is invertible if and only if it is *not* contained in any maximal ideal $M \subseteq R$. Thus, if $M$ is the unique maximal ideal of $R$, then $M$ consists precisely of all non-invertible elements of $R$.

Conversely, if the set $M$ of non-invertible elements of $R$ forms an ideal and $M'$ is a maximal ideal of $R$, then $M' \subseteq M$ (as $M'$ cannot contain an

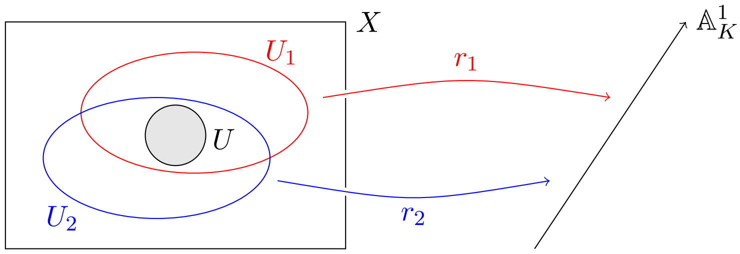


FIGURE 7. An equivalence of rational functions defined on open neighborhoods of $P \in X$. We require that $P \in U$ and $r_1|_U = r_2|_U$.

invertible element). Then $M' = M$ since $M'$ is maximal and it follows that $R$ is local. $\square$

*Example.* Let $K$ be a field, $X$ be an algebraic variety over $K$ and $P \in X$ be a point. Then we define the *local ring* of $X$ at $P$ as the subring $\mathcal{O}_{X,P} \subseteq K(X)$ consisting of the rational functions regular at $P$.

This is an example of a local ring. Indeed, note first that if $r \in \mathcal{O}_{X,P}$, then $R$ has an expression $r = \frac{f}{g}$ with $g(P) \neq 0$. If $r(P) \neq 0$, then $r^{-1} = \frac{g}{f}$ is also regular at $P$. In other words, the set of non-units of $\mathcal{O}_{X,P}$ equals

$$M = \{r \in \mathcal{O}_{X,P} \mid r(P) = 0\}$$

(see Exercise 4 in Section 2) and $M$ is clearly an ideal of $\mathcal{O}_{X,P}$.

The next aim is to define $\mathcal{O}_{X,P}$ for a point $P$ in a general (possibly reducible) algebraic set $X$. Since $K[X]$ may not be a domain, we cannot define $\mathcal{O}_{X,P}$ via the quotient field. However, we can define it as the $K$-algebra of germs of functions.

To this end, let $K$ be a field, $X$ be an algebraic set over $K$ and $P \in X$. We consider all functions $r\colon U \to \mathbb{A}^1_K$ defined on Zariski open neighborhoods $U$ of $P$ in $X$ which are of the following form: We require that there exist $f, g \in K[X]$ such that $g$ is non-zero everywhere in $U$ and $r$ is given by the assignment

$$\begin{aligned} r\colon U &\to \mathbb{A}^1_K, \\ Q &\mapsto \frac{f(Q)}{g(Q)}. \end{aligned}$$

This generalizes rational functions to possibly reducible varieties. Now we define an equivalence relation on this kind of functions by declaring $r_1\colon U_1 \to \mathbb{A}^1_K$ and $r_2\colon U_2 \to \mathbb{A}^1_K$ equivalent if there exists and open neighborhood $U \subseteq U_1 \cap U_2$ of $P$ such that $r_1|_U = r_2|_U$ (see Figure 7).

**Definition.** A an equivalence class $[r]_\sim$ of a function as above is called a *germ* of a rational function on $X$ at $P$. The *local ring* of $X$ at $P$ is defined as

$$\mathcal{O}_{X,P} = \{[r]_\sim \mid r\colon U \to \mathbb{A}^1_K\}.$$

The terminology is based on the observation that $\mathcal{O}_{X,P}$ has a natural structure of a ring, even a $K$-algebra. If $r_1\colon U_1 \to \mathbb{A}^1_K$ and $r\colon U_2 \to \mathbb{A}^1_K$ are functions, we can define $[r_1]_\sim + [r_2]_\sim$ as the function

$$\begin{aligned} U_1 \cap U_2 &\to \mathbb{A}^1_K, \\ Q &\mapsto r_1(Q) + r_2(Q). \end{aligned}$$

The multiplication of functions, the unary minus and the scalar multiplication are defined pointwise in a similar way. The constants $0, 1 \in \mathcal{O}_{X,P}$ can be taken as the germs of $0, 1 \in K[X]$, respectively. In fact, not only we obtain a commutative $K$-algebra structure on $\mathcal{O}_{X,P}$, but we even have a homomorphism of $K$-algebras

$$\begin{aligned} \varphi_P \colon K[X] &\to \mathcal{O}_{X,P}, \\ f &\mapsto [f]_\sim, \end{aligned}$$

which maps a polynomial function to its germ at $P$.

*Remark.* Note that the definition of a local rings is invariant under polynomial isomorphisms of algebraic sets. Indeed, if $f \colon X \to Y$ is an isomorphism of algebraic sets, then $f^* \colon K[Y] \to K[X]$ is an isomorphism of coordinate rings. Hence, if $P \in X$, the $f^*$ induces an isomorphism of $K$-algebras $\mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$. In other words, whatever property of $P$ can be defined in terms of its local ring $\mathcal{O}_{X,P}$, it is invariant under change of coordinates.

*Remark.* More generally, suppose that $X$ is an algebraic set, $f \in K[X]$ and let $u \colon Y \to X$ be the polynomial embedding as in Proposition 22. If $P \in X_f$ and $P' = u^{-1}(P) \in Y$, then $u^*$ induces an isomorphism of $K$-algebras

$$\mathcal{O}_{Y,P'} \overset{\cong}{\to} \mathcal{O}_{X,P}.$$

Indeed, $u$ is a homeomorphism onto the open subset $X_f$ of $X$, and as we are interested in arbitrary small open neighborhoods of $P$ in $X$ in the definition of $\mathcal{O}_{X,P}$, we may consider only the neighborhoods contained in $X_f$. On the other hand, $u^*$ identifies polynomial functions on $Y$ with certain ratios of polynomial functions on $X$ (Proposition 22), so ratios of polynomial function on $Y$ can be identified via $u^*$ with certain ratios of ratios of polynomial functions on $X$, which are again ratios of polynomial functions on $X$.

The next proposition shows that $\varphi_P$ is a localization of $K[X]$ at the maximal ideal $\mathrm{I}(P)$. To this end, recall that if $R$ is a ring and $I$ is a prime ideal, its complement $S = R \setminus I$ is a multiplicative set. The corresponding localization is customary called the localization of $R$ at $I$ and denoted by $R \to R_I$. It is easy to check that $R_I$ is a local ring whose maximal ideal (= the set of non-invertible elements) is $\{\frac{r}{s} \mid r \in I \text{ and } s \in R \setminus I\}$.

We leave it as an exercise for the reader to deduce the isomorphisms from the previous two remarks algebraically from the universal properties of the localizations in Propositions 32 and 22.

**Proposition 32.** *Let $K$ be an arbitrary field, $X$ be an algebraic set over $K$ and $P \in K$. Then the homomorphism $\varphi_P \colon K[X] \to \mathcal{O}_{X,P}$ which sends each polynomial function $f$ to its germ $[f]_\sim$ is a localization at the maximal ideal $M_P = \{f \in K[X] \mid f(P) = 0\}$.*

*Proof.* The strategy is similar to the proof of Proposition 22. First of all, notice that if $f \in K[X]$ is a polynomial function which is not contained in $M_P$, then the germ of the function

$$\begin{aligned} r\colon X_f &\to \mathbb{A}^1_K, \\ Q &\mapsto f(Q)^{-1} \end{aligned}$$

is a multiplicative inverse of $\varphi_P(f) = [f]_\sim$ in $\mathcal{O}_{X,P}$. We can therefore use the universal property of the localization $\alpha\colon K[X] \to K[X]_{M_P}$ to obtain a unique homomorphism of $K$-algebras $\overline{\varphi}_P\colon K[X]_{M_P} \to \mathcal{O}_{X,P}$ such that the triangle

$$\begin{tikzcd} K[X] \arrow[r, "\alpha"] \arrow[dr, "\varphi_P"'] & K[X]_{M_P} \arrow[d, dotted, "\exists!\overline{\varphi}"] \\ & \mathcal{O}_{X,P} \end{tikzcd}$$

commutes. In fact, the action of $\overline{\varphi}_P$ can be made quite explicit—it sends a fraction $\frac{f}{g}$ to the germ of the function $r\colon Q \mapsto \frac{f(Q)}{g(Q)}$ which is defined on an appropriate Zariski open neighborhood of $P$.

Our goal is to prove that $\overline{\varphi}_P\colon K[X]_{M_P} \to \mathcal{O}_{X,P}$ is an isomorphism. The surjectivity is almost tautological. Indeed, if $r\colon U \to \mathbb{A}^1_K$ is a function which acts as $Q \mapsto \frac{f(P)}{g(P)}$, then $[r]_\sim = \overline{\varphi}_P\big(\frac{f}{g}\big)$ merely by unraveling the definitions.

Regarding the injectivity of $\overline{\varphi}_P$, suppose that $\frac{f}{g} \in K[X]_{M_P}$ is such that $\overline{\varphi}_P\big(\frac{f}{g}\big) = 0$. By definition, this means that $\frac{f(Q)}{g(Q)}$ evaluates to zero on some Zariski open neighborhood $U$ of $P$. Without loss of generality, we can assume that $U$ is a basic open set, i.e. $U = X_t$ for some $t \in K[X]$. Since $P \in U$, we have $t \in K[X] \setminus M_P$. Now observe that $t(Q) \cdot f(Q) = 0$ for *every* point of $X$—either $Q \in X_t$ and we use the assumption, or $Q \notin X_t$ and then $t(Q) = 0$. In other words, we have $t \cdot f = 0$ in $K[X]$, which implies that $\frac{f}{g} = 0$ in $K[X]_{M_P}$ by Proposition 20. □

The latter proposition among others shows that the definition of $\mathcal{O}_{X,P}$ via germs agrees with the previous more special definition of $\mathcal{O}_{X,P}$ for varieties via their function fields

The proposition also allows us to deduce basic algebraic properties of $\mathcal{O}_{X,P}$. Most notably, although $\mathcal{O}_{X,P}$ typically is not a finitely generated algebra over a field (Exercise 2), it is still a noetherian ring. This is important as the theory of commutative noetherian rings is very well developed and noetherian rings are in general much better behaved than non-noetherian ones.

**Lemma 33.** *Let $R$ be a commutative noetherian ring and $S \subseteq R$ a multiplicative set. Then $S^{-1}R$ is also noetherian.*

*Proof.* Let $I \subseteq S^{-1}R$ be an ideal. We must show that $I$ is finitely generated in $S^{-1}R$. To this end, we let $J = \{r \in R \mid (\exists s \in S)\big(\frac{r}{s} \in I\big)\}$. It is completely straightforward to check that $J$ is an ideal of $R$ and that $I$ can be recovered from $J$ as

$$I = \Big\{\frac{r}{s} \mid r \in J \text{ and } s \in S\Big\}.$$

Since $R$ is noetherian, $J$ is finitely generated in $R$ and it immediately follows that $I$ is finitely generated in $S^{-1}R$. □

**Corollary 34.** *Let $X$ be an algebraic set and $P \in X$. Then $\mathcal{O}_{X,P}$ is noetherian.*

What kind of information does $\mathcal{O}_{X,P}$ give us about the point $P \in X$? To start with, there is an easy geometric interpretation for the situation where $\mathcal{O}_{X,P}$ is a domain. This happens precisely when $P$ is *not* in the intersection of two or more irreducible components of $X$.

**Proposition 35.** *Let $X$ be an algebraic set over a field $K$ and let $P \in X$ be a point. Then the following conditions are equivalent:*

(1) *$\mathcal{O}_{X,P}$ is a domain.*
(2) *The point $P$ lies on only one irreducible component of $X$*

*Proof.* Let $X = Z_1 \cup Z_2 \cup \cdots \cup Z_r$ be the decomposition to irreducible components in the sense of Theorem 5.

Suppose first that $P$ belongs to only one of the components $Z_i$. We can assume without loss of generality that $i = 1$, so that $P$ belongs to the Zariski open subset $U = Z_1 \setminus (Z_2 \cup Z_3 \cup \cdots \cup Z_r)$. We can further choose a basic open neighborhood $X_f$ of $P$ inside $U$ for some $f \in K[X]$. Note that $X_f \subseteq Z_1$ and it is also an open subset there. As $Z_1$ is irreducible, $X_f$ must be dense in $Z_1$ (Exercise 6 in Section 1). It follows that $X_f$ is an irreducible topological space (Exercise 8 in Section 1), and also that $Y$ is irreducible since it is homeomorphic to $X_f$.

Now let $u\colon Y \to X$ be the polynomial embedding with the image $X_f$ as in Proposition 22. As we know that $\mathcal{O}_{X,P} \cong \mathcal{O}_{Y,u^{-1}(P)}$ by the discussion before Proposition 32 and that $K[Y]$ is a domain, it follows that also $\mathcal{O}_{Y,u^{-1}(P)}$ is a domain.

Conversely, suppose that $P$ belongs to more than one irreducible component, say $P \in Z_1 \cap Z_2$. Since $Z_i \not\subseteq (Z_1 \cup \cdots \cup Z_{i-1} \cup Z_{i+1} \cup \cdots \cup Z_r)$ for any $i \in \{1, 2, \dots, r\}$, there exists for each $i$ a function $g_i \in K[X]$ which vanishes on all $Z_j$, $j \neq i$, but it is non-zero on $Z_i$.

In particular, $g_1 \cdot g_2 = 0$ in $K[X]$ and also $[g_1]_\sim \cdot [g_2]_\sim = 0$ in $\mathcal{O}_{X,P}$. On the other hand $[g_1]_\sim \neq 0$ in $\mathcal{O}_{X,P}$ since $g_1$ is non-zero on any Zariski open neighborhood $U$ of $P$. To see this, recall Exercise 6a in Section 2 and that $U \cap Z_1$ is a non-empty, so dense open subset of $Z_1$. An analogous argument for $Z_2$ shows that $[g_2]_\sim \neq 0$ in $\mathcal{O}_{X,P}$ as well, so $\mathcal{O}_{X,P}$ is not a domain. □

**TO DO:** Plane curves and their local properties.

**Exercises.**

(1) Let $K$ be an algebraically closed field and $U = \mathbb{A}^2_K \setminus \{(0,0)\}$. This is clearly a Zariski open set. Show that $U$ is *not* a basic open set in the sense of Lemma 30. Hint: Use Exercise 2 from Section 1.
(2) Let $K$ be a field and $M = (x) \subseteq K[x]$. Show that the localization $K[x]_M$ is not a finitely generated $K$-algebra over $K$.

## References

[AM69] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[G03] A. Gathmann, *Algebraic geometry*, Notes for a class taught at the University of Kaiserslautern 2002/2003. Available on-line: `http://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2002/alggeom-2002.pdf`

[F08] W. Fulton, *Algebraic curves, An introduction to algebraic geometry*, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. Available on-line: `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`

[Sh94] I. R. Shafarevich, *Basic algebraic geometry 1, Varieties in projective space*, Second edition, Translated from the 1988 Russian edition and with notes by Miles Reid, Springer-Verlag, Berlin, 1994.

[vdW49] B. L. van der Waerden, *Modern Algebra*, Vol. I., translated from the second revised German edition by Fred Blum, with revisions and additions by the author, Frederick Ungar Publishing Co., New York, N. Y., 1949.