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 December 16, 2017.

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

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

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

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

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 $S \subseteq K[x_1, x_2, \ldots, x_n]$, 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 $S = \{f_1, \ldots, f_r\}$ is finite, we will often write $\mathrm{V}(f_1, \ldots, f_r)$ 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 $S \subseteq K[x_1, x_2, \ldots, x_n]$ 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 $S_1, \ldots, S_n$ 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

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

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, τ), where X is a set and τ is a set of subsets of X such that:

(1) $\varnothing$ and X belong to τ.
(2) Arbitrary unions $\bigcup_{i\in I} U_i$ of elements $U_i \in \tau$ are again in τ.
(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 τ.

The subsets of X which belong to τ 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,

$$I = \{\sum_{i=1}^{r} a_i f_i \mid r \geq 0, f_1, \ldots, f_r \in S \text{ a } g_1, \ldots, g_r \in K[x_1, x_2, \ldots, x_n]\},$$

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, it 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 $I \subset R$ is finitely generated, i.e. there is $r \geq 0$ and polynomials $f_1, f_2, \ldots, f_r \in I$ such that
$$I = \{\sum_{i=1}^{r} a_i f_i \mid a_1, \ldots, a_i \in K[x_1, x_2, \ldots, x_n]\}.$$
(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]. □

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 $X = \mathrm{V}(f_1, f_2, \dots, f_r)$. □

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 $X_N = X_{N+1} = X_{N+2} = \cdots$. □

The latter corollary inspires the coming definition.

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

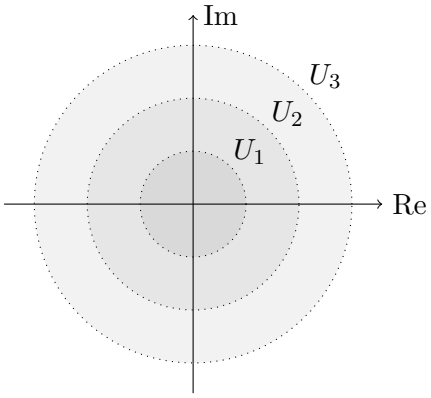


FIGURE 1. The reason why the Euclidean topology on $\mathbb{C}$ is not noetherian.

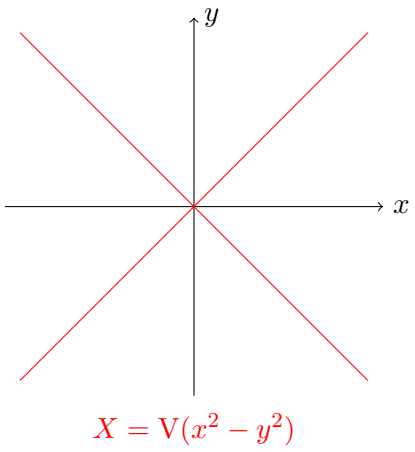


FIGURE 2. An example of a reducible algebraic set – X is the union of $X_1 = \mathrm{V}(x - y)$ and $X_2 = \mathrm{V}(x + y)$.

Definition. A non-empty topological space (X, τ) 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

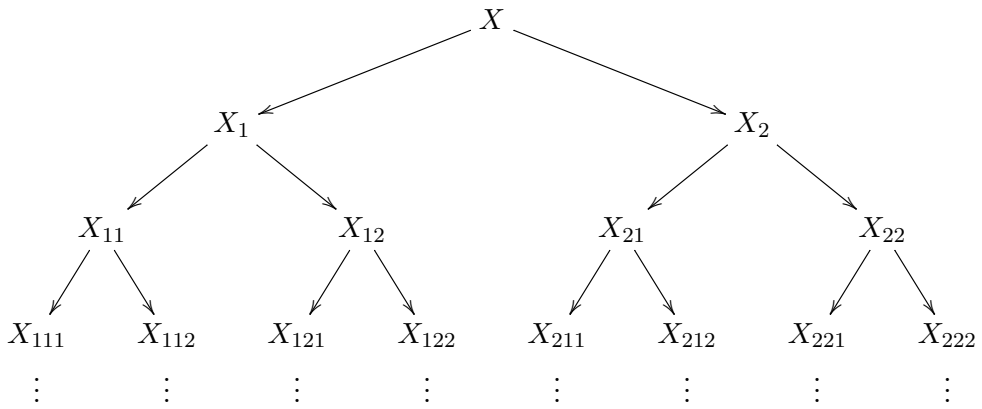


FIGURE 3. A tree of closed subsets of X in the proof of Theorem 5.

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

Theorem 5. *Let (X,τ) 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 $Z_1, Z_2, \ldots, Z_r$ 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,τ), 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 $X_i = Y_j$. Moreover, given any i, the index j such that $X_i = Y_j$ must be unique. Similarly, for each j there exists unique i with $Y_j = X_i$. It follows that $r = s$ and there is a permutation σ such that $X_i = Y_{\sigma(i)}$ for each $1 \leq i \leq r$. □

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, τ), 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 $Z_1 \supsetneq Z_2$. Since Z_2 is not minimal in $\mathcal{S}$ either, we find $Z_3 \in \mathcal{S}$ such that $Z_2 \supsetneq Z_3$, and so on. By induction, we can thus construct a chain

$$Z_1 \supsetneq Z_2 \supsetneq Z_3 \supsetneq Z_4 \supsetneq \cdots$$

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

In fact, the latter observation characterizes noetherian topological spaces.

Suppose now that (X, τ) 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 $Z_1, Z_2 \subsetneq Z$. 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. □

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 $\mathrm{I}(X) \subsetneq K[x_1, x_2, \ldots, x_n]$.

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 $f_1 \cdot f_2 \in K[x_1, x_2, \ldots, x_n]$. 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 $X_1, X_2 \subsetneq X$. 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 $X_1, X_2 \subsetneq X$. Then $\mathrm{I}(X_1), \mathrm{I}(X_2) \supsetneq \mathrm{I}(X)$ (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. □

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, τ) 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.

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 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 $f_1, f_2, \ldots, f_\ell \in K[x_1, x_2, \ldots, x_n]$ (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

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

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

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

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

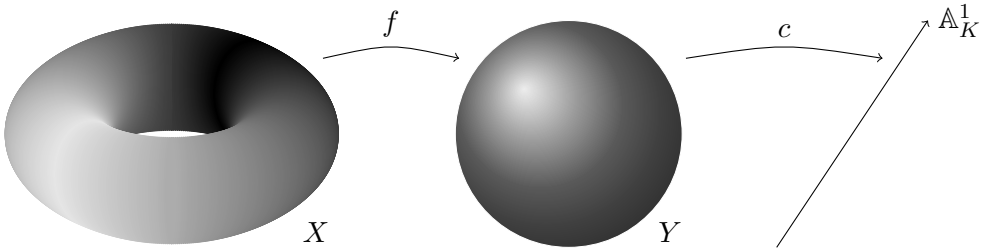


FIGURE 4. An illustration how the map $f^*\colon K[Y] \to K[X]$ acts. It is defined via $f^*\colon c \mapsto c \circ f$.

φ 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 φ is precisely $\mathrm{I}(X)$. The conclusion follows from the isomorphism theorem. □

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 $1 \leq i \leq n$, the *i-th coordinate function* is the function given by

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

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

$$f^*\colon K[Y] \to K[X],$$
$$c \mapsto c \circ f.$$

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, that $(g \circ f)^* = f^* \circ g^*$. 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 $1 \leq i \leq \ell$ 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 $Y = \mathrm{V}(g_1, g_2, \dots, g_\ell)$. We must

show that $g_j(f(P)) = 0$ for each $1 \leq j \leq r$ and $P \in X$. Using (2), this translates to the requirement that

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

To obtain the latter identity, it suffices to prove that

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

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

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

so it suffices to prove the identity

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

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

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

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

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

Now $g_j(Q)$ vanishes for each $1 \leq j \leq r$ and $Q \in Y$ because we started with $Y = \mathrm{V}(g_1, g_2, \ldots, g_\ell)$. 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 $K[Y] \to K[Y]$. We see immediately from (2) that $\alpha(c_i) = f^*(c_i)$ holds for the coordinate functions $c_1, c_2, \ldots, c_\ell \in K[Y]$. As the coordinate functions generate $K[Y]$ as a K-algebra, this implies that the homomorphisms α 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

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

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 $(b_1, b_2, \ldots, b_n)$ to $M^{-1} \cdot (b_1, b_2, \ldots, b_n)^t - M^{-1} \cdot \vec{c}$. More generally, is $Y \subseteq \mathbb{A}^n_K$ 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.

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.*

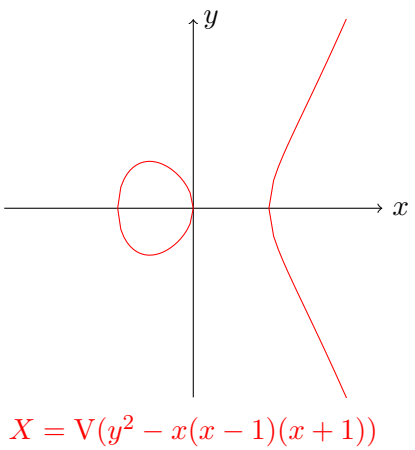


FIGURE 5. The zero set of the polynomial $y^2-x(x-1)(x+1)$ over the field of real numbers.

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 $X = \mathbb{A}^K_n$, then $K[X] = K[x_1, x_2, \ldots, x_n]$ and

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

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.

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 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 2×2 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 2×2 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 $U = U_1 \cap U_2 = X \setminus \mathrm{V}(x_2, x_4)$. 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 function from X to Y is a function $r\colon U \to Y$ where U is a non-empty Zariski open subset of X and there exist $r_1, r_2, \ldots, r_\ell \in K(X)$ such that

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

for each $P \in U$.

In the spirit of the discussion above, the symbol $r_i(P)$ for the evaluation of $r_i \in K(X)$ at P means that we pick a fraction $r_i = \frac{f}{g}$ with $f, g \in K[X]$ and $g(P) \neq 0$ and we put $r_i(P) = \frac{f(P)}{g(P)}$.

Lemma 15. *Let X, Y be varieties over K, let $\varnothing \neq U \subseteq X$ be Zariski open and let $r\colon U \to Y$ be a rational map. Then r is continuous.*

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 $V = \mathbb{A}^1_K \setminus \{b_1, \dots, b_r\}$, where $b_1, \dots, b_r \in K = \mathbb{A}^1_K$ are finitely many elements of K. Then, however,

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

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 $Z = \mathrm{V}(g_1, g_2, \dots, g_m) \subseteq Y$ is Zariski closed (here $g_1, g_2, \dots, g_m \in K[y_1, y_2, \dots, y_\ell]$), 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 $r^{-1}(Z)$. □

Literally, the definition of a rational $r\colon U \to Y$ function includes the choice of its domain, the non-empty Zariski open set U. However, we know already that we can extend the domain of definition of r to the (in general bigger) open set U' consisting of all points $P \in X$ at which all the rational functions $r_1, r_2, \dots, r_\ell$ are regular. We will call such points the *regular* points of r. Indeed, we can simply define $r'\colon U' \to Y$ again via

$$r'(P) = \big(r_1(P), r_2(P), \dots, r_n(P)\big).$$

Then r' is uniquely determined by r, the image of r' is still contained in $Y \subseteq \mathbb{A}^\ell_K$ (see Exercise 5) and $r'|_U = r$.

In the sequel, we will use the following terminology and notation which precisely capture the situations where the above extensions of two rations maps $r\colon U \to Y$ and $s\colon V \to Y$ are equal (recall Exercise 6 in Section 1).

Definition. Let X and Y be varieties over K and let $r\colon U \to Y$ and $s\colon V \to Y$ be two rational functions from X to Y (where $\varnothing \neq U, V \subseteq X$ are Zariski open). Then r and s are *equivalent* if there exists a non-empty Zariski open subset $W \subseteq U \cap V$ such that $r|_W = s|_W$.

We will denote an equivalence class of r by the symbol $r\colon X \dashrightarrow Y$ (the dashed arrow is to indicate that r is defined only on a subset of X).

The composition of a pair of polynomial maps or the composition of a rational map followed by a polynomial map (cf. the proof of Lemma 15) are always well defined rational maps. The question of when a pair of rational maps $r\colon X \dashrightarrow Y$ and $s\colon Y \dashrightarrow Z$ can be composed is, however, more delicate. At the very least, the image of r must contain at least one point $P \in Y$ at which s is regular. If this condition is satisfied, then the composition $s \circ r\colon X \dashrightarrow Z$ can be defined and is a rational map (or, more rigorously, an equivalence class of rational maps) again.

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 non-empty Zariski open. If the intersection $r(U) \cap V$ is nonempty, so is the preimage $r^{-1}(V) \subseteq U$. 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 $U \cap r^{-1}(V) \subseteq X$. The fact that $s \circ r$ is rational, i.e. that the coordinates of $s(r(P))$ are computed by evaluating elements of $K(X)$ at P, is proved in way completely analogous to Lemma 8(1).

An important situation in which the composition $s \circ r$ is always defined is when the image $r(U)$ is Zariski dense in X (equivalently, when the preimage $r^{-1}(V)$ of any non-empty open subset $V \subseteq Y$ is again non-empty). Note that this is in fact a property of the equivalence class of r, i.e. it does not depend on the particular choice of the domain of definition of r. For such rational maps $r\colon X \dashrightarrow Y$ we have an analogue of Theorem 12. Given any $s \in K(X)$, the composition $s \circ r\colon X \dashrightarrow \mathbb{A}^1_K$ is represented by a unique element of $K(Y)$, and we again 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. *equivalence classes of 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 equivalent 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 is equivalent to s.

To prove surjectivity, suppose that we have a homomorphism $\alpha \colon K(Y) \to K(X)$. If we evaluate α at the coordinate functions $c_i =: Y \to \mathbb{A}^1_K$, $i = 1, 2, \ldots, \ell$, 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 α as

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

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 $i = 1, 2, \ldots, \ell$ and $c_1, c_2, \ldots, c_\ell$ 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 $r(X) \subseteq Y$, we have $r^*(g) = g \circ r = 0$ in $K(X)$ and, hence, $g = 0$. Now the Zariski closure of $r(X)$ 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 7b.) □

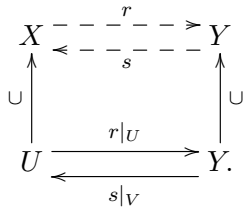
Analogous to the notion of a polynomial isomorphism, one can study the situation where there are two mutually inverse rational maps between varieties. This is of course a much coarser way to compare two varieties, but nevertheless it is a very useful notion.

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 equivalent 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.*



Proof. Denote by $U' \subseteq X$ the domain of definition of r and by $V' \subseteq Y$ the domain of definition of X. 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

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

for finite collections of points $P_1, P_2, \ldots, P_k \in X$ and $Q_1, Q_2, \ldots, Q_m \in Y$. We refer to Exercises 8 and 9 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 birationally equivalent to $\mathbb{A}^n_K$ only for one natural number n. Indeed, the birational equivalence implies that $K(X) \cong K(x_1, x_2, \ldots, x_n)$ and n can be recovered as the transcendence degree of $K(X)$. That is, n is the maximum number of elements $r_1, r_2, \ldots, r_n \in K(X)$ which satisfy no polynomial equation $g(r_1, r_2, \ldots, r_n) = 0$ with $0 \neq g \in K[x_1, x_2, \ldots, x_n]$.

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

It is well-known that the transcendence degree of $K(X)$ over K is equal to one 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)⇒(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)⇒(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 $K \subsetneq L \subseteq K(t)$, 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:

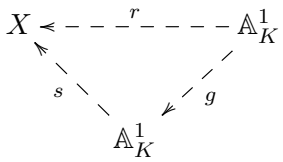
If apply the result to $L = r^*(K(X)) \subseteq K(t)$, we can express r^* as a composition of two K-algebra homomorphisms

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

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



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, $\mathbb{C}[X] \ncong \mathbb{C}[t]$ 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) 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 $h = \frac{y^2}{x^2}$.

(5) (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 5a and 5b 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 $f \neq g$.

(6) 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 α 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

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

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 $c_1, c_2, \dots, c_n\colon Y \to \mathbb{A}^1_K$.

(7) 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 6.

(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 5).
(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.

(8) 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 $K = \mathbb{C}$.

(9) 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 $K[x_1, x_2, \ldots, x_n]$ 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 now 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 $\mathbb{A}^2_K$).

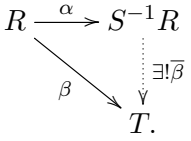
To start with, we briefly discuss basic fact about localization of commutative rings. Algebraically this means making certain elements of a ring formally invertible, in a way analogous to the construction of the field of rational numbers from the ring of integers (or to constructing quotient fields of 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.

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

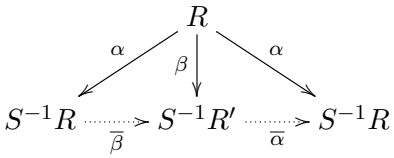
Definition. Let R be a commutative ring an $S \subseteq R$ a set of elements. A *localization* of R with respect to S is a ring homomorphism $\alpha\colon R \to S^{-1}R$ from R with the following properties:

(1) the element $\alpha(s)$ is an 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 $\beta = \overline{\beta} \circ \alpha$:



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 $\alpha = \overline{\alpha} \circ \beta$:



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 $s_1 s_2 \in S$. 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

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

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

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

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 $t = r_1 s_2 - r_2 s_1$ 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:

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

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 $S^{-1}R$ degenerated 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 $s_1 s_2 \in S$), 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*

$$\alpha\colon R \to R[x]/(xf - 1),$$
$$r \mapsto r + (xf - 1)$$

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 α 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 β_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. □

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

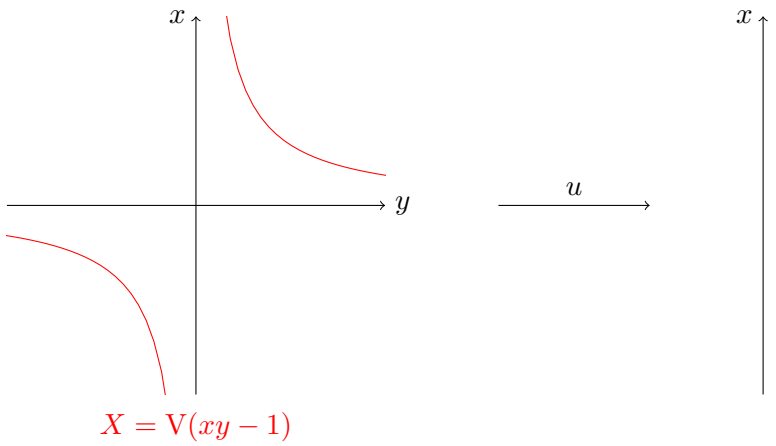


FIGURE 6. The easiest instance of Proposition 22. The polynomial map $u\colon (x,y) \mapsto x$ induces a homeomorphism between the red hyperbola and the Zariski open subset $\mathbb{A}^1_{\mathbb{R}} \setminus \{0\}$ of the line on the right. The algebra homomorphism $u^*\colon \mathbb{R}[x] \to \mathbb{R}[x,y]/(xy-1)$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

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,

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

and

$$u(U) = X_f \cap \{(a_1, a_2, \ldots, a_n) \mid \tilde{h}_i(a_1, a_2, \ldots, a_n) \neq 0 \ (\forall i = 1, \ldots, m)\},$$

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 α yields the K-algebra homomorphism

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

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

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]).

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 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 $I \subsetneqq K[x_1, x_2, \dots, x_n]$ 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 $M \subseteq K[x_1, x_2, \dots, x_n]$ and it suffices to prove that $\mathrm{V}(M) \neq \varnothing$. However, $L = K[x_1, x_2, \dots, x_n]/M$ 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

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

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

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

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

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

Note that if $X \subseteq \mathbb{A}^n_K$ is any subset, the ideal $\mathrm{I}(X) \subseteq K[x_1, x_2, \dots, x_n]$ 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

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

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

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

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

...

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 α 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).

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/main.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.