universität innsbruck
Department of Mathematics

Introduction to Classical Algebraic Geometry

Tim Netzer

∀¬6∃qλ∀

A⌐9EbYA

Contents

Introduction: What is Algebraic Geometry?

Algebraic geometry grew out of the attempt to understand arbitrary systems of polynomial equations over a field.
Systems of linear equations are treated exhaustively in linear algebra. Gaussian elimination provides a systematic method for computing all solutions, by parametrizing them with only a finite amount of data. This works so well because the solution set is an affine space, and is therefore geometrically easy to understand. The algebra behind this is the theory of vector spaces and linear maps, which is very well understood.
Passing to systems of *non-linear polynomial equations* makes the situation much more complicated. In general, there is no explicit algorithm that produces all solutions, and the geometry of the solution set can be far more intricate. To avoid some basic complications, one usually works over an algebraically closed field. This already removes difficulties that occur in one variable, as is familiar from algebra courses. Moreover, instead of trying to solve systems completely, we often classify their solution sets up to a suitable notion of isomorphism. Given an unknown system of equations, one can then try to identify it with a system whose geometry is already understood. This approach leads to the classification of affine solution sets by their associated *affine coordinate rings*. It translates the geometric problem into algebra, where it is often easier to handle. We develop this point of view in Section 1.

Further unexpected irregularities can arise for systems of polynomial equations. For instance, even a system of two equations in many variables may have no solution at all, although one might expect each equation to reduce the dimension by at most one. A similar phenomenon already occurs in linear algebra for non-homogeneous systems, but not for homogeneous ones. In algebraic geometry, such difficulties can often be avoided by homogenizing the problem, that is, by

passing from affine to *projective space*. After adding points at infinity, solution sets tend to behave much more regularly. We introduce this projective viewpoint in Section 3.

On the other hand, classifying solution sets up to isomorphism becomes more complicated in the projective setting. The approach via affine coordinate rings does not generalize directly. One therefore weakens the notion of isomorphism to an isomorphism that is defined *almost everywhere*. This leads to the notion of *birational equivalence*. A complete understanding of one system then gives an almost complete understanding of any birationally equivalent system. Birational equivalence again has a purely algebraic classification, this time through the *function fields* of varieties. We discuss this in Section 4.

The name *algebraic geometry* reflects the constant interplay between the geometry of solution sets and the algebra of the objects derived from their defining equations. Some problems are easier on the geometric side, while others are easier on the algebraic side. We will see many examples of this principle throughout these notes.

In Section 2 we consider algorithmic aspects. For example, given an explicit system of polynomial equations, we would like to decide whether the system has a solution. Since the fields under consideration are infinite, we cannot simply search through all possible points until a solution appears. Nevertheless, there are computational methods for answering such questions exactly, without numerical errors. These methods are provided by the theory of *Gröbner bases*, and are implemented in many computer algebra systems.

The literature on algebraic geometry is vast, so we mention only a small selection. Elementary approaches close in spirit to these notes can be found in the books of Harris [6], Hulek [8], and Shafarevich [10, 11]; for curves, see also Fulton [5]. Hartshorne [7] gives a comprehensive account of the modern theory of schemes, while Eisenbud & Harris [4] provide a somewhat gentler introduction. For commutative algebra we recommend Atiyah & Macdonald [1], Eisenbud [3], and Lang [9]. Algorithmic aspects are described, for example, in Becker & Weispfenning [2].

These lecture notes are based mainly on parts of Shafarevich's books and on unpublished lecture notes by Claus Scheiderer at the University of Konstanz. Any

remaining errors are my responsibility, and I am grateful for corrections and suggestions. I thank Martin Berger for corrections to a first version of the script, and Tom Drescher for providing many of the exercises and for helping translate the initial German version into English. I also thank Daniel Scharler for contributing many interesting exercises on applications of algebraic geometry in kinematics.

Chapter 1

Affine Varieties

1.1 Reminder from Algebra

All rings appearing in these lecture notes are *commutative* and have a *multiplicative identity element* 1. Most of the time, rings are denoted by R or S, and ideals by I or J.

Definition 1.1.1. Let $I \subseteq R$ be an ideal.
(i) The following set is again an ideal of R (Exercise 2), called the **radical of** I:

$$\sqrt{I} := \{a \in R \mid \exists n \in \mathbb{N} : \ a^n \in I\}\,.$$

If $I = \sqrt{I}$, then I is called a **radical ideal**.
(ii) An element $a \in R$ is called **nilpotent** if $a^n = 0$ for some $n \in \mathbb{N}$. The ideal

$$\mathrm{Nil}(R) := \sqrt{(0)}$$

of all nilpotent elements is called the **nilradical of** R.
(iii) R is called **reduced** if $\mathrm{Nil}(R) = (0)$, i.e. if there are no nilpotent elements except 0. △

Remark 1.1.2. Clearly $I \subseteq \sqrt{I}$ for every ideal I. In general, this inclusion is proper. For example, let $R = \mathbb{Z}$ and $I = (n)$, where $n = p_1^{e_1} \cdots p_r^{e_r}$ is the prime decomposition of n. Then $\sqrt{I} = (p_1 \cdots p_r)$. △

Lemma 1.1.3. *Let $I, J \subseteq R$ be ideals. Then*

(i) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

(ii) $\sqrt{I} = R \Leftrightarrow I = R$.

(iii) *If* $I \subseteq J$, *then* $\sqrt{J/I} = \sqrt{J}/I$ *in the quotient ring* R/I.

Proof. Exercise 2. □

As usual, we denote the set of all prime ideals of R by $\operatorname{Spec}(R)$.

Theorem 1.1.4. *For every ideal* $I \subseteq R$ *we have*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec}(R) \\ I \subseteq \mathfrak{p}}} \mathfrak{p}.$$

Proof. "$\subseteq$": Let $s \in \sqrt{I}$, i.e. $s^n \in I$ for some $n \in \mathbb{N}$. For every prime ideal $\mathfrak{p}$ with $I \subseteq \mathfrak{p}$ the prime ideal property yields that $s^n \in \mathfrak{p}$ implies $s \in \mathfrak{p}$.
"$\supseteq$": Let $s \in R \setminus \sqrt{I}$, i.e. $s^n \notin I$ for all $n \in \mathbb{N}$. Consider the multiplicative set $S = \{1, s, s^2, \cdots\}$ and the corresponding localization $R_s := S^{-1}R$ as well as the natural homomorphism

$$\begin{aligned} \varphi \colon R &\to R_s \\ a &\mapsto a/1. \end{aligned}$$

We have that $1 \notin IR_s$, otherwise $1/1 = a/s^n$ would hold for some $a \in I, n \in \mathbb{N}$, and this implies $s^m \in I$ for some m, a contradiction.
Hence there is a maximal ideal $\mathfrak{m}$ in R_s over IR_s, and $\mathfrak{p} := \varphi^{-1}(\mathfrak{m})$ is then a prime ideal in R with $I \subseteq \mathfrak{p}$. Because $s/1$ is invertible in R_s, this implies $s \notin \mathfrak{p}$. □

Corollary 1.1.5. $\operatorname{Nil}(R)$ *is the intersection of all prime ideals in* R.

Recall that a ring R is called **noetherian** if every ideal in R is finitely generated.

Theorem 1.1.6. *If* R *is a noetherian ring, then so is* $R[t]$.

Proof. Assume that $I \subseteq R[t]$ is an ideal that is not finitely generated. Iteratively, choose $p_1, p_2, \ldots \in I$ such that p_{n+1} has minimal degree in $I \setminus (p_1, \ldots, p_n)$. For $d_n = \deg(p_n)$ we have $d_1 \leqslant d_2 \leqslant \cdots$. Now let $a_n \in R$ be the leading coefficient of the polynomial p_n. Consider the ideal

$$J = (a_n \mid n \in \mathbb{N}) \subseteq R.$$

Since J is finitely generated by the assumption on R, there exists an identity

$$a_{m+1} = \sum_{i=1}^{m} b_i a_i$$

with $b_i \in R$. Define

$$g := p_{m+1} - \sum_{i=1}^{m} b_i p_i t^{d_{m+1}-d_i}.$$

By our construction we have $\deg(g) < \deg(p_{m+1})$, since the leading coefficients cancel. On the other hand, $p_{m+1} \in I \setminus (p_1, \ldots, p_m)$ implies

$$g \in I \setminus (p_1, \ldots, p_m).$$

This contradicts the choice of p_{m+1}. □

Corollary 1.1.7 (Hilbert's Basis Theorem)**.** *Let k be a field. Then $k[\underline{x}]$ is noetherian.*

Proof. A field has only the two ideals (0) and (1), both of which are finitely generated. Now apply Theorem 1.1.6 iteratively, adjoining one variable at a time. □

The most fundamental theorem in classical algebraic geometry is Hilbert's Nullstellensatz. We first prove it in its field-theoretic form and then interpret it geometrically. Before doing so, however, we need to study the *integrality* of ring extensions. This is a variant of the notion of algebraic field extensions that is specifically suited to rings.

Definition 1.1.8. Let $R \subseteq S$ be a ring extension.
(i) An element $b \in S$ is called **integral over** R if there are $a_0, \ldots, a_{n-1} \in R$ such that

$$a_0 + a_1 b + \cdots + a_{n-1} b^{n-1} + b^n = 0.$$

Such an equation is called an **integrality equation** for b over R.
(ii) S is called **integral over** R if every element $b \in S$ is integral over R. △

Remark 1.1.9. (i) The important detail for the integrality of b is that the corresponding integrality equation must be *monic*. If R is a field, then obviously every nontrivial equation can be normalized. Hence, in this case the integral elements in S over R are just the algebraic elements.
(ii) For $\mathbb{Z} \subseteq \mathbb{Q}$ the only integral elements over $\mathbb{Z}$ in $\mathbb{Q}$ are the elements of $\mathbb{Z}$ itself. More generally this is true for the inclusion $R \subseteq K$ of an unique factorization domain in its field of fractions (Exercise 5).

(*iii*) For $R \subseteq S$ and $b_1, \ldots, b_m \in S$ we define $R[b_1, \ldots, b_m]$ as the subring of S generated by $b_1, \ldots, b_m$ and R, i.e.

$$R[b_1, \ldots, b_m] = \left\{ \sum_{e \in \mathbb{N}^m} a_e b_1^{e_1} \cdots b_m^{e_m} \mid a_e \in R \right\}.$$

If we regard S as R-module, then $R[b_1, \ldots, b_m]$ is a submodule, and in particular an R-module by itself. △

Theorem 1.1.10. *Let $R \subseteq S$ be a ring extension and $b_1, \ldots, b_m \in S$. Then the following are equivalent:*

(i) $b_1, \ldots, b_m$ *are integral over* R.

(ii) $R[b_1, \ldots, b_m]$ *is finitely generated as an* R*-module.*

(iii) $R[b_1, \ldots, b_m]$ *is integral over* R.

Proof. (*i*) ⇒ (*ii*): By solving the integrality equation of b_1 for b_1^n we obtain

$$b_1^n = -\left(a_{n-1} b_1^{n-1} + \cdots + a_0\right)$$

for certain $a_i \in R$. So we can replace the nth power of b_1 with lower powers of b_1 and coefficients in R. By doing the analogue procedure with b_i we see that $R[b_1, \ldots, b_m]$ is generated by finitely many products $b_1^{e_1} \cdots b_m^{e_m}$.
(*ii*) ⇒ (*iii*): Finitely many elements $1 = c_1, \ldots, c_n$ generate the R-module $M := R[b_1, \ldots, b_m]$. Now let $c \in M$ be arbitrary. Since M is also a ring, we have $c \cdot c_i \in M$ and thus there are $a_{ij} \in R$ such that

$$c \cdot c_i = \sum_{j=1}^{n} a_{ij} c_j.$$

For the matrix

$$A = (a_{ij})_{i,j} \in \mathrm{Mat}_n(R)$$

we then have

$$A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = c \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

So $(c_1, \ldots, c_n)^t$ is in the kernel of

$$N := cI_n - A.$$

Since

$$\mathrm{adj}(N) \cdot N = \det(N) \cdot I_n$$

we obtain

$$\det(N) \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = 0.$$

Now $c_1 = 1$ implies $\det(N) = 0$. From the Leibniz formula for determinants we see

$$\det(N) = c^n + a_{n-1}c^{n-1} + \cdots + a_m$$

for certain $a_i \in R$. This yields an integrality equation of c over R.
$(iii) \Rightarrow (i)$ is trivial. □

1.2 Affine Algebraic Varieties

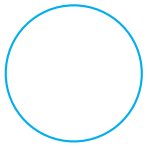
From now on let k always be an arbitrary field, and K an *algebraically closed extension field of* k. For example we can choose $K = \overline{k}$ to be the algebraic closure of k. But K can also be bigger, e.g. $k = \mathbb{Q}$ and $K = \mathbb{C}$. Essential will only be that K is algebraically closed! The field k is also called **coefficient field** and K is also called **coordinate field**. With $\underline{x}$ we denote the n-tuple of variables $(x_1, \ldots, x_n)$.

Definition 1.2.1. (i) Let $P \subseteq k[\underline{x}]$ be a set of polynomials. We define

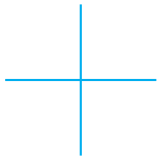
$$\mathcal{V}(P) = \{a \in K^n \mid p(a) = 0 \, \forall p \in P\}$$

and call $\mathcal{V}(P)$ the **affine variety defined by** P. It is the solution set (over K) of the system of polynomial equations defined by P.
(ii) A subset $V \subseteq K^n$ is called an **affine k-variety** if $V = \mathcal{V}(P)$ for a set $P \subseteq k[\underline{x}]$. Affine k-varieties are thus the solution sets for systems of polynomial equations (with coefficients in k).
(iii) A **hypersurface** is a variety defined by a single polynomial, that is, a variety of the form $\mathcal{V}(p)$ for some $p \in k[\underline{x}]$.
(iv) If $W \subseteq V$ are affine k-varieties, then W is called a **subvariety** of V.
(v) $\mathbb{A}^n := K^n$ is called the **n-dimensional affine space**. △

Example 1.2.2. Note: The following figures only show the *real points* of the respective affine variety in $\mathbb{A}^2$. However as is well known, $\mathbb{R}$ is not algebraically closed and we actually should consider the varieties over $K = \mathbb{C}$ for instance. Due to the dimension this is graphically hardly possible. But the real image usually (not always!) gives a good impression on the variety.
(i) Let $P = \{1 - x_1^2 - x_2^2\} \subseteq \mathbb{Q}[x_1, x_2]$. Then $\mathcal{V}(P)$ is a circle.



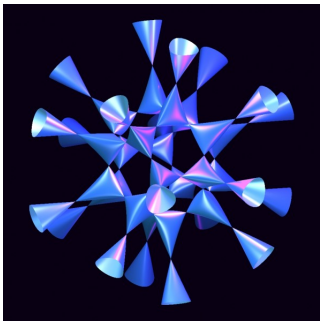
(ii) Let $P = \{x_1 x_2\} \subseteq \mathbb{Q}[x_1, x_2]$. Then $\mathcal{V}(P)$ is the union of the two coordinate axes.



(iii) Let $P = \{x_2^2 - x_1^2(x_1 + 1)\} \subseteq \mathbb{Q}[x_1, x_2]$. Then $\mathcal{V}(P)$ has the form of a ribbon.

(iv) Let $P = \{x_2^2 - x_1^3\} \subseteq \mathbb{Q}[x_1, x_2]$. Then $\mathcal{V}(P)$ is a curve with a cusp.

(v) Let $P = \{x_1^2 + x_2^2\} \subseteq \mathbb{Q}[x_1, x_2]$. Here the real image only shows the point $(0, 0)$. But we also have for example $(1, i) \in \mathcal{V}(P)$. Even worse is the case $P = \{x_1^2 + x_2^2 + 1\}$, in which we don't see anything in the real image. But again the variety is not empty, for example we have $(0, i) \in \mathcal{V}(P)$.
(vi) The following image shows a part of an affine hypersurface in $\mathbb{A}^3$. The defining equation has degree 6:



Author: Oliver Labs, www.imaginary.org, Project of the Mathematical Research Institute Oberwolfach, supported by the Klaus Tschira Foundation

(vii) So far the images have always shown hypersurfaces. But there are many more varieties besides hypersurfaces. For instance, every point $a \in k^n \subseteq \mathbb{A}^n$ is an affine k-variety because

$$\{a\} = \mathcal{V}(x_1 - a_1, \ldots, x_n - a_n)$$

and $x_1 - a_1, \ldots, x_n - a_n \in k[\underline{x}]$. For $a \in \mathbb{A}^n \setminus k^n$ this is no longer true in general. For example, $\{i\} \subseteq \mathbb{C} = \mathbb{A}^1$ is not an affine $\mathbb{R}$-variety. Every real polynomial that vanishes on i must also vanish on $-i$. But we have

$$i \in \{i, -i\} = \mathcal{V}(x_1^2 + 1) \subseteq \mathbb{C} = \mathbb{A}^1.$$

For $k = \mathbb{Q}$ and $K = \mathbb{C}$, this phenomenon becomes even more visible. The only polynomial in $\mathbb{Q}[\underline{x}]$ that vanishes at the point $a = \pi \in \mathbb{A}^1$ is the zero polynomial. In particular, the only affine $\mathbb{Q}$-variety in $\mathbb{A}^1$ containing a is the entire affine space. △

Lemma 1.2.3. *Let $P \subseteq k[\underline{x}]$ and let $I = (P)$ be the ideal in $k[\underline{x}]$ generated by P. Then*

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

Proof. We have $P \subseteq I \subseteq \sqrt{I}$, and thus $\mathcal{V}(\sqrt{I}) \subseteq \mathcal{V}(I) \subseteq \mathcal{V}(P)$. Now let $p \in \sqrt{I}$, that is

$$p^m = \sum_i f_i p_i$$

where $p_i \in P$, $f_i \in k[\underline{x}]$. From this we see that $a \in \mathcal{V}(P)$ implies $p^m(a) = 0$, and since fields don't have nontrivial zero divisors, we obtain $p(a) = 0$. Therefore we have $p = 0$ on $\mathcal{V}(P)$, and this shows $\mathcal{V}(P) \subseteq \mathcal{V}(\sqrt{I})$. □

Corollary 1.2.4. *Every affine k-variety V is of the form*

$$V = \mathcal{V}(p_1, \ldots, p_r)$$

with finitely many polynomials $p_1, \ldots, p_r \in k[\underline{x}]$.

Proof. Let $V = \mathcal{V}(P)$ with $P \subseteq k[\underline{x}]$. Then we have $(P) = (p_1, \ldots, p_r)$ by Corollary 1.1.7, and from Lemma 1.2.3 we get $V = \mathcal{V}(p_1, \ldots, p_r)$. □

Lemma 1.2.5. *(i) $\emptyset$ and $\mathbb{A}^n$ are affine k-varieties.*
(ii) If $V_1, V_2 \subseteq \mathbb{A}^n$ are affine k-varieties, then $V_1 \cup V_2$ is an affine k-variety.
(iii) If $V_\lambda \subseteq \mathbb{A}^n$ are affine k-varieties ($\lambda \in \Lambda$), then $\bigcap_{\lambda\in\Lambda} V_\lambda$ is an affine k-variety.
(iv) If $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ are affine k-varieties, then $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ is an affine k-variety.

Proof. (i): $\emptyset = \mathcal{V}(1), \mathbb{A}^n = \mathcal{V}(0)$. (ii): For two ideals $I_1, I_2 \subseteq k[\underline{x}]$ we have

$$\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2).$$

Both inclusions "$\subseteq$" are clear because the ideals get smaller. Now let $a \in \mathcal{V}(I_1 I_2)$ and $a \notin \mathcal{V}(I_1)$. Then there is a $p \in I_1$ with $p(a) \neq 0$. For every $q \in I_2$ we have $pq \in I_1 I_2$, and thus $0 = (pq)(a) = p(a)q(a)$. Since fields do not have nontrivial zero divisors, it follows that $q(a) = 0$ for all $q \in I_2$, hence $a \in \mathcal{V}(I_2)$.
(iii): For $V_\lambda = \mathcal{V}(P_\lambda)$ with $P_\lambda \subseteq k[\underline{x}]$ we obviously have $\bigcap_\lambda V_\lambda = \mathcal{V}(\bigcup_\lambda P_\lambda)$.
(iv): Let us write $V = \mathcal{V}(P)$ and $W = \mathcal{V}(Q)$ for certain subsets $P \subseteq k[x_1, \ldots, x_n]$ and $Q \subseteq k[y_1, \ldots, y_m]$. Then $P \cup Q \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ and

$$V \times W = \mathcal{V}(P \cup Q).$$ □

We want to put the constructions from the previous proof on record:

Corollary 1.2.6. *Let I_1, I_2, I_λ ($\lambda \in \Lambda$) be ideals in $k[\underline{x}]$. Then we have*

$$\mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2) = \mathcal{V}(I_1 I_2)$$

and

$$\bigcap_{\lambda\in\Lambda} \mathcal{V}(I_\lambda) = \mathcal{V}\left(\sum I_\lambda\right).$$ □

Definition 1.2.7. Let $V \subseteq \mathbb{A}^n$ be an arbitrary subset. Then

$$\mathcal{I}(V) := \{p \in k[\underline{x}] \mid p(a) = 0 \,\forall a \in V\}$$

is called the **vanishing ideal of** V. △

Lemma 1.2.8. *Let $V, W \subseteq \mathbb{A}^n$ be subsets. Then*
(i) $\mathcal{I}(V)$ is a radical ideal.
(ii) $V \subseteq W \Rightarrow \mathcal{I}(W) \subseteq \mathcal{I}(V)$.
(iii) $\mathcal{I}(V \cup W) = \mathcal{I}(V) \cap \mathcal{I}(W)$.
(iv) In case V is an affine k-variety we have $\mathcal{V}(\mathcal{I}(V)) = V$.
(v) Every descending chain $V_1 \supseteq V_2 \supseteq \cdots$ of affine k-varieties becomes stationary.

Proof. (i)-(iii) are clear. For (iv), let $V = \mathcal{V}(I)$ for some ideal I. Then $I \subseteq \mathcal{I}(V)$, and thus $V = \mathcal{V}(I) \supseteq \mathcal{V}(\mathcal{I}(V))$. The other inclusion "$\subseteq$" is clear. In (v), we obtain the ascending chain of ideals $\mathcal{I}(V_1) \subseteq \mathcal{I}(V_2) \subseteq \cdots$, which becomes stationary by Hilbert's Basis Theorem. Applying $\mathcal{V}(\cdot)$ and using (iv), we see that the chain of the V_i becomes stationary as well. □

Theorem 1.2.9 (Hilbert's Nullstellensatz, field theoretic form)**.** *Let F/k be a field extension such that F is finitely generated as k-algebra. Then F/k is finite (and thus algebraic).*

Proof. There are $\alpha_1, \ldots, \alpha_n \in F$ with $F = k[\alpha_1, \ldots, \alpha_n]$. We prove the claim by induction on n.
$n = 1$: Since $F = k[\alpha]$ is a field, there is a polynomial $p \in k[t]$ with $\alpha^{-1} = p(\alpha)$. This implies $\alpha \cdot p(\alpha) - 1 = 0$, and hence α is algebraic over k. But then the extension is finite.
$n-1 \to n$: We have $F = k(\alpha_1)[\alpha_2, \ldots, \alpha_n]$ because F is a field. By the induction hypothesis, $\alpha_2, \ldots, \alpha_n$ are algebraic over $k(\alpha_1)$. It is now enough to show that α_1 is algebraic over k. Then the entire extension F/k is algebraic and thus finite. Now $\alpha_2, \ldots, \alpha_n$ being algebraic over $k(\alpha_1)$ means that there are identities

$$u_i \alpha_i^d + \sum_{j=0}^{d-1} r_{ij} \alpha_i^j = 0$$

with $u_i, r_{ij} \in k[\alpha_1]$ after clearing denominators. Consider $u := u_2 \cdots u_n \in k[\alpha_1]$. Then $\alpha_2, \ldots, \alpha_n$ are integral over the ring $k[\alpha_1, 1/u]$, and by Theorem 1.1.10 the ring F is an integral extension of $k[\alpha_1, 1/u]$. Assume that α_1 is transcendental over k, i.e. that $k[\alpha_1]$ is isomorphic to a polynomial ring. Then we can choose an irreducible polynomial $p \in k[\alpha_1]$ such that $p \nmid u$ (there are infinitely many irreducible polynomials in the unique factorization domain $k[\alpha_1]$). Now p^{-1} satisfies an integrality equation

$$p^{-m} + b_1 p^{-(m-1)} + \cdots + b_m = 0$$

with $b_i \in k[\alpha_1, 1/u]$. Multiplication by p^m and a sufficiently large power of u yields

$$u^r + a_1 p + \cdots + a_m p^m = 0$$

with $a_i \in k[\alpha_1]$. This implies $p \mid u$, a contradiction. □

Corollary 1.2.10. *Let A be a finitely generated k-algebra and let $\mathfrak{m}$ be a maximal ideal in A. Then $A/\mathfrak{m}$ is a finite field extension of k.*

Proof. $A/\mathfrak{m}$ is still finitely generated as k-algebra and also a field. □

Corollary 1.2.11 (Hilbert's Nullstellensatz, geometric form)**.** *Let $I \subsetneq k[\underline{x}]$ be a proper ideal. Then $\mathcal{V}(I) \neq \emptyset$.*

Proof. Choose a maximal ideal $\mathfrak{m}$ of $k[\underline{x}]$ with $I \subseteq \mathfrak{m}$. By Corollary 1.2.10 $k[\underline{x}]/\mathfrak{m}$ is a finite field extension of k. Hence there is a k-embedding of $k[\underline{x}]/\mathfrak{m}$ into K, and we can assume

$$k \subseteq k[\underline{x}]/\mathfrak{m} \subseteq K.$$

Now let $a_i := \overline{x_i}$, the residue class of x_i in $k[\underline{x}]/\mathfrak{m} \subseteq K$. For every $p \in k[\underline{x}]$ we then have

$$p(a) = p(\overline{x}) = \overline{p},$$

and for $p \in I$ (even for $p \in \mathfrak{m}$) this implies $p(a) = 0$. Thus $a \in \mathcal{V}(I)$. □

Remark 1.2.12. In the last proof, without Corollary 1.2.10 we would only get that $\mathcal{V}(I)$ has an element over *some* extension field of k (namely $k[\underline{x}]/\mathfrak{m}$). With Corollary 1.2.10 we see that there exists an element over a finite extension field and thus over *any* algebraically closed extension field. Over k itself this does not have to be the case, as we can see for example for $k = \mathbb{Q}$ and $I = (x^2 - 2)$, or $k = \mathbb{R}$ and $I = (x^2 + 1)$. △

Remark 1.2.13. Corollary 1.2.11 says that a system of polynomial equations

$$p_1 = 0, \ldots, p_r = 0$$

with $p_i \in k[\underline{x}]$ does *not* have a solution over K if and only if there is an identity of the form

$$q_1 p_1 + \cdots + q_r p_r = 1$$

with $q_i \in k[\underline{x}]$. In Chapter 2 we will see how this last condition, and thus the solvability of polynomial equation systems, can be checked algorithmically. △

Theorem 1.2.14 (Hilbert's Nullstellensatz, ideal theoretic form)**.** *For every ideal $I \subseteq k[\underline{x}]$ we have*

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

Proof. "$\supseteq$" is clear. For "$\subseteq$" let $0 \neq p \in \mathcal{I}(\mathcal{V}(I))$. Consider the ideal

$$J = (I, tp - 1) \subseteq k[t, \underline{x}].$$

Since $p \equiv 0$ on $\mathcal{V}(I)$, we have $\mathcal{V}(J) = \emptyset$. By Corollary 1.2.11 there is an identity

$$1 = a(tp - 1) + \sum_i b_i p_i$$

with $a, b_i \in k[t, \underline{x}]$ and $p_i \in I$. Substituting p^{-1} for t and multiplying with a sufficiently large power of p yields

$$p^r = \sum_i \tilde{b}_i p_i,$$

with $\tilde{b}_i \in k[\underline{x}]$, hence $p \in \sqrt{I}$. □

Remark 1.2.15. Note that Theorem 1.2.14 is true for any choice of the algebraically closed field K, and that $\sqrt{I}$ does not depend on this choice. Thus it does not really matter over which algebraically closed field K we consider the variety. △

Example 1.2.16. For a hypersurface $V \subseteq \mathbb{A}^n$, say $V = \mathcal{V}(p)$, such that

$$p = p_1^{e_1} \cdots p_r^{e_r}$$

is the decomposition into irreducible polynomials, we have

$$\mathcal{I}(V) = (p_1 \cdots p_r).$$ △

Corollary 1.2.17. *Let $I, J \subseteq k[\underline{x}]$ be ideals. Then we have*

$$\mathcal{V}(I) \subseteq \mathcal{V}(J) \Leftrightarrow \sqrt{J} \subseteq \sqrt{I}.$$

Proof. From $\mathcal{V}(I) \subseteq \mathcal{V}(J)$ it obviously follows that $\mathcal{I}(\mathcal{V}(J)) \subseteq \mathcal{I}(\mathcal{V}(I))$, and by Theorem 1.2.14 therefore $\sqrt{J} \subseteq \sqrt{I}$. The other implication follows from Lemma 1.2.3 since $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$ and $\mathcal{V}(J) = \mathcal{V}(\sqrt{J})$. □

Corollary 1.2.18. *The map $V \mapsto \mathcal{I}(V)$ is an inclusion-reversing bijection between the set of all affine k-varieties in $\mathbb{A}^n$ and the set of all radical ideals in $k[\underline{x}]$. The inverse map is given by $I \mapsto \mathcal{V}(I)$.*

Proof. Lemma 1.2.8 (iv), Theorem 1.2.14, and Corollary 1.2.17. □

Remark 1.2.19. (i) In particular, maximal ideals in $k[\underline{x}]$ correspond to minimal affine k-varieties $\neq \emptyset$.
(ii) Let $a \in k^n \subseteq \mathbb{A}^n$. Then we have $\{a\} = \mathcal{V}(\mathfrak{m}_a)$, where

$$\mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n).$$

It is easy to see that $\mathcal{I}(\{a\}) = \mathfrak{m}_a$ holds. In particular $\mathfrak{m}_a$ is maximal.
(iii) Not every maximal ideal $\mathfrak{m} \subseteq k[\underline{x}]$ has to be of the form $\mathfrak{m}_a$, and not every nonempty minimal variety has to be of the form $\{a\}$. For $k = \mathbb{R}$ and $K = \mathbb{C}$, for instance, $\mathfrak{m} = (x_1^2 + 1)$ is maximal in $\mathbb{R}[x_1]$ and corresponds to the minimal $\mathbb{R}$-variety $\{i, -i\} \subseteq \mathbb{A}^1$. △

Corollary 1.2.20. *The mapping $a \mapsto \mathfrak{m}_a$ is a bijection between k^n and the maximal ideals in $k[\underline{x}]$ with residue field k. In case $k = \overline{k}$, these are all maximal ideals in $k[\underline{x}]$.*

Proof. Injectivity is clear, and we have $k[\underline{x}]/\mathfrak{m}_a = k$. For surjectivity, let $\mathfrak{m} \subseteq k[\underline{x}]$ be a maximal ideal with $k[\underline{x}]/\mathfrak{m} = k$. Let $a_i := \overline{x}_i \in k$. Then $\overline{x_i - a_i} = 0$, and thus $\mathfrak{m}_a \subseteq \mathfrak{m}$. Hence equality holds. Since $k[\underline{x}]/\mathfrak{m}$ is a finite field extension of k for every maximal ideal by Corollary 1.2.10, we always have $k[\underline{x}]/\mathfrak{m} = k$ if $k = \overline{k}$. □

1.3 The Zariski Topology

Definition 1.3.1. The **k-Zariski topology** on $\mathbb{A}^n$ has the affine k-varieties as its closed sets. The k-Zariski topology on a subset $X \subseteq \mathbb{A}^n$ is the induced subspace topology. △

As long as we discuss k-varieties, all topological notions refer to the k-Zariski topology.

Remark/Example 1.3.2. (i) The k-Zariski topology is indeed a topology. This is a consequence of Lemma 1.2.5.
(ii) The Zariski topology is the most natural topology on $\mathbb{A}^n$ in this setting, since its definition uses only polynomial equations and hence only the given field structure.

(iii) In the case $k = \overline{k} = K$ the closed subsets of $\mathbb{A}^1$ are exactly the finite subsets, as well as $\mathbb{A}^1$ (cf. Exercise 9).
(iv) The Zariski topology on $\mathbb{A}^{n+m} = \mathbb{A}^n \times \mathbb{A}^m$ does *not* coincide with the product topology (Exercise 17).
(v) For $k \subseteq k' \subseteq K$, the k'-Zariski topology is in general finer than the k-Zariski topology. For instance, $\{i\} \subseteq \mathbb{A}^1 = \mathbb{C}^1$ is closed in the $\mathbb{C}$-Zariski topology, but not in the $\mathbb{R}$-Zariski topology.
(vi) For every $p \in k[\underline{x}]$ the set

$$\mathcal{D}(p) := \{a \in \mathbb{A}^n \mid p(a) \neq 0\}$$

is open. Every open set is of the form

$$\mathcal{D}(p_1) \cup \cdots \cup \mathcal{D}(p_r),$$

where $p_1, \ldots, p_r \in k[\underline{x}]$ (cf. Corollary 1.2.4).
(vii) The map

$$a \mapsto (1/p(a), a)$$

defines a canonical bijection between the open set $\mathcal{D}(p) \subseteq \mathbb{A}^n$ and the variety $\mathcal{V}(tp - 1) \subseteq \mathbb{A}^{n+1}$. △

Lemma 1.3.3. *(i) For $X \subseteq \mathbb{A}^n$ we have $\overline{X} = \mathcal{V}(\mathcal{I}(X))$.*
(ii) $U_1 \cap U_2 \neq \emptyset$ holds for any two nonempty open sets $U_1, U_2 \subseteq \mathbb{A}^n$. In particular, every nonempty open set is dense in $\mathbb{A}^n$.
(iii) The Zariski topology is not Hausdorff.

Proof. (i) $\mathcal{V}(\mathcal{I}(X))$ is closed and contains X, which shows "$\subseteq$". For "$\supseteq$" note that $\mathcal{I}(X) \supseteq \mathcal{I}(\overline{X})$ and thus $\mathcal{V}(\mathcal{I}(X)) \subseteq \mathcal{V}(\mathcal{I}(\overline{X})) = \overline{X}$ (Lemma 1.2.8 (iv)).
(ii) $\mathcal{D}(p) \cap \mathcal{D}(q) = \emptyset$ implies $pq \equiv 0$ on $\mathbb{A}^n$ and therefore $pq = 0$, since K is infinite. It follows that $p = 0$ or $q = 0$, or equivalently $\mathcal{D}(p) = \emptyset$ or $\mathcal{D}(q) = \emptyset$.
(iii) Follows immediately from (ii). □

Definition 1.3.4. Let X be a topological space.
(i) X is called **irreducible** if $X \neq \emptyset$ and for all closed subsets $A, B \subseteq X$ we have

$$X = A \cup B \;\Rightarrow\; A = X \text{ or } B = X.$$

Otherwise X is called **reducible**.
(ii) $Y \subseteq X$ is called **irreducible component of** X if Y is a maximal irreducible subset of X (w.r.t. set inclusion and the subspace topology). △

Remark 1.3.5. For a subset $Y \subseteq X$, irreducibility (with respect to the subspace topology) can be stated as follows:

$$A, B \text{ closed in } X,\ Y \subseteq A \cup B \ \Rightarrow\ Y \subseteq A \text{ or } Y \subseteq B.$$

Note that irreducibility is a property of a topological space itself, and is not defined relative to an ambient space (in contrast to, for example, closedness). △

Lemma 1.3.6. *Let $X \neq \emptyset$ be a topological space.*
(i) The following are equivalent:
(a) X is irreducible.
(b) Every nonempty open subset of X is dense.
(c) Any two nonempty open subsets of X have a nonempty intersection.
(ii) For $Y \subseteq X$ we have: Y irreducible $\Leftrightarrow$ $\overline{Y}$ irreducible.
(iii) Every irreducible component of X is closed.

Proof. Exercise 21. □

Remark/Example 1.3.7. (i) For Hausdorff spaces, the notion of irreducibility is not very informative. A Hausdorff space X is irreducible if and only if $|X| = 1$. In particular, the irreducible components of a Hausdorff space are precisely the singleton subsets.
(ii) $\mathbb{A}^n$ is irreducible in the k-Zariski topology. This follows from Lemma 1.3.3 and Lemma 1.3.6. △

Lemma 1.3.8. *Every irreducible subset of a topological space X is contained in an irreducible component of X. In particular, X is the union of its irreducible components.*

Proof. Let $Y \subseteq X$ be irreducible. Consider

$$\mathcal{M} = \{Z \subseteq X \mid Z \text{ irreducible}, Y \subseteq Z\}.$$

The set $\mathcal{M}$ is nonempty since $Y \in \mathcal{M}$. Let $(Z_\lambda)_{\lambda\in\Lambda}$ be a chain in $\mathcal{M}$. Then $\bigcup_\lambda Z_\lambda$ is still irreducible: from $\bigcup_\lambda Z_\lambda \subseteq A \cup B$ with A, B closed, it follows for every λ that $Z_\lambda \subseteq A$ or $Z_\lambda \subseteq B$. Because the Z_λ form a chain, the same alternative must hold for all λ.
Therefore $\bigcup_\lambda Z_\lambda \in \mathcal{M}$, and by Zorn's Lemma $\mathcal{M}$ has a maximal element. This is obviously an irreducible component of X containing Y.
The second assertion follows from the fact that $\{x\} \subseteq X$ is irreducible for all $x \in X$. □

Remark 1.3.9. Every irreducible topological space is connected. In particular, every connected component of X is the union of irreducible components of X. △

Definition 1.3.10. A topological space X is called **noetherian** if every descending chain $A_1 \supseteq A_2 \supseteq \cdots$ of closed subsets of X is eventually stationary. △

Lemma 1.3.11. *For a topological space X the following are equivalent:*
(i) X is noetherian.
(ii) Every nonempty system of closed subsets of X contains a minimal element.
(iii) Every open subset of X is quasi-compact, i.e. every open cover has a finite subcover.

Proof. Exercise 22. □

Example 1.3.12. (*i*) Every subspace of a noetherian topological space is itself noetherian.
(*ii*) $\mathbb{A}^n$ is noetherian in the k-Zariski topology (Lemma 1.2.8 (*v*)).
(*iii*) Every affine k-variety is noetherian in the k-Zariski topology. △

Theorem 1.3.13. *Let X be a noetherian topological space. Then*
(i) X has only finitely many irreducible components.
(ii) If $X_1, \ldots, X_r$ are the pairwise distinct irreducible components of X, then

$$X_i \nsubseteq \bigcup_{j \neq i} X_j$$

for all $i = 1, \ldots, r$.
(iii) If $X = Y_1 \cup \cdots \cup Y_s$ is a covering with closed irreducible subsets Y_i which satisfy

$$Y_i \nsubseteq \bigcup_{j \neq i} Y_j$$

for all $i = 1, \ldots, s$, then $Y_1, \ldots, Y_s$ are the irreducible components of X.

Proof. (*i*) Let $\mathcal{M}$ be the set of all closed subsets of X that are *not* the union of finitely many irreducible subsets. We show that $\mathcal{M} = \emptyset$. Assume $\mathcal{M} \neq \emptyset$. Since X is noetherian, there exists a minimal element Y in $\mathcal{M}$. But then Y must be reducible, that is, $Y = Y_1 \cup Y_2$ with $Y_i \subseteq X$ closed and $Y_1, Y_2 \subsetneq Y$. This implies $Y_1, Y_2 \notin \mathcal{M}$, and hence Y_1, Y_2 are both unions of finitely many irreducible subsets. Therefore the same is true for Y, a contradiction.

In particular X is the union of finitely many irreducible subsets and by Lemma 1.3.8 of finitely many irreducible components $X_1, \ldots, X_r$. Now let Z be another irreducible component of X. Then

$$Z = \bigcup_{i=1}^{r} Z \cap X_i,$$

and since the X_i are closed and Z is irreducible, it follows $Z \subseteq X_i$ for some i. Because Z is even an irreducible component, we have equality. This proves (i).
(ii) From $X_i \subseteq \bigcup_{j\neq i} X_j$ we obtain $X_i \subseteq \bigcup_{j\neq i} X_i \cap X_j$, and as before $X_i \subseteq X_j$ for some $j \neq i$, a contradiction.
(iii) Again let $X_1, \ldots, X_r$ be the irreducible components of X. As before $X_i \subseteq \bigcup_j Y_j \cap X_i$ implies $X_i \subseteq Y_j$ for some j, and thus equality. So the irreducible components of X are among the Y_j. From $Y_i \nsubseteq \bigcup_{j\neq i} Y_j$ it follows that there are no further sets among the Y_j. □

Corollary 1.3.14. *Let V be an affine k-variety. Then there are irreducible affine k-varieties $V_1, \ldots, V_r$ with*

$$V = V_1 \cup \cdots \cup V_r$$

and

$$V_i \nsubseteq \bigcup_{j\neq i} V_j$$

for $i = 1, \ldots, r$. These constraints uniquely determine the V_i as the irreducible components of V.

Theorem 1.3.15. *Let V be an affine k-variety. Then*

$$V \text{ irreducible} \;\Leftrightarrow\; \mathcal{I}(V) \subseteq k[\underline{x}] \text{ prime ideal.}$$

Proof. Let $I := \mathcal{I}(V)$ and thus $V = \mathcal{V}(I)$.
First assume V is irreducible. $V \neq \emptyset$ implies $I \neq (1)$. Let $p, q \in k[\underline{x}]$ such that $pq \in I$. Then we have $V \subseteq \mathcal{V}(p) \cup \mathcal{V}(q)$, and from the irreducibility of V we deduce w.l.o.g. $V \subseteq \mathcal{V}(p)$. This means $p \in I$. Therefore I is a prime ideal.
Now assume I is a prime ideal and

$$V \subseteq \mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 I_2)$$

for two ideals $I_1, I_2 \subseteq k[\underline{x}]$. This implies $I_1 I_2 \subseteq I$ and from I being a prime ideal we obtain w.l.o.g. $I_1 \subseteq I$. This in turn yields $V \subseteq \mathcal{V}(I_1)$, and thus V is irreducible. □

Corollary 1.3.16. *The mapping $\mathfrak{p} \mapsto \mathcal{V}(\mathfrak{p})$ defines an inclusion-reversing bijection between $\mathrm{Spec}(k[\underline{x}])$ and the set of all irreducible affine k-varieties in $\mathbb{A}^n$.*

Corollary 1.3.17. *Every ideal $I \subseteq k[\underline{x}]$ is contained in only finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. We have*

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r.$$

$\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are called the **minimal prime divisors of** *I.*

Proof. The minimal prime ideals over I are the minimal prime ideals over $\sqrt{I}$, and by Corollary 1.2.18 and Corollary 1.3.16 these exactly correspond to the maximal irreducible subsets of $V = \mathcal{V}(I)$, of which there are only finitely many by Corollary 1.3.14. According to Theorem 1.1.4 the intersection of the minimal prime ideals containing I is the radical of I. □

Example 1.3.18. (i) Let $V = \mathcal{V}(p)$ be a hypersurface, and let $p_1, \ldots, p_r$ the irreducible factors of p. Then the varieties $\mathcal{V}(p_i)$ are the irreducible components of V, and the ideals (p_i) are the minimal prime divisors of (p).
(ii) The variety $\mathcal{V}(x_1x_2)$ (cf. Example 1.2.2 (ii)) has the two irreducible components $\mathcal{V}(x_1)$ and $\mathcal{V}(x_2)$. Here V is connected.
(iii) The variety $\mathcal{V}(x_1(x_1-1), x_2(x_1-1))$ has the two irreducible components $\mathcal{V}(x_1-1)$ and $\mathcal{V}(x_1, x_2)$. The easiest way to see this is Corollary 1.3.14. Here the irreducible components are also the connected components.
(iv) The variety $V = \mathcal{V}(x_1^2 + x_2^2) \subseteq \mathbb{A}^2 = \mathbb{C}^2$ is irreducible in the $\mathbb{R}$-Zariski topology, because $x_1^2 + x_2^2$ is irreducible in $\mathbb{R}[x_1, x_2]$. However, in the $\mathbb{C}$-Zariski topology V is reducible:

$$V = \mathcal{V}(x_1 + ix_2) \cup \mathcal{V}(x_1 - ix_2).$$

In both topologies V is connected. △

1.4 Regular Functions and Morphisms

Let $V \subseteq \mathbb{A}^n$ be an affine k-variety. Every polynomial $p \in k[\underline{x}]$ defines a polynomial map $p\colon \mathbb{A}^n \to K = \mathbb{A}^1$. Restricting the domain to V gives a map

$$p\colon V \to \mathbb{A}^1.$$

The restrictions of two polynomials $p, q \in k[\underline{x}]$ define the same map on V if and only if $p - q \equiv 0$ on V, equivalently if $p - q \in \mathcal{I}(V)$. *Thus the polynomial maps $V \to \mathbb{A}^1$ can be identified with the elements of $k[\underline{x}]/\mathcal{I}(V)$.*

Reminder: A k**-algebra** is a ring extension of k.

Definition 1.4.1. Let $V \subseteq \mathbb{A}^n$ be an affine k-variety. Then

$$k[V] := k[\underline{x}]/\mathcal{I}(V)$$

is called the **affine coordinate ring** or the **affine coordinate algebra of** V. We emphasize again that $\mathcal{I}(V)$, and therefore $k[V]$, does not depend on the choice of the algebraically closed field K.
Elements of $k[V]$ are called **regular functions on** V**.** Regular functions can be interpreted as polynomial functions on V. △

Example 1.4.2. (i) $k[\mathbb{A}^n] = k[\underline{x}]$ and $k[\emptyset] = \{0\}$.
(ii) If $V = \mathcal{V}(p)$ is a hypersurface and p is square free, then $k[V] = k[\underline{x}]/(p)$. △

Lemma 1.4.3. *(i) For every affine variety V the coordinate algebra $k[V]$ is a finitely generated reduced k-algebra.*
(ii) If $V, W \subseteq \mathbb{A}^n$ are affine varieties with $V \cap W = \emptyset$, then

$$k[V \cup W] \cong k[V] \times k[W].$$

In particular, for every finite variety $V = \{a_1, \ldots, a_r\} \subseteq k^n$ we have

$$k[V] \cong \underbrace{k \times \cdots \times k}_{r}.$$

Proof. (i) This follows from the fact that $k[\underline{x}]$ is finitely generated and $\mathcal{I}(V)$ is a radical ideal. For (ii), observe that

$$(1) = \mathcal{I}(V \cap W) = \sqrt{\mathcal{I}(V) + \mathcal{I}(W)} = \mathcal{I}(V) + \mathcal{I}(W),$$

where we have used Lemma 1.1.3 (ii) for the last equation. The Chinese Remainder Theorem gives

$$k[V \cup W] = k[\underline{x}]/(\mathcal{I}(V) \cap \mathcal{I}(W)) \cong k[\underline{x}]/\mathcal{I}(V) \times k[\underline{x}]/\mathcal{I}(W) = k[V] \times k[W].$$

The second claim follows from $k[\{a\}] = k[\underline{x}]/\mathfrak{m}_a \cong k$ for $a \in k^n$. □

Remark 1.4.4. The ideals of $k[V]$ are in bijection with the ideals of $k[\underline{x}]$ that contain $\mathcal{I}(V)$. The same is true for radical and prime ideals. These ideals, in turn, correspond to subvarieties of V. Thus we obtain the following relative version of Corollary 1.2.18:
The mapping

$$I \mapsto \mathcal{V}_V(I) := \{a \in V \mid p(a) = 0 \, \forall p \in I\}$$

yields a bijection between the radical ideals of $k[V]$ and the subvarieties of V. Under this bijection prime ideals exactly correspond to irreducible subvarieties. The inverse mapping is given by

$$W \mapsto \mathcal{I}_V(W) := \{p \in k[V] \mid p(a) = 0 \,\forall a \in W\}\,.$$

For $p \in k[V]$ let

$$\mathcal{D}_V(p) := \{a \in V \mid p(a) \neq 0\}\,.$$

Every open set in the k-Zariski topology of V is a finite union of such $\mathcal{D}(p_i)$. $\triangle$

Remark 1.4.5. In passing from V to $k[V]$, no information is lost: from $k[V]$ together with the generators $\overline{x}_1, \ldots, \overline{x}_n$, we can reconstruct V in several ways.
(i) Let $\pi\colon k[\underline{x}] \twoheadrightarrow k[V]$ be the canonical projection $x_i \mapsto \overline{x}_i$. Then we obviously have $\ker(\pi) = \mathcal{I}(V)$, and hence

$$V = \mathcal{V}(\ker(\pi)).$$

(ii) The following maps are mutually inverse bijections

$$\begin{aligned} K^n &\longleftrightarrow \mathrm{Hom}_{k-\mathrm{alg}}(k[\underline{x}], K) \\ a &\mapsto \mathrm{e}_a \\ (\alpha(x_1), \ldots, \alpha(x_n)) &\hookleftarrow \alpha. \end{aligned}$$

Here e_a denotes the evaluation of a polynomial in a. Under this bijection the points $a \in V$ exactly correspond to the homomorphisms $\alpha \in \mathrm{Hom}(k[\underline{x}], K)$ with $\alpha \equiv 0$ on $\mathcal{I}(V)$, and thus to the elements in $\mathrm{Hom}(k[V], K)$. Therefore we obtain the bijection

$$\begin{aligned} \mathrm{Hom}(k[V], K) &\to V \\ \alpha &\mapsto (\alpha(\overline{x}_1), \ldots, \alpha(\overline{x}_n)). \end{aligned}$$

$\triangle$

Corollary 1.4.6. *Every finitely generated reduced k-algebra A is isomorphic to the coordinate algebra of an affine k-variety.*

Proof. This follows immediately from the construction in Remark 1.4.5 (i): choose generators $a_1, \ldots, a_n$ of A and consider the surjection

$$\begin{aligned} \pi\colon k[\underline{x}] &\twoheadrightarrow A \\ x_i &\mapsto a_i. \end{aligned}$$

For $V = \mathcal{V}(\ker(\pi))$ we then have

$$k[V] = k[\underline{x}]/\mathcal{I}(V) = k[\underline{x}]/\ker(\pi) \cong A.$$

Here we use that $\ker(\pi)$ is a radical ideal, which follows from the fact that A is reduced. □

Definition 1.4.7. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine k-varieties.
(i) A **(k-)morphism from V to W** is a map

$$p\colon V \to W$$

for which there are $p_1, \ldots, p_m \in k[V]$ such that

$$p(a) = (p_1(a), \ldots, p_m(a)) \quad \forall a \in V.$$

In short, we write $p = (p_1, \ldots, p_m)$.
(ii) A (k-)morphism $p\colon V \to W$ is called **(k-)isomorphism** if there is a k-morphism $q\colon W \to V$ such that

$$q \circ p = \mathrm{id}_V \text{ and } p \circ q = \mathrm{id}_W.$$

(iii) Two affine k-varieties V, W are called **(k-)isomorphic** if there exists a (k-)isomorphism $p\colon V \to W$. In this situation we write $V \cong_k W$ (or $V \cong W$ in case k is clear from the context).
(iv) With $\mathrm{Hom}_k(V, W)$ we denote the set of all k-morphisms from V to W. △

Theorem 1.4.8. *Let $p\colon V \to W$ be a k-morphism. For every $q \in k[W]$ the composition*

$$p^*(q) := q \circ p \in k[V]$$

is a regular function on V. The map p^* defined by

$$\begin{aligned} p^*\colon k[W] &\to k[V] \\ q &\mapsto p^*(q) \end{aligned}$$

is a k-algebra homomorphism. The map

$$\begin{aligned} {}^*\colon \mathrm{Hom}(V, W) &\to \mathrm{Hom}(k[W], k[V]) \\ p &\mapsto p^* \end{aligned}$$

is bijective.

Proof. Since the composition of two polynomial maps is again polynomial, the composition of two k-morphisms is again a k-morphism. Thus $p^*(q) = q \circ p \in \mathrm{Hom}(V, \mathbb{A}^1) = k[V]$. The map p^* is clearly a k-algebra homomorphism. It remains to show that * is bijective. To do this, we explicitly define the inverse map. We have

$$k[W] = k[y_1, \ldots, y_m]/\mathcal{I}(W) = k[\overline{y}_1, \ldots, \overline{y}_m].$$

Now let $\varphi\colon k[W] \to k[V]$ be a k-algebra homomorphism. Let

$$p_\varphi := (\varphi(\overline{y}_1), \ldots, \varphi(\overline{y}_m)) \in \mathrm{Hom}(V, \mathbb{A}^m).$$

We show that in fact $p_\varphi\colon V \to W$. For $q \in k[\underline{y}]$ and $a \in V$ we have

$$q(p_\varphi(a)) = q(\varphi(\overline{y}_1)(a), \ldots, \varphi(\overline{y}_m)(a)) = \varphi(q(\overline{y}))(a) = \varphi(\overline{q})(a).$$

If $q \in \mathcal{I}(W)$, then $\overline{q} = 0$ in $k[W]$, and hence $q(p_\varphi(a)) = 0$. This proves $p_\varphi(a) \in W$, and thus $p_\varphi \in \mathrm{Hom}(V, W)$. Now the map defined by

$$\begin{aligned} \mathrm{Hom}(k[W], k[V]) &\to \mathrm{Hom}(V, W) \\ \varphi &\mapsto p_\varphi \end{aligned}$$

is the inverse map of * (Exercise 35). □

Remark 1.4.9. We put the following on record once more: For $k[W] = k[\underline{y}]/\mathcal{I}(W)$ the inverse of

$$\begin{aligned} {}^*\colon \mathrm{Hom}(V, W) &\to \mathrm{Hom}(k[W], k[V]) \\ p &\mapsto p^* \end{aligned}$$

is the map

$$\begin{aligned} \mathrm{Hom}(k[W], k[V]) &\to \mathrm{Hom}(V, W) \\ \varphi &\mapsto (\varphi(\overline{y}_1), \ldots, \varphi(\overline{y}_m)). \end{aligned}$$

△

Remark 1.4.10. The bijections from Remark 1.4.9 yield an *equivalence of categories* between the category of affine k-varieties with k-morphisms and the category of finitely generated reduced k-algebras with k-algebra homomorphisms. Without defining these terms precisely, we summarize the point as follows:
First, every finitely generated reduced k-algebra is the coordinate algebra of some k-variety (Corollary 1.4.6). Moreover, the map * is a bijection, i.e. morphisms of

varieties and homomorphisms of the associated algebras correspond one-to-one. Finally, * has the following *functorial property*: for each $p \in \mathrm{Hom}(V, W)$ and $q \in \mathrm{Hom}(W, X)$ we have

$$(q \circ p)^* = p^* \circ q^*$$

as well as

$$\mathrm{id}_V^* = \mathrm{id}_{k[V]}.$$

It follows that every problem about varieties can be translated into an equivalent problem about finitely generated reduced algebras, and vice versa. In particular, we obtain the following result. △

Theorem 1.4.11. *A k-morphism $p\colon V \to W$ is an isomorphism of varieties if and only if $p^*\colon k[W] \to k[V]$ is an isomorphism of k-algebras. In particular, we have*

$$V \cong W \Leftrightarrow k[V] \cong k[W].$$

Proof. Exercise 36. □

Example 1.4.12. (i) First simple examples of k-morphisms are

- inclusions of subvarieties $\mathcal{V}_V(I) \hookrightarrow V$ for $I \subseteq k[V]$.
- projections $\pi\colon V_1 \times V_2 \to V_1;\ (a, b) \mapsto a$, for affine varieties V_1, V_2.

(ii) Let $P = \mathcal{V}(x_1^2 - x_2) \subseteq \mathbb{A}^2$ be a parabola, and let $\pi\colon P \to \mathbb{A}^1;\ (a_1, a_2) \mapsto a_1$. Then π is a k-isomorphism. One can either write down the inverse map $r \mapsto (r, r^2)$ directly, or consider

$$k[P] = k[x_1, x_2]/(x_1^2 - x_2) = k[\overline{x}_1, \overline{x}_2] = k[\overline{x}_1]$$

and $k[\mathbb{A}^1] = k[t]$, together with the induced map

$$\begin{aligned} \pi^*\colon k[\mathbb{A}^1] &\to k[P] \\ t &\mapsto \overline{x}_1. \end{aligned}$$

Then π^* is clearly an isomorphism with inverse $\overline{x}_1 \mapsto t, \overline{x}_2 \mapsto t^2$.
(iii) Let $C = \mathcal{V}(x_1^3 - x_2^2)$ be a cuspidal curve (cf. Example 1.2.2 (iv)). Then there is a morphism

$$\begin{aligned} p\colon \mathbb{A}^1 &\to C \\ r &\mapsto (r^2, r^3) \end{aligned}$$

that is even bijective, as is easily verified (Exercise 37). Hence the curve C admits a bijective *polynomial parametrization* by $\mathbb{A}^1$. However, p is *not* a k-isomorphism. Indeed, an inverse map would have to take roots, which cannot be done polynomially. A precise proof uses coordinate algebras. We have $k[C] = k[x_1, x_2]/(x_1^3 - x_2^2) = k[\overline{x}_1, \overline{x}_2], k[\mathbb{A}^1] = k[t]$ and

$$\begin{aligned} p^*\colon k[C] &\to k[\mathbb{A}^1] \\ \overline{x}_1 &\mapsto t^2 \\ \overline{x}_2 &\mapsto t^3. \end{aligned}$$

The map p^* is clearly not surjective, and hence neither p^* nor p is an isomorphism (by Theorem 1.4.11). *Thus bijectivity of a k-morphism does not imply that it is an isomorphism!* △

Theorem 1.4.13. *Let $p\colon V \to W$ be a k-morphism between affine varieties and let $p^*\colon k[W] \to k[V]$ be the induced algebra homomorphism of the coordinate algebras.*
(i) For every ideal $J \subseteq k[W]$ we have

$$p^{-1}(\mathcal{V}_W(J)) = \mathcal{V}_V(p^*(J)).$$

In particular, the preimage of an affine variety under a morphism is again an affine variety.
(ii) For every ideal $I \subseteq k[V]$ we have

$$\overline{p(\mathcal{V}_V(I))} = \mathcal{V}_W((p^*)^{-1}(I)).$$

In particular, we have $\mathcal{I}_W(p(V)) = \ker(p^*)$.

Proof. For $a \in V$ and $q \in k[W]$ we have $q(p(a)) = p^*(q)(a)$. This implies (i) because of

$$\begin{aligned} p(a) \in \mathcal{V}_W(J) &\Leftrightarrow q(p(a)) = 0 \,\forall q \in J \\ &\Leftrightarrow p^*(q)(a) = 0 \,\forall q \in J \\ &\Leftrightarrow a \in \mathcal{V}_V(p^*(J)). \end{aligned}$$

(ii) For $q \in k[W]$ we have

$$\begin{aligned} q \equiv 0 \text{ on } \overline{p(\mathcal{V}_V(I))} &\Leftrightarrow q \equiv 0 \text{ on } p(\mathcal{V}_V(I)) \\ &\Leftrightarrow q \circ p \equiv 0 \text{ on } \mathcal{V}_V(I) \\ &\Leftrightarrow p^*(q) \in \mathcal{I}_V(\mathcal{V}_V(I)) = \sqrt{I} \\ &\Leftrightarrow q \in (p^*)^{-1}\left(\sqrt{I}\right) = \sqrt{(p^*)^{-1}(I)} \\ &\Leftrightarrow q \equiv 0 \text{ on } \mathcal{V}_W((p^*)^{-1}(I)). \end{aligned}$$

But when two varieties have the same vanishing ideal, they are equal by Lemma 1.2.8 (iv). In particular, we get for $I = (0)$ that

$$\mathcal{I}_W(p(V)) = \mathcal{I}_W(\overline{p(V)}) = \mathcal{I}_W(\mathcal{V}_W(\ker(p^*))) = \sqrt{\ker(p^*)} = \ker(p^*),$$

because $\ker(p^*)$ is a radical ideal, since $k[V]$ is reduced. □

Remark/Example 1.4.14. (i) Every k-morphism $p\colon V \to W$ between affine k-varieties is continuous with respect to the k-Zariski topology. This follows from Theorem 1.4.13 (i). In particular, an isomorphism is always a homeomorphism of the underlying topological spaces.
(ii) A k-morphism between affine varieties can be a homeomorphism with respect to the Zariski topology *without* being an isomorphism. Example 1.4.12 (iii) demonstrates this (Exercise 37).
(iii) The image $p(V)$ of a variety under a morphism is in general neither closed nor open. For example, for

$$\begin{aligned} p\colon \mathbb{A}^2 &\to \mathbb{A}^2 \\ (a_1, a_2) &\mapsto (a_1, a_1 a_2) \end{aligned}$$

we have

$$p(\mathbb{A}^2) = \mathbb{A}^2 \setminus \{(0, b) \mid b \neq 0\}.$$

(iv) If V is irreducible, then so is $\overline{p(V)}$. This follows either by a direct topological argument using continuity of p, or algebraically from the fact that $k[V]$ is a domain and thus $\mathcal{I}_W(\overline{p(V)}) = \ker(p^*)$ is a prime ideal. △

To conclude this chapter, we address finite varieties.

Definition 1.4.15. An ideal $I \subseteq k[\underline{x}]$ is called 0**-dimensional** if

$$\dim_k k[\underline{x}]/I < \infty$$

holds. △

Theorem 1.4.16. *For an ideal $I \subseteq k[\underline{x}]$ the following are equivalent:*

(i) *I is 0-dimensional*

(ii) $|\mathcal{V}(I)| < \infty$

(iii) *$I \cap k[x_i] \neq \{0\}$ for all $i = 1, \ldots, n$.*

If this is fulfilled, then $\mathcal{V}(I) \subseteq \overline{k}^n$ *and* $|\mathcal{V}(I)| \leqslant \dim_k k[\mathcal{V}(I)] \leqslant \dim_k k[\underline{x}]/I$.

Proof. First let $V := \mathcal{V}(I) \subseteq K^n$ be a finite set. By Hilbert's Nullstellensatz we have

$$\sqrt{I} = \bigcap_{a \in V \cap \overline{k}^n} \mathcal{I}(\{a\}).$$

Applying the fundamental theorem on homomorphisms to the evaluation map e_a yields

$$k[\underline{x}]/\mathcal{I}(\{a\}) \cong k[a_1, \ldots, a_n],$$

and for $a \in \overline{k}^n$ the right-hand side is a field. Therefore $\mathcal{I}(\{a\})$ is a maximal ideal of $k[\underline{x}]$ for all $a \in V \cap \overline{k}^n$. Hence

$$\sqrt{I} = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$$

is a finite intersection of maximal ideals. Since the $\mathfrak{m}_i$ are pairwise distinct and maximal, it obviously follows that $\mathfrak{m}_i + \mathfrak{m}_j = (1)$ holds for $i \neq j$. The Chinese Remainder Theorem now yields

$$k[V] = k[\underline{x}]/\sqrt{I} \cong L_1 \times \cdots \times L_r,$$

where $L_i = k[\underline{x}]/\mathfrak{m}_i$ is a finite algebraic field extension of k by Corollary 1.2.10. Together with Remark 1.4.5 (ii) we obtain

$$V = \mathrm{Hom}_k\left(k[V], K\right) = \mathrm{Hom}_k\left(L_1 \times \cdots \times L_r, K\right) = \mathrm{Hom}_k\left(L_1 \times \cdots \times L_r, \overline{k}\right).$$

For the last equality we used that the elements of all L_i fulfill polynomial equations over k, and are thus always mapped to $\overline{k}$ by k-algebra homomorphisms. This already shows $V \subseteq \overline{k}^n$. Because of

$$\mathrm{Hom}_k\left(L_1 \times \cdots \times L_r, \overline{k}\right) = \bigcup_{i=1}^{r} \mathrm{Hom}_k\left(L_i, \overline{k}\right)$$

(Exercise 40), we now have

$$\begin{aligned} |V| &= \sum_{i=1}^{r} |\mathrm{Hom}_k\left(L_i, \overline{k}\right)| \\ &\leqslant \sum_{i=1}^{r} [L_i : k] \\ &= \dim_k k[V] \\ &\leqslant \dim_k k[\underline{x}]/I. \end{aligned}$$

This proves the last statement. Now for the equivalence of (i)–(iii) let

$$\pi_i \colon \mathbb{A}^n \to \mathbb{A}^1$$

be the projection onto the i-th component. We have

$$\begin{aligned} V \text{ finite } &\Leftrightarrow \pi_i(V) \text{ finite for all } i = 1, \ldots, n \\ &\Leftrightarrow \overline{\pi_i(V)} \text{ finite for all } i = 1, \ldots, n, \end{aligned}$$

where we have used $\pi_i(V) \subseteq \overline{k}$ for the last equivalence. By Theorem 1.4.13 the variety $\overline{\pi_i(V)}$ is defined by the ideal $I \cap k[x_i]$, and thus (ii) is equivalent to (iii). For $(iii) \Rightarrow (i)$ we use that for every i some $x_i^{d_i}$ can modulo I be replaced by lower powers of x_i. Therefore $k[\underline{x}]/I$ is finite dimensional. For $(i) \Rightarrow (iii)$ we use that $k[x_i]/\left(I \cap k[x_i]\right)$ can be embedded into $k[\underline{x}]/I$. Therefore $k[x_i]/\left(I \cap k[x_i]\right)$ is finite dimensional, which can only be true if $I \cap k[x_i] \neq \{0\}$. □

Example 1.4.17. Again note that $\mathcal{V}(I)$ must be defined in K^n and not in k^n. For example, $\mathcal{V}(x_1^2+x_2^2)$ is not finite, since $k[x_1, x_2]/(x_1^2+x_2^2)$ is not a finite-dimensional k-vector space. In $\mathbb{R}^2$, however, we see only a single point of the variety. △

Chapter 2

Algorithmic Aspects

The previous chapter raised several questions that we would also like to answer algorithmically. For example:

- Given $p, p_1, \ldots, p_r \in k[\underline{x}]$, is it true that $p \in (p_1, \ldots, p_r)$?
- Given ideals $I = (p_1, \ldots, p_r), J = (q_1, \ldots, q_s) \subseteq k[\underline{x}]$, find generators for the ideals $I \cap J, (I : J), \sqrt{I}$.
- Given a homomorphism $\varphi\colon k[\underline{x}] \to k[\underline{y}]$ and an ideal $J = (q_1, \ldots, q_r) \subseteq k[\underline{y}]$, find generators for $\varphi^{-1}(J)$.

The theory of *Gröbner bases* allows us to settle such questions algorithmically, using *symbolic computations*, i.e. exact computations rather than numerical approximations (at least when all input data are exact, for example for polynomials over $\mathbb{Q}$). These algorithms are implemented in most computer algebra systems used today.

2.1 Monomial Ideals

Notation 2.1.1. Let again k be a field and set $\underline{x} = (x_1, \ldots, x_n)$. For $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ and $c \in k$ we call

$$\underline{x}^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

a **monomial**, and

$$c\underline{x}^\alpha$$

a **term**. We further set

$$|\alpha| = \alpha_1 + \cdots + \alpha_n.$$

The monomials form a k-vector space basis of $k[\underline{x}]$. For

$$p = \sum_{\alpha \in \mathbb{N}^n} p_\alpha \underline{x}^\alpha \in k[\underline{x}]$$

we define

$$\operatorname{supp}(p) = \{\alpha \in \mathbb{N}^n \mid p_\alpha \neq 0\}.$$

Note that $\operatorname{supp}(p)$ is finite for every polynomial p. The **degree** $\deg(p)$ of p is defined as

$$\deg(p) = \max\{|\alpha| \mid \alpha \in \operatorname{supp}(p)\}.$$

The **natural partial ordering** on $\mathbb{N}^n$ is defined by

$$\alpha \leqslant \beta :\Leftrightarrow \alpha_i \leqslant \beta_i \, \forall i = 1, \ldots, n. \qquad \triangle$$

Definition 2.1.2. An ideal $I \subseteq k[\underline{x}]$ is called **monomial** if it is generated by monomials. $\triangle$

Lemma 2.1.3. *Let $M \subseteq \mathbb{N}^n$ and $I = (\underline{x}^\alpha \mid \alpha \in M)$. Then the elements of I are precisely the k-linear combinations of monomials $\underline{x}^\beta$ with $\alpha \leqslant \beta$ for some $\alpha \in M$.*

Proof. This is clear. $\square$

Remark 2.1.4. (i) The monomials $\underline{x}^\beta$ with $\alpha \leqslant \beta$ for some $\alpha \in M$ in fact form a k-vector space basis of I.
(ii) A general ideal $I \subseteq k[\underline{x}]$ will often not contain even a single monomial, for example $I = (x_1 + 1) \subseteq k[x_1]$. $\triangle$

Theorem 2.1.5 (Dickson's Lemma)**.** *For every subset $M \subseteq \mathbb{N}^n$, the set $M_{\min}$ of minimal elements with respect to $\leqslant$ is finite.*

Proof. By Hilbert's Basis Theorem, the ideal

$$I := (\underline{x}^\alpha \mid \alpha \in M)$$

admits a finite generating set. Thus there is a finite subset $S \subseteq M$ such that

$$\forall \beta \in M \; \exists \alpha \in S \quad \alpha \leqslant \beta.$$

This implies that the set of minimal elements of M is contained in S, and is therefore finite. $\square$

2.2 Monomial Orderings and Gröbner Bases

Definition 2.2.1. A **monomial ordering** is a total ordering $\preccurlyeq$ on $\mathbb{N}^n$ such that, for all $\alpha, \beta, \gamma \in \mathbb{N}^n$:

(i) $0 \preccurlyeq \alpha$

(ii) $\alpha \preccurlyeq \beta \Rightarrow \alpha + \gamma \preccurlyeq \beta + \gamma$. △

Remark/Example 2.2.2. (i) A monomial ordering can also be understood as a total ordering of the monomials of $k[\underline{x}]$, via

$$\underline{x}^\alpha \preccurlyeq \underline{x}^\beta :\Leftrightarrow \alpha \preccurlyeq \beta.$$

Condition (ii) in Definition 2.2.1 then simply means compatibility with multiplication:

$$\underline{x}^\alpha \preccurlyeq \underline{x}^\beta \;\Rightarrow\; \underline{x}^\alpha \underline{x}^\gamma \preccurlyeq \underline{x}^\beta \underline{x}^\gamma.$$

(ii) For $n = 1$ there exists exactly one monomial ordering: $1 \prec x_1 \prec x_1^2 \prec \cdots$. For $n \geqslant 2$ there are more, for example the **lexicographic ordering**

$$\alpha \preccurlyeq_{\text{lex}} \beta \;:\Leftrightarrow\; \alpha = \beta \text{ or } \alpha_i < \beta_i \text{ for } i = \min\{j \mid \alpha_j \neq \beta_j\}$$

or the **graded-lexicographic ordering**

$$\alpha \preccurlyeq_{\text{grlex}} \beta \;:\Leftrightarrow\; |\alpha| < |\beta| \text{ or } (|\alpha| = |\beta| \text{ and } \alpha \preccurlyeq_{\text{lex}} \beta)\,. \qquad \triangle$$

Lemma 2.2.3. *Monomial orderings are well-orderings on $\mathbb{N}^n$, i.e. every nonempty subset has a smallest element.*

Proof. Let $\preccurlyeq$ be a monomial ordering and let $\emptyset \neq M \subseteq \mathbb{N}^n$. By Theorem 2.1.5, the set $M_{\min}$ of minimal elements with respect to $\leqslant$ is finite. But $\alpha \leqslant \beta$ implies $\alpha \preccurlyeq \beta$, and thus the smallest element of $M_{\min}$ with respect to $\preccurlyeq$ is also the smallest element of M. □

Notation 2.2.4. Let $\preccurlyeq$ be a monomial ordering and let $0 \neq p = \sum_\alpha p_\alpha \underline{x}^\alpha \in k[\underline{x}]$. Let $\gamma = \max_{\preccurlyeq} \operatorname{supp}(p)$. We define

$$\operatorname{LM}_{\preccurlyeq}(p) = \underline{x}^\gamma \quad \operatorname{LC}_{\preccurlyeq}(p) = p_\gamma \quad \operatorname{LT}_{\preccurlyeq}(p) = p_\gamma \underline{x}^\gamma$$

and call these the **leading monomial, leading coefficient**, and **leading term** of p. We call p **monic** if $\operatorname{LC}_{\preccurlyeq}(p) = 1$. We set

$$\operatorname{LM}_{\preccurlyeq}(0) = \operatorname{LC}_{\preccurlyeq}(0) = \operatorname{LT}_{\preccurlyeq}(0) = 0.$$

If the monomial ordering is clear from the context, we sometimes omit the subscript $\preccurlyeq$ and write $\operatorname{LM}(p)$ instead of $\operatorname{LM}_{\preccurlyeq}(p)$, etc. △

Lemma 2.2.5. *For $p, q \in k[\underline{x}]$ we have*

$$\mathrm{LM}(pq) = \mathrm{LM}(p) \cdot \mathrm{LM}(q)$$

and

$$\mathrm{LM}(p+q) \preccurlyeq \max\{\mathrm{LM}(p), \mathrm{LM}(q)\},$$

where equality holds in the second equation if $\mathrm{LM}(p) \neq \mathrm{LM}(q)$.

Proof. This is clear. □

Definition 2.2.6. Let $I \subseteq k[\underline{x}]$ be an ideal and let $\preccurlyeq$ be a monomial ordering. We call

$$\mathrm{LI}_{\preccurlyeq}(I) := (\mathrm{LM}_{\preccurlyeq}(p) \mid p \in I)$$

the **leading ideal of I with respect to $\preccurlyeq$**. A monomial *not* contained in $\mathrm{LI}_{\preccurlyeq}(I)$ is called a **standard monomial of I with respect to $\preccurlyeq$.** △

Remark 2.2.7. (i) $\mathrm{LI}(I)$ is a monomial ideal. The monomials contained in it are precisely the $\mathrm{LM}(p)$ with $p \in I$, since $\underline{x}^{\beta}\mathrm{LM}(p) = \mathrm{LM}(\underline{x}^{\beta}p)$.
(ii) $I = (p_1, \ldots, p_r)$ implies

$$(\mathrm{LM}(p_1), \ldots, \mathrm{LM}(p_r)) \subseteq \mathrm{LI}(I),$$

but this is in general *not an equality!* In a representation

$$p = \sum_i q_i p_i \in I$$

the leading terms of the sum on the right can cancel. Thus, from p alone, we do not have control over the complexity of the q_i. For example, for $I = (p_1, p_2)$ with $p_1 = xy + 1, p_2 = y^2 - 1$, we find

$$x + y = yp_1 - xp_2 \in I,$$

and thus, depending on the monomial ordering, either x or y belongs to $\mathrm{LI}(I)$. On the other hand, $\mathrm{LM}(p_1) = xy$ and $\mathrm{LM}(p_2) = y^2$ for every monomial ordering, and

$$x, y \notin \left(xy, y^2\right).$$

This is precisely the problem that the notion of a Gröbner basis will solve. △

Theorem 2.2.8 (Macaulay)**.** *Let $I \subseteq k[\underline{x}]$ be an ideal and let $\preccurlyeq$ be a monomial ordering. Then the standard monomials of I with respect to $\preccurlyeq$ form a k-vector space basis of $k[\underline{x}]/I$.*

Proof. Linear independence: Let $p = \sum_i p_i \underline{x}^{\alpha_i} \in I$ with $\underline{x}^{\alpha_i} \notin \mathrm{LI}(I)$ for all i. If $p_i \neq 0$ for some i, then $\mathrm{LM}(p)$ is one of the $\underline{x}^{\alpha_i}$, and thus belongs to $\mathrm{LI}(I)$, a contradiction.
Generating set: Denote by V the k-vector space spanned by the standard monomials of I. We will show that $V + I = k[\underline{x}]$. Assume for contradiction that this fails. Choose $p \in k[\underline{x}] \setminus (V + I)$ with smallest leading monomial with respect to $\preccurlyeq$ (using Lemma 2.2.3). Then $\mathrm{LM}(p)$ is not a standard monomial: otherwise $\mathrm{LT}(p) \in V$, and hence $p - \mathrm{LT}(p) \notin V + I$, contradicting minimality. So we must have $\mathrm{LM}(p) \in \mathrm{LI}(I)$, i.e. there exists $q \in I$ with $\mathrm{LM}(q) = \mathrm{LM}(p)$. Now consider

$$h = p - \frac{\mathrm{LC}(p)}{\mathrm{LC}(q)} q.$$

We have $h \notin V + I$, but $\mathrm{LM}(h) \prec \mathrm{LM}(p)$, again a contradiction. □

Definition 2.2.9. Let $I \subseteq k[\underline{x}]$ be an ideal, let $\preccurlyeq$ be a monomial ordering, and let V be the subspace of $k[\underline{x}]$ spanned by the standard monomials of I with respect to $\preccurlyeq$. By Theorem 2.2.8, for every $p \in k[\underline{x}]$ there exists a *uniquely determined* $q \in V$ with

$$p \equiv q \mod I.$$

We call this q **the canonical form of** p **modulo** I **(with respect to** $\preccurlyeq$**)**, and use the notation

$$q = \mathrm{cf}_{I,\preccurlyeq}(p).$$

Note that

$$\mathrm{cf}_{I,\preccurlyeq} \colon k[\underline{x}] \to V$$

is a surjective linear map with I as its kernel. △

Definition 2.2.10. Let $I \subseteq k[\underline{x}]$ be an ideal and let $\preccurlyeq$ be a monomial ordering. A *finite* subset $G \subseteq I$ with $0 \notin G$ is called a **Gröbner basis of** I **(with respect to** $\preccurlyeq$**)** if

$$\mathrm{LI}_{\preccurlyeq}(I) = (\mathrm{LM}_{\preccurlyeq}(g) \mid g \in G).$$

A finite subset $G \subseteq k[\underline{x}]$ is called a **Gröbner basis (with respect to** $\preccurlyeq$**)** if G is a Gröbner basis of the ideal (G). △

Lemma 2.2.11. *Let $J \subseteq I$ be ideals with $\mathrm{LI}_{\preccurlyeq}(J) = \mathrm{LI}_{\preccurlyeq}(I)$. Then $J = I$.*

Proof. From $\mathrm{LI}_{\preccurlyeq}(I) = \mathrm{LI}_{\preccurlyeq}(J)$ we see that both ideals have the same standard monomials. Thus the space V spanned by those standard monomials is the same for both ideals, and from $k[\underline{x}] = V \oplus I = V \oplus J$ (Theorem 2.2.8) we immediately obtain $I = J$. □

Theorem 2.2.12. *Every ideal $I \subseteq k[\underline{x}]$ has a Gröbner basis (with respect to every monomial ordering), and each such Gröbner basis generates I as an ideal.*

Proof. By Hilbert's Basis Theorem, the monomial ideal $\mathrm{LI}_{\preccurlyeq}(I)$ is generated by finitely many monomials $\mathrm{LM}_{\preccurlyeq}(p_1), \ldots, \mathrm{LM}_{\preccurlyeq}(p_r)$ with $p_i \in I$. Then the set $G = \{p_1, \ldots, p_r\}$ is clearly a Gröbner basis of I with respect to $\preccurlyeq$.
Now set $J = (p_1, \ldots, p_r)$. Then $J \subseteq I$ is an ideal with $\mathrm{LI}_{\preccurlyeq}(J) = \mathrm{LI}_{\preccurlyeq}(I)$, and by Lemma 2.2.11 we get $I = J$. Thus G generates I. □

Example 2.2.13. (i) Consider $I = (p_1, p_2) \subseteq k[x, y]$ with $p_1 = xy + 1, p_2 = y^2 - 1$ as in Remark 2.2.7 (ii). We have seen there that $\{p_1, p_2\}$ is not a Gröbner basis of I for any monomial ordering.
(ii) Consider $I = (p_1, p_2) \subseteq k[x, y, z]$ with $p_1 = x + z$, $p_2 = y + z$.

- With respect to the lexicographic monomial ordering $z \prec y \prec x$, we have

  $$\mathrm{LM}_{\preccurlyeq}(p_1) = x, \quad \mathrm{LM}_{\preccurlyeq}(p_2) = y,$$

  and thus

  $$\mathrm{LI}_{\preccurlyeq}(I) \supseteq (x, y).$$

  On the other hand, $I \cap k[z] = (0)$, which can for example be seen from $\mathcal{V}(I) = \{(t, t, -t) \mid t \in K\}$. Thus the leading monomial of an element of I cannot be a power of z, since the monomial ordering would imply that only z appears in the polynomial. Hence each leading monomial is divisible by either x or y, and this implies $\mathrm{LI}_{\preccurlyeq}(I) = (x, y)$. So $\{p_1, p_2\}$ is a Gröbner basis of I with respect to $\preccurlyeq$.

- Now let $\preccurlyeq$ be a monomial ordering with $x \prec z, y \prec z$. Then

  $$\mathrm{LM}_{\preccurlyeq}(p_1) = \mathrm{LM}_{\preccurlyeq}(p_2) = z.$$

  From

  $$x - y = p_1 - p_2 \in I$$

  we see that either x or y belongs to $\mathrm{LI}_{\preccurlyeq}(I)$. So $\{p_1, p_2\}$ is not a Gröbner basis of I with respect to $\preccurlyeq$. △

2.3 The Buchberger Algorithm

Throughout this section, let $\preccurlyeq$ be a fixed monomial ordering on $\mathbb{N}^n$. All notions such as $\mathrm{LM}(p)$, $\mathrm{LI}(I)$, and Gröbner basis refer to this ordering.

Theorem 2.3.1 (Division Algorithm). *Let $0 \neq g_1, \ldots, g_s \in k[\underline{x}]$. For every $p \in k[\underline{x}]$ there exist $q_1, \ldots, q_s, r \in k[\underline{x}]$ with*

$$p = q_1 g_1 + \cdots + q_s g_s + r$$

and:

(1) no monomial in r is divisible by any $\mathrm{LM}(g_i)$;

(2) $\mathrm{LM}(q_i g_i) \preccurlyeq \mathrm{LM}(p)$ for all $i = 1, \ldots, s$.

Proof. Write $p = \sum_\alpha p_\alpha \underline{x}^\alpha$. If no monomial in p is divisible by any $\mathrm{LM}(g_i)$, we simply set $q_1 = \cdots = q_s = 0$ and $r = p$.
Otherwise, let $\underline{x}^\alpha$ be the largest monomial in p (with respect to $\preccurlyeq$) that is divisible by some $\mathrm{LM}(g_i)$, say $\underline{x}^\alpha = \underline{x}^\beta \cdot \mathrm{LM}(g_i)$. We now set

$$q := \frac{p_\alpha}{\mathrm{LC}(g_i)} \cdot \underline{x}^\beta \quad \text{and} \quad \tilde{p} = p - q g_i.$$

The coefficient of $\underline{x}^\alpha$ in $\tilde{p}$ vanishes, and each monomial of $\tilde{p}$ that is divisible by some $\mathrm{LM}(g_i)$ is strictly smaller than $\underline{x}^\alpha$ (otherwise it would already appear in p). We iterate this process, which terminates after finitely many steps because $\preccurlyeq$ is a well-ordering. We finally obtain a polynomial r in which no monomial is divisible by any $\mathrm{LM}(g_i)$. Backwards substitution yields the desired identity. Note that in the first step we have

$$\mathrm{LM}(q g_i) = \underline{x}^\beta \mathrm{LM}(g_i) = \underline{x}^\alpha \preccurlyeq \mathrm{LM}(p)$$

and thus

$$\mathrm{LM}(\tilde{p}) \preccurlyeq \mathrm{LM}(p).$$

□

Remark 2.3.2. (i) The proof of Theorem 2.3.1 is constructive. Given p and $g_1, \ldots, g_s$, we can find the q_i and r explicitly through the given procedure.
(ii) The polynomials q_i and r are *not* uniquely determined by conditions (1) and (2) in Theorem 2.3.1. The division algorithm allows choices, and these can indeed lead to different results.

- Let $n = 1$ and $g_1 = x, g_2 = x + 1$. With $p = x$ we have

$$p = g_1 + 0 = g_2 - 1.$$

  Both identities satisfy (1) and (2), and can indeed arise from the division algorithm.

- Let $n = 2$ and $g_1 = xy + 1, g_2 = y^2 - 1$ as in Example 2.2.13 (i). For $p = xy^2 - x$ we have

$$p = yg_1 - (x + y) = xg_2 + 0.$$

  Both identities satisfy (1) and (2), independently of the monomial ordering, and can arise through the division algorithm. △

Definition 2.3.3. A polynomial r satisfying the conditions from Theorem 2.3.1 is called **a normal form of** p **modulo** $g_1, \ldots, g_s$ **with respect to** $\preccurlyeq$. This should not be confused with the canonical form $\mathrm{cf}_I(p)$ from Definition 2.2.9, which is uniquely determined. △

Corollary 2.3.4. *If $\{g_1, \ldots, g_s\}$ is a Gröbner basis of I, then every normal form r of p modulo $g_1, \ldots, g_s$ coincides with the canonical form:*

$$r = \mathrm{cf}_I(p).$$

In particular, the division algorithm always leads to the same normal form r, independent of the choices made.

Proof. Let r be a normal form. Then every monomial in r is a standard monomial of I, due to property (1) in Theorem 2.3.1, and since the $\mathrm{LM}(g_i)$ generate the leading ideal of I. On the other hand we have $p \equiv r$ modulo I. But these two properties precisely characterize $\mathrm{cf}_I(p)$. □

We will now develop a method to actually compute a Gröbner basis for a given ideal. We will need some preliminaries for this.

Definition 2.3.5. Let $p, q \in k[\underline{x}] \setminus \{0\}$. Then

$$S(p, q) := \frac{\mathrm{LT}(q) \cdot p - \mathrm{LT}(p) \cdot q}{\gcd(\mathrm{LM}(p), \mathrm{LM}(q))}$$

is called the S**-polynomial of** p **and** q. △

Remark 2.3.6. (i) The S-polynomial is indeed a polynomial. The greatest common divisor of $\mathrm{LM}(p)$ and $\mathrm{LM}(q)$ divides the numerator.
(ii) The leading terms in the numerator cancel by construction, so one has

$$\mathrm{LM}(S(p,q)) \prec \mathrm{lcm}(\mathrm{LM}(p), \mathrm{LM}(q)).$$

The next lemma states that cancellation of leading monomials in a linear combination is essentially always due to this phenomenon in S-polynomials. △

Lemma 2.3.7. *Let $g_1, \ldots, g_s \in k[\underline{x}] \setminus \{0\}$ all have the same leading monomial $\mathrm{LM}(g_i) = \underline{x}^\alpha$. Let $a_1, \ldots, a_s \in k$ with*

$$\mathrm{LM}\left(\sum_{i=1}^{s} a_i g_i\right) \prec \underline{x}^\alpha.$$

Then $\sum_i a_i g_i$ is a linear combination of the $S(g_i, g_{i+1})$, for $i = 1, \ldots, s-1$.

Proof. Set $b_i := \mathrm{LC}(g_i)$ and $p_i := \frac{1}{b_i} g_i$ for $i = 1, \ldots, s$. From

$$\mathrm{LM}\left(\sum_{i=1}^{s} a_i g_i\right) \prec \underline{x}^\alpha$$

we obtain

$$\sum_{i=1}^{s} a_i b_i = 0.$$

With $p_{s+1} = 0$ we thus get:

$$\begin{aligned}\sum_{i=1}^{s} a_i g_i &= \sum_{i=1}^{s} a_i b_i p_i \\ &= \sum_{i=1}^{s} \left(\sum_{j=1}^{i} a_j b_j\right)(p_i - p_{i+1}) \\ &= \sum_{i=1}^{s-1} \left(\sum_{j=1}^{i} a_j b_j\right)(p_i - p_{i+1}).\end{aligned}$$

The last equality uses $\sum_{i=1}^{s} a_i b_i = 0$. The claim now follows from

$$S(g_i, g_j) = \frac{b_j \underline{x}^\alpha g_i - b_i \underline{x}^\alpha g_j}{\underline{x}^\alpha} = b_j g_i - b_i g_j = b_i b_j (p_i - p_j).$$ □

Theorem 2.3.8 (Buchberger Criterion for Gröbner bases). *Let $g_1, \ldots, g_s \in k[\underline{x}] \setminus \{0\}$, and let h_{ij} be a normal form of $S(g_i, g_j)$ with respect to $g_1, \ldots, g_s$, for all $i, j \in \{1, \ldots, s\}$. Then $\{g_1, \ldots, g_s\}$ is a Gröbner basis if and only if $h_{ij} = 0$ for all $i < j$.*

Proof. We set $I = (g_1, \ldots, g_s)$. First assume that $\{g_1, \ldots, g_s\}$ is a Gröbner basis. From Corollary 2.3.4 we obtain that $h_{ij} = \mathrm{cf}_I(S(g_i, g_j))$ is the canonical form with respect to I. Since $S(g_i, g_j) \in I$ we thus have $h_{ij} = 0$ for all $i < j$.
For the other direction assume $h_{ij} = 0$ for all $i < j$. We have to show that for all $0 \neq p \in I$ there exists some $i \in \{1, \ldots, s\}$ with

$$\mathrm{LM}(g_i) | \mathrm{LM}(p).$$

By assumption there exists an identity

$$p = \sum_{i=1}^{s} q_i g_i \tag{$*$}$$

with $q_i \in k[\underline{x}]$. Let

$$\underline{x}^{\gamma} := \max\{\mathrm{LM}(q_i g_i) \mid i = 1, \ldots, s\}.$$

We now show that if $\mathrm{LM}(p) \prec \underline{x}^{\gamma}$ holds, we can find a new identity as in $(*)$, in which γ is strictly smaller. By iteration we then end up with $\mathrm{LM}(p) = \underline{x}^{\gamma}$, proving that $\mathrm{LM}(p)$ is divisible by some $\mathrm{LM}(g_i)$.
So assume $\mathrm{LM}(p) \prec \underline{x}^{\gamma}$. After relabelling we can assume

$$\gamma_1 = \cdots = \gamma_t = \gamma \succ \gamma_{t+1}, \ldots, \gamma_s$$

where $\underline{x}^{\gamma_i} = \mathrm{LM}(q_i g_i)$. We rewrite $(*)$ as

$$p = \underbrace{\sum_{i=1}^{t} \mathrm{LT}(q_i) g_i}_{\tilde{p}} + \sum_{i=1}^{t} (q_i - \mathrm{LT}(q_i)) g_i + \sum_{i=t+1}^{s} q_i g_i.$$

Every term in $\tilde{p}$ has $\underline{x}^{\gamma}$ as its leading monomial, every other term has a strictly smaller leading monomial. We further have $\mathrm{LM}(\tilde{p}) \prec \underline{x}^{\gamma}$, since this is true for p. So it suffices to find a representation

$$\tilde{p} = \sum_{j=1}^{s} \tilde{q}_j g_j \tag{$**$}$$

with $\mathrm{LM}(\tilde{q}_j g_j) \prec \underline{x}^\gamma$ for all j.
To the polynomials $\mathrm{LM}(q_i)g_i$ ($i = 1, \ldots, t$) we can apply Lemma 2.3.7. So $\tilde{p}$ is a linear combination of the

$$s_{ij} := S\left(\mathrm{LM}(q_i)g_i, \mathrm{LM}(q_j)g_j\right) \qquad \text{for } i < j = 1, \ldots t.$$

Setting $\underline{x}^{\alpha_i} := \mathrm{LM}(g_i)$ we get $\mathrm{LM}(q_i) = \underline{x}^{\gamma-\alpha_i}$ and thus

$$\begin{aligned} s_{ij} &= \frac{1}{\underline{x}^\gamma}\left(\underline{x}^{\gamma-\alpha_j}\mathrm{LT}(g_j)\underbrace{\mathrm{LM}(q_i)}_{\underline{x}^{\gamma-\alpha_i}}g_i - \underline{x}^{\gamma-\alpha_i}\mathrm{LT}(g_i)\underbrace{\mathrm{LM}(q_j)}_{\underline{x}^{\gamma-\alpha_j}}g_j\right) \\ &= \underline{x}^{\gamma-\alpha_i-\alpha_j}\underbrace{\left(\mathrm{LT}(g_j)g_i - \mathrm{LT}(g_i)g_j\right)}_{S(g_i,g_j)\cdot\gcd(\underline{x}^{\alpha_i},\underline{x}^{\alpha_j})} \\ &= \underline{x}^{\beta_{ij}} \cdot S(g_i, g_j). \end{aligned}$$

Here

$$\underline{x}^{\beta_{ij}} = \underline{x}^{\gamma-\alpha_i-\alpha_j} \cdot \gcd(\underline{x}^{\alpha_i}, \underline{x}^{\alpha_j}) = \frac{\underline{x}^\gamma}{\mathrm{lcm}(\underline{x}^{\alpha_i}, \underline{x}^{\alpha_j})}$$

holds. Our conditions $h_{ij} = 0$ now provide identities

$$S(g_i, g_j) = \sum_{k=1}^{s} p_{ijk} g_k$$

with $\mathrm{LM}(p_{ijk}g_k) \preccurlyeq \mathrm{LM}(S(g_i, g_j))$. In total we see that $\tilde{p}$ is a linear combination of the elements

$$\sum_{k=1}^{s} p_{ijk}\underline{x}^{\beta_{ij}} g_k,$$

and from $\mathrm{LM}(S(g_i, g_j)) \prec \mathrm{lcm}(\underline{x}^{\alpha_i}, \underline{x}^{\alpha_j})$ (by Remark 2.3.6 (ii)) we get

$$\mathrm{LM}(p_{ijk}\underline{x}^{\beta_{ij}} g_k) = \underline{x}^{\beta_{ij}}\mathrm{LM}(p_{ijk}g_k) \preccurlyeq \underline{x}^{\beta_{ij}}\mathrm{LM}(S(g_i, g_j)) \prec \underline{x}^\gamma.$$

That is precisely the desired identity ($**$). □

Theorem 2.3.9 (Buchberger Algorithm). *Let $g_1, \ldots, g_s \in k[\underline{x}] \setminus \{0\}$. The following algorithm terminates after finitely many steps, and outputs a Gröbner basis of $I = (g_1, \ldots, g_s)$:*

- *Compute a normal form h_{ij} of $S(g_i, g_j)$ with respect to $g_1, \ldots, g_s$, for all $1 \leqslant i < j \leqslant s$.*

- *If $h_{ij} = 0$ for all $i < j$, terminate and output $\{g_1, \ldots, g_s\}$.*
- *If $h_{ij} \neq 0$ for some i, j, add it to the list of generators and start again.*

Proof. We have $S(g_i, g_j) \in I$ for all i, j. This implies $h_{ij} \in I$ for all i, j, and thus I is not enlarged by adding the h_{ij}. Upon termination of the algorithm we obtain a Gröbner basis of I, by Theorem 2.3.8. What remains to show is that the algorithm does indeed terminate after finitely many steps.
If $h_{ij} \neq 0$ then

$$(\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)) \subsetneq (\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s), \mathrm{LM}(h_{ij}))\,,$$

since none of the monomials in h_{ij} is divisible by some $\mathrm{LM}(g_i)$. By Hilbert's Basis Theorem this can happen only finitely many times. □

Remark 2.3.10. (i) All steps in the Buchberger Algorithm are constructive. The $S(g_i, g_j)$ are explicitly given, and a normal form h_{ij} can be computed with the division algorithm (Theorem 2.3.1). Thus, if the input data can be represented exactly on a computer (for example if all polynomials have rational coefficients), a computer can compute a Gröbner basis exactly.
(ii) The algorithm described above will in general produce a very redundant Gröbner basis.
(iii) If G is a Gröbner basis of I and $p, q \in G$ with $p \neq q$ and $\mathrm{LM}(p) | \mathrm{LM}(q)$, then $G \setminus \{q\}$ is also a Gröbner basis of I. △

Definition 2.3.11. A Gröbner basis G is called **minimal**, if

$$\mathrm{LM}(p) \nmid \mathrm{LM}(q)$$

for all $p, q \in G, p \neq q$. △

Lemma 2.3.12. *Let G be a minimal Gröbner basis and let $I = (G)$. Then the $\mathrm{LM}(g)$ ($g \in G$) are exactly the distinct minimal monomials (with respect to $\leqslant$) in $\mathrm{LI}(I)$.*

Proof. Every minimal monomial (with respect to $\leqslant$) in $\mathrm{LI}(I)$ must be of the form $\mathrm{LM}(g)$ for some $g \in G$. Conversely, a minimal Gröbner basis can only provide these monomials. □

Remark 2.3.13. Any two minimal Gröbner bases generating the same ideal I have the same cardinality. They are minimal with respect to inclusion and also have the smallest possible cardinality. △

Definition 2.3.14. A Gröbner basis G is called **reduced** if all $g \in G$ are monic, and for $p \neq q \in G$ we have:

$$\mathrm{LM}(p) \text{ divides no monomial of } q.$$

Clearly, every reduced Gröbner basis is also minimal. △

Theorem 2.3.15. *Every ideal $I \subseteq k[\underline{x}]$ admits a unique reduced Gröbner basis (with respect to the fixed monomial ordering $\preccurlyeq$).*

Proof. Existence: Let G be a minimal Gröbner basis of I. We call an element $g \in G$ *reduced with respect to* G if no monomial of g is divisible by some $\mathrm{LM}(q)$ for $q \in G \setminus \{g\}$. Now choose and fix some $g \in G$ and compute a normal form g' of g with respect to $G \setminus \{g\}$. Then set

$$G' := (G \setminus \{g\}) \cup \{g'\}.$$

From $0 \neq g' \in I$ and $\mathrm{LM}(q) \nmid \mathrm{LM}(g')$ for all $q \in G \setminus \{g\}$ we get $\mathrm{LM}(g) = \mathrm{LM}(g')$. So G' is again a minimal Gröbner basis of I. Now g' is reduced with respect to G', since it is a normal form with respect to $G \setminus \{g\}$. Iterating this procedure, we obtain a reduced Gröbner basis.
Uniqueness: Let G, G' be two reduced Gröbner bases of I. By minimality and Lemma 2.3.12, the sets $\mathrm{LM}(G)$ and $\mathrm{LM}(G')$ coincide. For $g \in G$, let $g' \in G'$ be the unique element with $\mathrm{LM}(g) = \mathrm{LM}(g')$. Then $g - g' \in I$, and if $g - g' \neq 0$, we find $q \in G, q' \in G'$ with

$$\mathrm{LM}(q), \mathrm{LM}(q') \mid \mathrm{LM}(g - g').$$

On the other hand, $\mathrm{LM}(g-g') \prec \mathrm{LM}(g) = \mathrm{LM}(g')$, which implies $q \neq g$ and $q' \neq g'$. Since $\mathrm{LM}(g - g')$ is a monomial of either g or g', this contradicts reducedness of either G or G'. Thus $g - g' = 0$, which implies $G = G'$. □

Remark/Example 2.3.16. (i) The computation of a reduced Gröbner basis of I from a given Gröbner basis in the last proof is constructive.
(ii) Let $g_1, \ldots, g_s \in k[\underline{x}]$ be linear forms, say $g_i = \sum_{j=1}^{n} c_{ij} x_j$. Let

$$A = (c_{ij})_{i,j} \in \mathrm{M}_{s \times n}(k)$$

be the matrix of coefficients and

$$B = (b_{ij})_{i,j} \in \mathrm{M}_{s \times n}(k)$$

its reduced row-echelon form (pivots are 1, and pivotal columns are otherwise 0). Let $q_i = \sum_{j=1}^{n} b_{ij}x_j$ for $i = 1, \ldots, r(= \operatorname{rank}(A))$. If $\preccurlyeq$ is a monomial ordering with $x_1 \succ x_2 \succ \cdots \succ x_n$, then $\{q_1, \ldots, q_r\}$ is the reduced Gröbner basis of $(g_1, \ldots, g_s)$ (Exercise 56). The Buchberger Algorithm, together with the construction of reduced Gröbner bases, thus generalizes Gaussian elimination from linear algebra.
(*iii*) Let $n = 1$ and $p, q \in k[x] \setminus \{0\}$. The only minimal Gröbner basis of

$$(p, q) = (\gcd(p, q))$$

is $\{\gcd(p, q)\}$, up to scaling. The Buchberger Algorithm thus generalizes the Euclidean Algorithm for $k[x]$. △

2.4 Applications

In this section, we see how the theory of Gröbner bases gives constructive answers to the questions from the beginning of this chapter. We emphasize once more that the computation of (reduced) Gröbner bases and the division algorithm are constructive.

Application 2.4.1 (Membership in an ideal)**.** Let $p, p_1, \ldots, p_s \in k[\underline{x}]$ be given. The question whether p belongs to $I = (p_1, \ldots, p_s)$ can be solved as follows. Choose an arbitrary monomial ordering $\preccurlyeq$. Then compute a Gröbner basis $\{g_1, \ldots, g_t\}$ of I with respect to $\preccurlyeq$ and a normal form r of p modulo $g_1, \ldots, g_t$. We know that $r = \operatorname{cf}_{I,\preccurlyeq}(p)$, and thus

$$p \in I \;\Leftrightarrow\; r = 0.$$

This approach also provides a representation $p = \sum_{i=1}^{s} q_i p_i$ when $p \in I$. First, if $r = 0$ in the division algorithm, we obtain a representation

$$p = \sum_{i=1}^{t} \tilde{q}_i g_i.$$

However, in the construction of the Gröbner basis $\{g_1, \ldots, g_t\}$, we may have added some h_{ij} to the p_i (see Theorem 2.3.9). Since the $S(p_i, p_j)$ are explicit combinations of the p_i, so are the h_{ij}. After iterative substitutions, we therefore obtain an explicit representation

$$p = \sum_{i=1}^{s} q_i p_i. \qquad \triangle$$

Application 2.4.2 (Solvability of a system of polynomial equations)**.** In Corollary 1.2.13 we have seen that a system of equations

$$p_1(x) = 0, \ldots, p_s(x) = 0$$

with $p_i \in k[\underline{x}]$ has a common solution in an algebraically closed field extension of k if and only if

$$1 \notin (p_1, \ldots, p_s) \subseteq k[\underline{x}].$$

We can thus use Application 2.4.1 to decide solvability. In fact, 1 belongs to the ideal if and only if the Gröbner basis contains 1. This follows directly from the definition of a Gröbner basis. △

Application 2.4.3 (Membership in the radical)**.** Checking whether

$$p \in \sqrt{(p_1, \ldots, p_s)}$$

holds is also possible with Gröbner bases (see Exercise 59). △

Application 2.4.4 (Containment and equality of ideals)**.** One has

$$I = (p_1, \ldots, p_s) \subseteq (q_1, \ldots, q_t) = J$$

if and only if $p_i \in J$ for all i. From Application 2.4.1, we know how to check this. In particular, we can also check whether $I = J$. △

Application 2.4.5 (Elimination)**.** Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. The ideal

$$I_j := I \cap k[x_{j+1}, \ldots, x_n]$$

is called the **j-th elimination ideal of I**. Its geometric meaning was studied in Theorem 1.4.13 (ii): it defines the closure of the projection of $\mathcal{V}(I)$ onto the coordinates $x_{j+1}, \ldots, x_n$. The following theorem explains how to compute generators of I_j. △

Theorem 2.4.6. *Let G be a Gröbner basis of I with respect to the lexicographic monomial ordering with $x_1 \succ \cdots \succ x_n$. Then $G \cap k[x_{j+1}, \ldots, x_n]$ is a Gröbner basis of I_j with respect to this monomial ordering. In particular, it generates I_j.*

Proof. Let $p \in I_j$ be fixed. From $p \in I$ we know that there is some $g \in G$ with $\mathrm{LM}(g)|\mathrm{LM}(p)$. Since $x_1, \ldots, x_j$ do not appear in p, they also do not appear in $\mathrm{LM}(g)$ and thus, by the choice of the monomial ordering, not in g. Hence $g \in G \cap k[x_{j+1}, \ldots, x_n]$. □

Example 2.4.7. Consider

$$I = \left(x^2 + y + z - 1, y^2 + x + z - 1, z^2 + x + y - 1\right) \subseteq k[x, y, z].$$

The reduced Gröbner basis of I with respect to the lexicographic monomial ordering with $x \succ y \succ z$ consists of the following four polynomials:

$$\begin{aligned} g_1 &= x + y + z^2 - 1 \\ g_2 &= y^2 - y - z^2 + z \\ g_3 &= 2yz^2 + z^4 - z^2 \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1). \end{aligned}$$

Thus

$$I \cap k[y, z] = (g_2, g_3, g_4)$$

and

$$I \cap k[z] = (g_4).$$

In particular, the projection of $\mathcal{V}(I)$ onto the third coordinate consists of $0, 1$ and $-1 \pm \sqrt{2}$. △

Application 2.4.8 (Finite varieties)**.** Let $I \subseteq k[\underline{x}]$ be an ideal. We can check whether $\mathcal{V}(I)$ is finite, i.e. whether I is a 0-dimensional ideal (see Theorem 1.4.16). To this end, we compute generators for the ideals $I \cap k[x_i]$, as demonstrated in Theorem 2.4.6. We then simply check whether $I \cap k[x_i] \neq \{0\}$ holds for all i. If this is true, consider $M_i := \mathcal{V}(I \cap k[x_i]) \subseteq \mathbb{A}^1$. Then

$$\mathcal{V}(I) \subseteq M_1 \times \cdots \times M_n,$$

and we can directly check the finitely many elements of $M_1 \times \cdots \times M_n$ for membership in $\mathcal{V}(I)$. △

Example 2.4.9. With the equations from Example 2.4.7, we obtain

$$I \cap k[x] = (g_4(x)),\ I \cap k[y] = (g_4(y)) \text{ and } I \cap k[z] = (g_4(z)).$$

Thus $\mathcal{V}(I)$ is indeed finite and contained in

$$\{0, 1, -1 \pm \sqrt{2}\}^3 \subseteq K^3.$$

We then find

$$\mathcal{V}(I) = \left\{ (-1 \pm \sqrt{2}) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}. \qquad \triangle$$

Application 2.4.10 (Inverse images of ideals)**.** Let $\varphi\colon k[\underline{x}] \to k[\underline{y}]$ be a homomorphism of k-algebras, given by $\varphi(x_i) = p_i \in k[\underline{y}]$ for $i = 1, \ldots, n$. Let $J = (g_1, \ldots, g_s) \subseteq k[\underline{y}]$ be an ideal. We want to compute generators for $\varphi^{-1}(J)$; see Theorem 1.4.13 for the geometric interpretation. The following theorem shows how to reduce this to elimination. △

Theorem 2.4.11. *Let* $\tilde{J} := (x_1 - p_1, \ldots, x_n - p_n, g_1, \ldots, g_s) \subseteq k[\underline{x}, \underline{y}]$. *Then*

$$\varphi^{-1}(J) = \tilde{J} \cap k[\underline{x}].$$

Proof. For every commutative ring R and $a \in R^m$, the evaluation map

$$\begin{aligned} R[z_1, \ldots, z_m] &\to R \\ p &\mapsto p(a_1, \ldots, a_m) \end{aligned}$$

has kernel $(z_1 - a_1, \ldots, z_m - a_m)$. This is easiest to see when $a = 0$; the general case follows by a linear change of variables. Thus the homomorphism

$$\begin{aligned} \psi\colon k[\underline{x}, \underline{y}] &\to k[\underline{y}] \\ x_i &\mapsto p_i \\ y_i &\mapsto y_i \end{aligned}$$

has kernel $(x_1 - p_1, \ldots, x_n - p_n)$. We also have $\psi = \varphi$ on $k[\underline{x}]$. This implies

$$\varphi^{-1}(J) = \psi^{-1}(J) \cap k[\underline{x}],$$

and the claim now follows from the following identity in $k[\underline{x}, \underline{y}]$:

$$\psi^{-1}(J) = (g_1, \ldots, g_s) + \ker(\psi).$$

Here "$\supseteq$" is obvious. For "$\subseteq$", we use that for all $p \in k[\underline{x}, \underline{y}]$ we have

$$\psi(p - \psi(p)) = \psi(p) - \psi(p) = 0.$$

Thus $p \in \psi^{-1}(J)$ implies

$$p = \underbrace{\psi(p)}_{\in J} + \underbrace{(p - \psi(p))}_{\in \ker(\psi)} \in (g_1, \ldots, g_s) + \ker(\psi). \qquad \square$$

Example 2.4.12. Consider the following morphism of varieties:

$$\begin{aligned} p\colon \mathbb{A}^2 &\to \mathbb{A}^3 \\ (a,b) &\mapsto (ab, ab^2, a^2). \end{aligned}$$

On coordinate rings, it corresponds to the following homomorphism:

$$\begin{aligned} p^*\colon k[x,y,z] &\to k[u,v] \\ x &\mapsto uv \\ y &\mapsto uv^2 \\ z &\mapsto u^2. \end{aligned}$$

With the method described above, we can compute

$$\ker(p^*) = (x^4 - y^2 z).$$

By Theorem 1.4.13 we thus have

$$\overline{p(\mathbb{A}^2)} = \mathcal{V}(x^4 - y^2 z).$$

We see that the full y-axis is contained in $\overline{p(\mathbb{A}^2)}$, while the image of p contains only the point $(0,0,0)$ on this axis. △

Application 2.4.13 (Intersection of ideals)**.** Let $I = (p_1, \ldots, p_s)$ and $J = (q_1, \ldots, q_r)$ be ideals in $k[\underline{x}]$. Generators for the product IJ are easy to find: just take the pairwise products $p_i q_j$. It is harder to compute generators for the intersection $I \cap J$. The following theorem shows how to do this with elimination (already settled in Application 2.4.5). △

Theorem 2.4.14. *Let t be a new variable and let Q be the ideal generated by*

$$tp_1, \ldots, tp_s, (1-t)q_1, \ldots, (1-t)q_r$$

in $k[\underline{x}, t]$. Then

$$I \cap J = Q \cap k[\underline{x}].$$

Proof. For "$\subseteq$" let $p \in I \cap J$. From $p = tp + (1-t)p$ we get $p \in Q$.
For "$\supseteq$" let

$$k[\underline{x}] \ni p = t \sum_i h_i p_i + (1-t) \sum_j g_j q_j \in Q,$$

where $h_i, g_j \in k[\underline{x}, t]$. Substituting $t = 0$ gives $p \in J$, and substituting $t = 1$ gives $p \in I$. □

Application 2.4.15 (Homogenization of an ideal)**.** For $I \subseteq k[x_1, \ldots, x_n]$ we let

$$I^h = \left(p^h \mid p \in I\right) \subseteq k[x_0, \ldots, x_n]$$

be its homogenization (see Theorem 3.3.18 for the geometric interpretation). If $I = (p_1, \ldots, p_s)$, then in general we have

$$\left(p_1^h, \ldots, p_s^h\right) \subsetneq I^h,$$

see Remark 3.3.19. We now want to compute generators for I^h. To this end, we call a monomial ordering $\preccurlyeq$ **degree compatible** if

$$|\alpha| < |\beta| \Rightarrow \alpha \prec \beta$$

for all $\alpha, \beta \in \mathbb{N}^n$. For example, the graded-lexicographic monomial ordering is degree compatible. The following theorem shows how to compute generators for I^h. △

Theorem 2.4.16. *Let $\preccurlyeq$ be a degree compatible monomial ordering on $\mathbb{N}^n$ and let G be a Gröbner basis of the ideal $I \subseteq k[x_1, \ldots, x_n]$ with respect to $\preccurlyeq$. Then in $k[x_0, \ldots, x_n]$ we have*

$$I^h = \left(g^h \mid g \in G\right).$$

Proof. On $k[x_0, \ldots, x_n]$ we define a monomial ordering by

$$x_0^r \cdot \underline{x}^\alpha \preccurlyeq' x_0^s \underline{x}^\beta :\Leftrightarrow \underline{x}^\alpha \prec \underline{x}^\beta \text{ or } (\alpha = \beta \text{ and } r \leqslant s).$$

Let $G^h = \left\{g^h \mid g \in G\right\}$. We show that G^h is even a Gröbner basis of I^h with respect to $\preccurlyeq'$; this implies the statement.
For $0 \neq p \in k[x_1, \ldots, x_n]$ we have

$$\deg\left(\mathrm{LM}_\preccurlyeq(p)\right) = \deg(p),$$

by degree compatibility of $\preccurlyeq$. This immediately implies

$$\mathrm{LM}_{\preccurlyeq'}(p^h) = \mathrm{LM}_\preccurlyeq(p)$$

for all $p \in k[x_1, \ldots, x_n]$. By Lemma 3.3.16 (i), every homogeneous $q \in I^h$ is of the form

$$q = x_0^r \cdot p^h$$

for some $p \in I$. Thus

$$\mathrm{LM}_{\preccurlyeq'}(q) = x_0^r \cdot \mathrm{LM}_{\preccurlyeq'}(p^h).$$

Since G is a Gröbner basis of I, there exists some $g \in G$ with

$$\mathrm{LM}_{\preccurlyeq'}(g^h) = \mathrm{LM}_\preccurlyeq(g) \mid \mathrm{LM}_\preccurlyeq(p) = \mathrm{LM}_{\preccurlyeq'}(p^h).$$

This implies $\mathrm{LM}_{\preccurlyeq'}(g^h) | \mathrm{LM}_{\preccurlyeq'}(q)$, as required. □

Chapter 3

Projective Varieties

3.1 Projective Spaces

Definition 3.1.1. Let K be a field and V a K-vector space.
(i) The **projective space** $\mathbb{P}(V)$ is the set of all one-dimensional K-subspaces of V.
(ii) The **dimension** of a projective space is defined as

$$\dim \mathbb{P}(V) := \dim_K(V) - 1.$$

(iii) If $W \subseteq V$ is a K-subspace, then $\mathbb{P}(W)$ is called a **linear** or **projective subspace** of $\mathbb{P}(V)$. Linear subspaces of $\mathbb{P}(V)$ of dimension $0, 1, 2$, and $\dim \mathbb{P}(V) - 1$ are called **(projective) points, lines, planes**, and **hyperplanes**, respectively.
(iv) We write

$$\mathbb{P}^n(K) := \mathbb{P}(K^{n+1})$$

and call $\mathbb{P}^n(K)$ the n**-dimensional projective space over** K. △

The elements of $\mathbb{P}(V)$ are the sets $[v] = K \cdot v$ for $0 \neq v \in V$. Thus two nonzero vectors define the same point precisely when they differ by a nonzero scalar:

$$[v] = [w] \Leftrightarrow \exists c \in K^* \quad v = cw.$$

Definition 3.1.2. Elements of $\mathbb{P}^n(K)$ are usually written in **homogeneous coordinates**. For $0 \neq (a_0, \ldots, a_n) \in K^{n+1}$ we write

$$(a_0 : \ldots : a_n) := [(a_0, \ldots, a_n)] = K \cdot (a_0, \ldots, a_n) \in \mathbb{P}^n(K).$$

The colon notation indicates that we mean not the vector itself, but the line spanned by it. In particular, $(0 : \ldots : 0)$ is *not defined*. We have

$$(a_0 : \ldots : a_n) = (b_0 : \ldots : b_n) \Leftrightarrow \exists c \in K^* \quad a_i = cb_i \text{ for } i = 0, \ldots, n.$$

Equivalently, one may check equality by the equations

$$(a_0 : \ldots : a_n) = (b_0 : \ldots : b_n) \Leftrightarrow a_i b_j = a_j b_i \text{ for all } i, j = 0, \ldots, n.$$

Indeed, two nonzero vectors $(a_0, \ldots, a_n)$ and $(b_0, \ldots, b_n)$ are collinear if and only if the matrix

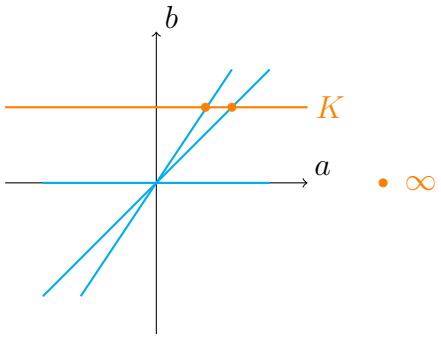
$$\begin{pmatrix} a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_n \end{pmatrix}$$

has rank 1, i.e. if and only if all its 2×2-minors vanish. △

Example 3.1.3. (i) $\mathbb{P}^0(K)$ consists of exactly one point.
(ii) $\mathbb{P}^1(K)$ can be identified with $K \cup \{\infty\}$ via

$$\begin{aligned} \mathbb{P}^1(K) &\to K \cup \{\infty\} \\ (a : b) &\mapsto a/b \text{ if } b \neq 0 \\ (a : 0) &\mapsto \infty. \end{aligned}$$

Geometrically this corresponds to intersecting lines through the origin in K^2 with the line $b = 1$. Every line through the origin corresponds to exactly one point on the line $b = 1$, except for the line $b = 0$, which corresponds to ∞.



(iii) As a set, $\mathbb{P}^n(\mathbb{R})$ can be identified with $S^n/\sim$, where S^n is the unit sphere in $\mathbb{R}^{n+1}$ and $a \sim -a$ for all $a \in S^n$. In differential-geometric terms, this is a compact smooth manifold of dimension n; for $n \geqslant 2$ it is non-orientable.

(iv) $\emptyset$ and $\mathbb{P}(V)$ are linear subspaces of $\mathbb{P}(V)$. We have $\dim \emptyset = -1$ because $\emptyset = \mathbb{P}(\{0\})$. Every intersection of linear subspaces is again a linear subspace:

$$\bigcap_i \mathbb{P}(W_i) = \mathbb{P}\left(\bigcap_i W_i\right).$$

A line in $\mathbb{P}(V)$ is of the form $\mathbb{P}(W)$ for a 2-dimensional subspace $W \subseteq V$. △

Theorem 3.1.4. *Let $U_1 = \mathbb{P}(W_1)$ and $U_2 = \mathbb{P}(W_2)$ be linear subspaces of $\mathbb{P}(V)$. Then*

$$\dim U_1 + \dim U_2 = \dim(U_1 \cap U_2) + \dim \mathbb{P}(W_1 + W_2).$$

In particular, $\dim U_1 + \dim U_2 \geqslant \dim \mathbb{P}(V)$ already implies $U_1 \cap U_2 \neq \emptyset$. Hence any two lines in $\mathbb{P}^2(K)$ intersect.

Proof. This follows immediately from the dimension formula for vector spaces

$$\dim_K W_1 + \dim_K W_2 = \dim_K(W_1 \cap W_2) + \dim_K(W_1 + W_2)$$

after subtracting 2 from both sides. □

Definition 3.1.5. Let $f\colon V \hookrightarrow W$ be an injective linear map. Then

$$\begin{aligned} \mathbb{P}(f)\colon \mathbb{P}(V) &\to \mathbb{P}(W) \\ [v] &\mapsto [f(v)] \end{aligned}$$

is well defined. If f is bijective, then $\mathbb{P}(f)^{-1} = \mathbb{P}(f^{-1})$ and $\mathbb{P}(f)$ is called a **projectivity from $\mathbb{P}(V)$ to $\mathbb{P}(W)$.** △

Theorem 3.1.6. *The projectivities from $\mathbb{P}(V)$ to itself form a group isomorphic to*

$$\mathrm{PGL}(V) := \mathrm{GL}(V)/\left(K^* \cdot \mathrm{id}_V\right).$$

Proof. Let P be the group of projectivities. Consider the group homomorphism

$$\begin{aligned} \mathrm{GL}(V) &\twoheadrightarrow P \\ f &\mapsto \mathbb{P}(f). \end{aligned}$$

The kernel consists of those $f \in \mathrm{GL}(V)$ for which every vector is an eigenvector. It is well-known that these are precisely the multiples of the identity (see Exercise 64). □

Example 3.1.7. For $f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ we have

$$\mathbb{P}(f)\colon (x : y) \mapsto (ax + by : cx + dy).$$

Under the identification $\mathbb{P}^1(K) = K \cup \{\infty\}$ from Example 3.1.3 (ii), this becomes the map

$$r \mapsto \frac{ar + b}{cr + d},$$

with the usual convention that a zero denominator gives the value ∞, and that ∞ maps to a/c if $c \neq 0$ and to ∞ if $c = 0$. This is called a **Möbius transformation** of the line. △

Construction 3.1.8. In $\mathbb{P}^n(K)$ the set

$$H := \{(a_0 : \ldots : a_n) \mid a_0 = 0\}$$

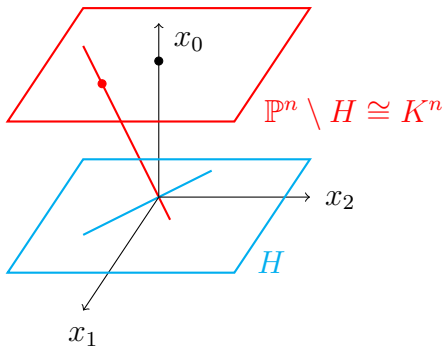
is a hyperplane; in particular, $H \cong \mathbb{P}^{n-1}(K)$. Its complement is naturally identified with affine n-space by the bijection

$$\begin{aligned} \mathbb{P}^n(K) \setminus H &\leftrightarrow K^n \\ (a_0 : \ldots : a_n) &\mapsto \left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \\ (1 : b_1 : \ldots : b_n) &\leftarrow\!\shortmid (b_1, \ldots, b_n). \end{aligned}$$

More generally, for every hyperplane $W \subseteq V$ and every fixed $v \in V \setminus W$, there is a bijection

$$\begin{aligned} W &\to \mathbb{P}(V) \setminus \mathbb{P}(W) \\ w &\mapsto [v + w] \end{aligned}$$

(see Exercise 65). Thus $\mathbb{P}(V)$ is obtained from an affine copy of W by adjoining the projective space $\mathbb{P}(W)$. The points in $\mathbb{P}(W)$ are the **points at infinity** with respect to this affine chart.



△

3.2 Graded Rings

In this section we discuss the algebra underlying projective spaces. For this purpose, always let $(G, +, 0)$ be an abelian group.

Definition 3.2.1. (i) A G**-graded ring** is a ring R together with additive subgroups $R_g \subseteq R$ for every $g \in G$, such that

$$R = \bigoplus_{g \in G} R_g$$

$$\text{and } R_g \cdot R_h \subseteq R_{g+h}$$

for all $g, h \in G$.
(ii) An element $a \in R$ is called **homogeneous** if $a \in R_g$ for some $g \in G$. If $a \neq 0$, we call $\deg(a) := g$ the **degree** of a. We set $\deg(0) := -\infty$.
(iii) Every element $a \in R$ has a unique decomposition

$$a = \sum_{g \in G} a_g,$$

where a_g is homogeneous of degree g, and only finitely many a_g are nonzero. With this notation, a_g is called the **homogeneous component of degree** g **of** a.
(iv) If R, S are two G-graded rings, then a ring homomorphism $\varphi\colon R \to S$ is called **graded** if

$$\varphi(R_g) \subseteq S_g$$

holds for all $g \in G$. △

Example 3.2.2. (i) Every ring R can be trivially G-graded by $R_0 := R$ and $R_g := \{0\}$ for $g \neq 0$.
(ii) On $R = k[\underline{x}]$ a $\mathbb{Z}$-grading is uniquely defined by

$$k \subseteq R_0 \text{ and } \deg(x_i) = 1.$$

Here R_d consists precisely of the polynomials

$$p = \sum_{|\alpha| = d} p_\alpha \underline{x}^\alpha,$$

and $R_d = \{0\}$ for $d < 0$. This grading is also called the **standard grading** of $k[\underline{x}]$.
(iii) More generally, we can prescribe $k \subseteq R_0$ and $\deg(x_i) = d_i \in \mathbb{Z}$, and obtain a unique such grading on $R = k[\underline{x}]$, called a **weighted degree-grading**.
(iv) For $R = k[\underline{x}]$ there is for instance also the $\mathbb{Z}^n$-grading with $R_\alpha = k \cdot \underline{x}^\alpha$ for $\alpha \in \mathbb{N}^n$ and $R_\beta = \{0\}$ for $\beta \in \mathbb{Z}^n \setminus \mathbb{N}^n$. △

Lemma 3.2.3. *For every G-graded ring R we have $1 \in R_0$, and R_0 is a subring of R.*

Proof. Write

$$1 = \sum_{g \in G} e_g$$

with $e_g \in R_g$. For homogeneous $a \in R_h$ we then have

$$a = 1 \cdot a = \sum_g e_g a$$

and from $e_g a \in R_{g+h}$ it follows that $e_0 a = a$ holds. Here we used the uniqueness of the decomposition into homogeneous summands. This implies $e_0 a = a$ for all $a \in R$, and hence $e_0 = 1$. □

Remark 3.2.4. In graded rings, computations are sometimes easier than in ungraded rings. For example, we will often use the following fact: If

$$a = \sum_i b_i c_i$$

and both a and all c_i are homogeneous, then the b_i can be assumed to be homogeneous as well, with

$$\deg(b_i) = \deg(a) - \deg(c_i).$$

Indeed, we can replace each b_i by its homogeneous component of degree $\deg(a) - \deg(c_i)$ and the equation will still hold. △

Lemma 3.2.5. *Let R be a G-graded ring and $I \subseteq R$ an ideal. Then the following conditions on I are equivalent:*

(i) $a \in I \Rightarrow a_g \in I$ *for all* $g \in G$

(ii) $I = \bigoplus_{g \in G} (I \cap R_g)$

(iii) I *is generated by homogeneous elements.*

Proof. Exercise 67. □

Definition 3.2.6. An ideal I satisfying the conditions in Lemma 3.2.5 is called a **homogeneous ideal**. △

Example 3.2.7. (i) Let $\varphi\colon R \to S$ be a graded homomorphism. Then $\ker(\varphi)$ is a homogeneous ideal. More generally, $\varphi^{-1}(J)$ is a homogeneous ideal for every homogeneous ideal $J \subseteq S$.
(ii) If R is $\mathbb{Z}$-graded with $R_d = \{0\}$ for $d < 0$, then

$$R_+ = \bigoplus_{d \geqslant 1} R_d$$

is a homogeneous ideal. It is called the **irrelevant ideal**. If the ring R_0 is a field, then every proper homogeneous ideal is contained in R_+. In order to make the set of proper homogeneous ideals have several maximal elements, R_+ is often disregarded.
(iii) With respect to the grading in Example 3.2.2 (iv), the homogeneous ideals are precisely the ideals generated by monomials (cf. Definition 2.1.2). △

Lemma 3.2.8. *Let R be a G-graded ring.*
(i) Sums, products, and intersections of homogeneous ideals in R are again homogeneous.
(ii) If I is a homogeneous ideal, then R/I becomes G-graded via the grading

$$(R/I)_g := R_g/I$$

for $g \in G$.

Proof. (i) is clear, for example using property (i) in Lemma 3.2.5. For (ii), first note that the R_g/I are additive subgroups of R/I. It is also clear that $R_g/I \cdot R_h/I \subseteq R_{g+h}/I$ and that $R/I = \sum_g R_g/I$. It remains to show that the sum is direct. So let $a_g \in R_g$ such that

$$\sum_g \overline{a}_g = 0 \text{ in } R/I.$$

This means $\sum_g a_g \in I$, and from the homogeneity of I it follows that $a_g \in I$ for all g. Hence $\overline{a}_g = 0$ for all g. □

Remark 3.2.9. Let I be a homogeneous ideal of the graded ring R, and equip R/I with the grading just introduced. Then the homogeneous ideals of R/I correspond exactly to the homogeneous ideals J of R with $I \subseteq J$. △

From now on we assume that G is an **ordered abelian group**, i.e. that there is a total ordering $\leqslant$ on G such that

$$a \leqslant b \Rightarrow a + c \leqslant b + c$$

for all $a, b, c \in G$. In practice, we will almost always have $G = \mathbb{Z}$, where such an ordering exists. From now on, our ring R is always G-graded.

Lemma 3.2.10. *Let I be a proper homogeneous ideal in R. Then I is a prime ideal if and only if for all homogeneous $a, b \in R$ we have*

$$ab \in I \Rightarrow a \in I \text{ or } b \in I.$$

Proof. One implication is trivial. Now let $a, b \in R$, not necessarily homogeneous, with $a, b \notin I$. Further, let $g, h \in G$ be maximal indices with respect to $\leqslant$ such that $a_g \notin I$ and $b_h \notin I$. Then

$$(ab)_{g+h} = a_g b_h + \underbrace{\cdots}_{\in I}$$

because for $g' \neq g, h' \neq h$ with $g' + h' = g + h$, either $g < g'$ or $h < h'$ must hold. By assumption, $a_g b_h \notin I$, and hence also $(ab)_{g+h} \notin I$. Since I is homogeneous, we obtain $ab \notin I$. □

Lemma 3.2.11. *All minimal prime ideals over the homogeneous ideal I are also homogeneous.*

Proof. Exercise 69. □

Corollary 3.2.12. *For every homogeneous ideal I of R, the radical $\sqrt{I}$ is the intersection of all homogeneous prime ideals over I. In particular, $\sqrt{I}$ is itself homogeneous.*

Lemma 3.2.13. *Let R be a G-graded ring and $M \subseteq R$ a multiplicative subset consisting of homogeneous elements. Then the localization $M^{-1}R$ becomes a G-graded ring via the grading*

$$(M^{-1}R)_g := \left\{ \frac{a}{m} \mid m \in M, a \in R_{\deg(m)+g} \right\}.$$

Proof. Clearly $(M^{-1}R)_g$ is an additive subgroup of $M^{-1}R$, and we have $(M^{-1}R)_g \cdot (M^{-1}R)_h \subseteq (M^{-1}R)_{g+h}$ as well as

$$M^{-1}R = \sum_g (M^{-1}R)_g.$$

It remains to show that the sum is direct. So let

$$0 = \sum_g \frac{a_g}{m_g} = \frac{\sum_g a_g \prod_{h \neq g} m_h}{\prod_h m_h} \text{ in } M^{-1}R$$

be a finite sum with $a_g \in R$ homogeneous, $m_g \in M$, and

$$\deg(a_g) = \deg(m_g) + g.$$

Then there is an $m \in M$ such that

$$m \cdot \left(\sum_g a_g \prod_{h \neq g} m_h \right) = 0 \text{ in } R.$$

Here the summand with index g is homogeneous of degree

$$\deg(m) + g + \deg \left(\prod_h m_h \right).$$

Since these degrees are distinct for distinct g, it follows that

$$m \cdot a_g \cdot \prod_{h \neq g} m_h = 0$$

for all g, and this implies $\frac{a_g}{m_g} = 0$ in $M^{-1}R$ for all g. □

Definition 3.2.14. Let M be a multiplicative set consisting of homogeneous elements in R. The subring

$$R_{(M)} := (M^{-1}R)_0 = \left\{ \frac{a}{m} \mid a \in R_{\deg(m)} \right\}$$

of the localization $M^{-1}R$ is called the **homogeneous localization with respect to** M. We will see its geometric interpretation, for example, in Theorem 4.1.20 below. △

Example 3.2.15. (*i*) Let $m \in R$ be homogeneous of degree $g \in G$. Set $M = \{1, m, m^2, \ldots\}$ and write

$$R_{(m)} = R_{(M)} = \left\{ \frac{a}{m^r} \mid a \in R_{r \cdot g} \right\}.$$

(*ii*) Let $\mathfrak{p} \subseteq R$ be a homogeneous prime ideal, and M the set of all *homogeneous* elements in $R \setminus \mathfrak{p}$. Then M is a multiplicative set and we call

$$R_{(\mathfrak{p})} := R_{(M)} = \left\{ \frac{a}{m} \mid a, m \in R \text{ homogeneous }, m \notin \mathfrak{p}, \deg(a) = \deg(m) \right\}$$

the **homogeneous localization of** R **in** $\mathfrak{p}$.
(*iii*) Note that there is a natural homomorphism $R \to M^{-1}R$, but in general there is no such homomorphism from R to $R_{(M)}$. △

3.3 Projective Algebraic Varieties

Again let k be an arbitrary field and let K be an algebraically closed extension field. We write

$$\mathbb{P}^n := \mathbb{P}^n(K) = \mathbb{P}(K^{n+1}).$$

Note that, in the sense of Definition 3.1.1, we regard K^{n+1} as a K-vector space, not as a k-vector space. Thus elements of $\mathbb{P}^n$ are one-dimensional K-subspaces of K^{n+1}. From now on, set $\underline{x} = (x_0, \ldots, x_n)$ and always equip $k[\underline{x}]$ with the standard grading. For *homogeneous* $p \in k[\underline{x}]$, $v \in K^{n+1}$, and $\lambda \in K$, we have

$$p(\lambda \cdot v) = \lambda^{\deg(p)} \cdot p(v).$$

Thus if a homogeneous polynomial vanishes at a point, it vanishes on the entire line spanned by that point. Hence, for $a = [v] \in \mathbb{P}^n$, the equation

$$p(a) = 0 \ :\Leftrightarrow \ p(v) = 0$$

is well defined. Similarly, we write $p(a) \neq 0$ if $p(v) \neq 0$. For arbitrary $p \in k[\underline{x}]$, write

$$p = p_0 + p_1 + \cdots + p_d$$

with homogeneous $p_i \in k[\underline{x}]_i$ and define

$$p(a) = 0 \ :\Leftrightarrow \ p_0(a) = p_1(a) = \cdots = p_d(a) = 0.$$

Because

$$p(\lambda \cdot v) = p_0(v) + \lambda \cdot p_1(v) + \lambda^2 \cdot p_2(v) + \cdots + \lambda^d \cdot p_d(v),$$

this is equivalent to

$$p(\lambda v) = 0 \text{ for all } \lambda \in K,$$

i.e. p vanishes on the entire line spanned by v.

Definition 3.3.1. Let $P \subseteq k[\underline{x}]$ and $\emptyset \neq V \subseteq \mathbb{P}^n$.
(i) We define

$$\mathcal{V}_+(P) = \{a \in \mathbb{P}^n \mid p(a) = 0 \text{ for all } p \in P\}$$

and

$$\mathcal{I}_+(V) := \{p \in k[\underline{x}] \mid p(a) = 0 \text{ for all } a \in V\}.$$

We call $\mathcal{V}_+(P)$ the **projective variety** defined by P, and $\mathcal{I}_+(V)$ the **vanishing ideal** of V.
(ii) A set of the form $\mathcal{V}_+(P)$ with $P \subseteq k[\underline{x}]$ is called a **projective k-variety**.
(iii) We set

$$\widehat{V} := \bigcup_{a \in V} a = \left\{ v \in K^{n+1} \mid v \neq 0, [v] \in V \right\} \cup \{0\}$$

and call $\widehat{V}$ the **affine cone over** V.
(iv) We set

$$\mathcal{I}_+(\emptyset) := (x_0, \ldots, x_n)$$

(the irrelevant ideal) and

$$\widehat{\emptyset} := \{0\}.$$

(v) For homogeneous $p \in k[\underline{x}]$ let

$$\mathcal{D}_+(p) := \{a \in \mathbb{P}^n \mid p(a) \neq 0\} = \mathbb{P}^n \setminus \mathcal{V}_+(p). \qquad \triangle$$

Remark 3.3.2. (i) For arbitrary $V \subseteq \mathbb{P}^n$ we have

$$\mathcal{I}_+(V) = \mathcal{I}(\widehat{V}).$$

In particular, $\mathcal{I}_+(V)$ is a radical ideal. On the other hand, by the definition of "$p(a) = 0$", the ideal $\mathcal{I}_+(V)$ is also homogeneous.
(ii) For $M \subseteq k[\underline{x}]$, let M_h be the set of all homogeneous components of elements in M, and let $I = (M_h)$ be the ideal generated by this set. Then

$$\mathcal{V}_+(M) = \mathcal{V}_+(M_h) = \mathcal{V}_+(I) = \mathcal{V}_+\left(\sqrt{I}\right).$$

(iii) We have

$$\mathcal{V}_+\left(k[\underline{x}]\right) = \mathcal{V}_+((x_0, \ldots, x_n)) = \emptyset$$

and

$$\mathcal{V}_+(0) = \mathbb{P}^n.$$

For homogeneous ideals I, J, I_λ $(\lambda \in \Lambda)$ we have

$$\mathcal{V}_+(I) \cup \mathcal{V}_+(J) = \mathcal{V}_+(I \cap J) = \mathcal{V}_+(IJ)$$

and

$$\bigcap_{\lambda \in \Lambda} \mathcal{V}_+(I_\lambda) = \mathcal{V}_+\left(\sum_{\lambda \in \Lambda} I_\lambda\right).$$

(iv) For arbitrary subsets $V_\lambda \subseteq \mathbb{P}^n$ ($\lambda \in \Lambda$) we have

$$\widehat{\bigcup_\lambda V_\lambda} = \bigcup_\lambda \widehat{V}_\lambda \text{ and } \widehat{\bigcap_\lambda V_\lambda} = \bigcap_\lambda \widehat{V}_\lambda.$$

(v) If $I \subsetneq k[\underline{x}]$ is a *homogeneous* ideal, then

$$\widehat{\mathcal{V}_+(I)} = \mathcal{V}(I) \subseteq \mathbb{A}^{n+1}.$$

This is because for every point $v \in \mathcal{V}(I)$ we have $[v] \subseteq \mathcal{V}(I)$, since I is generated by homogeneous elements. Note that this is not true for $I = k[\underline{x}]$, because $\widehat{\emptyset} = \{0\} \neq \emptyset$. For $I = (x_0, \ldots, x_n)$, however, it is true. The statement is also false for non-homogeneous ideals. For instance, by definition we have

$$\mathcal{V}_+(x_0 - 1) = \emptyset \subseteq \mathbb{P}^1, \quad \widehat{\mathcal{V}_+(x_0 - 1)} = \{0\}, \quad \mathcal{V}(x_0 - 1) = \{(1, r) \mid r \in K\} \subseteq \mathbb{A}^2. \qquad \triangle$$

Definition 3.3.3. The **k-Zariski topology on** $\mathbb{P}^n$ is the topology whose closed sets are the projective k-varieties. By Remark 3.3.2 (iii), this is indeed a topology. $\triangle$

Lemma 3.3.4. *(i) A subset $V \subseteq \mathbb{P}^n$ is closed if and only if $\widehat{V} \subseteq \mathbb{A}^{n+1}$ is closed.*
(ii) The k-Zariski topology on $\mathbb{P}^n$ is noetherian.

Proof. For (i), first let $V = \mathcal{V}_+(I)$ for a homogeneous ideal $I \neq 1$ (cf. Remark 3.3.2 (ii)). Then by Remark 3.3.2 (v) we have $\widehat{V} = \mathcal{V}(I)$, which is closed in $\mathbb{A}^{n+1}$. Conversely, let $\widehat{V} \subseteq \mathbb{A}^{n+1}$ be closed. Then $I := \mathcal{I}(\widehat{V})$ is a homogeneous ideal $\neq 1$, because $\widehat{V}$ is nonempty and a union of lines through the origin. For $W := \mathcal{V}_+(I)$ we then have

$$\widehat{W} = \mathcal{V}(I) = \widehat{V},$$

where the last equality uses the closedness of $\widehat{V}$. Hence $V = W = \mathcal{V}_+(I)$ is closed.
For (ii), let

$$V_0 \supseteq V_1 \supseteq \cdots$$

be a descending chain of closed sets in $\mathbb{P}^n$. Then

$$\widehat{V}_0 \supseteq \widehat{V}_1 \supseteq \cdots$$

is a descending chain of closed sets in $\mathbb{A}^{n+1}$. This chain becomes stationary, and therefore the original chain does as well. $\square$

Theorem 3.3.5. *Let $I \neq 1$ be a homogeneous ideal in $k[\underline{x}]$, and let $V \subseteq \mathbb{P}^n$ be a subset. Then we have*

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

(ii) $\mathcal{V}_+(\mathcal{I}_+(V)) = \overline{V}$.

(iii) $V \mapsto \mathcal{I}_+(V)$ *is a bijection between the closed subsets of $\mathbb{P}^n$ and the homogeneous radical ideals $\neq 1$ in $k[\underline{x}]$. The inverse map is given by $I \mapsto \mathcal{V}_+(I)$.*

Proof. (i) follows from

$$\mathcal{I}_+(\mathcal{V}_+(I)) = \mathcal{I}(\widehat{\mathcal{V}_+(I)}) = \mathcal{I}(\mathcal{V}(I)) = \sqrt{I},$$

where we use Remark 3.3.2 and Theorem 1.2.14. Statement (ii) follows immediately from the definition of the Zariski topology, because $\mathcal{V}_+(\mathcal{I}_+(V))$ is the smallest closed superset of V. Finally, (iii) follows from (i) and (ii). □

Remark 3.3.6. In the affine case, the empty variety is defined precisely by the ideal $I = (1)$ and by no other ideal (cf. Theorem 1.2.11). In projective space, $\emptyset$ arises either from a homogeneous system of equations that is already unsolvable in $\mathbb{A}^{n+1}$, i.e. from the trivial homogeneous radical ideal $k[\underline{x}]$, or from a homogeneous system that defines $\{0\}$ in $\mathbb{A}^{n+1}$, for example from the irrelevant ideal $k[\underline{x}]_+$. Both are homogeneous radical ideals, and in Theorem 3.3.5 we have chosen $k[\underline{x}]_+$.
The not necessarily radical homogeneous ideals that define $\emptyset \subseteq \mathbb{P}^n$ can be described even more precisely. To do this, we consider the **ideal quotient**

$$(I : J) = \{a \in A \mid aJ \subseteq I\},$$

and define

$$(I : J^\infty) := \bigcup_{d=0}^{\infty} (I : J^d).$$

Since $(I : J^\infty)$ is the union of the ascending chain

$$I \subseteq (I : J) \subseteq (I : J^2) \subseteq \cdots,$$

it is again an ideal. It is called the **saturation of I with respect to J**. △

Theorem 3.3.7. *Let $I \subseteq k[\underline{x}]$ be a homogeneous ideal and $\mathfrak{m} = (x_0, \ldots, x_n)$ the irrelevant ideal. Then the following are equivalent:*

(i) $\mathcal{V}_+(I) = \emptyset$

(ii) $\mathfrak{m}^d \subseteq I$ *for some* $d \geqslant 0$

(iii) $(I : \mathfrak{m}^\infty) = (1)$

(iv) $k[\underline{x}]_d \subseteq I$ *for some* $d \geqslant 0$.

Proof. We have $(I : \mathfrak{m}^\infty) = \bigcup_{d \geqslant 0}(I : \mathfrak{m}^d)$ and therefore

$$(I : \mathfrak{m}^\infty) = (1) \Leftrightarrow 1 \in (I : \mathfrak{m}^d) \text{ for some } d \geqslant 0 \Leftrightarrow \mathfrak{m}^d \subseteq I \text{ for some } d \geqslant 0.$$

This shows the equivalence of (ii) and (iii). For $(i)\Rightarrow(ii)$, let $V = \mathcal{V}_+(I) = \emptyset$ and $I \neq 1$. From Theorem 3.3.5 it follows that

$$\mathfrak{m} = \mathcal{I}_+(V) = \sqrt{I},$$

and in particular $x_i^r \in I$ for all i and some r. This implies $\mathfrak{m}^{r(n+1)} \subseteq I$, as is easily verified. The implication $(ii)\Rightarrow(iv)$ follows immediately from

$$k[\underline{x}]_d \subseteq \mathfrak{m}^d.$$

Finally, $(iv)\Rightarrow(i)$ holds because $\mathcal{V}_+(x_0^d, \ldots, x_n^d) = \emptyset$. □

Definition 3.3.8. Let $V \subseteq \mathbb{P}^n$ be a projective k-variety. Then the $\mathbb{Z}$-graded k-algebra

$$k_+[V] := k[\underline{x}]/\mathcal{I}_+(V)$$

is called the **projective coordinate ring of** V (the grading is defined as in Lemma 3.2.8 (ii)). △

Remark 3.3.9. Let $V \subseteq \mathbb{P}^n$ be a projective k-variety.
(i) The affine cone $\widehat{V} \subseteq \mathbb{A}^{n+1}$ over V is an affine k-variety, and we have $\mathcal{I}(\widehat{V}) = \mathcal{I}_+(V)$. Therefore

$$k[\widehat{V}] = k_+[V]$$

holds for the *ungraded* rings.
(ii) The elements of $k_+[V]$ *cannot* be regarded as functions on V as in the affine case. Although the condition $p(v) = 0$ is well defined for $p \in k_+[V]$ and $v \in V$, the *value* $p(v)$ is not. However, if $p, q \in k_+[V]$ are *homogeneous of the same degree*, then

$$v \mapsto \frac{p(v)}{q(v)}$$

is a well-defined map $V \setminus \mathcal{V}_+(q) \to \mathbb{A}^1$.
(iii) For a homogeneous ideal $J \subseteq k_+[V]$ we define

$$\mathcal{V}_{V,+}(J) := \{v \in V \mid p(v) = 0 \,\forall p \in J\},$$

and for a homogeneous element $p \in k_+[V]$ we define

$$\mathcal{D}_{V,+}(p) := V \setminus \mathcal{V}_{V,+}(p).$$

The homogeneous radical ideals of $k_+[V]$ correspond to the homogeneous radical ideals of $k[\underline{x}]$ that contain $\mathcal{I}_+(V)$, and these in turn correspond to the projective k-subvarieties of V. Thus we obtain the following analogue of Remark 1.4.4: the map $\mathcal{V}_{V,+}(\cdot)$ yields a bijection between homogeneous radical ideals $\neq 1$ in $k_+[V]$ and k-subvarieties of V. △

Construction 3.3.10. For $i \in \{0, \ldots, n\}$ consider the well-defined bijection

$$\begin{aligned} \phi_i \colon \mathcal{D}_+(x_i) &\to \mathbb{A}^n \\ (a_0 : \ldots : a_n) &\mapsto \left(\frac{a_0}{a_i}, \ldots, \widehat{\frac{a_i}{a_i}}, \ldots, \frac{a_n}{a_i}\right) \\ (b_1 : \ldots : 1 : \ldots : b_n) &\leftarrow\!\shortmid (b_1, \ldots, b_n). \end{aligned}$$

For simplicity, we restrict ourselves to the case $i = 0$. For $0 \neq p \in k[x_1, \ldots, x_n]$ we define

$$p^h := x_0^{\deg(p)} \cdot p\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in k[x_0, \ldots, x_n]_{\deg(p)}$$

$$0^h := 0$$

and call p^h the **homogenization of** p **by** x_0. For $\deg(p) = d$ and $p = \sum_{|\alpha| \leqslant d} p_\alpha \underline{x}^\alpha$ we have

$$p^h := \sum_{|\alpha| \leqslant d} p_\alpha \cdot x_0^{d-|\alpha|} \cdot \underline{x}^\alpha.$$

Thus we make p homogeneous by multiplying every monomial in p that does not have the maximal degree d by a suitable power of x_0. For example,

$$(x_1^2 - x_2 + 1)^h = x_1^2 - x_0 x_2 + x_0^2.$$

It is clear from the definition that

$$(p_1 \cdot p_2)^h = p_1^h \cdot p_2^h.$$

Conversely, let $q \in k[x_0, \ldots, x_n]$ be homogeneous. Then we set

$$\tilde{q} := q(1, x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$$

and call $\tilde{q}$ the **dehomogenization of** q **by** x_0. We clearly have

$$\widetilde{p^h} = p,$$

and

$$x_0^m \cdot (\tilde{q})^h = q \text{ for some } m \geqslant 0.$$

In the last equation, $m \geqslant 1$ occurs if and only if the degree of q decreases when dehomogenized, that is, when every monomial in q is divisible by x_0. Hence $m = \deg(q) - \deg(\tilde{q})$. In the following lemma, we show that homogenization and dehomogenization correspond precisely to applying ϕ_0 on the geometric side. △

Lemma 3.3.11. *With the previous constructions, for $p \in k[x_1, \ldots, x_n]$ we obtain*

$$\phi_0^{-1}\left(\mathcal{V}(p)\right) = \mathcal{V}_+(p^h) \cap \mathcal{D}_+(x_0),$$

and for homogeneous $q \in k[x_0, \ldots, x_n]$ we obtain

$$\phi_0\left(\mathcal{V}_+(q) \cap \mathcal{D}_+(x_0)\right) = \mathcal{V}(\tilde{q}).$$

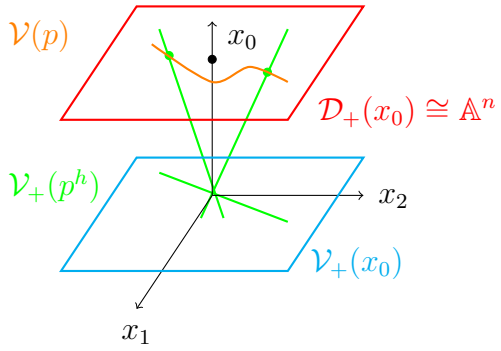
Proof. We have

$$\begin{aligned}
\phi_0^{-1}\left(\mathcal{V}(p)\right) &= \left\{(a_0 : \ldots : a_n) \mid a_0 \neq 0, p\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = 0\right\} \\
&= \left\{(a_0 : \ldots : a_n) \mid a_0 \neq 0, a_0^{\deg(p)} \cdot p\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) = 0\right\} \\
&= \left\{(a_0 : \ldots : a_n) \mid a_0 \neq 0, p^h(a_0, \ldots, a_n) = 0\right\} \\
&= \mathcal{V}_+(p^h) \cap \mathcal{D}_+(x_0)
\end{aligned}$$

and

$$\begin{aligned}
\phi_0\left(\mathcal{V}_+(q) \cap \mathcal{D}_+(x_0)\right) &= \left\{\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \mid a_0 \neq 0, q(a_0, \ldots, a_n) = 0\right\} \\
&= \left\{\left(\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right) \mid a_0 \neq 0, a_0^{\deg(q)} q\left(1, \frac{a_1}{a_0} \ldots, \frac{a_n}{a_0}\right) = 0\right\} \\
&= \{(b_1, \ldots, b_n) \mid \tilde{q}(b_1, \ldots, b_n) = 0\} \\
&= \mathcal{V}(\tilde{q}).
\end{aligned}$$

□



Theorem 3.3.12. *For all $i \in \{0, \dots, n\}$, the map $\phi_i \colon \mathcal{D}_+(x_i) \to \mathbb{A}^n$ is a homeomorphism with respect to the Zariski topologies.*

Proof. ϕ_i is bijective, and by Lemma 3.3.11, images and preimages of closed sets are closed. □

Remark 3.3.13. Theorem 3.3.12 implies that

$$\mathbb{P}^n = \mathcal{D}_+(x_0) \cup \cdots \cup \mathcal{D}_+(x_n)$$

is an open cover by subsets homeomorphic to $\mathbb{A}^n$. △

Definition 3.3.14. Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. The **homogenization** I^h of I is the homogeneous ideal

$$I^h := \left(p^h \mid p \in I\right) \subseteq k[x_0, \dots, x_n]. \qquad \triangle$$

Corollary 3.3.15. *We have*

$$\phi_0^{-1}(\mathcal{V}(I)) = \mathcal{V}_+(I^h) \cap \mathcal{D}_+(x_0).$$

Proof.

$$\begin{aligned}\phi_0^{-1}\left(\mathcal{V}(I)\right) &= \phi_0^{-1}\left(\bigcap_{p\in I} \mathcal{V}(p)\right) = \bigcap_{p\in I} \phi_0^{-1}\left(\mathcal{V}(p)\right) \\ &= \mathcal{D}_+(x_0) \cap \bigcap_{p\in I} \mathcal{V}_+(p^h) = \mathcal{D}_+(x_0) \cap \mathcal{V}_+(I^h),\end{aligned}$$

where we have used Lemma 3.3.11. □

Lemma 3.3.16. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal.*
(i) Every homogeneous $q \in I^h$ is of the form $q = x_0^r \cdot p^h$ for some $p \in I$.
(ii) We have $\sqrt{I^h} = \sqrt{I}^h$. In particular, the homogenization of a radical ideal is again a radical ideal.

Proof. For (i), write $q = \sum_i g_i p_i^h$ with $g_i \in k[x_0, \ldots, x_n]$ and $p_i \in I$. Since q and all p_i^h are homogeneous, we may assume that the g_i are homogeneous as well. Thus

$$q = \sum_i x_0^{r_i} \tilde{g}_i^h p_i^h$$

with $\deg(g_i) + \deg(p_i) = \deg(q) =: d$ and $r_i = \deg(g_i) - \deg(\tilde{g}_i)$. We have

$$d' := \deg\left(\sum_i \tilde{g}_i p_i\right) \leqslant d,$$

since every term in the sum has degree at most d. We obtain

$$\begin{aligned} x_0^{d-d'}\left(\sum_i \tilde{g}_i p_i\right)^h &= x_0^{d-d'} \cdot \sum_i x_0^{d'-\deg(\tilde{g}_i)-\deg(p_i)} \tilde{g}_i^h p_i^h \\ &= \sum_i x_0^{d-\deg(\tilde{g}_i)-\deg(p_i)} \tilde{g}_i^h p_i^h \\ &= \sum_i x_0^{r_i} \tilde{g}_i^h p_i^h = q. \end{aligned}$$

This shows (i). (ii) is Exercise 70. □

Definition 3.3.17. For every affine k-variety $V \subseteq \mathbb{A}^n$, the set

$$\overline{V} := \overline{\phi_0^{-1}(V)} \subseteq \mathbb{P}^n$$

is called the **projective closure of V in $\mathbb{P}^n$** (with respect to ϕ_0^{-1}). We will often suppress ϕ_0 in the notation. Since $\mathbb{P}^n$ induces precisely the Zariski topology on $\mathbb{A}^n$, we have $\overline{V} \cap \mathbb{A}^n = V$. △

Theorem 3.3.18. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. For the projective closure we then have*

$$\overline{\mathcal{V}(I)} = \mathcal{V}_+\left(I^h\right) \text{ and } \mathcal{I}_+\left(\overline{\mathcal{V}(I)}\right) = \sqrt{I^h} = \sqrt{I}^h = \mathcal{I}(\mathcal{V}(I))^h.$$

Proof. Let $V := \mathcal{V}(I)$. The first assertion follows from the second by applying $\mathcal{V}_+(\cdot)$. First let $p \in \sqrt{I} = \mathcal{I}(V)$. Then $p^h \equiv 0$ on $\phi_0^{-1}(V)$ by Lemma 3.3.11. Hence $p^h \equiv 0$ also holds on $\overline{\phi_0^{-1}(V)} = \overline{V}$, i.e. $p^h \in \mathcal{I}_+\left(\overline{V}\right)$. This shows $\sqrt{I}^h \subseteq \mathcal{I}_+\left(\overline{V}\right)$. Conversely, let $g \in \mathcal{I}_+\left(\overline{V}\right)$, and assume without loss of generality that g is homogeneous. Write $g = x_0^m g_1$ with $x_0 \nmid g_1$. Then $g_1 \equiv 0$ on $\mathcal{D}_+(x_0) \cap \overline{V}$, and hence $\tilde{g}_1 \equiv 0$ on V again by Lemma 3.3.11. This implies $\tilde{g}_1 \in \sqrt{I}$, and $g_1 = \tilde{g}_1^h$ holds because $x_0 \nmid g_1$. Thus g_1, and likewise g, lie in $\sqrt{I}^h$. □

Remark 3.3.19. For $I = (p_1, \ldots, p_s)$ we have

$$\left(p_1^h, \ldots, p_s^h\right) \subseteq I^h,$$

but in general this is *not an equality*. For $p_1 = x_1, p_2 = x_1 + 1$ we have

$$I = (p_1, p_2) = (1)$$

and therefore $I^h = (1)$. But

$$\left(p_1^h, p_2^h\right) = (x_1, x_1 + x_0) \neq (1).$$ △

Definition 3.3.20. (*i*) Let $V \subseteq \mathbb{A}^n$ be an affine k-variety and let $\overline{V} \subseteq \mathbb{P}^n$ be its projective closure. Let $H = \mathcal{V}_+(x_0) \subseteq \mathbb{P}^n$. Then the points in

$$H \cap \overline{V} = \overline{V} \setminus V$$

are called the **points at infinity of** V. They form a closed set in $H = \mathbb{P}^{n-1}$.
(*ii*) For $0 \neq p \in k[x_1, \ldots, x_n]$, write $p = p_0 + p_1 + \cdots + p_d$ with p_i homogeneous of degree i and $p_d \neq 0$. Then

$$\mathrm{LF}(p) := p_d$$

is called the **leading form** of p. Note that

$$\mathrm{LF}(p) = p^h(0, x_1, \ldots, x_n).$$

(*iii*) For an ideal $I \subseteq k[x_1, \ldots, x_n]$, the ideal

$$\mathrm{LF}(I) := (\mathrm{LF}(p) \mid p \in I)$$

is called the **leading form ideal of** I. It is a homogeneous ideal in $k[x_1, \ldots, x_n]$. △

Corollary 3.3.21. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and $V = \mathcal{V}(I) \subseteq \mathbb{A}^n$. Let $H = \mathcal{V}_+(x_0)$. Then we have*

$$\overline{V} \cap H = \mathcal{V}_+(\mathrm{LF}(I)) \subseteq H \cong \mathbb{P}^{n-1},$$

where we consider $H \cong \mathbb{P}^{n-1}$ with homogeneous coordinates $(x_1 : \ldots : x_n)$. In particular, we have $\mathcal{I}_+(\overline{V} \cap H) = \sqrt{\mathrm{LF}(I)}$ in $k[x_1, \ldots, x_n]$.

Proof. Since $\overline{V} = \mathcal{V}_+(I^h)$, we obtain in $\mathbb{P}^n$ that

$$\overline{V} \cap H = \mathcal{V}_+((x_0) + I^h) = \mathcal{V}_+((x_0) + \mathrm{LF}(I)),$$

because $p^h \equiv \mathrm{LF}(p)$ modulo (x_0). Restricting to H, we obtain $\mathcal{V}_+(\mathrm{LF}(I)) \subseteq H = \mathbb{P}^{n-1}$. □

Example 3.3.22. (i) The projective closure of an affine hypersurface

$$\mathcal{V}(p) \subseteq \mathbb{A}^n$$

with $0 \neq p \in k[x_1, \ldots, x_n]$ is

$$\overline{V} = \mathcal{V}_+(p^h)$$

because $(p)^h = (p^h)$. If p is square-free, then $\mathcal{I}_+\left(\overline{V}\right) = \sqrt{(p)}^h = (p)^h = (p^h)$. The points at infinity of V are the roots of $\mathrm{LF}(p)$ in $\mathcal{V}_+(x_0) = \mathbb{P}^{n-1}$.
(ii) For $p \in k[x_1, x_2]$ with $\deg(p) \geqslant 1$, consider the affine curve $V = \mathcal{V}(p) \subseteq \mathbb{A}^2$. There is a factorization

$$\mathrm{LF}(p) = c \cdot \prod_{i=1}^{d} (a_i x_1 + b_i x_2)$$

with $(a_i : b_i) \in \mathbb{P}^1\left(\overline{k}\right)$ and $c \in k^*$, where the $(a_i : b_i)$ are uniquely determined. This factorization can be obtained by factoring $\mathrm{LF}(p)(x_1, 1) \in k[x_1]$ over $\overline{k}$ and re-homogenizing the factors. Hence the points at infinity of V are precisely

$$(0 : b_i : -a_i) \in \mathbb{P}^2 \qquad i = 1, \ldots, d,$$

or, equivalently, the points

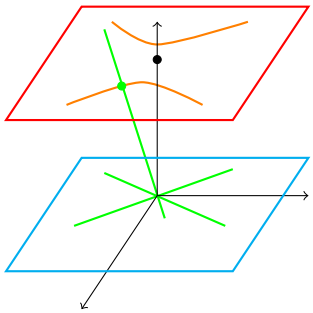
$$(b_i : -a_i) \in \mathbb{P}^1 = \mathcal{V}_+(x_0) \qquad i = 1, \ldots, d.$$

(iii) For $p = x_1^2 - x_2^2 - 1$ the set $\mathcal{V}(p)$ is a hyperbola. Since

$$\mathrm{LF}(p) = x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2),$$

we obtain the two points at infinity

$$(0:1:1) \qquad (0:1:-1).$$



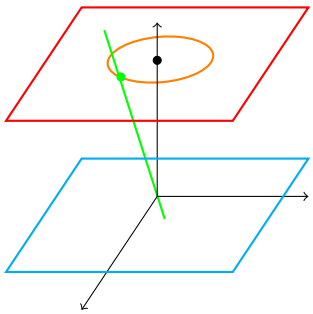
(*iv*) For $p = (x_1 - a_1)^2 + (x_2 - a_2)^2 - r^2$, the set $\mathcal{V}(p)$ is a circle. Since

$$\mathrm{LF}(p) = x_1^2 + x_2^2,$$

there are two points at infinity,

$$(0:1:\sqrt{-1}) \qquad (0:1:-\sqrt{-1}),$$

which cannot be seen in the real picture.

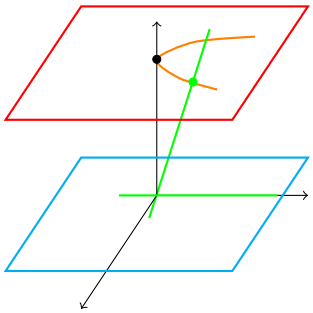


(*v*) For $p = x_1^2 - x_2$, the set $\mathcal{V}(p)$ is a parabola. Since

$$\mathrm{LF}(p) = x_1^2,$$

we obtain just the single point at infinity

$$(0:0:1).$$

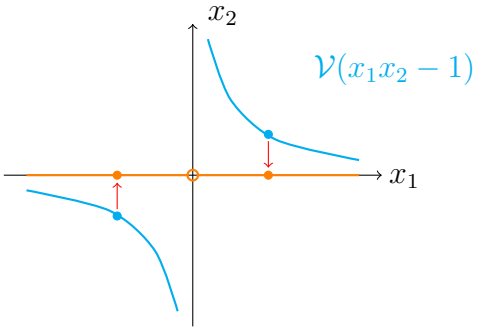


△

Remark 3.3.23. Even if $I \subseteq k[\underline{x}]$ is a radical ideal, this need not be true for $\mathrm{LF}(I)$. This can be seen, for instance, in the last example $I = (x_1^2 - x_2)$. Here $\mathrm{LF}(I) = (x_1^2)$. △

3.4 The Fundamental Theorem of Elimination Theory

In Section 1.4 we saw that the image of an affine variety under a morphism is not necessarily closed, and hence is not necessarily again an affine variety. An example is the projection of the variety $\mathcal{V}(x_1x_2-1) \subseteq \mathbb{A}^2$ onto the x_1-coordinate. Its image is $\mathbb{A}^1 \setminus \{0\}$.



The reason the image fails to be closed is that the preimage of a point $a \in \mathbb{A}^1$ "vanishes towards infinity" as a approaches 0. In projective space, points at infinity are available, and this is why the situation changes. In this section, let

$$\underline{x} = (x_0, \ldots, x_m), \quad \underline{y} = (y_1, \ldots, y_n)$$

be two tuples of variables. A polynomial $p \in k[\underline{x}, \underline{y}]$ is called **homogeneous in** $\underline{x}$ if it is homogeneous in the polynomial ring $(k[\underline{y}])[\underline{x}]$ with respect to the standard grading. This means that for every monomial $\underline{x}^\alpha \underline{y}^\beta$ of p we have $|\alpha| = d$ for

some fixed $d \in \mathbb{N}$. Now let $p_1, \ldots, p_r \in k[\underline{x}, \underline{y}]$ be homogeneous in $\underline{x}$. Then the following set is well defined:

$$X := \{(a, b) \in \mathbb{P}^m \times \mathbb{A}^n \mid p_1(a, b) = \cdots = p_r(a, b) = 0\}.$$

Let

$$\begin{aligned} \pi \colon \mathbb{P}^m \times \mathbb{A}^n &\to \mathbb{A}^n \\ (a, b) &\mapsto b \end{aligned}$$

be the projection onto the second component.

Theorem 3.4.1 (Fundamental Theorem of Elimination Theory)**.** *The set $\pi(X)$ is k-closed in $\mathbb{A}^n$.*

Proof. For $b \in \mathbb{A}^n$ we have

$$b \in \pi(X) \;\Leftrightarrow\; \mathcal{V}_+(p_1(\underline{x}, b), \ldots, p_r(\underline{x}, b)) \neq \emptyset.$$

Let $R = K[\underline{x}]$ with the standard grading. From Theorem 3.3.7 it follows that

$$b \in \pi(X) \;\Leftrightarrow\; R_d \nsubseteq (p_1(\underline{x}, b), \ldots, p_r(\underline{x}, b)) \;\forall d \geqslant 0.$$

For $d \geqslant 0$, let

$$Y_d := \{b \in \mathbb{A}^n \mid R_d \nsubseteq (p_1(\underline{x}, b), \ldots, p_r(\underline{x}, b))\}.$$

Then

$$Y_0 \supseteq Y_1 \supseteq Y_2 \supseteq \cdots \quad \text{and} \quad \bigcap_{d \geqslant 0} Y_d = \pi(X).$$

Hence it suffices to show that Y_d is closed for all sufficiently large d. Let $d_i = \deg_{\underline{x}}(p_i)$ and $d \geqslant \max\{d_1, \ldots, d_r\}$. Then

$$\begin{aligned} b \notin Y_d &\Leftrightarrow R_d \subseteq (p_1(\underline{x}, b), \ldots, p_r(\underline{x}, b)) \\ &\Leftrightarrow \text{the } \underline{x}^\alpha \cdot p_i(\underline{x}, b) \text{ with } |\alpha| = d - d_i \text{ span the entire space } R_d \text{ over } K. \end{aligned}$$

For the second equivalence we have used Remark 3.2.4. When we expand the $\underline{x}^\alpha \cdot p_i(\underline{x}, b)$ in a suitable basis of R_d (for example, the monomial basis) and write the coefficients into a matrix B, the entries of B are polynomials over k in b. Altogether, we obtain

$$b \notin Y_d \Leftrightarrow \operatorname{rank}(B) \geqslant \dim_K R_d.$$

Equivalently,

$$\begin{aligned} b \in Y_d &\Leftrightarrow \operatorname{rank}(B) < \dim_K R_d \\ &\Leftrightarrow \text{all minors of } B \text{ of size } \dim_K R_d \text{ vanish.} \end{aligned}$$

The last condition defines a k-closed set. □

Remark 3.4.2. The Fundamental Theorem of Elimination Theory states that for all $\underline{x}$-homogeneous polynomials $p_1, \ldots, p_r \in k[\underline{x}, \underline{y}]$ there are $q_1, \ldots, q_s \in k[\underline{y}]$ such that for all $b \in K^n$ we have

$$\left(\exists a \in \mathbb{P}^m(K) : \bigwedge_i p_i(a, b) = 0 \right) \Leftrightarrow \bigwedge_j q_j(b) = 0.$$

That is, the existential quantifier can be eliminated. △

Remark 3.4.3. All varieties are noetherian in the Zariski topology and are therefore quasi-compact, i.e. every open cover has a finite subcover. In non-Hausdorff spaces, the notion of quasi-compactness is often not very helpful. The Fundamental Theorem of Elimination Theory is a kind of alternative compactness property for $\mathbb{P}^n$. A Hausdorff space X is compact if and only if, for every Hausdorff space Y, the projection

$$\pi \colon X \times Y \to Y$$

maps closed sets to closed sets. This is proven in Exercise 73. △

We also obtain the Fundamental Theorem of Elimination Theory for $\mathbb{P}^m \times \mathbb{P}^n$. Let

$$\underline{x} = (x_0, \ldots, x_m) \quad \underline{y} = (y_0, \ldots, y_n)$$

and let $p_i \in k[\underline{x}, \underline{y}]$ be *bihomogeneous*, i.e. homogeneous in both $\underline{x}$ and $\underline{y}$. Then

$$X = \{(a, b) \in \mathbb{P}^m \times \mathbb{P}^n \mid p_1(a, b) = \cdots = p_r(a, b) = 0\}$$

is well defined. Let $\pi \colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$ be the projection.

Corollary 3.4.4. *The set $\pi(X) \subseteq \mathbb{P}^n$ is closed.*

Proof. Let $X' \subseteq \mathbb{P}^m \times \mathbb{A}^{n+1}$ be the set of roots of the p_i, and let

$$\pi' \colon \mathbb{P}^m \times \mathbb{A}^{n+1} \to \mathbb{A}^{n+1}$$

be the projection. By Theorem 3.4.1, the image $\pi'(X')$ is closed in $\mathbb{A}^{n+1}$. On the other hand, we clearly have $\pi'(X') = \widehat{\pi(X)}$, and the assertion follows from Lemma 3.3.4 (*i*). □

Corollary 3.4.5. *Let $p_1, \ldots, p_r \in k[x_0, \ldots, x_m]$ be homogeneous, and let $f_0, \ldots, f_n \in k[x_0, \ldots, x_m]$ be homogeneous of the same degree. Further, let*

$$V = \mathcal{V}_+(p_1, \ldots, p_r) \subseteq \mathbb{P}^m$$

and assume that

$$V \cap \mathcal{V}_+(f_0, \ldots, f_n) = \emptyset.$$

Then the image of the well-defined map

$$\begin{aligned} f \colon V &\to \mathbb{P}^n \\ a &\mapsto (f_0(a) : \ldots : f_n(a)) \end{aligned}$$

is closed in $\mathbb{P}^n$.

Proof. The graph

$$\Gamma_f := \{(a, b) \in \mathbb{P}^m \times \mathbb{P}^n \mid a \in V, b = f(a)\}$$

can be defined bihomogeneously by the equations $p_i(a) = 0$ for $i = 1, \ldots r$ and

$$b_j f_k(a) - b_k f_j(a) = 0$$

for $j, k = 0, \ldots, n$. By Corollary 3.4.4, the set

$$f(V) = \pi(\Gamma_f)$$

is closed in $\mathbb{P}^n$. □

The last corollary illustrates how the Fundamental Theorem of Elimination Theory can be applied in situations where compactness would be invoked for Hausdorff spaces. The set V is quasi-compact in the Zariski topology and the map f is continuous. Thus the image is again quasi-compact, and in Hausdorff spaces this would imply that the image is closed.

Chapter 4

Quasi-Projective Varieties

In this chapter we further generalize the notions of varieties and morphisms, to reach a more flexible framework. In particular we obtain a suitable notion of morphism for projective varieties.

4.1 Quasi-Projective Varieties, Regular Functions and Morphisms

Definition 4.1.1. Let X be a topological space. A subset $Y \subseteq X$ is called **locally closed in** X, if it fulfills one of the following equivalent conditions:

(i) Y is relatively open in $\overline{Y}$

(ii) There exists an open subset $O \subseteq X$ and a closed subset $A \subseteq X$ with $Y = O \cap A$. △

Remark 4.1.2. (i) Open and closed subsets of X are locally closed. Finite intersections of locally closed subsets of X are locally closed.
(ii) For a locally closed subset $Y \subseteq X$ and $Z \subseteq Y$ we have

$$Z \text{ locally closed in } Y \;\Leftrightarrow\; Z \text{ locally closed in } X.$$

(iii) Inverse images of locally closed sets under continuous maps are locally closed. △

Definition 4.1.3. A **quasi-projective** k**-variety** V is a locally closed subset of some $\mathbb{A}^n$ oder $\mathbb{P}^n$, with respect to the k-Zariski topology. If $W \subseteq V$ is a locally closed

(closed, open) subset, we call W a locally closed (closed, open) **subvariety** of V. △

Remark 4.1.4. Closed sets are defined by polynomial equations, open sets by their complements. So a quasi-projective variety can be seen as the set of solutions to a system of polynomial equations and inequations (and unions thereof). △

Definition 4.1.5. Let $V \subseteq \mathbb{A}^n$ ($V \subseteq \mathbb{P}^n$, respectively) be a locally closed subset.
(i) A **(k-)regular function on** V is a function

$$f\colon V \to \mathbb{A}^1$$

with the following property: For all $a \in V$ there exists an open neighborhood $U \subseteq V$ of a and polynomials $p, q \in k[x_1, \ldots, x_n]$ (homogeneous polynomials $p, q \in k[x_0, \ldots, x_n]$ of the same degree, respectively) with $q \neq 0$ on U, and

$$f(b) = \frac{p(b)}{q(b)}$$

for all $b \in U$.
(ii) By $\mathcal{O}(V)$ we denote the set of all k-regular functions on the quasi-projective variety V. △

Lemma 4.1.6. *Let V be a quasi-projective variety.*
(i) The set $\mathcal{O}(V)$ is a k-algebra with respect to pointwise operations.
(ii) For every $f \in \mathcal{O}(V)$ the set

$$\mathcal{V}_V(f) := \{a \in V \mid f(a) = 0\}$$

is closed in V, and the set

$$\mathcal{D}_V(f) := V \setminus \mathcal{V}_V(f)$$

is open in V.
(iii) If $f \in \mathcal{O}(V)$ fulfills $f(a) \neq 0$ for all $a \in V$, then $\frac{1}{f}$ is a regular function on V.
(iv) If $W \subseteq V$ is locally closed and $f \in \mathcal{O}(V)$, then $f_{|W} \in \mathcal{O}(W)$. The restriction map $\mathcal{O}(V) \to \mathcal{O}(W)$ is a homomorphism of algebras.

Proof. (i) and (iv) are obvious. For (ii) it is enough to show that for each $a \in V$ there exists an open neighborhood $U \subseteq V$ with $U \cap \mathcal{V}_V(f)$ closed in U. Now if $f = \frac{p}{q}$ holds on an open neighborhood U of a, then $\mathcal{V}_V(f) \cap U = \mathcal{V}(p) \cap U$ is closed in U. Statement (iii) is easy, since $f^{-1} = \frac{q}{p}$ holds on U, if $f = \frac{p}{q}$ on U. □

Remark 4.1.7. (i) For each quasi-projective variety V and each locally closed subset $W \subseteq V$ the algebra $\mathcal{O}(W)$ is defined, since W itself is locally closed in $\mathbb{A}^n$ or $\mathbb{P}^n$. For each inclusion $W' \subseteq W$ we have the restriction map $\mathcal{O}(W) \to \mathcal{O}(W')$, which is a k-algebra homomorphism.
(ii) The property of being regular (of a function $f\colon V \to \mathbb{A}^1$) is *local* with respect to V. That is, whenever $V = \bigcup_{i\in I} U_i$ is an open covering, then

$$f \text{ regular } \Leftrightarrow \ f_{|_{U_i}} \text{ regular for all } i \in I.$$

(iii) From now on we will say **variety** instead of *quasi-projective k-variety*. △

We will first show that the notion of a regular function coincides with the one from Definition 1.4.1, in case the variety is affine.

Theorem 4.1.8. *Let $V \subseteq \mathbb{A}^n$ be closed and $s \in k[V]$. Then the canonical homomorphism*

$$k[V]_s \to \mathcal{O}\left(\mathcal{D}_V(s)\right)$$

is an isomorphism.

Proof. Injectivity: Take $p/s^m \in k[V]_s$ and assume $p/s^m = 0$ in $\mathcal{O}\left(\mathcal{D}_V(s)\right)$. Then $p_{|_{\mathcal{D}_V(s)}} \equiv 0$, so $ps \equiv 0$ on V, and thus $ps = 0$ in $k[V]$. This implies $\frac{p}{s^m} = 0$ in $k[V]_s$.
For surjectivity let $f \in \mathcal{O}\left(\mathcal{D}_V(s)\right)$. By quasi-compactness of $\mathcal{D}_V(s)$ there exists a finite open covering

$$\mathcal{D}_V(s) = U_1 \cup \cdots \cup U_r$$

and elements $p_i, q_i \in k[V]$ with

$$f = \frac{p_i}{q_i} \text{ on } U_i.$$

Without loss of generality we can even assume $U_i = \mathcal{D}_V(s_i)$ for certain $s_i \in k[V]$. From $U_i \subseteq \mathcal{D}_V(q_i)$ we conclude

$$U_i = \mathcal{D}_V(q_i^2 s_i),$$

and since

$$\frac{p_i}{q_i} = \frac{p_i q_i s_i}{q_i^2 s_i} \text{ on } U_i$$

we can finally assume

$$U_i = \mathcal{D}_V(q_i)$$

as well as

$$p_i \equiv 0 \text{ on } \mathcal{V}_V(q_i).$$

We now have

$$p_i q_j = p_j q_i$$

as elements of $k[V]$, for all $i, j = 1, \ldots, r$. This is because on $\mathcal{V}_V(q_i q_j)$ both sides vanish, and on $\mathcal{D}_V(q_i q_j) = U_i \cap U_j$ we can divide by $q_i q_j$ pointwisely and obtain

$$\frac{p_i}{q_i} = \frac{p_j}{q_j},$$

since both sides represent f on $U_i \cap U_j$. From $\mathcal{D}_V(s) = U_1 \cup \cdots \cup U_r$ we conclude

$$\mathcal{V}_V(s) = \mathcal{V}_V(q_1 \ldots, q_r),$$

and Hilbert's Nullstellensatz implies

$$s \in \sqrt{(q_1, \ldots, q_r)} \subseteq k[V].$$

So let

$$s^m = b_1 q_1 + \cdots + b_r q_r$$

for some $m \geqslant 1$ and $b_1, \ldots, b_r \in k[V]$. We set

$$p := p_1 b_1 + \cdots + p_r b_r$$

and claim that

$$f = \frac{p}{s^m}$$

holds on the whole of $\mathcal{D}_V(s)$. For $i = 1, \ldots, r$ we indeed have

$$q_i p = \sum_{j=1}^{r} q_i p_j b_j = \sum_{j=1}^{r} q_j p_i b_j = p_i \sum_{j=1}^{r} q_j b_j = p_i s^m,$$

and this means

$$\frac{p}{s^m} = \frac{p_i}{q_i} = f \text{ on } U_i = \mathcal{D}_V(q_i). \qquad \square$$

Corollary 4.1.9. *For every affine variety $V \subseteq \mathbb{A}^n$ we have $\mathcal{O}(V) = k[V]$, i.e. every regular function on V is globally defined by a polynomial.*

Regular functions on a projective variety will be classified in Theorem 4.3.16 below. We first define and study morphisms between varieties. Also here we will later ensure that the new definition coincides with the old one in the affine case.

Definition 4.1.10. (i) Let V, W be quasi-projective k-varieties. A k**-morphism** from V to W is a continuous map

$$\phi\colon V \to W$$

such that for every *open* subset $W' \subseteq W$ and every $g \in \mathcal{O}(W')$ we have

$$g \circ \phi_{|_{\phi^{-1}(W')}} \in \mathcal{O}(\phi^{-1}(W')).$$

(ii) A morphism $\phi\colon V \to W$ is an **isomorphism**, if there exists a morphism $\psi\colon W \to V$ with $\phi \circ \psi = \mathrm{id}_W$, $\psi \circ \phi = \mathrm{id}_V$. △

Remark 4.1.11. (i) The map

$$\phi^*(g) := g \circ \phi_{|_{\phi^{-1}(W')}}$$

is called **pullback** of g by ϕ. A continuous map ϕ thus is a morphism, if each pullback of a locally defined regular function on W is a regular function on the respective inverse image.
(ii) For $W' \subseteq W$ open, the induced mapping

$$\phi^*\colon \mathcal{O}(W') \to \mathcal{O}(\phi^{-1}(W'))$$

is a k-algebra homomorphism. If ϕ is an isomorphism, then so is ϕ^*.
(iii) If $\phi\colon V \to W$ and $\psi\colon W \to X$ are morphisms, then so is

$$\psi \circ \phi\colon V \to X.$$

For $X' \subseteq X$ open we have

$$(\psi \circ \phi)^* = \phi^* \circ \psi^*\colon \mathcal{O}(X') \to \mathcal{O}(\psi^{-1}(X')) \to \mathcal{O}((\psi \circ \phi)^{-1}(X')).$$

(iv) Being a morphism is a *local property* with respect to the domain variety. That means, if $V = \bigcup_{i \in I} V_i$ is an open covering and $\phi\colon V \to W$ is a mapping, then ϕ is a morphism if and only if all restrictions

$$\phi_{|_{V_i}}\colon V_i \to W$$

are morphisms. This is immediate from Remark 4.1.7 (ii) and the fact that continuity is a local property.
(v) Being a morphism is also local with respect to the image variety. That means, if $W = \bigcup_{i\in I} W_i$ is an open covering and $\phi\colon V \to W$ is a *continuous* mapping, then ϕ is a morphism if and only if

$$\phi_{|_{\phi^{-1}(W_i)}} : \phi^{-1}(W_i) \to W_i$$

is a morphism, for all $i \in I$. △

The following Lemma shows that domains and codomains of morphisms can be restricted.

Lemma 4.1.12. *Let V be a k-variety and $V' \subseteq V$ a locally closed subset.*
(i) The inclusion $V' \hookrightarrow V$ is a morphism.
(ii) If $\phi\colon W \to V$ is a morphism with $\phi(W) \subseteq V'$, so the induced mapping $\phi'\colon W \to V'$ is again a morphism.

Proof. (i) is obvious, since the restriction of a regular function onto a locally closed subset is again a regular function. For (ii) let $U \subseteq V'$ be open in V', and take $g \in \mathcal{O}(U)$. Note that U need not be open in V. But without loss of generality we can assume $g = \frac{p}{q}$ on the whole of U, for some polynomials p, q (by making U smaller, if necessary). Then $\frac{p}{q}$ is regular on the open subset $\mathcal{D}_V(q)$ of V, and thus $f := \phi^*\left(\frac{p}{q}\right)$ is regular on $\phi^{-1}(\mathcal{D}_V(q))$. But then also $f_{|_{\phi^{-1}(U)}}$ is regular, and it coincides with $\phi'^*(g)$. □

Theorem 4.1.13. *Let V, W be varieties, and assume $W \subseteq \mathbb{A}^m$ is closed. Let*

$$\phi = (\phi_1, \ldots, \phi_m)\colon V \to W$$

be a mapping. Then ϕ is a morphism if and only if

$$\phi_i \in \mathcal{O}(V) \text{ for } i = 1, \ldots, m.$$

In particular, the morphisms $V \to \mathbb{A}^1$ are precisely the regular functions on V.

Proof. First assume $\phi_1, \ldots, \phi_m \in \mathcal{O}(V)$. For each $p \in k[W]$ we then have $\phi^*(p) = p(\phi_1, \ldots, \phi_m) \in \mathcal{O}(V)$, since $\mathcal{O}(V)$ is a k-algebra. For $q \in k[W]$ we know that

$$\phi^{-1}(\mathcal{D}_W(q)) = \mathcal{D}_V\left(\phi^*(q)\right)$$

is open in V (by Lemma 4.1.6 (ii)), and the pullback of the regular function

$$\frac{p}{q} \in \mathcal{O}\left(\mathcal{D}_W(q)\right)$$

is

$$\phi^*\left(\frac{p}{q}\right) = \frac{\phi^*(p)}{\phi^*(q)},$$

which is regular on $\phi^{-1}(\mathcal{D}_W(q))$ by Lemma 4.1.6 (iii). So ϕ is a morphism, since every regular function is locally of the form $\frac{p}{q}$.
Conversely, if ϕ is a morphism, then

$$\phi_i = \phi^*(x_i) \in \mathcal{O}(V),$$

since $x_i \in \mathcal{O}(W)$. □

Corollary 4.1.14. *Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be closed. Then a mapping*

$$\phi\colon V \to W$$

is a morphism (in the sense of the new Definition 4.1.10), if there are regular functions $p_1, \ldots, p_m \in k[V]$ with

$$\phi = (p_1, \ldots, p_m).$$

For affine varieties, the new Definition thus coincides with the old Definition 1.4.7.

Proof. By Theorem 4.1.13, ϕ is a morphism if and only if $\phi_i \in \mathcal{O}(V)$ holds for all i. Furthermore we have $\mathcal{O}(V) = k[V]$ by Corollary 4.1.9. □

Remark 4.1.15. A morphism of varieties can be a homeomorphism of topological spaces, without being an isomorphism of varieties. This can be seen in Example 1.4.12 (iii). △

Theorem 4.1.16. *For all $i = 0, \ldots, n$ the mapping*

$$\begin{aligned} \phi_i\colon \mathcal{D}_+(x_i) &\to \mathbb{A}^n \\ (a_0 : \ldots : a_n) &\mapsto \left(\frac{a_0}{a_i}, \ldots, \widehat{\frac{a_i}{a_i}}, \ldots, \frac{a_n}{a_i}\right) \end{aligned}$$

is an isomorphism of varieties.

Proof. We know from Theorem 3.3.12 that ϕ_i is a homeomorphism. By Theorem 4.1.13 ϕ_i is also a morphism of varieties, since its components x_j/x_i are regular functions on $\mathcal{D}_+(x_i)$. For the inverse functions let us only consider $i = 0$, and let $p, q \in k[x_0, \ldots, x_n]$ be homogeneous functions of the same degree. If $\tilde{p} = p(1, x_1, \ldots, x_n)$ and $\tilde{q} = q(1, x_1, \ldots, x_n)$ are their dehomogenizations, then

$$\phi_0 \left(\mathcal{D}_+(x_0) \cap \mathcal{D}_+(q) \right) = \mathcal{D}(\tilde{q})$$

and

$$\left(\phi_0^{-1}\right)^* \left(\frac{p}{q} \right) = \frac{\tilde{p}}{\tilde{q}}$$

is a regular function on $\mathcal{D}(\tilde{q})$. Again, every regular function is locally of the form p/q, and thus ϕ_0^{-1} is a morphism of varieties. □

Theorem 4.1.17. *Let $V \subseteq \mathbb{A}^n$ be closed and let $s \in k[V]$. Then the open subvariety $\mathcal{D}_V(s)$ of V is isomorphic to the closed subvariety*

$$V' := \left\{ (a, t) \mid a \in V, t \in \mathbb{A}^1, t \cdot s(a) - 1 = 0 \right\} \subseteq \mathbb{A}^{n+1}.$$

In particular we have $k[V'] \cong \mathcal{O}(\mathcal{D}_V(s)) = k[V]_s$.

Proof. The mapping

$$\begin{aligned} \phi \colon V' &\to V \\ (a, t) &\mapsto a \end{aligned}$$

is a morphism with domain $\operatorname{im}(\phi) = \mathcal{D}_V(s)$. Thus also $\phi \colon V' \to \mathcal{D}_V(s)$ is a morphism. The inverse mapping

$$\begin{aligned} \psi \colon \mathcal{D}_V(s) &\to V' \\ a &\mapsto \left(a, \frac{1}{s(a)} \right) \end{aligned}$$

is also a morphism, since its components are regular functions on $\mathcal{D}_V(s)$. □

We now extend the notions of an affine and a projective variety.

Definition 4.1.18. A quasi-projective k-variety V is called **affine** (**projective**, respectively), if V is isomorphic to a closed subvariety of some $\mathbb{A}^n$ ($\mathbb{P}^n$ respectively). If V is affine, we also write $k[V]$ instead of $\mathcal{O}(V)$. △

Remark/Example 4.1.19. (i) If V is an affine variety and $s \in k[V]$, then the open subvariety $\mathcal{D}_V(s)$ is also affine, and we have $k[\mathcal{D}_V(s)] = k[V]_s$. Indeed, an isomorphism $\phi\colon V \to W$ to a closed subset $W \subseteq \mathbb{A}^n$ restricts to an isomorphism

$$\mathcal{D}_V(s) \to \mathcal{D}_W((\phi^{-1})^*(s))$$

by Lemma 4.1.12. We can then apply Theorem 4.1.17 for W.
(ii) The open subvariety $\mathcal{D}_+(x_i) \subseteq \mathbb{P}^n$ is affine, by Theorem 4.1.16.
(iii) Every open subvariety of $\mathbb{A}^1$ is affine. Since $k[x_1]$ is a principal ideal domain, every open subset is in fact of the form $\mathcal{D}(s)$ for some $s \in k[x_1]$.
(iv) In general, open subvarieties of affine varieties are not affine. For example,

$$\mathbb{A}^2 \setminus \{(0,0)\}$$

is not affine (Exercise 74).
(v) Every closed subvariety of an affine (projective) variety is again affine (projective, respectively).
(vi) Every quasi-projective variety is an open subvariety of a projective variety. For locally closed $V \subseteq \mathbb{P}^n$ this is clear by definition, and a closed $V \subseteq \mathbb{A}^n$ is open in the projective closure $\overline{V}$. △

Theorem 4.1.20. *Let $V \subseteq \mathbb{P}^n$ be closed and $i \in \{0, \dots, n\}$. Then the open subset*

$$V_i := V \cap \mathcal{D}_+(x_i)$$

of V is affine, and the canonical homomorphism

$$k_+[V]_{(\overline{x}_i)} \to k[V_i]$$

is an isomorphism.

Proof. As a closed subset of the affine variety $\mathcal{D}_+(x_i)$, V_i is affine. Elements of $k_+[V]_{(\overline{x}_i)}$ are of the form $\frac{p}{\overline{x}_i^r}$ with $p \in k_+[V]$ homogeneous of degree r. Thus they define regular functions on V_i. This defines a canonical homomorphism $\varphi\colon k_+[V]_{(\overline{x}_i)} \to k[V_i]$ which is injective, since $\varphi\left(\frac{p}{\overline{x}_i^r}\right) = 0$ implies $p \equiv 0$ on V_i, and thus $\overline{x}_i p \equiv 0$ on V. We therefore obtain $\overline{x}_i p = 0$ in $k_+[V]$ and thus $\frac{p}{\overline{x}_i^r} = 0$ in $k_+[V]_{(\overline{x}_i)}$.
For surjectivity first note that the coordinate algebra of an affine variety is generated by the coordinate functions. With respect to the isomorphism $\mathcal{D}_+(x_i) \cong \mathbb{A}^n$ the coordinate functions are exactly the x_j/x_i on $\mathcal{D}_+(x_i)$, and the coordinate functions of V_i are thus $\overline{x}_j/\overline{x}_i$. They however all lie in the image of φ. □

Corollary 4.1.21. *Every variety admits a basis of open sets that consists of affine open sets.*

Proof. If the variety V is affine, this follows from Theorem 4.1.17, since the $\mathcal{D}_V(s)$ for $s \in k[V]$ form a basis of open sets. Every projective variety is covered by open affine subsets, by Theorem 4.1.20, and thus the statement is also true for projective varieties and open subsets of such. □

Example 4.1.22. (i) Let $p_0, \ldots, p_n \in k[x_0, \ldots, x_m]$ be homogeneous of the same degree. Then the mapping

$$\begin{aligned} \phi\colon \mathbb{P}^m \setminus \mathcal{V}_+(p_0, \ldots, p_n) &\to \mathbb{P}^n \\ a &\mapsto (p_0(a) : \ldots : p_n(a)) \end{aligned}$$

is a morphism. In fact $\mathbb{P}^m \setminus \mathcal{V}_+(p_0, \ldots, p_n)$ is the union of open sets $\mathcal{D}_+(p_i)$ and it suffices to show that

$$\phi\colon \mathcal{D}_+(p_i) \to \mathbb{P}^n$$

is a morphism for all $i = 0, \ldots, n$. Under the isomorphism

$$\phi(\mathcal{D}_+(p_i)) \subseteq \mathcal{D}_+(x_i) \cong \mathbb{A}^n$$

the mapping ϕ translates to

$$a \mapsto \left(\frac{p_0(a)}{p_i(a)}, \ldots, \widehat{\frac{p_i(a)}{p_i(a)}}, \ldots, \frac{p_n(a)}{p_i(a)} \right).$$

This however is a morphism by Theorem 4.1.13, since $\frac{p_j}{p_i}$ is regular on $\mathcal{D}_+(p_i)$.
(ii) A special case of (i) are linear morphisms. Let M be a matrix of size $(n+1) \times (m+1)$ over k with $\operatorname{rank}(M) = m+1$. Then

$$\begin{aligned} \phi_M\colon \mathbb{P}^m &\to \mathbb{P}^n \\ [v] &\mapsto [Mv] \end{aligned}$$

is a morphism, and we have $\phi_{MN} = \phi_M \circ \phi_N$. In case $m = n$ we obtain a group homomorphism

$$\mathrm{GL}_{n+1}(k) \to \mathrm{Aut}_k(\mathbb{P}^n)$$

with kernel $k^* I$. This gives an embedding

$$\mathrm{PGL}_{n+1}(k) \hookrightarrow \mathrm{Aut}_k(\mathbb{P}^n),$$

which can be shown to be surjective.
(*iii*) Consider the following morphism:

$$\begin{aligned}\phi\colon \mathbb{P}^1 &\to \mathbb{P}^2\\ (a_0 : a_1) &\mapsto (a_0^2 : a_0a_1 : a_1^2).\end{aligned}$$

We have

$$\phi(\mathbb{P}^1) \subseteq \mathcal{V}_+(x_1^2 - x_0x_2) =: C$$

and thus $\phi\colon \mathbb{P}^1 \to C$ is also a morphism, even an isomorphism. To see this we define the inverse morphism as

$$\begin{aligned}\psi\colon C &\to \mathbb{P}^1\\ (b_0 : b_1 : b_2) &\mapsto \begin{cases} (b_0 : b_1) \text{ if } b_0 \neq 0\\ (b_1 : b_2) \text{ if } b_2 \neq 0\end{cases}\end{aligned}$$

We have $C \subseteq \mathcal{D}_+(x_0) \cup \mathcal{D}_+(x_2)$, and on the intersection within C both definitions coincide, since $b_0b_2 = b_1^2$. Thus ψ is well-defined on C and a morphism, since on both subsets $C \cap \mathcal{D}_+(x_0), C \cap \mathcal{D}_+(x_2)$ it is one, by (*i*). It is now easily checked that ψ is inverse to ϕ. △

Remark 4.1.23. We have just shown

$$\mathbb{P}^1 \cong C = \mathcal{V}_+(x_1^2 - x_0x_2) \subseteq \mathbb{P}^2.$$

Let us now compare the projective coordinate rings of both varieties. We have

$$k_+[C] = k[x_0, x_1, x_2]/(x_1^2 - x_0x_2)$$

and

$$\dim_k k_+[C]_1 = 3,$$

since $(x_1^2 - x_0x_2)$ does not contain any homogeneous polynomial of degree 1. This implies that $k_+[C]$ is *not* generated by 2 elements as a k-algebra (the homogeneous terms of degree 1 of two generators would otherwise span $k_+[C]_1$ over k). On the other hand, $k_+[\mathbb{P}^1] = k[x_0, x_1]$ is obviously generated by two elements. So we have

$$\mathbb{P}^1 \cong C \text{ and } k_+[\mathbb{P}^1] \ncong k_+[C].$$

The projective coordinate ring is thus not even invariant under isomorphism! This is a significant difference to the affine case, where it even classifies isomorphism completely. △

4.2 The Veronese Embedding

In this section we introduce the Veronese Embedding, which can be used to linearize equations. We will show that we can reduce every setup to quadratic equations in projective space

Construction 4.2.1. Let $\underline{x} = (x_0, \ldots, x_n)$ and $d \geqslant 1$ be fixed. Let

$$m_0, m_1, \ldots, m_N \in k[\underline{x}]$$

be all monomials in $\underline{x}$ of degree (exactly) d. We have $N = \binom{n+d}{n}$ by Exercise 46. As in Example 4.1.22 (i) we obtain a k-morphism

$$\begin{aligned} v_d \colon \mathbb{P}^n &\to \mathbb{P}^N \\ a &\mapsto (m_0(a) : \ldots : m_N(a)) \end{aligned}$$

which is called the **Veronese embedding of degree** d. Its image

$$V_n^d := v_d(\mathbb{P}^n)$$

is called the **Veronese variety of degree** d. △

Theorem 4.2.2. *The Veronese variety $V_n^d = v_d(\mathbb{P}^n)$ is a closed subvariety of $\mathbb{P}^N$, and*

$$v_d \colon \mathbb{P}^n \to V_n^d$$

is an isomorphism of k-varieties.

Proof. Note that we know closedness of V_n^d already from Corollary 3.4.5. However, we will provide an explicit description by homogeneous equations, since we need it for the later construction of the inverse morphism. Set

$$J := \{\alpha \in \mathbb{N}^n \mid |\alpha| = d\}.$$

We can use homogeneous coordinates $(z_\alpha : \alpha \in J)$ on $\mathbb{P}^N$ and have

$$v_d(a) = (a^\alpha)_{\alpha \in J}$$

for all $a \in \mathbb{P}^n$. Now let $Z \subseteq \mathbb{P}^N$ be the zero set of all quadratic polynomials of the form

$$z_\alpha z_\beta - z_\gamma z_\delta$$

for $\alpha, \beta, \gamma, \delta \in J$ with $\alpha + \beta = \gamma + \delta$. Then clearly $V_n^d \subseteq Z$, since

$$a^\alpha a^\beta = a^{\alpha+\beta} = a^{\gamma+\delta} = a^\gamma a^\delta$$

holds for all such $\alpha, \beta, \gamma, \delta$. Thus

$$v_d \colon \mathbb{P}^n \to Z$$

is a morphism of varieties. We will now define an inverse mapping. To this end let $\beta \in J$ and $i \in \{0, \ldots, n\}$ with $\beta_i \geqslant 1$. We define

$$\begin{aligned} \phi_{\beta,i} \colon Z \cap \mathcal{D}_+(z_\beta) &\to \mathbb{P}^n \\ (b_\alpha)_{\alpha \in J} &\mapsto \left(b_{\beta - e_i + e_0} : b_{\beta - e_i + e_1} : \ldots : b_{\beta - e_i + e_n}\right). \end{aligned}$$

Then $\phi_{\beta,i}$ is a well-defined morphism as in Example 4.1.22 (i) (the image of $\phi_{\beta,i}$ lies inside $\mathcal{D}_+(x_i)$). Now let $\beta, \gamma \in J, \beta_i \geqslant 1, \gamma_j \geqslant 1$ and $b \in Z \cap \mathcal{D}_+(z_\beta) \cap \mathcal{D}_+(z_\gamma)$. We then have

$$\phi_{\beta,i}(b) = \phi_{\gamma,j}(b).$$

As explained in Definition 3.1.2 it is enough to show

$$b_{\beta - e_i + e_k} b_{\gamma - e_j + e_l} = b_{\beta - e_i + e_l} b_{\gamma - e_j + e_k}$$

for all $k, l = 0, \ldots, n$ to obtain this. But the last equation is true by definition of Z, since the indices on both sides sum up to the same tuple.
The $\phi_{\beta,i}$ thus define a global morphism

$$\phi \colon Z \to \mathbb{P}^n.$$

We have $\phi \circ v_d = \mathrm{id}_{\mathbb{P}^n}$: for $a \in \mathbb{P}^n$ just choose some i with $a_i \neq 0$ and set $\beta := de_i$. Then $a^\beta = a_i^d \neq 0$ and thus $v_d(a) = (a^\alpha)_{\alpha \in J} \in \mathcal{D}_+(z_\beta)$. We therefore have

$$\begin{aligned} \phi(v_d(a)) &= \phi_{\beta,i}(v_d(a)) \\ &= \left(a^{\beta - e_i + e_0} : \ldots : a^{\beta - e_i + e_n}\right) \\ &= \left(a_i^{d-1} a_0 : \ldots, a_i^{d-1} a_n\right) \\ &= a. \end{aligned}$$

Conversely we also have $v_d \circ \phi = \mathrm{id}_Z$: choose $\beta \in J, i \in \{0, \ldots, n\}$ with $\beta_i \geqslant 1$ and $b \in Z \cap \mathcal{D}_+(z_\beta)$. Then

$$v_d(\phi(b)) = \left(b_{\beta - e_i + e_0}^{\alpha_0} \cdots b_{\beta - e_i + e_n}^{\alpha_n}\right)_{\alpha \in J}$$

and this defines the same point as $b = (b_\alpha)_{\alpha\in J}$ in $\mathbb{P}^N$. To see this we show the following equality, for all $\gamma, \delta \in J$:

$$b_\gamma \cdot b^{\delta_0}_{\beta-e_i+e_0} \cdots b^{\delta_n}_{\beta-e_i+e_n} = b_\delta \cdot b^{\gamma_0}_{\beta-e_i+e_0} \cdots b^{\gamma_n}_{\beta-e_i+e_n}.$$

Note that the indices on both sides sum up to the same:

$$\gamma + \delta_0 \cdot (\beta - e_i + e_0) + \cdots + \delta_n \cdot (\beta - e_i + e_n) = \gamma + d \cdot (\beta - e_i) + \delta = \cdots$$

Thus the equation above is a consequence of the equations defining Z (Exercise 80). □

Remark 4.2.3. (i) We have found explicit equations defining the Veronese variety V_n^d of degree d. If $\mathbb{P}^N$ is equipped with homogeneous coordinates $(z_\alpha)_{|\alpha|=d}$, these are

$$z_\alpha z_\beta - z_\gamma z_\delta$$

with $\alpha+\beta = \gamma+\delta$. In particular, Z is an intersection of quadratic hypersurfaces, so-called **quadrics**.
(ii) For $n = 1$ one has

$$\begin{aligned} v_d \colon \mathbb{P}^1 &\to \mathbb{P}^d \\ (a_0 : a_1) &\mapsto (a_0^d : a_0^{d-1}a_1 : \cdots : a_0 a_1^{d-1} : a_1^d) \end{aligned}$$

The image V_1^d is also called **rational normal curve of degree** d. In case $d = 2$ it is the curve from Example 4.1.22 (iii).
(iii) For every locally closed subvariety V of $\mathbb{P}^n$, the Veronese embedding v_d defines an isomorphism between V and $v_d(V) \subseteq \mathbb{P}^N$. △

Remark 4.2.4. Let $p \in k[x_0, \ldots, x_n]$ be homogeneous of degree d, and write $p = \sum_{|\alpha|=d} p_\alpha \underline{x}^\alpha$. Then for $a \in \mathbb{P}^n$ we have

$$a \in \mathcal{V}_+(p) \;\Leftrightarrow\; v_d(a) \in \mathcal{V}_+\left(\sum_{|\alpha|=d} p_\alpha z_\alpha\right).$$

The isomorphism v_d thus maps the degree d hypersurface $\mathcal{V}_+(p)$ to the intersection of V_n^d with a hyperplane. A slightly more general statement is the following Theorem. △

Theorem 4.2.5. *Every closed k-subvariety of $\mathbb{P}^n$ is isomorphic (via some v_d) to an intersection*

$$V_n^d \cap L$$

where L is a linear subspace of $\mathbb{P}^N$ defined over k.

Proof. For $p \in k[\underline{x}]$ homogeneous and all $r \geqslant 0$ we have

$$\mathcal{V}_+(p) = \mathcal{V}_+(x_0^r p, \ldots, x_n^r p).$$

Thus every closed subset of $\mathbb{P}^n$ is definable with homogeneous equations of the same degree, and the statement follows from the last remark. □

Corollary 4.2.6. *Every projective k-variety is isomorphic to an intersection of quadratic k-hypersurfaces in some $\mathbb{P}^n$.*

Proof. The linear space L from the last theorem is isomorphic to some $\mathbb{P}^n$, and V_n^d is defined by quadratic equations. □

We will now prove a generalization of Theorem 4.1.20 to general hypersurfaces (and a projective version of Theorem 4.1.8).

Theorem 4.2.7. *Let $V \subseteq \mathbb{P}^n$ be closed and $s \in k_+[V]$ homogeneous. Then the open subset $\mathcal{D}_{V,+}(s)$ of V is affine, with*

$$k[\mathcal{D}_{V,+}(s)] = k_+[V]_{(s)}.$$

Proof. It is enough to prove the statement for $V = \mathbb{P}^n$, since for homogeneous $t \in k[\underline{x}]$ we know that $\mathcal{D}_{V,+}\left(\bar{t}\right) = V \cap \mathcal{D}_+(t)$ is a closed subvariety of the affine variety $\mathcal{D}_+(t) \subseteq \mathbb{P}^n$, and thus also affine. In addition, construction of quotients and homogeneous localization commute:

$$(R/I)_{\left(\bar{t}\right)} \cong R_{(t)}/\left(I\right).$$

So assume $V = \mathbb{P}^n$ and let $s \in k[\underline{x}]$ be homogeneous of degree d. Consider the Veronese embedding

$$v_d \colon \mathbb{P}^n \to \mathbb{P}^N$$

and let $H_s \subseteq \mathbb{P}^N$ be the hypersurface associated to $\mathcal{V}_+(s) \subseteq \mathbb{P}^n$. We have

$$\mathcal{D}_+(s) = v_d^{-1}(\mathbb{P}^N \setminus H_s) \cong V_n^d \cap \left(\mathbb{P}^N \setminus H_s\right).$$

From $\mathbb{P}^N \setminus H_s \cong \mathbb{A}^N$ we obtain that $\mathcal{D}_+(s)$ is an affine variety. The canonical homomorphism

$$k[\underline{x}]_{(s)} \to \mathcal{O}\left(\mathcal{D}_+(s)\right)$$

is injective, as we have seen in the proof of Theorem 4.1.20. Surjectivity follows exactly in the same way, since the generating coordinate functions on $\mathbb{P}^N \setminus H_s \cong \mathbb{A}^N$ are precisely the z_α/s, which correspond to the $\underline{x}^\alpha/s \in k[\underline{x}]_{(s)}$ under the isomorphism v_d. □

4.3 Direct Products

In the affine setting there is a canonical identification $\mathbb{A}^m \times \mathbb{A}^n = \mathbb{A}^{m+n}$, and for two closed subsets $V \subseteq \mathbb{A}^m, W \subseteq \mathbb{A}^n$ we know that $V \times W$ is closed in $\mathbb{A}^{m+n}$. We can thus easily form direct products of affine varieties in the sense of Chapter 1. This is harder for projective varieties. For example, there is *no* canonical identification between $\mathbb{P}^m \times \mathbb{P}^n$ and $\mathbb{P}^{m+n}$. But for vector spaces V, W over the same field, there is a well-defined embedding

$$\begin{aligned} \mathbb{P}(V) \times \mathbb{P}(W) &\to \mathbb{P}(V \otimes W) \\ ([v], [w]) &\mapsto [v \otimes v] \end{aligned}$$

the so-called **Segre-Embedding**. We now examine it in the case of $\mathbb{P}^m$ and $\mathbb{P}^n$ in more detail.

Construction 4.3.1. For $m, n \geqslant 1$ we identify $\mathbb{P}^{mn+m+n}$ with the projective space

$$\mathbb{P}\left(\mathrm{Mat}_{(m+1)\times(n+1)}(K)\right).$$

For a matrix $A \in \mathrm{Mat}_{(m+1)\times(n+1)}(K)$ one has

$$\mathrm{rank}(A) = 1 \;\Leftrightarrow\; A = uv^t$$

for certain column vectors $0 \neq u \in K^{m+1}, 0 \neq v \in K^{n+1}$. Here u, v are uniquely determined up to scaling. The mapping

$$\begin{aligned} K^{m+1} \times K^{n+1} &\to \mathrm{Mat}_{(m+1)\times(n+1)} \\ (u, v) &\mapsto uv^t \end{aligned}$$

thus induces a well-defined injective mapping

$$\sigma\colon \mathbb{P}^m \times \mathbb{P}^n \hookrightarrow \mathbb{P}\left(\mathrm{Mat}_{(m+1)\times(n+1)(K)}\right) = \mathbb{P}^{mn+m+n},$$

the so-called **Segre-embedding**. Its image

$$S_{m,n} := \{[A] \mid \operatorname{rank}(A) = 1\}$$

is called **Segre variety**. $S_{m,n}$ is really a k-closed subset of $\mathbb{P}^{mn+m+n}$, since it is defined by the vanishing of all 2×2-minors of A. △

Definition 4.3.2. If we talk about $\mathbb{P}^m \times \mathbb{P}^n$ as a variety from now on, we always mean the projective k-variety $S_{m,n}$. Even if we work with the Cartesian product $\mathbb{P}^m \times \mathbb{P}^n$ set-theoretically, all statements that refer to the structure of a variety are to be understood in $S_{m,n}$ via σ. △

Theorem 4.3.3. *(i) Both projections*

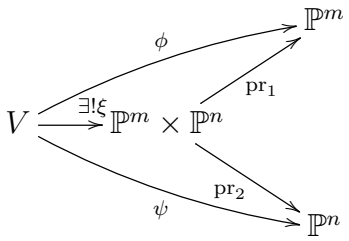
$$\mathrm{pr}_1 \colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^m, \quad \mathrm{pr}_2 \colon \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^n$$

are morphisms of varieties.
(ii) If $\phi \colon V \to \mathbb{P}^m$ and $\psi \colon V \to \mathbb{P}^n$ are morphisms of varieties, then

$$\begin{aligned}(\phi, \psi) \colon V &\to \mathbb{P}^m \times \mathbb{P}^n \\ a &\mapsto (\phi(a), \psi(a))\end{aligned}$$

is also a morphism.
(iii) The projective variety $\mathbb{P}^m \times \mathbb{P}^n$, together with the morphisms pr_1 and pr_2, fulfills the universal property of a direct product:

For any two morphisms $\phi \colon V \to \mathbb{P}^m$, $\psi \colon V \to \mathbb{P}^n$ there is exactly one morphism $\xi \colon V \to \mathbb{P}^m \times \mathbb{P}^n$ such that $\mathrm{pr}_1 \circ \xi = \phi, \mathrm{pr}_2 \circ \xi = \psi$.



Proof. (*i*) If we translate to $S_{m,n}$ via σ, we have for $[A] \in S_{m,n}$

$$\mathrm{pr}_1([A]) = [u],$$

where u is an arbitrary non-zero column of A. This yields a local definition of pr_1 as a morphism in the sense of Example 4.1.22 (*i*), on open subsets of $S_{m,n}$ defined

by the non-vanishing of a certain column. For pr_2 we use the same argument with rows instead.
(ii) Choose a local definition

$$\phi = (1 : \phi_1 : \ldots : \phi_m) \colon \phi^{-1}\left(\mathcal{D}_+(x_0)\right) \to \mathcal{D}_+(x_0) \subseteq \mathbb{P}^m$$

$$\psi = (1 : \psi_1 : \ldots : \psi_n) \colon \psi^{-1}\left(\mathcal{D}_+(y_0)\right) \to \mathcal{D}_+(y_0) \subseteq \mathbb{P}^n$$

with regular functions ϕ_i, ψ_i. Via the identification

$$\mathcal{D}_+(x_0) \times \mathcal{D}_+(y_0) \overset{\sigma}{\longleftrightarrow} \mathcal{D}_+(z_{00}) \subseteq \mathbb{P}\left(\mathrm{Mat}_{(m+1)\times(n+1)}(K)\right)$$

the mapping (ϕ, ψ) then translates to

$$\begin{aligned} \phi^{-1}\left(\mathcal{D}_+(x_0)\right) \cap \psi^{-1}\left(\mathcal{D}_+(y_0)\right) &\to \mathcal{D}_+(z_{00}) \\ a &\mapsto \begin{pmatrix} 1 & \psi_1(a) & \cdots & \psi_n(a) \\ \phi_1(a) & \phi_1(a)\psi_1(a) & & \\ \vdots & & \ddots & \\ \phi_m(a) & & & \phi_m(a)\psi_n(a) \end{pmatrix} \end{aligned}$$

Since $\mathcal{D}_+(z_{00})$ is affine and all components are regular functions, (ϕ, ψ) is a morphism. (iii) is then clear, since ξ is uniquely determined by ϕ and ψ. □

Remark 4.3.4. (i) If $V \subseteq \mathbb{P}^m$ and $W \subseteq \mathbb{P}^n$ are locally closed subsets, then

$$\mathrm{pr}_1^{-1}(V) \cap \mathrm{pr}_2^{-1}(W) \subseteq S_{m,n}$$

is also locally closed, as the inverse image with respect to morphisms. In the direct product $\mathbb{P}^m \times \mathbb{P}^n$, via σ, this corresponds to the product $V \times W$. In this way we can understand the direct product of any two k-varieties as a k-variety, and $V \times W$ fulfills the universal property of direct products. This is immediate from Theorem 4.3.3 and Lemma 4.1.12. The triple

$$(V \times W, \mathrm{pr}_1, \mathrm{pr}_2)$$

is uniquely determined up to isomorphism, by the universal property.
(ii) For closed subsets $V \subseteq \mathbb{A}^m, W \subseteq \mathbb{A}^n$ we have already constructed the direct product $V \times W \subseteq \mathbb{A}^{m+n}$ explicitly, in the first chapter. It obviously has the universal property, and thus coincides with the new construction. In particular, the direct product of affine varieties is again affine.

(iii) The direct product of projective varieties is again projective, by construction. (iv) In Section 3.4 we have considered $\mathbb{P}^m \times \mathbb{P}^n$ just as a set, and we have used bihomogeneous polynomials to construct subsets X. We now observe that these sets X are precisely the closed subsets with respect to our structure as a variety. Homogeneous polynomials on $S_{m,n}$ correspond, via σ, directly to bihomogeneous polynomials on $\mathbb{P}^m \times \mathbb{P}^n$, which are homogeneous of the same degree in both types of variables $\underline{x}$ and $\underline{y}$. With the same argument as in the proof of Theorem 4.2.5 we see that this is not a restriction. △

Example 4.3.5. $\mathbb{P}^1 \times \mathbb{P}^1$ is the variety of singular 2×2-matrices in $\mathbb{P}\left(\mathrm{Mat}_{2\times 2}(K)\right)$, and thus a quadric in $\mathbb{P}^3$:

$$\mathbb{P}^1 \times \mathbb{P}^1 = \mathcal{V}_+\left(\det\begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix}\right) = \mathcal{V}_+(x_0x_3 - x_1x_2) \subseteq \mathbb{P}^3.$$

On $\mathbb{P}^1 \times \mathbb{P}^1$ there are two families of lines :

$$\{a\} \times \mathbb{P}^1 \text{ as well as } \mathbb{P}^1 \times \{a\},$$

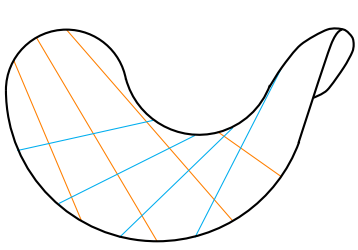
for $a \in \mathbb{P}^1$. If $a = (a_0 : a_1)$ for example, then

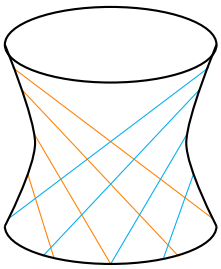
$$\{a\} \times \mathbb{P}^1 = \left\{ \begin{pmatrix} b_0 & b_1 \\ b_2 & b_3 \end{pmatrix} \mid \operatorname{rank}\begin{pmatrix} a_0 & b_0 & b_1 \\ a_1 & b_2 & b_3 \end{pmatrix} = 1 \right\},$$

and this is defined by the two linear equations

$$a_0x_2 - a_1x_0 \text{ und } a_0x_3 - a_1x_1$$

within $S_{1,1}$. The same is true for $\mathbb{P}^1 \times \{a\}$. Any two different lines from the same family are disjoint, any two lines from different families intersect in precisely one point. The following picture shows two affine sections of $\mathbb{P}^1 \times \mathbb{P}^1$, on the left with $\mathcal{D}_+(x_0)$, on the right with $\mathcal{D}_+(x_0 + x_3)$:





One can show that any two infinite closed subsets of $\mathbb{P}^2$ have nonempty intersection (compare Corollaries 4.3.18 and 4.3.19) . In particular we obtain $\mathbb{P}^1 \times \mathbb{P}^1 \ncong \mathbb{P}^2$. △

Theorem 4.3.6. *Let V, W be k-varieties and V projective. Then for any closed $X \subseteq V \times W$ the image $\mathrm{pr}_2(X)$ is closed in W.*

Proof. For $\tilde{X} \subseteq S_{m,n}$ closed we know that $\tilde{X} \subseteq \mathbb{P}^m \times \mathbb{P}^n$ is definable by bihomogeneous polynomials, and $\tilde{X} \cap (\mathbb{P}^m \times \mathbb{A}^n)$ is definable by $\underline{x}$-homogeneous polynomials. Thus the statement follows for affine W directly from Theorem 3.4.1, since $\tilde{X} \cap (V \times W) \subseteq \mathbb{P}^m \times \mathbb{A}^n$ is again definable like that. For general W we choose an open covering $W = \bigcup_{i \in I} W_i$ by affine subsets W_i and consider $X_i := X \cap (V \times W_i)$ in $V \times W_i$. Then $\mathrm{pr}_2(X_i) = \mathrm{pr}_2(X) \cap W_i$ is closed in W_i, and this implies the statement. □

The following Lemma proves that quasi-projective varieties are **separated**. Often, nice arguments about topological spaces use the Hausdorff property. But varieties are not Hausdorff, unfortunately. However, separateness can often be used instead. Note that a topological space is Hausdorff if and only if the diagonal $\{(x, x) \mid x \in X\}$ is closed in $X \times X$ (with respect to the product topology).

Lemma 4.3.7 (Separateness)**.** *For every k-variety V, the diagonal*

$$\Delta_V := \{(a, a) \mid a \in V\}$$

is a closed subset of $V \times V$.

Proof. Let $\iota \colon V \hookrightarrow \mathbb{P}^n$ be a locally closed embedding. By the universal property, the morphisms

$$V \times V \xrightarrow{\mathrm{pr}_1} V \xrightarrow{\iota} \mathbb{P}^n$$

$$V \times V \xrightarrow{\mathrm{pr}_2} V \xrightarrow{\iota} \mathbb{P}^n$$

induce a morphism

$$\iota \times \iota \colon V \times V \hookrightarrow \mathbb{P}^n \times \mathbb{P}^n,$$

and Δ_V is the inverse image of $\Delta_{\mathbb{P}^n}$. So it suffices to prove the statement for $V = \mathbb{P}^n$. With respect to the identification

$$\mathbb{P}^n \times \mathbb{P}^n \xleftarrow{\sigma} S_{n,n}$$

the diagonal corresponds to the symmetric matrices in $S_{n,n}$. So within $S_{n,n}$, $\Delta_{\mathbb{P}^n}$ is defined by the equations

$$z_{ij} - z_{ji} \quad \text{for } i, j = 0, \dots, n.$$

This proves closedness. □

Remark 4.3.8. Alternatively, one can define $\Delta_{\mathbb{P}^n}$ within $\mathbb{P}^n \times \mathbb{P}^n$ by the bihomogeneous equations

$$x_i y_j - x_j y_i = 0$$

for $i, j = 0, \dots, n$. △

The following statement is obvious for Hausdorff spaces. We will see how we can prove it with separateness instead.

Lemma 4.3.9 (Identity Theorem)**.** *Let V, W be varieties and $\phi, \psi \colon V \to W$ morphisms with $\phi \equiv \psi$ on a Zariski dense subset $U \subseteq V$. Then $\phi = \psi$.*

Proof. The set

$$V' := \{a \in V \mid \phi(a) = \psi(a)\}$$

is dense in V, and also the inverse image of Δ_W under the morphism

$$(f, g) \colon V \to W \times W.$$

So V' is closed, and this implies $V' = V$. □

Theorem 4.3.10. *Let $\phi \colon V \to W$ be a morphism of varieties. Then its graph*

$$\Gamma_\phi := \{(a, \phi(a)) \mid a \in V\}$$

is a closed subset of $V \times W$. The graph morphism

$$\begin{aligned} \gamma_\phi \colon V &\to \Gamma_\phi \\ a &\mapsto (a, \phi(a)) \end{aligned}$$

is an isomorphism.

Proof. Γ_ϕ is the inverse image of Δ_W under the morphism

$$\begin{aligned} \phi \times \mathrm{id}_W \colon V \times W &\to W \times W \\ (a, b) &\mapsto (\phi(a), b). \end{aligned}$$

Thus Γ_ϕ is closed. The universal property of the product implies that γ_ϕ is a morphism, and the inverse mapping

$$\begin{aligned} \Gamma_\phi &\to V \\ (a, \phi(a)) &\mapsto a \end{aligned}$$

is the restriction of the projection, and thus also a morphism. □

Corollary 4.3.11. *For every variety V we have $V \cong \Delta_V$, via $a \mapsto (a, a)$.*

Proof. This follows from Theorem 4.3.10, applied to $\phi = \mathrm{id}_V \colon V \to V$. □

Corollary 4.3.12. *Let V be a variety and let $U_1, \ldots, U_r$ be open affine subsets of V. Then $U_1 \cap \cdots \cap U_r$ is also affine.*

Proof. It is clearly enough to consider the case $r = 2$. Then

$$U_1 \cap U_2 \cong \Delta_{U_1 \cap U_2}$$

and

$$\Delta_{U_1 \cap U_2} = (U_1 \times U_2) \cap \Delta_V.$$

Thus $\Delta_{U_1 \cap U_2}$, as a closed subset of the affine variety $U_1 \times U_2$, is affine. □

Theorem 4.3.13. *Let V be projective and $\phi \colon V \to W$ a morphism. Then $\phi(V)$ is closed in W.*

Proof. We know by Theorem 4.3.10 that Γ_ϕ is closed in $V \times W$, and thus

$$\phi(V) = \mathrm{pr}_2(\Gamma_\phi)$$

is closed in W by Theorem 4.3.6. □

Definition 4.3.14. Let V be a locally closed subset of $\mathbb{A}^n$ (or $\mathbb{P}^n$). Let $k \subseteq L \subseteq K$ be an intermediate field. Then

$$V(L) := V \cap L^n,$$

or

$$V(L) := V \cap \left\{ [v] \in \mathbb{P}^n \mid v \in L^{n+1} \right\},$$

respectively, is called the set of **L-rational points of V**. △

Remark 4.3.15. (i) Let V be a k-variety and $k \subseteq L \subseteq K$ an intermediate field. For every $f \in \mathcal{O}(V)$ we then have

$$f\left(V(L)\right) \subseteq L,$$

since f is defined locally by fractions of polynomials over k. For every k-morphism $\phi\colon V \to W$ we thus have

$$\phi\left(V(L)\right) \subseteq W(L),$$

since ϕ is defined locally by regular functions. In particular, every isomorphism yields a bijection between the set of L-rational points.
(ii) Finding L-rational points on a variety can be very hard. For example, the fact that

$$\mathcal{V}_+(z^n - x^n - y^n) \subseteq \mathbb{P}^2(\mathbb{C})$$

does not have (nontrivial) $\mathbb{Q}$-rational points for any n is exactly the famous Fermat's last theorem. △

Theorem 4.3.16. *Let V be an irreducible projective k-variety. Then $\mathcal{O}(V)$ is a finite field extension of k. If $V(k) \neq \emptyset$, then $\mathcal{O}(V) = k$, i.e. every regular function is constant.*

Proof. Let $a \in V$ and $f \in \mathcal{O}(V)$ with $f(a) = 0$. Consider f as a morphism

$$f\colon V \to \mathbb{A}^1.$$

By Theorem 4.3.13 f has a closed image, and thus either $f(V) = \mathbb{A}^1$ or $f(V)$ is finite. Now

$$f\colon V \to \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$$

is also a morphism with closed image, and thus $f(V) = \mathbb{A}^1$ is impossible. So

$$f(V) = \{0, r_1, \ldots, r_d\} = \mathcal{V}(p) \subseteq \mathbb{A}^1$$

for some $p \in k[t]$. Write $p = t^s q$ with $q(0) \neq 0$. Then $f(V) = \{0\} \dot\cup \mathcal{V}(q)$. Now $f(V)$ is irreducible (since V is irreducible), and this implies $f(V) = \{0\}$. We have thus shown that a regular function with a zero must be constant. So $\mathcal{O}(V)$ is a field, by Lemma 4.1.6 (iii).
By Hilbert's Nullstellensatz we have $V(\overline{k}) \neq \emptyset$, and thus there exists a finite field extension L/k and some $a \in V(L)$. The k-algebra homomorphism

$$\begin{aligned} \mathcal{O}(V) &\to L \\ f &\mapsto f(a) \end{aligned}$$

is injective, as we have just shown. Thus $\mathcal{O}(V)$ is a finite field extension of k. In case $V(k) \neq \emptyset$, the same argument shows $\mathcal{O}(V) = k$. □

Corollary 4.3.17. *If V is both affine and projective, then $|V| < \infty$.*

Proof. V has only finitely many irreducible components, each one of which is again closed and thus both affine and projective. So we can assume that V is irreducible. By Theorem 4.3.16 we have

$$\dim_k k[V] = \dim_k \mathcal{O}(V) < \infty,$$

and thus V is finite by Theorem 1.4.16. □

Corollary 4.3.18. *Let $V \subseteq \mathbb{P}^n$ be a hypersurface and $Z \subseteq \mathbb{P}^n$ an infinite closed set. Then $V \cap Z \neq \emptyset$.*

Proof. Let $V = \mathcal{V}_+(p)$ for some homogeneous $p \in k[\underline{x}]$. Now $V \cap Z = \emptyset$ would imply that $Z \subseteq \mathcal{D}_+(p)$ is a closed subset of an affine variety, which is itself affine. This implies $|Z| < \infty$, a contradiction. □

Corollary 4.3.19. *For $n \geqslant 2$, any two hypersurfaces in $\mathbb{P}^n$ have nonempty intersection.*

Proof. By Corollary 4.3.18 it is enough to show that hypersurfaces are infinite. It is enough to consider affine hypersurfaces and the case $K = \overline{k}$. So let $V = \mathcal{V}(p) \neq \emptyset$ be a hypersurface in $\mathbb{A}^n$. Choose some i with $p \notin k[x_i]$. Then $(p) \cap k[x_i] = \{0\}$, and from Theorem 1.4.13 we see that

$$\mathrm{pr}_i(V) \subseteq \mathbb{A}^1 = \overline{k}$$

is k-Zariski dense, and thus infinite. □

4.4 Rational Functions and Maps

We will now generalize the notion of a morphism, to obtain enough of such mappings also for projective varieties.

Definition 4.4.1. Let V, W be k-varieties.
(i) A **rational map** $f\colon V \dashrightarrow W$ is an equivalence class of morphisms

$$\phi\colon U \to W$$

on open and dense subsets U of V, under the following equivalence relation:

$$(\phi\colon U \to W) \sim (\psi\colon U' \to W)$$
$$\vdots$$
$$\exists U'' \subseteq U \cap U' \text{ open and dense in } V \text{ with } \phi \equiv \psi \text{ on } U''.$$

We then also write $f = [\phi]$ for the equivalence class of ϕ.
(ii) The set of all rational maps from V to W is denoted by

$$\mathrm{Rat}_k(V, W).$$

(iii) A rational map $f\colon V \dashrightarrow \mathbb{A}^1$ is called a **rational function** on V. △

Definition 4.4.2. Let $f\colon V \dashrightarrow W$ be a rational map. Then

$$\mathrm{dom}(f) := \bigcup \{U \mid U \subseteq V \text{ open and dense}, \exists \phi\colon U \to W \text{ with } f = [\phi]\}$$

is called the **domain** of f. △

Theorem 4.4.3. *Let $f\colon V \dashrightarrow W$ be a rational map. Then there exists a morphism $f_0\colon \mathrm{dom}(f) \to W$, such that every representative of f is a restriction of f_0.*

Proof. Let $\phi\colon U \to W$ and $\psi\colon U' \to W$ be to representatives of f. By the Identity Theorem 4.3.9 we have $\phi \equiv \psi$ on $U \cap U'$. Thus f_0 can be defined locally by the representatives of f. □

Remark/Example 4.4.4. (i) For every open and dense subset $U \subseteq V$ we have $\mathrm{Rat}_k(V, W) = \mathrm{Rat}_k(U, W)$.
(ii) Let V be an irreducible affine k-variety and $F = \mathrm{Quot}(k[V])$. Then every element of F defines a rational function on V. If $\frac{a}{b}$ with $a, b \in k[V], b \neq 0$, then $\frac{a}{b}\colon \mathcal{D}_V(b) \to \mathbb{A}^1$ is a morphism. Since $\mathcal{D}_V(b)$ is open and nonempty, it is automatically dense in V, and we obtain the rational function $f = [\frac{a}{b}]$. If

$$\frac{a}{b} = \frac{c}{d}$$

is another representation of the same fraction, the morphisms $\frac{a}{b}$ and $\frac{c}{d}$ coincide on the open and dense subset $\mathcal{D}_V(bd) = \mathcal{D}_V(b) \cap \mathcal{D}_V(d)$, and thus define the same rational function.
(iii) In general, $\mathrm{dom}(f)$ can be larger then visible at first sight. For example, consider the projective curve

$$C = \mathcal{V}_+(x_0^3 - x_0x_1^2 - x_1x_2^2) \subseteq \mathbb{P}^2.$$

The rule

$$(a_0 : a_1 : a_2) \mapsto (a_0 : a_1)$$

defines a morphism

$$C \setminus \{(0:0:1)\} \to \mathbb{P}^1,$$

and thus a rational map $f\colon C \to \mathbb{P}^1$. On the other hand, there exists the morphism

$$(a_0 : a_1 : a_2) \mapsto (a_2^2 : a_0^2 - a_1^2),$$

defined on $C \setminus \{(1 : \pm 1 : 0)\}$. On all points of C where both morphisms are defined, they are easily checked to coincide. So f is defined on the whole of C, i.e. it is even a global morphism.
(iv) Let $V \subseteq \mathbb{P}^m$ be closed and irreducible. Every tuple $p_0, \ldots, p_n \in k_+[V]$ of homogeneous elements $\neq 0$ of the same degree then defines the rational map

$$f = (p_0 : \ldots : p_n)\colon V \dashrightarrow \mathbb{P}^n$$

with $\mathrm{dom}(f) \supseteq V \setminus \mathcal{V}_+(p_1, \ldots, p_n)$. △

Theorem 4.4.5. *Let V be a k-variety. Then the rational functions on V form a k-algebra $k(V)$, with respect to pointwise operations. If V is irreducible, $k(V)$ is a field, called the* **function field of** *V.*

Proof. For two rational functions $f_1, f_2\colon V \dashrightarrow \mathbb{A}^1$, $f_1 \pm f_2, f_1 \cdot f_2$ are regular functions (and thus morphisms) on $\mathrm{dom}(f_1) \cap \mathrm{dom}(f_2)$, and thus rational functions on V. If V is irreducible and $f\colon V \dashrightarrow \mathbb{A}^1$ not identically zero, then $\{a \in \mathrm{dom}(f) \mid f(x) \neq 0\}$ is open, nonempty and thus dense in V. On this set one can define $\frac{1}{f}$ as a regular function, and thus $k(V)$ is a field. □

From now on we will restrict ourselves to irreducible varieties. Then every nonempty open subset is automatically dense.

Theorem 4.4.6. *Let V be an irreducible variety.*

(i) One has $k(V) = k(U)$ for every open subset $U \neq \emptyset$ in V.

(ii) One has $k(V) = \bigcup_U \mathcal{O}_V(U)$, where the union runs over all nonempty open subsets of V.

(iii) The field extension $k \subseteq k(V)$ is finitely generated.

(iv) If V is affine, then $k(V) = \mathrm{Quot}(k[V])$.

Proof. (i) is clear from Remark 4.4.4 (i). (ii) is also clear, since the elements of $\mathcal{O}_V(U)$ are morphisms from U to $\mathbb{A}^1$. (iv) follows from

$$k(V) = \bigcup_{\emptyset \neq U \text{ open}} \mathcal{O}(U) = \bigcup_{s \in k[V], s \neq 0} \mathcal{O}(\mathcal{D}_V(s)) = \bigcup_s k[V]_s = \mathrm{Quot}(k[V]),$$

where we have used Theorem 4.1.8. For (iii) we can assume that V is affine, using (i), since by Corollary 4.1.21 V admits a nonempty affine open subset. For affine varieties the statement follows from (iv), since $k[V]$ is finitely generated as a k-algebra, and thus $\mathrm{Quot}(k[V])$ is finitely generated as a field. □

Remark 4.4.7. Let $V \subseteq \mathbb{P}^n$ be closed and irreducible. Then $k_+[V]$ is a $\mathbb{Z}$-graded ring. Let T be the set of all homogeneous elements $\neq 0$, and consider the field

$$k_+[V]_{(T)} = (k_+[V]_T)_0 = \left\{ \frac{p}{q} \mid p, 0 \neq q \in k_+[V] \text{ homogeneous of same degree} \right\}.$$

Then in complete analogy to the affine setting we have $k(V) = k_+[V]_{(T)}$, this time using Theorem 4.2.7. △

Example 4.4.8. (i) $k(\mathbb{A}^n) = k(\mathbb{P}^n) = k(x_1, \ldots, x_n)$. This field is called the **rational function field in n variables**.
(ii) If $p \in k[x_1, \ldots, x_n]$ is irreducible, for $V = \mathcal{V}(p) \subseteq \mathbb{A}^n$ we have

$$k(V) = \mathrm{Quot}\left(k[x_1, \ldots, x_n]/p\right). \qquad \triangle$$

Remark 4.4.9. Rational maps can in general *not* be composed! For example, consider

$$f \colon \mathbb{A}^1 \to \mathbb{A}^2, a \mapsto (a, 0)$$

and

$$g \colon \mathbb{A}^2 \dashrightarrow \mathbb{A}^1; (a, b) \mapsto a/b,$$

where $\mathrm{im}(f) \cap \mathrm{dom}(g) = \emptyset$ and $g \circ f$ is thus not defined. △

Definition 4.4.10. Let V, W be varieties with V irreducible.
(i) A morphism $\phi \colon V \to W$ is called **dominant**, if $\phi(V)$ is dense in W.
(ii) A rational map $f \colon V \dashrightarrow W$ is called **dominant**, if one (equivalently every) of its representing morphisms is dominant.
(iii) The set of all dominant rational maps is denoted by

$$\mathrm{Rat}_k^{\mathrm{dom}}(V, W). \qquad \triangle$$

Remark 4.4.11. (*i*) If $\phi\colon V \to W$ and $\psi\colon W \to X$ are dominant morphisms, then $\psi \circ \phi$ is also dominant.
(*ii*) A morphism $\phi\colon V \to W$ of affine varieties is dominant if and only if the associated ring homomorphism $\phi^*\colon k[W] \to k[V]$ is injective. This is immediate from Theorem 1.4.13. △

Note again that we now assume all varieties to be irreducible!

Theorem 4.4.12. *Let $f\colon V \dashrightarrow W, g\colon W \dashrightarrow X$ be rational maps, and assume f is dominant. Then $g \circ f\colon V \dashrightarrow X$ is a well-defined rational map. If also g is dominant, then so is $g \circ f$.*

Proof. Let $\phi\colon V' \to W$ and $\psi\colon W' \to X$ be representatives of f and g. Then $\phi^{-1}(W') \neq \emptyset$, since ϕ has dense image. Thus $\phi^{-1}(W')$ is dense in V, and the morphism $\psi \circ \phi$ is defined here. So we obtain the rational map $g \circ f\colon V \dashrightarrow X$, and the definition does obviously not depend on the choice of the representatives ϕ and ψ. The rest of the statement is clear. □

Definition 4.4.13. (*i*) A dominant rational map $f\colon V \dashrightarrow W$ is called **birational equivalence** (or just **birational**), if there exists a dominant rational map $g\colon W \dashrightarrow V$ with $g \circ f = \mathrm{id}_V$ and $f \circ g = \mathrm{id}_W$.
(*ii*) Two varieties V, W are called **(k-)birationally equivalent**, if there exists a birational equivalence $f\colon V \dashrightarrow W$.
(*iii*) A variety is called **(k-)rational**, if it is birationally equivalent to some $\mathbb{P}^n$. △

Example 4.4.14. (*i*) Let V be irreducible and $\emptyset \neq U \subseteq V$ open. Then the inclusion $U \hookrightarrow V$ is a birational equivalence. In particular, $\mathbb{A}^n$ is birationally equivalent to $\mathbb{P}^n$, and every irreducible variety is birationally equivalent to some affine variety.
(*ii*) For every irreducible projective variety $V \subseteq \mathbb{P}^n$, the affine cone $\widehat{V} \subseteq \mathbb{A}^{n+1}$ is irreducible and birationally equivalent to $V \times \mathbb{A}^1$. In fact, there are mutually inverse mappings

$$V \times \mathbb{A}^1 \dashrightarrow \widehat{V}$$
$$((a_0 : \ldots : a_n), t) \mapsto t \cdot \left(1, \frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}\right)$$

(without loss of generality assume $V \cap \mathcal{D}_+(x_0) \neq \emptyset$), as well as

$$\widehat{V} \dashrightarrow V \times \mathbb{A}^1$$
$$(a_0, \ldots, a_n) \mapsto ((a_0 : \ldots : a_n), a_0),$$

defined on $\widehat{V} \setminus (0, \ldots, 0)$.
(iii) If $f\colon V \dashrightarrow W$ is dominant and $V(k)$ is Zariski dense, then $W(k)$ is Zariski dense in W. In particular, if V, W are birationally equivalent varieties, $V(k)$ is dense in V if and only if $W(k)$ is dense in W. For a rational variety V, $V(k)$ is always dense in V (at least if k is infinite). △

Theorem 1.4.8 and Theorem 1.4.11 can now easily be proven for rational maps as well. For field extensions $k \subseteq E, k \subseteq F$ we denote by $\mathrm{Hom}_k(E, F)$ the set of k-embeddings of E to F, as usual.

Theorem 4.4.15. *Let V, W be irreducible k-varieties.*
(i) Every dominant rational map $f\colon V \dashrightarrow W$ induces a k-embedding $f^*\colon k(W) \hookrightarrow k(V)$ of function fields. This assignment is functorial, i.e. we have $\mathrm{id}^* = \mathrm{id}$ and $(g \circ f)^* = f^* \circ g^*$ for dominant $g\colon W \dashrightarrow X$.
(ii) The mapping $^*\colon \mathrm{Rat}_k^{\mathrm{dom}}(V, W) \to \mathrm{Hom}_k(k(W), k(V))$ is bijective.
(iii) A dominant rational map $f\colon V \dashrightarrow W$ is a birational equivalence if and only if $f^*\colon k(W) \to k(V)$ is an isomorphism of fields.

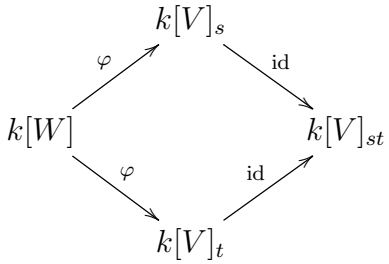
Proof. (i) is clear. For (ii) we can assume V, W to be affine. We now construct the inverse mapping to *. To this end, let $\varphi\colon k(W) \to k(V)$ be a k-embedding. Since $k[W]$ is a finitely generated k-algebra, there exists some $0 \neq s \in k[V]$ with

$$\varphi\,|_{k[W]}\colon k[W] \to k[V]_s = k[\mathcal{D}_V(s)].$$

By Theorem 1.4.8 this $\varphi\,|_{k[W]}$ corresponds to a morphism

$$f_0\colon D_V(s) \to W$$

of affine varieties. Now let $f = [f_0]\colon V \dashrightarrow W$ be the rational map represented by f_0. It does not depend on the choice of s, as can be seen in the following diagram, using the equivalence of categories (Remark 1.4.10):



The assignment $\varphi \mapsto f$ defines the inverse mapping to *, as is easily checked (φ is already uniquely determined by $\varphi\,|_{k[W]}$, and $\varphi\,|_{k[W]}$ corresponds to f_0).
(iii) If f is a birational equivalence, f^* is an isomorphism, by functoriality from (i). Conversely, if $\varphi\colon k(V) \to k(W)$ is an inverse embedding to f^*, and if $\varphi = g^*$ for some $g \in \mathrm{Rat}_k^{\mathrm{dom}}(W, V)$, then

$$(f \circ g)^* = g^* \circ f^* = \varphi \circ f^* = \mathrm{id}_{k(W)}.$$

From bijectivity of * we obtain $f \circ g = \mathrm{id}_W$ (analogously for $g \circ f$). So f is a birational equivalence. □

Corollary 4.4.16. *For two irreducible k-varieties V and W, the following are equivalent:*
(i) V and W are birationally equivalent.
(ii) $k(V) \cong_k k(W)$
(iii) There are open subsets $\emptyset \neq V' \subseteq V, \emptyset \neq W' \subseteq W$ with $V' \cong W'$.

Proof. "$(i) \Leftrightarrow (ii)$" is clear from Theorem 4.4.15. Also clear is "$(iii) \Rightarrow (i)$" . For "$(i) \Rightarrow (iii)$" let $f\colon V_0 \to W$ and $g\colon W_0 \to V$ be morphisms on open and dense subsets, with $g \circ f = \mathrm{id}_{f^{-1}(W_0)}$ and $f \circ g = \mathrm{id}_{g^{-1}(V_0)}$. This immediately implies

$$f\colon f^{-1}(W_0) \xrightarrow{\cong} g^{-1}(V_0). \qquad \square$$

Corollary 4.4.17. *An irreducible variety V is rational if and only if $k(V)$ is a rational function field $k(x_1, \ldots, x_n)$.*

Example 4.4.18. Let $C = \mathcal{V}(y^2 - x^2 - x^3) \subseteq \mathbb{A}^2$ be the curve from Example 1.2.2 (iii). The rational function

$$\begin{aligned} f\colon C &\dashrightarrow \mathbb{A}^1 \\ (a, b) &\mapsto \frac{b}{a} \end{aligned}$$

is a birational equivalence. The inverse mapping is

$$\begin{aligned} g\colon \mathbb{A}^1 &\to C \\ r &\mapsto (r^2 - 1, r(r^2 - 1)). \end{aligned}$$

So C is a rational curve and $k(C) = k(x)$. Geometrically, f maps each point of $C \setminus \{(0, 0)\}$ to the slope of the line through 0 and the point. We obtain an isomorphism between the open subsets $C \setminus \{(0, 0)\}$ and $\mathbb{A}^1 \setminus \{\pm 1\}$. Thus we have solved the equation $y^2 - x^2 - x^3 = 0$ almost completely. △

Example 4.4.19. (i) Let $H \subseteq \mathbb{P}^n$ be a k-hyperplane, and $z \in \mathbb{P}^n(k) \setminus H$. For every point $z \neq a \in \mathbb{P}^n$ we denote by $\pi(a) \in H$ the intersection point of the line spanned by z and a with H. We obtain a rational map

$$\pi \colon \mathbb{P}^n \dashrightarrow H = \mathbb{P}^{n-1},$$

called **projection from z**. We can choose coordinates such that $z = (1 : 0 : \ldots : 0)$ and $H = \mathcal{V}_+(x_0)$. Then

$$\pi(a_0 : \ldots : a_n) = (0 : a_1 : \ldots : a_n),$$

and $\pi \colon \mathbb{P}^n \setminus \{z\} \to H$ is a morphism.
(ii) More generally, let Z, L be linear subspaces of $\mathbb{P}^n$, with $Z \cap L = \emptyset$ and $\dim(Z) + \dim(L) = n - 1$ (i.e. they come from k-subspaces $\tilde{Z}, \tilde{L} \subseteq K^{n+1}$ with $\tilde{Z} \oplus \tilde{L} = K^{n+1}$). Every point $a \in \mathbb{P}^n \setminus Z$ corresponds to a line through the origin $v \subseteq K^{n+1}$, for which $\operatorname{span}(\tilde{Z}, v) \cap \tilde{L}$ is one-dimensional. This defines a rational map

$$\pi \colon \mathbb{P}^n \dashrightarrow L$$

called **projection from Z**. If coordinates are chosen such that $L = \mathcal{V}_+(x_0, \ldots, x_m)$ and $Z = \mathcal{V}_+(x_{m+1}, \ldots, x_n)$, then

$$\pi(a_0 : \ldots : a_n) = (0 : \ldots : 0 : a_{m+1} : \ldots : a_n).$$

If $V \subseteq \mathbb{P}^n$ is an irreducible variety with $V \not\subseteq Z$, then $\pi \mid_V \colon V \dashrightarrow L$ is again a rational map. $\triangle$

A **quadric** Q is a variety in $\mathbb{P}^n$ defined by a quadratic polynomial. If $\operatorname{char}(k) \neq 2$, we can assume $Q = \mathcal{V}_+(c_0 x_0^2 + \cdots + c_r x_r^2)$ with $c_i \in k^\times$, after a change of basis (diagonalization of quadratic forms). For $r \geqslant 2$ the quadric Q is irreducible (Exercise 75). Q is called **non-degenerate**, if $r = n$.

Theorem 4.4.20. *Let k be infinite with $\operatorname{char}(k) \neq 2$, and let $Q = \mathcal{V}_+(q) \subseteq \mathbb{P}^n$ be a non-degenerate quadric. We then have*

$$Q \text{ } k\text{-rational} \Leftrightarrow Q(k) \neq \emptyset.$$

Proof. "$\Rightarrow$ is clear from Example 4.4.14 (iii). For "$\Leftarrow$" choose $z \in Q(k)$ and a k-hyperplane $H \subseteq \mathbb{P}^n$ with $z \notin H$. The projection from z yields a k-rational map

$$\pi \colon Q \dashrightarrow H.$$

We now construct an inverse mapping. To this end, for $b \in H$ we intersect the line spanned by z and b with Q. In most cases this will define exactly one point besides z, which is the inverse image of b with respect to π.
So let $z = [v]$ and $b = [w]$. We choose $s \in K$ with $q(sv + w) = 0$ and then set $a = [sv + w]$. We have

$$q(sv + w) = s^2 q(v) + 2sb_q(v, w) + q(w) = 2sb_q(v, w) + q(w),$$

where b_q is the symmetric bilinear form defined by q. The equation $0 = q(sv+w)$ can be solved uniquely for s, in case $b_q(v, w) \neq 0$, and yields

$$a = [2b_q(v, w)w - q(w)v] .$$

Outside of the k-hyperplane $L = \{[w] \mid b_q(v, w) = 0\}$ we thus obtain a morphism $f \colon \mathbb{P}^n \setminus L \to Q$, which defines an inverse rational map $f \colon H \dashrightarrow Q$ to π, by restriction (H can be chosen with $H \nsubseteq L$). □

Example 4.4.21. The proof of Theorem 4.4.20 provides us with an explicit birational equivalence. For example, let $q = x_0x_1 + x_2^2 - x_3^2$ and $Q = \mathcal{V}_+(q) \subseteq \mathbb{P}^3$. We choose $z = (1 : 0 : 0 : 0) \in Q$ and $H = \mathcal{V}_+(x_0)$. The map $\pi \colon Q \dashrightarrow H$ is thus defined by the rule

$$\pi(a_0 : a_1 : a_2 : a_3) = (0 : a_1 : a_2 : a_3).$$

The inverse mapping now has the following form:

$$\begin{aligned} f \colon H = \mathbb{P}^2 &\dashrightarrow Q \\ (0 : b_1 : b_2 : b_3) &\mapsto (b_3^2 - b_2^2 : b_1^2 : b_1b_2 : b_1b_3), \end{aligned}$$

and defines a rational parametrization of Q. △

Example 4.4.22. There exists a birational equivalence between $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$. It is defined by the rule

$$\begin{aligned} \mathbb{P}^1 \times \mathbb{P}^1 &\dashrightarrow \mathbb{P}^2 \\ ((a_0 : a_1), (b_0 : b_1)) &\mapsto (a_0b_0, a_0b_1, a_1b_0) \\ (b_0 : b_2), (b_0 : b_1) &\leftarrow\!\shortmid (b_0 : b_1 : b_2). \end{aligned}$$

△

Bibliography

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

[2] T. Becker and V. Weispfenning. *Gröbner bases*, vol. 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[3] D. Eisenbud. *Commutative algebra*, vol. 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[4] D. Eisenbud and J. Harris. *The geometry of schemes*, vol. 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[5] W. Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[6] J. Harris. *Algebraic geometry*, vol. 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[7] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[8] K. Hulek. *Elementare algebraische Geometrie*. Vieweg Studium: Aufbaukurs Mathematik. [Vieweg Studies: Mathematics Course]. Friedr. Vieweg & Sohn, Braunschweig, 2000. Grundlegende Begriffe und Techniken mit zahlreichen Beispielen und Anwendungen. [Basic concepts and techniques with various examples and applications].

[9] S. Lang. *Algebra*, vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edn., 2002.

[10] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, russian edn., 2013. Varieties in projective space.

[11] ———. *Basic algebraic geometry. 2*. Springer, Heidelberg, 2013. Schemes and complex manifolds, Translated from the 2007 third Russian edition by Miles Reid.

Exercises

Exercise 1. Let R be a ring and $I \subseteq R$ and ideal. Recall the definition of the quotient ring R/I, and show the following:

(i) I is a radical ideal $\Leftrightarrow$ R/I is reduced.

(ii) I is a prime ideal $\Leftrightarrow$ R/I is an integral domain.

(iii) I is a maximal ideal $\Leftrightarrow$ R/I is a field.

(iv) Maximal ideals are prime, and prime ideals are radical.

(v) If $\varphi\colon R \to S$ is a ring homomorphism and $J \subseteq S$ is an ideal, then $\varphi^{-1}(J)$ is an ideal in R. If J is radical/prime, then so is $\varphi^{-1}(J)$. If J is a maximal ideal, how about $\varphi^{-1}(J)$?

Exercise 2. (i) Show that for every ideal I the radical $\sqrt{I}$ (cf. Def 1.1.1) is again an ideal.
(ii) Prove Lemma 1.1.3.

Exercise 3. Let R be a ring, $S \subseteq R$ a multiplicative subset, and $I \subseteq R$ an ideal. Show the following:

(i) There is a canonical bijection between ideals of R/I, and ideals in R that contain I.

(ii) The bijection from (i) preserves radical/prime/maximal ideals.

(iii) There is a canonical bijection between prime ideals of the localization $S^{-1}R$ and prime ideals of R that are disjoint to S.

(iv) Is (iii) also true for arbitrary ideals?

Exercise 4. Let R be a ring. Show the following:

(i) Every prime ideal $\mathfrak{p} \subseteq R$ contains a minimal prime ideal of R.

(ii) Every minimal prime ideal of R contains only zero divisors.

Hint: examine the localization $R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1}R$

(iii) If R is reduced, the set of zero divisors of R is precisely the union of all minimal prime ideals of R.

Exercise 5. Let R be a unique factorization domain and let K be its field of fractions. Show that the only elements in K that are integral over R are the elements of R itself.

Exercise 6. Let R be a ring. Recall the definition of an R-module. An R-module M is called **Noetherian** if every submodule is finitely generated. Show that the direct sum of two Noetherian R-modules is again Noetherian.

Exercise 7. Show that:

(i) $k[x, y]/(x^2 - y)$ is isomorphic to the polynomial ring $k[t]$ in one variable.

(ii) $k[x, y]/(xy - 1)$ is not isomorphic to $k[t]$.

(iii) If k is algebraically closed, then for every quadratic irreducible polynomial $p \in k[x, y]$ the algebra $k[x, y]/(p)$ is isomorphic to $k[x, y]/(x^2 - y)$ or to $k[x, y]/(xy - 1)$.

Exercise 8. Let $p, q \in k[t]$ be univariate polynomials, and set $g := \gcd(p, q)$. Show $\mathcal{V}(p, q) = \mathcal{V}(g)$.

Exercise 9. Let k be an algebraically closed field. Show that every finite subset of k^n is an affine k-variety.

Exercise 10. Let $p_1 = x^2 - yz, p_2 = xz - x$ and $I = (p_1, p_2) \subseteq \mathbb{Q}[x, y, z]$.

(i) Sketch or plot the real points of $\mathcal{V}(I)$ in $\mathbb{R}^3$.

(ii) Is I a prime ideal?

(iii) Find three different prime ideals in $\mathbb{Q}[x, y, z]$ that contain I.

(iv) Find generators for $\sqrt{I}$.

Exercise 11. Let $I = (p_1, \ldots, p_r s)$, $J = (q_1, \ldots, q_s) \subseteq k[\underline{x}]$ be ideals. Show the following:

(*i*) $I + J := \{p + q \mid p \in I, q \in J\}$ is the smallest ideal containing both I and J.

(*ii*) $I + J = (p_1, \ldots, p_r, q_1, \ldots, q_s)$.

(*iii*) $\mathcal{V}(I + J) = \mathcal{V}(I) \cap \mathcal{V}(J)$.

Exercise 12. Let $I = (p_1, \ldots, p_r) \subseteq k[\underline{x}]$ an ideal and y a new variable. Show the following:

(*i*) $p \in \sqrt{I} \Leftrightarrow 1 \in (p_1, \ldots, p_r, 1 - yp) \subseteq k[\underline{x}, y]$.

(*ii*) $\sqrt{(x_1 x_2, (x_1 - x_2)x_1)} = (x_1)$.

Exercise 13. Let $a, b, c, d \in \mathbb{R}$ and $d \neq 0$. Consider the following ideals:

$$\begin{aligned} \mathfrak{m}_1 &:= (x - a, y - b) \\ \mathfrak{m}_2 &:= (x - a, (y - b)^2 + d^2) \\ \mathfrak{m}_3 &:= ((x - a)^2 + d^2, y - (bx + c)). \end{aligned}$$

Show that $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3$ are maximal ideals in $\mathbb{R}[x, y]$, and that each maximal ideal of $\mathbb{R}[x, y]$ is of one of that forms.

Exercise 14. Let $V \subseteq \mathbb{C}^n$ be an affine $\mathbb{C}$-variety. Show that V is an affine $\mathbb{R}$-variety if and only if V is closed under coordinatewise complex conjugation.

Exercise 15. Let $O \subseteq \mathbb{C}$ be non-empty and open with respect to the Euclidean topology on $\mathbb{C}$. Show that O is an affine $\mathbb{R}$-variety if and only if $O = \mathbb{C}$. Then extend the statement to $\mathbb{C}^n$.

Exercise 16. Let a robotic arm in $\mathbb{R}^2$ be given by two rods of length 2 and 1, connected by swivel joints, as can be seen in Figure 4.1. The angles α and β can take arbitrary real values.

(*i*) Show that the set of all points that A can reach in $\mathbb{R}^2$ is the intersection of an affine $\mathbb{R}$-variety in $\mathbb{C}^2$ with $\mathbb{R}^2$ (i.e. it is the set of real points of this variety).

(*ii*) Show that the set of all points that B can reach in $\mathbb{R}^2$ is not the set of real points of an affine variety in $\mathbb{C}^2$.

(*iii*) Sketch or plot the sets of points that A and B can reach in $\mathbb{R}^2$.

(*iv*) Show that the set of all points that B can reach in $\mathbb{R}^2$ is the projection of the real points of an affine variety in $\mathbb{C}^4$.

(*v*) Determine the set of all positions of A in $\mathbb{C}^2$, from which B can reach the positions $(2,0), (3,0), (4,0)$.

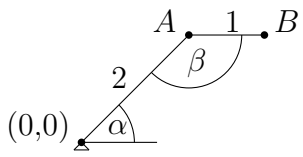


Figure 4.1: Planar robotic arm

Exercise 17. Show that the Zariski topology on $\mathbb{A}^{n+m} = \mathbb{A}^n \times \mathbb{A}^m$ does not coincide with the product topology.

Exercise 18. Let k be a field and K an algebraically closed field extension. Let

$$V = \left\{(t, t^2, t^3) \mid t \in K\right\} \subseteq K^3.$$

(*i*) Show that V is an affine k-variety, and find defining equations for V.

(*ii*) Compute $\mathcal{I}(V)$.

(*iii*) Show that V is a subvariety of $\mathcal{V}(xz - y^2)$.

Exercise 19. Let V and W be affine k-varieties with $V \subseteq W$. Show

$$W = V \cup \overline{(W \setminus V)}.$$

Exercise 20. Let R be a ring and denote by $\operatorname{Spec}(R)$ the set of all prime ideals of R. For a subsets $I \subseteq R$ and $V \subseteq \operatorname{Spec}(R)$ we define

$$\begin{aligned} \mathcal{V}(I) &:= \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\} \\ \mathcal{I}(V) &:= \bigcap_{\mathfrak{p} \in V} \mathfrak{p}. \end{aligned}$$

(*i*) Prove an analogue of Hilbert's Nullstellensatz in this setup.

(*ii*) Show that the sets $\mathcal{V}(I)$ fulfill the axioms for closed sets of a topology.

(*iii*) If $\varphi\colon R \to S$ is a ring homomorphism, then the map

$$\begin{aligned} \operatorname{Spec}(S) &\to \operatorname{Spec}(R) \\ \mathfrak{q} &\mapsto \varphi^{-1}(\mathfrak{q}) \end{aligned}$$

is continuous with respect to the topologies from (*ii*).

Exercise 21. Prove Lemma 1.3.6.

Exercise 22. Prove Lemma 1.3.11.

Exercise 23.

(*i*) Find a set $X \subseteq \mathbb{A}^n$, such that the topological space X (with respect to the Zariski topology) contains an open set $Y \subseteq X$, which is not dense in X.

(*ii*) Show that each non-discrete set $X \subseteq \mathbb{A}^n$ is not hausdorff (also see Lemma 1.3.3).

Exercise 24. Show that $\mathrm{GL}_n(K)$ is open in the k-Zariski topology.

Exercise 25. Let $V \subseteq \mathbb{A}^3$ be the affine variety defined by the following equations:

$$x^2 - yz = 0 \quad \text{und} \quad xz - x.$$

Show that V has 3 irreducible components and find their prime ideals.

Exercise 26. Let $V = \mathcal{V}(y^2 - z^3, x^2 - z) \subseteq \mathbb{A}^3$. Show that V is a union of two subvarieties (curves), and find definig equation for these curves.
Hint: Consider $(x^4 + x^2z + z^2)(x^2 - z) - (y^2 - z^3) \in (y^2 - z^3, x^2 - z)$.

Exercise 27. Let $V = V_1 \cup V_2 \subseteq \mathbb{A}^3$ be the union of the two curves $V_1 = \mathcal{V}(x^3 - y, x^2 - z)$ and $V_2 = \mathcal{V}(x^3 + y, x^2 - z)$. Further let $W = \mathcal{V}(xy) \subseteq \mathbb{A}^2$.

(*i*) Show that also W is a union of two strict subvarieties (curves) $W = V_3 \cup V_4$, and find defining equations for V_3 and V_4.

(*ii*) Show that there exist polynomial mappings $p_i : V_i \to \mathbb{A}$ and $q_i = \mathbb{A} \to V_i$, such that $p_i \circ q_i = \mathrm{id}_{\mathbb{A}}$ and $q_i \circ p_i = \mathrm{id}_{V_i}$, for $i = 1, \ldots, 4$.

(*iii*) Do there exist polynomial mappings $p : V \to W$ and $q : W \to V$, such that $p \circ q = \mathrm{id}_W$ and $q \circ p = \mathrm{id}_V$? Sketch a proof of your answer.

Exercise 28. Prove Corollary 1.3.17 for ideals I in an arbitrary noetherian ring A.

Exercise 29. Compute the Zariski closure of the following sets in $\mathbb{A}^2$:

(i) The projection of $\mathcal{V}(xy-1)$ onto the x-axis.

(ii) The boundary of the positive orthant in $\mathbb{R}^2$.

(iii) The graph of the sine function

$$\{(x, \sin(x)) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$$

in $\mathbb{R}^2$.

Exercise 30.

(i) Let R be a ring and I, $J \subseteq R$ ideals in R. Show that

$$(I : J) := \{a \in R \mid aJ \subseteq I\}$$

is an ideal in R, containing I.

(ii) Compute generators for $(xz, yz) : (z) \subseteq k[x, y, z]$ and determine

$$\mathcal{V}((xz, yz) : (z)) \subseteq \mathbb{A}^3.$$

(iii) Compute generators for $(y^2 - z^3, x^2 - z) : (x^2 - z, x^3 - y) \subseteq k[x, y, z]$ and determine $\mathcal{V}((y^2 - z^3, x^2 - z) : (x^2 - z, x^3 - y)) \subseteq \mathbb{A}^3$.

Exercise 31. Let $V \subseteq \mathbb{A}^n$ be an affine k-variety.

(i) Show that V is irreducible if and only if $k[V]$ is an integral domain.

(ii) Assume V is reducible. Show that there exist polynomials $p, q \in k[x_1, \ldots, x_n]$ with

$$V = (V \cap \mathcal{V}(p)) \cup (V \cap \mathcal{V}(q)),$$

with $V \cap \mathcal{V}(p) \subsetneq V$, $V \cap \mathcal{V}(q) \subsetneq V$ and $V \subseteq \mathcal{V}(pq)$.

Exercise 32.

(i) Let $V = \{(t, t^2, t^3) : t \in \mathbb{C}\} \subseteq \mathbb{C}^3$ and $p_1 = 2x^2 + y^2$, $p_2 = z^2 - y^3 + 3xz$, $q_1 = 2y + xz$, $q_2 = 3y^2$. Show that $p_1 = q_1$ and $p_2 = q_2$ holds in $k[V]$.

(*ii*) Show that $\mathcal{V}(x^3 + xy^2 - xz, yx^2 + y^3 - yz) \subseteq \mathbb{C}^3$ is reducible.

Exercise 33. Let $V = \mathcal{V}(x^2 - y^2z^2 + z^3) \subseteq \mathbb{C}^3$ and

$$\begin{aligned} \varphi\colon V &\to \mathbb{C} \\ (a_1, a_2, a_3) &\mapsto a_3. \end{aligned}$$

(*i*) Find defining equations for the affine $\mathbb{R}$-variety

$$\varphi(c)^{-1} = \{a \in V \mid \varphi(a) = c\}$$

where $c \in \mathbb{R}$.

(*ii*) Show $\varphi(c)^{-1} \cap \mathbb{R}^3 \neq \emptyset$ for all $c \in \mathbb{R}$.

(*iii*) Sketch or plot $\varphi(c)^{-1}$ for $c \in \{-2, -1, 0, 1, 2\}$.

(*iv*) Sketch or plot $\psi(c)^{-1}$ for $c \in \{-2, -1, 0, 1, 2\}$, where

$$\begin{aligned} \psi\colon V &\to \mathbb{C} \\ (a_1, a_2, a_3) &\mapsto a_1^2 + a_2^2. \end{aligned}$$

Exercise 34. Let K be algebraically closed with prime field k. Show that

$$\big\{A \in K^{n\times n} \mid A \text{ singular}\big\}$$

is an irreducible affine k-variety.

Exercise 35. Show that the mappings $p \mapsto p^*$ and $\varphi \mapsto p_\varphi$ from the proof of Theorem 1.4.8 are mutually inverse.

Exercise 36. Prove Theorem 1.4.11.

Exercise 37. Show that the map

$$\begin{aligned} \mathbb{A}^1 &\to \mathcal{V}(x_1^3 - x_2^2) \subseteq \mathbb{A}^2 \\ r &\mapsto (r^2, r^3) \end{aligned}$$

is a homeomorphism with respect to the Zariski topology.

Exercise 38. Show that the following $\mathbb{Q}$-varieties are isomorphic:

(*i*) $\mathcal{V}(x^2 - y) \subseteq \mathbb{A}^2$ and $\mathbb{A}^1$

(*ii*) $\mathcal{V}(x^3 - y, x^2 - z) \subseteq \mathbb{A}^3$ and $\mathbb{A}^1$

Show that the following $\mathbb{Q}$-varieties are not isomorphic:

(*iii*) $\mathcal{V}(xy - 1) \subseteq \mathbb{A}^2$ and $\mathbb{A}^1$

(*iv*) $\mathcal{V}(y^2 - z^3, x^2 - z) \subseteq \mathbb{A}^3$ and $\mathcal{V}(xy) \subseteq \mathbb{A}^2$

Exercise 39. Let

$$V_1 = \mathcal{V}(y - x^2, z + x^3 + 2x) \subseteq \mathbb{C}^3$$
$$V_2 = \mathcal{V}(x^2 + 2xz + 2y^2 + 3y, xy + 2x + z, xz + y^2 + 2y) \subseteq \mathbb{C}^3$$

and $\pi_i \colon V_i \to \mathbb{C}; (a_1, a_2, a_3) \mapsto a_1$ for $i = 1, 2$.

(*i*) Show that π_1 is bijective and compute its inverse function.

(*ii*) Show that π_2 is bijective and compute its inverse function.

Exercise 40. Let A, B, C be k-algebras where C is a domain. Show that there is a bijection between $\mathrm{Hom}_k(A \times B, C)$ and

$$\mathrm{Hom}_k(A, C) \cup \mathrm{Hom}_k(B, C)$$

(cf. proof of Theorem 1.4.16).

Exercise 41. Let a closed toggle chain in $\mathbb{R}^2$ be given, consisting of four rods of lengths a, b, c, and d, connected with swivel joints, as depicted in Figure 4.2.

(*i*) Show that the points that A can reach in $\mathbb{R}^2$ (midpoint of upper rod) are the real points of an affine $\mathbb{R}$-variety, for $a = b = c = d = 5$, and for $a = 3, b = 9, c = 10, d = 13$.

(*ii*) Sketch or plot the set of points in $\mathbb{R}^2$ that A can reach for $a = b = c = d = 5$ and $a = 3, b = 9, c = 10, d = 13$.

Exercise 42. Let an ellipse compass in $\mathbb{R}^2$ be given, consisting of two slides that can move along the x- and y-axis, respectively. Both slides are joint to a rod of length l via swivel joints, see Figure4.3.

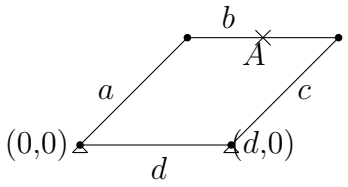


Figure 4.2: Closed toggle chain

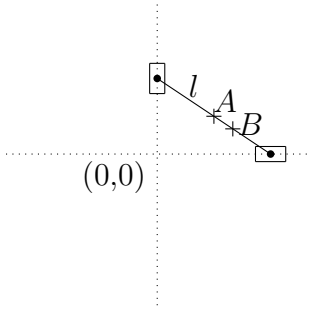


Figure 4.3: Ellipse compass

(i) Show that the sets of points that A and B can reach in $\mathbb{R}^2$ (midpoint and quarter point of rod, respectively) are the real points of affine $\mathbb{R}$-varieties, where we set $l = 2$.

(ii) Sketch or plot the sets of points that A and B can reach in $\mathbb{R}^2$.

Exercise 43. Show that every orthogonal matrix $A \in \mathbb{R}^{2\times 2}$ with $\det(A) = 1$ is of the form

$$\frac{1}{1+t^2}\begin{bmatrix} 1-t^2 & -2t \\ 2t & 1-t^2 \end{bmatrix}$$

for some $t \in \mathbb{R} \cup \{\infty\}$, where $p(\infty) := \mathrm{LC}(p)$ for $p \in \mathbb{R}[t]$.

Exercise 44. Every element of the group $\mathrm{SE}(2)$ of Euclidean motions can be seen as a mapping

$$\mathbb{R}^2 \to \mathbb{R}^2 : \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \frac{1}{1+t^2}\begin{bmatrix} 1-t^2 & -2t \\ 2t & 1-t^2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \tag{4.1}$$

where $v_1, v_2 \in \mathbb{R}$ and $t \in \mathbb{R} \cup \{\infty\}$ We again consider the ellipse compass from Exercise 42.

(i) Sketch or plot the set of points that A and B can reach in $\mathbb{R}^2$, by proceeding as follows:
Define a coordinate system at the moving rod, and one in the fixed plane. Map the points of the moving system to the fixed system by the mapping (4.1), where v_1, v_2 and t are yet to be determined. You thus obtain trajectories of the corresponding points, which still depend on the points and the parameters v_1, v_2 and t. By suitable choice of points, of which the trajectories are known, it is possible to determine two of the three parameters v_1, v_2 and t. The remaining parameter then parametrizes the trajectories.

(ii) Let the inverse mechanism to the ellipse compass be given: Two slides are connected by swivel joints to a plane ($= \mathbb{R}^2$). The distance of the slides is $l = 2$. Two rods of lengths $2l = 4$ can slide through the slides. The two rods are connected at a fixed angle of 90 degree in their midpoints, see Figure 4.4. Sketch or plot the set of points that C (intersection point of rods) and D (quarter point of a rod) can reach in $\mathbb{R}^2$.

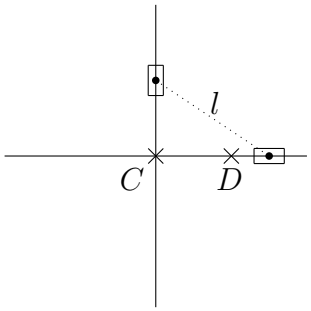


Figure 4.4: Inverse ellipse compass

Exercise 45. Let three rods of lengths l_1, l_2 and l_3 be given. The rods are connected to a plane ($= \mathbb{R}^2$) with swivel joints at one end, and with a movable platform at the other end, see Figure 4.5. The platform is an isosceles triangle with basis $c = 14$ and height $h_c = 10$. By changing the lengths of the rods, the platform can move. Sketch or plot the position of the platform in $\mathbb{R}^2$ for $l_1 = 9$, $l_2 = 8$ and $l_3 = 10$, where you can compute the solutions numerically Hint: Use the mapping (4.1).

Exercise 46. Show that there are $\binom{n+d}{n}$ monomials of degree d in the variables $x_0, \ldots, x_n$.

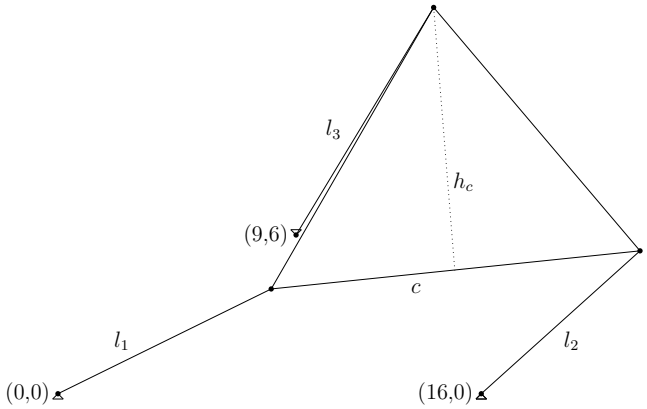


Figure 4.5: Planar 3-RPR mechanism

Exercise 47. Show that the radical of a monomial ideal $I \subseteq k[\underline{x}]$ is again monomial. Is the converse also true?

Exercise 48. Let $I \subsetneq k[\underline{x}]$ be a monomial ideal, and

$$C(I) := \{\alpha \in \mathbb{N}^n : \underline{x}^\alpha \notin I\}$$

the set of exponents, whose monomials that are not contained in I. Further set

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0), \\ e_2 &= (0, 1, \ldots, 0), \\ &\vdots \\ e_n &= (0, \ldots, 0, 1), \\ [e_{i_1}, \ldots, e_{i_r}] &= \{a_1 e_{i_1} + \ldots + a_r e_{i_r} \mid a_j \in \mathbb{N}, 1 \leqslant j \leqslant r\}. \end{aligned}$$

for $i_1 < \ldots < i_r$.

(*i*) Show that $\mathcal{V}(I)$ is the union of finitely many coordinate subspaces (i.e. varieties of the form $\mathcal{V}(x_{l_1}, \ldots, x_{l_s})$).

(*ii*) Show

$$\mathcal{V}(x_{l_1}, \ldots, x_{l_s}) \subseteq \mathcal{V}(I) \iff [e_{i_1}, \ldots, e_{i_r}] \subseteq C(I)$$

wohere $\{l_1, \ldots, l_s\} \uplus \{i_1, \ldots, i_r\} = \{1, \ldots, n\}$.

Exercise 49.

(i) Order the following monomials with respect to the lexicographic monomial ordering, and the degree-lexicographic monomial ordering, both in case of $x > y > z$ and $x < y < z$:

$$\{x, y, z, x^2, z^2, x^3\}, \{x^2y^8, x^5yz^4, xyz^3, xy^4\}$$

(ii) Consider $\mathbb{N}$ with the usual ordering. Between any two numbers there exist only finitely many other numbers. Is the same also true for all monomial orderings on $\mathbb{N}^n$, if $n \geqslant 2$?

Exercise 50. Show the following:

(i) Every monomial ordering $\preccurlyeq$ on $\mathbb{N}^n$ can be extended to a linear ordering $\preccurlyeq$ on $\mathbb{Q}^n$, with the following property:

$$\alpha \preccurlyeq \beta \Rightarrow \alpha + \gamma \preccurlyeq \beta + \gamma$$

for all $\alpha, \beta, \gamma \in \mathbb{Q}^n$.

(ii) Let $\preccurlyeq$ be an ordering on $\mathbb{Q}^n$ as in (i). Show that the following set is a hyperplane in $\mathbb{R}^n$:

$$H = \{x \in \mathbb{R}^n \mid \forall \epsilon > 0 \, \exists q_+, q_- \in B_\epsilon(x) \cap \mathbb{Q}^n : q_+ \preccurlyeq 0 \preccurlyeq q_-\}.$$

Hint for the dimension: Show $\mathbb{Q}^n \nsubseteq H$, and that for $q \preccurlyeq 0 \preccurlyeq p$ in $\mathbb{Q}^n$ the connecting line always meets H.

(iii) Compute H from (ii) on case of $\preccurlyeq_{\text{lex}}$.

Exercise 51. Show that the following rule defines a monomial ordering on $\mathbb{N}^2$:

$$\alpha \preccurlyeq \beta \quad :\Leftrightarrow \quad \alpha_1 + \alpha_2\sqrt{2} \leqslant \beta_1 + \beta_2\sqrt{2}.$$

Show that every element from $\mathbb{N}^2$ has a direct predecessor with respect to $\preccurlyeq$. Is this true for every monomial ordering?

Exercise 52. Let $k[\underline{x}]$ be equipped with a lexicographic monomial ordering $\preccurlyeq_{\text{lex}}$. Show that for any ideal $I \subseteq k[\underline{x}]$, the following are equivalent:

(i) $\mathcal{V}(I)$ is finite.

(*ii*) For every $i = 1, \ldots, n$ there exists $p_i \in I$ with $\mathrm{LM}(p_i) = x_i^{d_i}$.

Exercise 53. (*i*) Compute a normal form of $x^7y^2 + x^3y^2 - y + 1$ modulo $xy^2 - x, x - y^3$, with respect to the lexicographic ordering and with respect to the degree-lexicographic ordering (with $x > y$). What happens if $xy^2 - x, x - y^3$ is replaced by $x - y^3, xy^2 - x$?

(*ii*) Repeat (*i*) for $xy^2 - x$ and $xy + 1, y^2 - 1$. What do you notice?

Exercise 54. Prove the converse assertion of Corollary 2.3.4: Let $I \subseteq k[\underline{x}]$ be an ideal and $G = \{g_1, \ldots, g_s\}$ a subset of I, such that for every $p \in k[\underline{x}]$, any normal form of p modulo G coincides with the canonical form $\mathrm{cf}_I(p)$. Then G is a Gröbner basis of I.

Exercise 55. Let $I = (p) \subseteq k[\underline{x}]$ be a principal ideal. Show that every Gröbner basis of I contains a constant multiple of p.

Exercise 56. Prove the assertion in Remark 2.3.16(*ii*).

Exercise 57. Let $g_1, g_2 \in k[x]$ be polynomials for which $\mathrm{LM}(g_1), \mathrm{LM}(g_2)$ are relatively prime. Show that 0 is the only normal form of $S(g_1, g_2)$ modulo g_1, g_2. What does this mean for the Buchberger Algorithm in general, and in particular when applied to a set of linear polynomials?

Exercise 58. Let $\mathfrak{p} \subseteq k[\underline{x}]$ be a prime ideal. Show that all elements from the reduced Gröbner basis of $\mathfrak{p}$ are irreducible in $k[\underline{x}]$. Is the converse also true?

Exercise 59. Show how $p \in \sqrt{(p_1, \ldots, p_s)}$ can be checked with Gröbner bases (cf. Application 2.4.3).

Exercise 60. For each ideal below, find all points of its variety:

$$(x^2y - 1, xy^2 - y),$$
$$(x^2 + y, x^4 + 2x^2y + y^2 + 3),$$
$$(y^5 - z^4, xz^3 - y^4, xy - z, x^2z^2 - y^3, x^3z - y^2, x^4 - y)$$

Exercise 61. Use a computer algebra system to determine whether the polynomial p is in the ideal I, and if so, find an ideal representation.

(*i*) $p = xy^3 - z^2 + y^5 - z^3, I = (y - x^3, x^2y - z)$.

(*ii*) $p = x^3z - 2y^2, I = (xz - y, xy + 2z^2, y - z)$.

Exercise 62. Consider the ideal

$$I := (x^2 + y^2 + z^2 - 4, x^2 + 2y^2 - 5, xz - 1) \subseteq \mathbb{Q}[x, y, z].$$

Use a computer algebra system to compute generators for $I \cap \mathbb{Q}[x]$, $I \cap \mathbb{Q}[y]$ and $I \cap \mathbb{Q}[z]$.

Exercise 63. Let

$$V := \left\{(u + v, u^2 + 2uv, u^3 + 3u^2v) \mid u, v \in \mathbb{C}\right\} \subseteq \mathbb{C}^3.$$

Use a computer algebra system to find generators for the ideal $\mathcal{I}(V)$.

Exercise 64. Let V be a vector space and $f\colon V \to V$ an injective linear map with $\mathbb{P}(f) = \mathrm{id}_{\mathbb{P}(V)}$. Show that f is a constant multiple of id_V.

Exercise 65. Let V be a vector space and $W \subseteq V$ a hyperplane. Show that for any fixed $v \in V \setminus W$, the map

$$\begin{aligned} W &\to \mathbb{P}(V) \setminus \mathbb{P}(W) \\ w &\mapsto [v + w] \end{aligned}$$

is a well-defined bijection.

Exercise 66. For $i = 1, 2$ let $w_i \in \mathbb{R}^2, v_i \in \mathbb{R}^2 \setminus \{0\}$ and consider the lines

$$L_i := \{w_i + tv_i \mid t \in \mathbb{R}\} \subseteq \mathbb{R}^2.$$

If we extend the L_i to projective lines in $\mathbb{P}^2(\mathbb{R})$ via Construction 3.1.8, where do they intersect?

Exercise 67. Prove Lemma 3.2.5.

Exercise 68. Show directly that the radical of a homogeneous ideal is again homogeneous (with ordered index group G).

Exercise 69. Prove Lemma 3.2.11.

Exercise 70. Show that $\sqrt{I}^h = \sqrt{I^h}$ holds for ideals $I \subseteq k[x_1, \ldots, x_n]$ (cf. Lemma 3.3.16).

Exercise 71. Consider

$$V := \left\{(t^3, t^4, t^5) \mid t \in \mathbb{C}\right\} \subseteq \mathbb{C}^3.$$

Show that $\mathcal{I}(V)$ is homogeneous with respect to some nontrivial $\mathbb{Z}$-grading of $\mathbb{C}[x, y, z]$, and determine homogeneous generators for this ideal. Show that $\mathcal{I}(V)$ cannot be generated by 2 polynomials.

Exercise 72. Let $V \subseteq \mathbb{A}^n$ be an affine variety with no points at infinity. Show that V is finite.

Exercise 73. Show that a Hausdorff space X is compact if and only if for all Hausdorff spaces Y the projection

$$\pi\colon X \times Y \to Y$$

maps closed sets to closed sets (cf. Remark 3.4.3).

Exercise 74. Show that the variety $V := \mathbb{A}^2 \setminus \{(0,0)\}$ is not affine.
Hint: First compute $\mathcal{O}(V)$. If V was affine, to which simple affine variety would V be isomorphic? Why can't this be?

Exercise 75. Let $Q = \mathcal{V}_+(c_0x_0^2 + \cdots + c_rx_r^2) \subseteq \mathbb{P}^n$ be a quadric with $c_i \neq 0$ for all i. Show that Q is irreducible for all $r \geqslant 2$. What holds for $r < 2$?

Exercise 76. Consider the three (affine) *conic sections*

$$\begin{aligned} V_1 &:= \mathcal{V}(x^2 + y^2 - 1) \\ V_2 &:= \mathcal{V}(x^2 - y^2 - 1) \\ V_3 &:= \mathcal{V}(x^2 - y) \end{aligned}$$

in $\mathbb{C}^2$, and let $\overline{V}_i$ denote the projective closure of V_i in $\mathbb{P}^2(\mathbb{C})$. Show that for all $i, j = 1, 2, 3$ there exists a projectivity $\varphi_{ij}\colon \mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C})$ with

$$\varphi_{ij}\left(\overline{V}_i\right) = \overline{V}_j.$$

Why is a similar statement wrong in the affine space?

Exercise 77. Show that a field K is finitely generated over k if and only if $K = k(V)$ holds for an irreducible k-variety V.

Exercise 78. Let $L_1 = \mathcal{V}_+(x_0, x_1)$ and $L_2 = \mathcal{V}_+(x_2, x_3)$ be two skew lines in $\mathbb{P}^3$. Show that $L_1 \cup L_2$ cannot be defined with 2 homogeneous equations. Does it work with 3? How many polynomials does one need to generate $\mathcal{I}(L_1 \cup L_2)$?

Exercise 79. (i) Show that a localization of a noetherian ring is again noetherian. (ii) Let R be a ring and $\mathfrak{p}$ a prime ideal in R. Then the localization $R_\mathfrak{p}$ has exactly one maximal ideal, namely $\mathfrak{p}R_\mathfrak{p}$. Show that

$$R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong \mathrm{Quot}(R/\mathfrak{p}).$$

Exercise 80. Let $J = \{\alpha \in \mathbb{N}^n \mid |\alpha| = d\}$, $N = |J|$, and let $Z \subseteq \mathbb{P}^N$ be the projective variety defined by the equations

$$z_\alpha z_\beta = z_\delta z_\gamma$$

for $\alpha, \beta, \gamma, \delta \in J$ with $\alpha + \beta = \gamma + \delta$. Now let $\xi_1, \ldots, \xi_r, \eta_1, \ldots, \eta_r \in J$ such that

$$\sum_i \xi_i = \sum_i \eta_i.$$

Show that for $b = (b_\alpha)_{\alpha \in J} \in Z$ we then have

$$b_{\xi_1} \cdots b_{\xi_r} = b_{\eta_1} \cdots b_{\eta_r}.$$